Risk Management Knowledgebase

System Design Document

Version 1.0

April 28, 2016

THIS PAGE INTENTIONALLY LEFT BLANK

Revision History

Version	Date	Name	Description
0.01-0.17	23 Oct 2015	Michael Cho	Initial pre-decisional draft for internal review
0.18	11 April 2016	John J. Szucs	Security-related updates for ATO package
0.19	18 April 2016	Jason Cronin	Maintenance and Contingency Planning updates for ATO package
1.0	28 April 2016	Craig Fleming	Approved for release

System Design Document Approval

As a designated authority for the RMK virtual datacenter (VDC), I certify to the best of my ability that the System Design Document (SDD) is complete and that the information contained here in provides an accurate representation of the RMK system design and supporting infrastructure.

This document will be modified as changes occur and will remain under version control, in accordance with DISA's contingency planning policy.

X _____

Craig A. Fleming
Chief, Cyber Operational Assessment Branch (RE22)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

"*He who defends everything defends nothing*" – Frederick the Great (1712-1786)

1.1 Scope

This System Design Document (SDD) describes the Risk Management Knowledgebase (RMK), a data integration solution to improve the quality of cybersecurity risk posture assessments that is currently not feasible through any single data set. RMK is designed to ingest, disambiguate, index, process and retrieve massive quantities of IT network and cybersecurity data at operational speeds to better support risk management decision making.

RMK is being developed for the Defense Information Systems Agency's (DISA) Office of the Risk Management Executive (RME). RMK is designed to provide the near real-time risk posture assessments and risk mitigation prioritization. Prior to RMK, risk posture assessments were accomplished through manually intensive and convoluted business processes to collate and merge data from disjointed systems data sources. As a result, risk mitigation prioritization was generally conducted in an ad hoc manner using subjective analysis. RMK will support risk management activities to better assess, identify, prioritize and defend against cybersecurity risks to DISA assets for which the RME is responsible. Future iterations may expand the scope of RMK to support other Department of Defense organizations.

As further described within this SDD, RMK will be designed, developed and implemented in frequent incremental releases in accordance with the Agile development methodology. Nevertheless, the SDD will continue to be used as the definitive guide in the continual development of RMK capabilities and features. Furthermore, in accordance with the Agile development methodology, as understanding of the RMK requirements continue to be refined and improved through subsequence releases, this SDD will also be updated as appropriate to reflect the latest description of RMK.

Where applicable, sections of this SDD have been annotated with a two-letter code in parenthesis to identify alignment with a control family from the NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*

1.2 Background

DISA is a combat service support agency that delivers critical warfighting capabilities to the Department of Defense (DoD). The majority of DISA's services, functions, and capabilities operate within the cyber domain, which remains a highly contested operational environment where the risk of data loss and compromise remains high.

The RME is the senior official within DISA who is responsible for identifying, assessing, and prioritizing cybersecurity risks to the DoD enterprise. The RME maintains cybersecurity awareness and is also responsible for developing, implementing, and monitoring appropriate mitigations for DoD systems, networks, programs, and data. The RME makes decisions and weighs various competing requirements in order to effectively and efficiently secure DISA's

portion of the broader DoD Information Network (DoDIN) environment. The risk management process necessarily involves the prioritization of finite resources in order to achieve an acceptable level of risk for the enterprise by which the most serious risks are safeguarded against.

The Cyber Operational Assessment Branch (RE22) operates within the RME office. RE22 supports the mission of the RME by developing cybersecurity risk posture assessments that provide objective and subjective assessments of different components of the DoDIN environment. RE22's mission statement is:

> Assure the Agency's information systems and platform information technology possess the necessary security measures and operate at an acceptable level of risk to assure their availability, integrity, authentication, confidentiality, and nonrepudiation through continuous monitoring, and meets statutory and DoD Chief Information Officer mandates.

The current approach to cybersecurity assessment is fragmented, labor intensive, and protracted. It presently consists of multiple formal and informal cyber reporting systems, each designed to provide a very specific but limited view of the Agency's cybersecurity posture. Additionally, the resulting medley of systems does not interoperate and fail to provide a holistic perspective of the Agency's cybersecurity posture necessary to understand, manage, and mitigate the operational risks. RE22 has subsequently implemented manual processes to correlate data received from these different fragmented systems in an attempt to provide a more integrated approach. However, the cycle time for these manual processes do not provide for the level of cybersecurity risk management needed for DISA to effectively and securely operate in today's cyber environment. DISA currently lacks the ability to conduct continuous assessments based on integrated cybersecurity posture data. In most cases, risk management decisions are made on an informal, reactive, and subjective understanding of system risks and broader operational context.

1.3 Objectives

The RE22 Branch seeks to migrate away from the current platform-centric enterprise architecture that relies on manually intensive business processes in an attempt connect data from disparate cybersecurity systems. A net-centric architecture, as per DoD policy, will enable automated exchanges between cybersecurity systems thereby making all cyber posture data available in a cohesive, disambiguated, and rapid manner to better support operational risk assessments and risk management decisions.

RMK will provide an integrated view of data from existing cyber reporting systems. Figure 1 provides a sample of the many cybersecurity assessment systems and data sources currently deployed by DISA that collectively form DISA's cybersecurity assessment ecosystem. These systems are generally configured to not interact with other systems, thereby limiting their full potential to contribute to cybersecurity risk assessment and management. The purpose of the Risk Management Knowledgebase is not to create new data, but rather collect data from existing systems in order to better organize, integrate, and correlate cybersecurity posture data into searchable and exchangeable formats. These new data formats will be used to support the Cyber

Operational Assessment Branch and will be made freely available to other DISA organizations, thus enabling new and novel analysis of cybersecurity data. The automated integration of data that will be provided by the RMK system will replace several existing manual processes and improve the speed by which risk management decisions are currently being made.

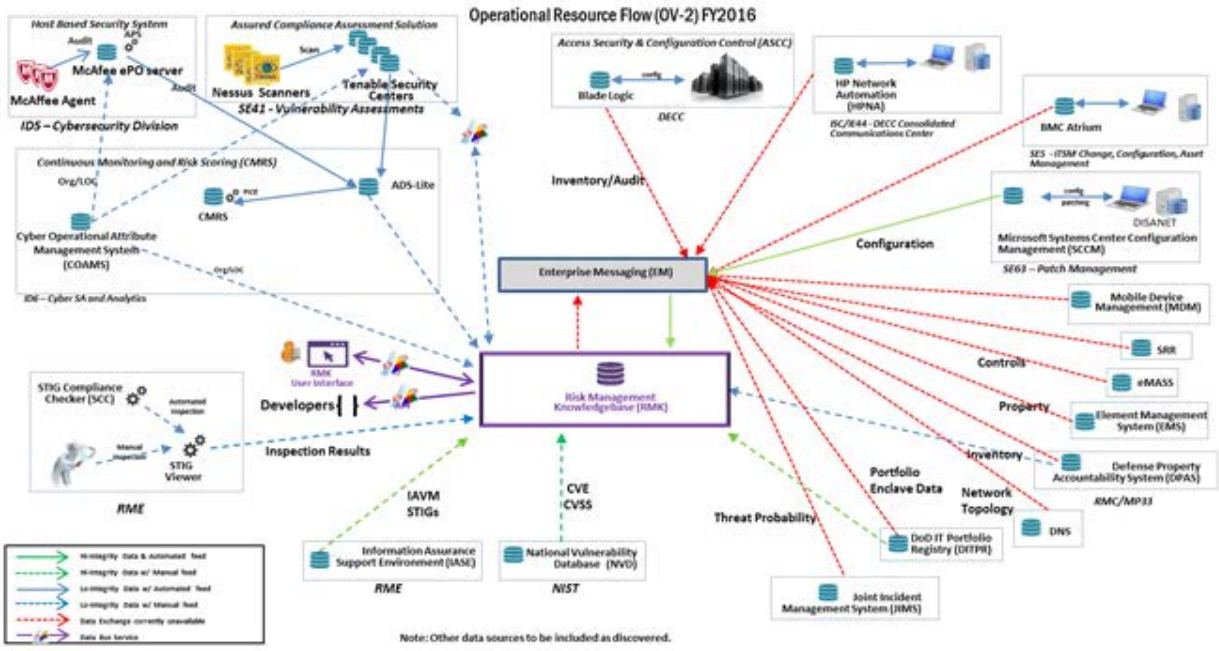


Figure 1. DISA Cybersecurity Assessment Ecosystems

2 REQUIREMENTS

The RMK system will provide the capability to integrate cybersecurity posture data generated from multiple information security systems operated across the DISA enterprise in order to provide a holistic cybersecurity risk posture assessment. The system shall be able to ingest, disambiguate, indexing, store, and retrieve data related to information security. The RMK will then be able to present data to users and other systems in useful and meaningful formats that enhance risk posture awareness and risk mitigation decision making.

2.1 Enterprise Data Bus

RMK performs the function of an Enterprise Data Bus, providing a common access point to obtain cybersecurity data that exist throughout the DISA enterprise. The Enterprise Data Bus eliminates multiple and redundant point-to-point systems in the information security systems architecture. A system can share its data with all other information security systems and also retrieve data from any other information security system with access to the Enterprise Data Bus. This approach minimizes the aggregate information security data stored by the entirety of the DISA enterprise and ensures that the available data is current and from authoritative data sources.

While a traditional Enterprise Service Bus model is focused on system call interoperability, allowing a system to use its native system call formats to access other systems regardless of format, the Enterprise Data Bus model is a disambiguation, storage, and index model that directly provides the requested data. This is necessary because the high-performance level required does not allow for the time-consuming and excessive intra-system communications involved in a traditional Enterprise Service Bus model.

While the RMK is designed to manage large quantities of data, it remains an operational data store and differs from a traditional Big Data store. The principal design objective with the Enterprise Data Bus is to provide quick retrieval at operational speeds of requested data. This requires careful design of how information security data is ingested, disambiguated, indexed, and stored to facilitate efficient retrieval. Data is exposed via published Application Program Interfaces (API) and made accessible via system web calls. Consumer systems can be other information security systems, lightweight applets, or even web portal services. The RMK Enterprise Data Bus though, will maximize the use of machine-to-machine system calls and minimize the use of any human intervention, or scripts designed to interface with human interfaces.

The target architecture is to create a common enterprise data bus which can be accessed across the enterprise and allow for individual organizations to develop customized lightweight applications to access the data to perform specialized queries, reports, and analysis.

2.2 Asset and Enclosure Organization

Information technology capabilities are a result of multiple systems and components interacting to ultimately provide the end-user with a product, service, or information. The interrelationships between different systems and their components are often difficult to trace, which is compounded by the introduction of virtualization technologies that creates systems within systems. These system interrelationships make it difficult to understand and define divisions of cybersecurity responsibility, which in turn makes it further difficult to assess cybersecurity risk and to decide upon mitigation actions.

The asset is the elemental unit of assessing and managing cybersecurity risk which is monitored and reported on by various tools and capabilities employed across the DISA enterprise. RMK integrates data from these various tools to generate an asset inventory and provide a holistic cybersecurity risk assessment. Examples of assets, which may also be referred to as endpoints, include workstations, servers, virtualized servers, routers, or firewalls. These assets have configurable attributes that can be monitored and reported on, such as network configurations, operating system configuration, and application configurations.

RMK employs a simple hierarchy of individual assets that can belong to one or multiple enclosures as depicted in Figure 2. Data from individual assets can be aggregated according to enclosures to allow for risk assessment and risk management at the enclosure level. RMK is being developed to support three types of enclosures, although more can be added as the requirements evolve.

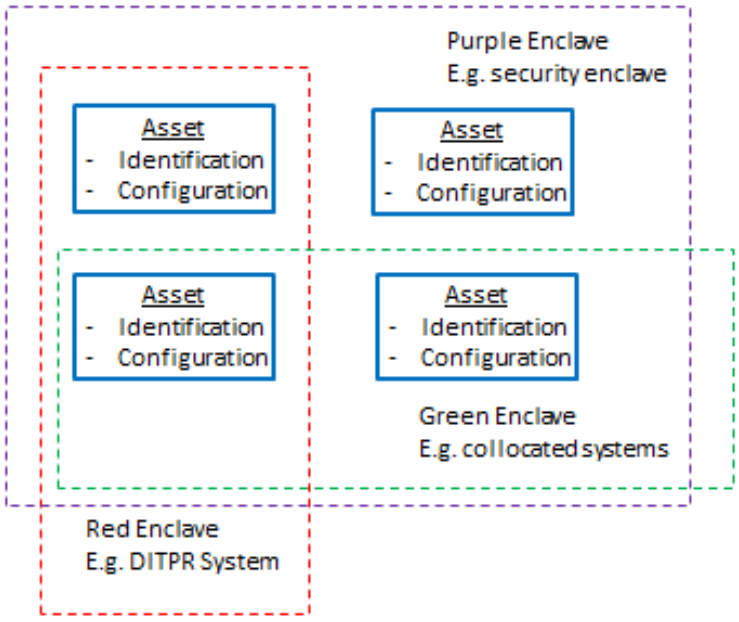


Figure 2. Assets and Enclaves

2.2.1 System Enclosure

A System Enclosure is a grouping of assets by a programmatically defined system-of-record with actual funding and authorizations. A System Enclosure is usually composed of multiple end points, which are typically servers, to provide a defined functional capability in support of user requirements. Examples of a System Enclosure can be found in the DoD Information Technology Portfolio Registry (DITPR). System Enclosures represent the traditional unit of assessment for cybersecurity risk management since each System Enclosure is required to have formal management, funding, and authorization.

2.2.2 Virtual Enclosure

A Virtual Enclosure is a user-defined grouping of assets based on a user's specific interests or responsibilities. An example of a Virtual Enclosure would be a superset of a System Enclosure and additional associated cybersecurity infrastructure assets that may be external to the System Enclosure. This type of grouping would provide a perspective of transitive risks, in which a weakness or vulnerability of one system impacts the risk posture of another system. This type of Virtual Enclosure could be beneficial for the Information System Security Manager to holistically view, assess, and understand the overall cybersecurity risks to the system-of-record by additionally accounting for externally connected systems or assets.

Another example of a Virtual Enclosure could be all the systems under the responsibility of a given DISA Directorate. This type of Virtual Enclosure would enable risk assessments at the DISA Directorate level and aide in prioritizing mitigations. This level of risk assessments and

mitigations would be a significant improvement for DISA Directorate's who were previously required to manually aggregate different risk data for the systems under their purview.

A third example of a Virtual Enclave could be critical networking capability sets that are not necessarily under a well-defined management structure as would be associated with a System Enclosure. Examples of this type of Virtual Enclave could be the Joint Regional Security Stack (JRSS), Standardized Tactical Entry Point (STEP), Internet Access Point. By creating a Virtual Enclave for these capability sets, the RMK defines a unit for risk assessment that can be used to automate risk management processes for other enclaves.

2.2.3 Network Enclosure

A Network Enclosure is a grouping of network infrastructure assets that provide telecommunication services for other assets. Examples of a Network Enclosure could include routers, switches, or firewalls that comprise an individual circuit, Local Area Network, or Wide Area Network.

2.3 Risk Posture Assessment

The RMK provides a primary benefit to the DISA RME by providing a calculation methodology to derive a quantitative risk posture assessment. Previous efforts to derive, assess, and quantify the enterprise risk posture have been based on measuring compliance with information security directives or otherwise a subjective assessment of cybersecurity risk. While compliance is definitely a component of risk management, it fails to provide an adequate picture upon which risk can be understood and mitigation decisions can be made.

The RMK implements the Joint Enterprise Risk Assessment Model (JERAM) developed by U.S. Cyber Command. The JERAM assesses cybersecurity risk for all monitored assets against two criteria: probability and impact. However, the JERAM does not provide a methodology on how to derive probability and impact scores. The RMK employs a scoring algorithm based on several sub-scores to plot against the JERAM risk matrix.

The probability of cybersecurity risk is a measure of how successfully a vulnerability could be exploited. The RMK scores the probability based on factors such as system configuration, access vector, access complexity, authentication requirements, exploitability, and target distribution. Many sub-scores are provided by the NVD, from which the RMK pulls the Common Vulnerability Scoring System (CVSS) score for known vulnerabilities. Additional sub-scores are derived from scans, audits, and assessments from other cybersecurity systems.

The impact of cybersecurity risk is a measure of the potential impact of a risk if actualized or otherwise exploited. The RMK scores the impact based on factors such as the impact to data confidentiality, data integrity, data availability, collateral systems, and mission operations. Like the probability score, many of the impact sub-scores are provided by the NVD. However, unlike the probability score, the RMK employs a sub-score unique to DISA called the Cyber Terrain Score (CyTS). The CyTS is an operational assessment of the overall significance or value of an

asset or enclave to the DISA mission. The CyTS is defined by the DISA Center for Operations and is further elaborated upon in Appendix E, Cyber Terrain Score.

Likelihood	Mission Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Low (11)	Medium (16)	High (20)	Very High (23)	Very High (25)
High	Low (7)	Medium (13)	Medium (18)	High (21)	Very High (24)
Moderate	Low (4)	Low (8)	Medium (15)	Medium (19)	High (22)
Low	Very Low (2)	Low (5)	Low (9)	Medium (14)	Medium (17)
Very Low	Very Low (1)	Very Low (3)	Low (6)	Low (10)	Low (12)

Figure 3. JERAM Risk Level Assessment Matrix

The cybersecurity risk probability score and impact score are plotted on the JERAM Risk Level Assessment Matrix depicted in the figure. Cybersecurity risks that have both Very High impact and Very High likelihood are assessed with an overall cybersecurity risk assessment of Very High and subsequently plotted in the upper-right portion of the matrix. Conversely, cybersecurity risks that have both Very Low impact and Very Low likelihood are assessed with an overall cybersecurity risk assessment of Very Low and are therefore subsequently plotted in the lower-left portion of the matrix.

The RMK can provide a risk score for enclosures by aggregating the individual risk scores of the component assets. By providing risk scores for different enclaves, a derived risk posture assessment can be provided for different levels of the organization to provide for the appropriate level of management and response.

2.4 Cybersecurity Risk Management Roles

The Risk Management Knowledgebase will allow for different roles and associated permissions with respect to the data contained within the RMK.

2.4.1 Information System Security Manager

The Information System Security Manager (ISSM) is directly responsible for configuration of the assets within a defined enclave. There may be multiple Information System Security Managers for a single enclosure. They are responsible for monitoring cybersecurity risk and developing mitigation actions specific to that asset. In addition, they provide information necessary to certify and accredit the system enclosure that the asset is a part of.

2.4.2 Risk Management Assessor

The Risk Management Assessor works for the Risk Management Executive and assesses cybersecurity risks for the purpose of system assessments and authorizations.

2.4.3 Authorizing Official Representative

The DISA Authorizing Official Representative (AO Rep) conducts technical reviews to support decision making activities by the Authorizing Official.

2.4.4 Senior Information Security Officer

The DISA Senior Information Security Officer (SISO) coordinates cybersecurity activities on behalf of the DISA Authorizing Official.

2.4.5 Authorizing Official

The Authorizing Official is officially appointed by the DISA Director. The Authorizing Official has the authority to formally approve systems, based on assessed risk, to operate on the DISA IT enterprise.

The Authorizing Official is also appointed as the Risk Management Executive. In this capacity, the Risk Management Executive is responsible for assessing and mitigating risk for the entirety of the DISA IT enterprise. By having visibility of assessed risk for all DISA enclaves, the Risk Management Executive can make enterprise-wide mitigation decisions such as resourcing or task orders that best provide for cybersecurity.

2.4.6 Directorate Executive

The Directorate Executive is responsible for the operations of IT systems under their purview. They are responsible for maintaining visibility of cybersecurity risks for their IT systems and allocating appropriate resources to mitigate those risks.

2.5 Risk Mitigation Prioritization

The RMK will provide prioritized mitigations to allow Information System Security Managers and System Administrators to understand what mitigation actions should be accomplished before others. Prior to the Risk Management Knowledgebase, there was no system or processes that could prioritize all the possible mitigations required for a system. As a result, Information System Security Managers and System Administrators often prioritized mitigation activities based on workload or perceived benefit that in reality did not reduce overall risk. In other cases, the Information System Security Managers and System Administrators were directed to perform very specific mitigation activities through various task orders and directives that did not account for workload and other ongoing mitigation activities. The Risk Management Knowledgebase derives its prioritization from the scoring algorithm used to produce the risk posture score, and in essence pre-calculates the effects of various mitigations in order to prioritize which mitigation actions will produce the greatest impact on the risk posture score.

2.6 System Certification and Accreditation

The RMK will support System Certification and Accreditation processes used by the Risk Management Executive to authorize systems to operate on the DISA network. These authorizations include Interim Authority to Test (IATT), Interim Authority to Operate (IATO), and Authority to Operate (ATO). The Risk Management Knowledgebase will provide system certifiers with a risk posture score that can be used to assess the risk of authorizing a system. Should the Risk Management Executive determine that the risks are too great for a system and not approve the system to operate, the Risk Management Knowledgebase will provide a list of prioritized mitigations that could be used to lower the risk posture score.

Furthermore, the RMK will provide the ability for system owners, Information System Security Managers, and System Administrators the ability to document a Mitigation Plan of Action and Milestones (POA&M). This feature will allow users to acknowledge each vulnerability and document reasons why the vulnerability has not yet been mitigated, and a plan by which the vulnerability will eventually be mitigated. While a mitigation POA&M does not reduce system risk, it provides a means to communicate additional information to the DISA Authorizing Official to warrant an acceptance of risk and allow for conditional system authorization. Appendix F provides additional information on RMK's POA&M functionality.

The RMK offers new possibilities to manage routine and non-routine re-certifications and audits. Currently re-certifications are conducted on a fixed time interval, and audits are generally not conducted at all. It may be possible to modify existing business processes so that re-certifications are event-driven when significant change to system risk impact or risk probability occurs. Furthermore, significant change to system risk could be used for security audits and determining how to apportion security resources.

2.7 DISA Operations

The RMK will support the DISA Center for Operations by providing near real-time risk posture assessments on assets and enclaves that support informed decision making in support of the DISA IT enterprise. Currently, risk posture assessment take days or weeks to form, and often the operational context has changed by the time the risk posture assessment is completed. With the Risk Management Knowledgebase, the DISA Center for Operations will have an accurate understanding of DISA's current risk posture, and can focus attention or resources on those risks that could impact DISA's operation of its IT enterprise.

The RMK bridges the knowledge domains between cyber operations and cybersecurity risk management. The cyber operations knowledge domain is traditionally focused externally, tracking and managing active attacks on the network. The cybersecurity risk management knowledge domain is traditionally internally focused, identifying and mitigating vulnerabilities on the network. These two knowledge domains have often been exclusive to each other, and information was exchanged in very general terms via task orders or reports. The Risk Management Knowledgebase helps bridge these two domains by allowing cyber operations and cyber security activities to marry specific attacks with specific vulnerabilities, thus allowing risk mitigation activities to be more focused and effective.

A key feature of the RMK is the ability to define enclaves of various assets or of other enclaves. This feature will be particularly useful for the DISA Center for Operations by defining enclaves of operational value, which may be geographic, organizational, or functional. These enclaves could be further defined for assets that are directly supporting real-world operations, thus ensuring that any risks are appropriately mitigated so as not to impact real-world operations. Enclaves could also be created for high-visibility systems, such as Department of Defense enterprise services that are operated by DISA, so that the DISA Center for Operations has visibility if any of these high-visibility systems are operating with risk. From a cybersecurity perspective, the ability to define enclaves and query for specific vulnerabilities enhances DISA's ability to ascertain the risk against known exploits and prioritize mitigation actions.

The DISA Center for Operations also provides significant input to the Risk Management Knowledgebase by managing the Cyber Terrain Score for DISA systems and enclaves. This feature is fully described in Appendix E.

3 SYSTEM ARCHITECTURE

3.1 Applicable Standards

3.1.1 Risk Management Framework

To the greatest extent possible, the RMK applies the Risk Management Framework (RMF) principles and methodologies published by the National Institute of Standards and Technology (NIST). While numerous other frameworks exist, NIST's RMF offers a single, comprehensive framework and is published by the U.S. Government. Per the Department of Defense Instructure (DoDI) 8510.01, *Risk Management Framework for DoD Information Technology*, the DoD has elected to adopt NIST standards for risk management and is currently in the process of migrating from the previous DoD Information Assurance Certification and Accreditation Process (DIACAP) to the NIST RMF. Furthermore, vulnerability data from the NIST National Vulnerability Database (NVD) is used by the RMK in assessing risk posture.

NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal information Systems* provides relevant guidance for the development of the RMK to support DISA's broader cybersecurity objectives. NIST 800-37 characterizes the RMF as encouraging "the use of automation to provide senior leaders the necessary information to make cost effective, risk based decision with regard to the organizational information systems supporting their core missions and business functions."

3.1.2 Security Content Automation Protocol

The Security Content Automation Protocol (SCAP) is the NIST-defined suite of interoperability specifications so that security data can be exchanged via Extensible Markup Language (XML). The RMK leverages SCAP-compliant tools implemented throughout the enterprise to maximize automated machine-to-machine data exchanges. The increased usage of the RMK will intensify the demand to implement SCAP-compliant tools or features currently not being implemented.

3.2 Design Principles

3.2.1 Cybersecurity Systems Integration

DISA currently employs various cybersecurity systems to perform different aspects of cybersecurity risk management, such as configuration management, vulnerability assessments, security control audits, and system authorizations. This ecosystem has evolved over the years with systems entering, evolving, and departing the ecosystem for various technical, programmatic, and strategic pressures.

Some of these systems belong to formal DoD acquisition portfolios while others were developed within DISA to support specific local needs. One common characteristic amongst most of these systems is the lack of automated data exchange between systems. While many of these systems are built upon commercial products that are capable of supporting automated data exchange (namely though HTTP system calls), they have not been configured to do so. The consequences to the enterprise include redundant system investments, excessive computing resources applied to process similar information, and lost manpower used to engineer and design point-to-point data exchanges when deemed necessary. An inventory of known systems is provided in Appendix D. A part of the RMK effort is a continuous review and inventory of systems throughout the DISA enterprise in order to capture a complete as possible view of DISA's information security ecosystem.

The RMK architecture acknowledges that many of these multiple information security systems are necessary. They can provide user-specific content and address a range of technical requirements that cannot be addressed by any single system. Furthermore, multiple systems minimize both acquisition risks and information security risks that could be associated with a single, large information security system. However, the RMK seeks to add value to the current information security ecosystem by providing a common platform to integrate and disambiguate cybersecurity risk data from disparate data sources. Currently, very few systems in the ecosystem exchange data, and where they do it is via individual system-to-system interfaces.

An ecosystem whereby all systems have the ability to share with each other dramatically improves the productivity of each individual system. This sharing of information among the different systems further allows the ecosystem to mature, thereby highlighting and integrating those systems that prove essential as well as highlighting those systems that do not.

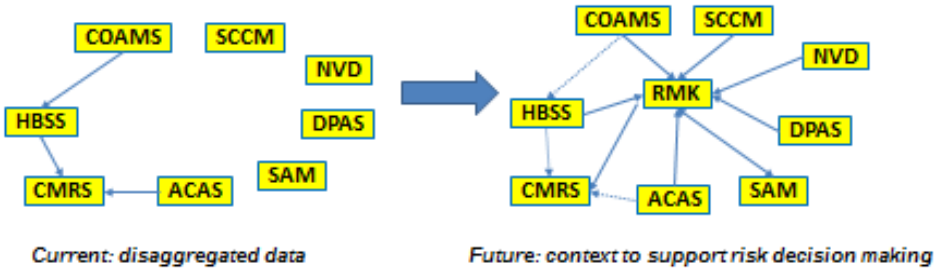


Figure 4. Data Centric Integration

3.2.2 Net Centricity

The DoD Net-Centric Services Strategy identified "information" as a strategic asset that greatly enhances mission effectiveness. It called for a fundamental shift in how information technology is provided and managed, shifting from a system or platform-centric approach to a data-centric approach. This approach as illustrated in Figure-3, demonstrates how the data is utilized to support business processes and functions. Net-Centricity calls for data to be made visible, accessible, and understandable in a machine-to-machine fashion.

The RMK employs the tenets of Net-Centricity by providing the foundational infrastructure by which data can be made visible, accessible, and understandable. The increase in quantity and quality of data from a Net-Centric approach greatly enhances the business functions of risk assessment and mitigation planning, which in turn improves DISA's cybersecurity posture.

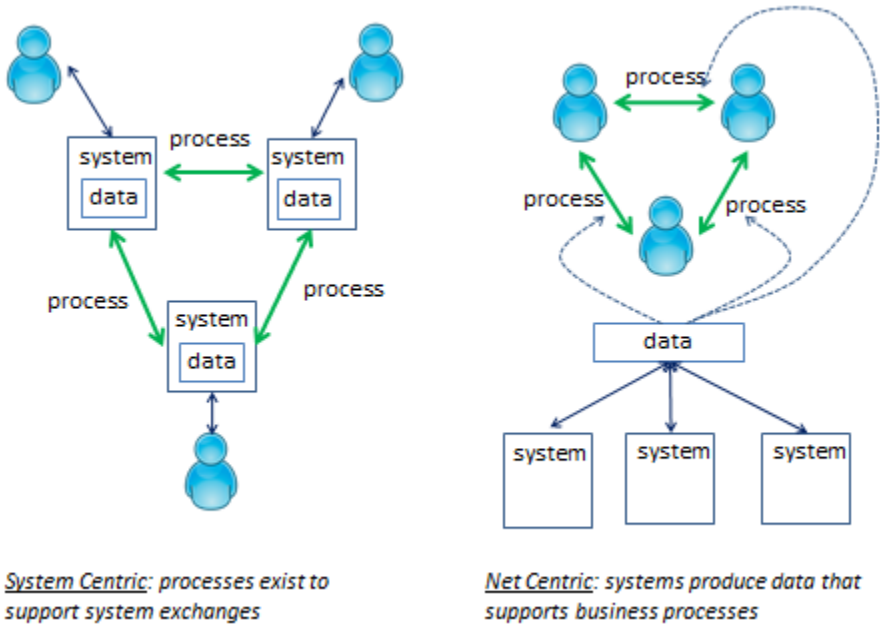


Figure 5. System Centric versus Net Centric Design

RMK employs industry standards to expose and deliver data via web services for machine-to-machine communications. However, for those data sources that do not have the inherit ability to support Net-Centricity, these machine-to-machine data exchanges will employ Enterprise Messaging, a DISA-provisioned enterprise service for message brokering. Data sources will publish their data via the Enterprise Messaging service, to be subsequently consumed by authorized data consumers. The use of Enterprise Messaging will ensure widest dissemination of risk management data to authorized data consumers while eliminating the need to configure countless and redundant point-to-point system data exchanges.

The implementation of the DISA-provisioned Enterprise Messaging service will position DISA to more closely resemble a true net-centric organization able to better utilize all its available data in an automated manner to more effectively and efficiently support risk management decision making. The current business paradigm involves extensive manual correlation of very large data-sets in spreadsheets and briefing slides resulting in decision cycle times that are completely incongruent and ineffective in today's contested cyber domain. Enterprise Messaging provides a sustainable architecture for data sharing by which data sources configure once to publish to the service. After an initial configuration, all current and new subscribers will be able to access published data with zero additional effort on the part of the Program Managers or System Administrators. Furthermore, this methodology of using Enterprise Messaging supports the growing demand for data sharing across DISA thereby improving cybersecurity risk assessments, risk mitigations, and infrastructure vulnerability management.

The Risk Management Knowledgebase will be instantiated as Virtual Machines within a Virtual Data Center hosted by the DISA milCloud Infrastructure as a Service (IaaS) service.

3.3 System Architecture

From the perspective of high-level system architecture, RMK is a virtualized enclave composed of the following components, illustrated in Figure 6.

The core functions of the RMK system are:

- Ingest data on IT organizations, assets, and vulnerabilities from numerous external systems, such as HBSS, SCCM, ACAS, ASCC, and others.
- Building and maintaining organizational models of IT infrastructure.
- Analyzing and visualizing cybersecurity risks in organizational and technical contexts.
- Lightweight automated tracking of required Plan of Action and Milestones (POA&M).

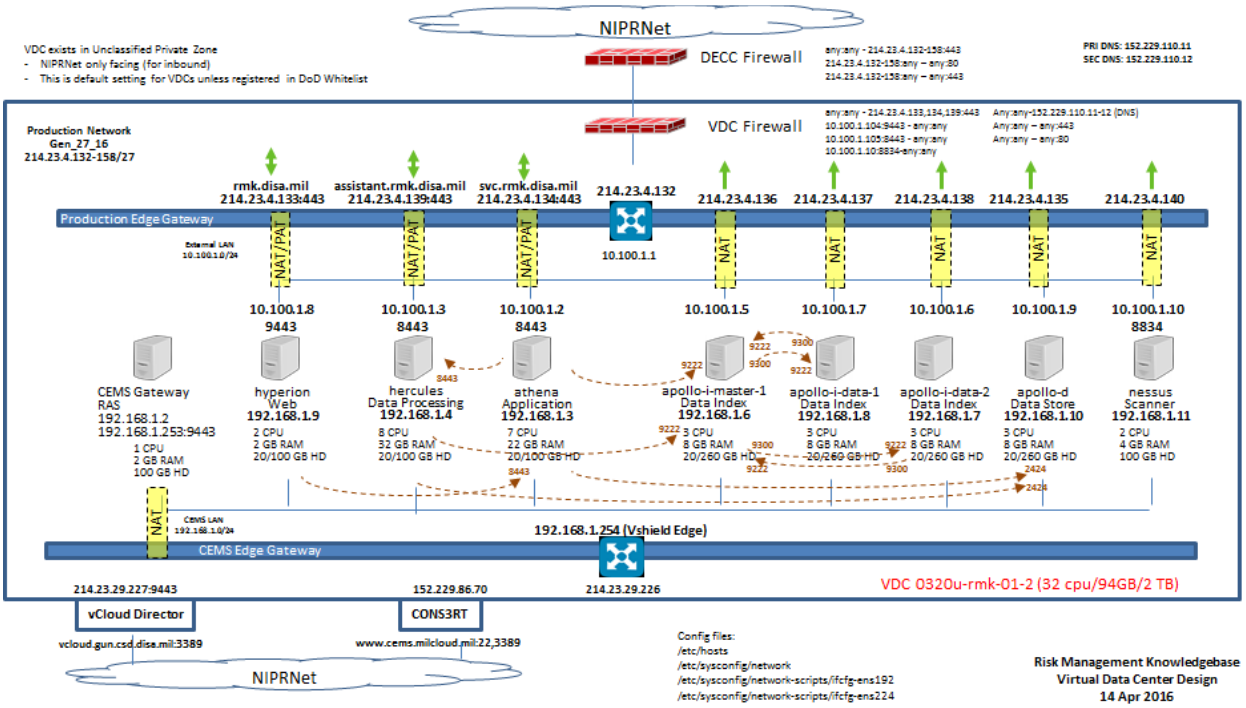


Figure 6. RMK implementation in milCloud

Key elements of underlying infrastructure, outside the accreditation boundary of the RMK system, are:

- milCloud: Infrastructure as a Service (IaaS) cloud hosting environment, provided by DISA and based on the commercial off-the-shelf (COTS) VMware vSphere virtualization products. RMK will use the milCloud hosting environment at the Defense Enterprise Computing Center (DECC) in Montgomery, Alabama. The DECC's connection to the NIPRNET is protected by a DECC-managed firewall.

- RMK VDC: RMK will be deployed as a Virtual Data Center (VDC) within the milCloud IaaS environment. This VDC is protected by a virtual firewall and includes several elements of COTS infrastructure software: vCloud Director, CONS3RT, and vShield Edge.

- CEMS Gateway: Interface between the RMK VDC to the DISA-provided Cloud Ecosystem Management Service (CEMS) cloud management tools, based on the COTS CONS3RT product. The CEMS remote access server is maintained by CEMS. The Mission Partner VDC IA Manager (IAM) will need to coordinate server administration and STIG/scan results with the CEMS team in order to permit the external network connectivity required. For this reason, again, the CEMS server maintenance requirements are CEMS PMO responsibility.

From an Information Assurance perspective, the accreditation boundary is bound by the virtual data center container. Within this container, RMK operates the following components:

- "hyperion": This is the Web front-end server for the RMK application. It is based on the Jetty open-source Web server (http://www.eclipse.org/jetty) and only serves Web content, (consisting of HTML, CSS, and JavaScript files) to users' Web browsers.

- "athena": This is the Web application server for the RMK application. It is based, in part on the same Jetty Web server component used by "hyperion." It also includes the open-source RESTlet framework for REST-style Web services (http://www.restlet.org), Venio's "Soterium" integrated application framework, and RMK-specific application code.

- "apollo-i-master-1": This is the master index server for the RMK application, used to efficiently locate records in the data store. It is based on the open-source ElasticSearch search and indexing engine (https://www.elastic.co/products/elasticsearch). In the RMK application, ElasticSearch is configured as a three-shard cluster. As the master shard, this shard coordinates indexing and search activity across the entire cluster, as well as serving as a shard itself.

- "apollo-i-data-1" and "apollo-i-data-2": These servers are the secondary shards in the ElasticSearch indexing cluster. Indexing and search workload is distributed to these shards by the master shard to scale-out the cluster for improved indexing and search performance and for redundancy.

- "apollo-d": This is the database server, used to store the vertex and edge data that make up the underlying knowledgebase for RMK and indexed by the ElasticSearch components described in the preceding two paragraphs. RMK is based on the open-source OrientDB multi-model NoSQL database (http://www.orientdb.com).

- "hercules": This is the extract, transform, and load (ETL) server. It handles the batch workload for importing data from external data sources.

The current implementation of RMK will be deployed only on the NIPRNET and operate at the UNCLASSIFIED//FOUO level.

3.3.1 Baseline

The RMK baseline does not include any hardware components. RMK operates in the milCloud virtualized IaaS cloud computing environment. The underlying hardware components for the VDC and its constituent virtual machines are outside the accreditation boundary of this system.

The operating system/platform baseline consists of the following components:

- Red Hat Enterprise Linux (RHEL) 7.2.
- Oracle Java Runtime Environment (JRE), Standard Edition, Version 8, Update 91

The application software consists of the following components:

- Soterium, Version 1.4.x: Integrated full-stack application framework.
- RMK, Version 1.7.x: Risk Management Knowledgebase application.

The application uses the following third-party components, which are also part of the software baseline:

- JCProgress, Version 0.3.1, https://github.com/pmairif/jcprogress: this is an open-source library that provides a progress bar for console environments.
- Apache POI, Version 3.13, http://poi.apache.org/: this is an open-source library for reading and writing Microsoft Office file formats. It is specifically used to read DITPR files, which are provided in Microsoft Excel format.
- stax-api, Version 1.0.1: This is the Oracle-provided Streaming API for XML. It is used to parse XML files received from various data providers, such as SCCM.
- Jackson, Version 2.6.2, https://github.com/FasterXML/jackson: This is an open-source library for parsing and generating JavaScript Object Notation (JSON) documents, which are used extensively through the RMK architecture.
- GSON, Version 2.5, https://github.com/google/gson: Google-developed open source library for serializing/de-serializing Java objects to and from JSON format.
- Guava, Version 19.0, https://github.com/google/guava: Google-developed open source library containing core library classes, including collections, caching, primitives support, concurrency libraries, common annotations, string processing, and I/O.
- Google HTTP Client, Version 1.21.0, https://github.com/google/google-http-java-client: Google-developed HTTP Client Library for Java is a flexible, efficient, and powerful Java library for accessing any resource on the web via HTTP.
- JSON Simple, Version 1.1.1, https://github.com/fangyidong/json-simple: Simple JSON encoding and decoding library. Supplements other JSON libraries and is also indirectly used via some of the other components.
- OrientDB, Version 2.1.9, http://orientdb.com: Multi-model distributed database.
- JavaMail, Version 1.5.5, http://www.oracle.com/technetwork/java/javamail/index.html: The Oracle-provided JavaMail API provides a platform-independent and protocol-independent framework to build mail and messaging applications. The JavaMail API is available as an optional package for use with the Java SE platform and is also included in the Java EE platform.
- JAXB, Version 2.1.12, https://jaxb.java.net/: Reference Implementation (RI) of JAXB, the Java Architecture for XML Binding.

- Boilerpipe, Version 1.2.2, https://code.google.com/archive/p/boilerpipe/: Open-source library to remove tags and spurious content from HTML content.

- Apache Commons Codec, Version 1.10, http://commons.apache.org/proper/commons-codec/: A new data structure for accurate on-line accumulation of rank-based statistics such as quantiles and trimmed means.

- Apache Commons Collections, Version 3.2.2, http://commons.apache.org/proper/commons-collections/: Builds on the JDK collection classes by providing new interfaces, implementations and utilities.

- Apache Commons File Upload, Version 1.3.1, http://commons.apache.org/proper/commons-fileupload/: Provides robust, high-performance, file upload capability to your servlets and web applications.

- Apache HTTP Components, Version 4.5, http://hc.apache.org/: Low-level Java components focused on HTTP and associated protocols.

- Apache Commons IO, Version 2.4, http://commons.apache.org/proper/commons-io: Low-level Java I/O library.

- Apache Commons Lang, Version 2.6, http://commons.apache.org/proper/commons-lang: Provides numerous helper utilities for the java.lang API, notably String manipulation methods, basic numerical methods, object reflection, concurrency, creation, serialization, and System properties. Additionally, it contains basic enhancements to java.util.Date and a series of utilities dedicated to help with building methods, such as hashCode, toString and equals.

- Apache Commons Logging, Version 1.2, http://commons.apache.org/proper/commons-logging/: The Logging package is an ultra-thin bridge between different logging implementations. Commons-logging includes support for a number of popular logging implementations.

- Apache Log4j, Version 1.2.17, http://logging.apache.org/log4j/2.x/: Java logging framework.

- Apache Commons Compress, Version 1.4.1, http://commons.apache.org/proper/commons-compress/: The Apache Commons Compress library defines an API for working with ar, cpio, Unix dump, tar, zip, gzip, XZ, Pack200, bzip2, 7z, arj, lzma, snappy, DEFLATE and Z files.

- Apache Commons CSV, Version 1.2, http://commons.apache.org/proper/commons-csv/: Commons CSV reads and writes files in variations of the Comma Separated Value (CSV) format.

- Apache Commons Math, Version 3.4, http://commons.apache.org/proper/commons-math/: Commons Math is a library of lightweight, self-contained mathematics and statistics components addressing the most common problems not available in the Java programming language or Commons Lang.

- ElasticSearch, Version 2.3.1, https://www.elastic.co/products/elasticsearch. High-performance, scalable indexing and search engine.

- JSON-java, as of July 29, 2015, https://github.com/stleary/JSON-java. Reference implementation of a JSON package in Java.

- Reflections, Version 0.9.10, https://github.com/ronmamo/reflections. Reflections provides powerful run-time access to metadata about Java classes and packages.

- Restlet, Version 2.3.5, https://restlet.com/projects/restlet-framework/. Restlet Framework is a library for building Web APIs in the REST architecture style.

- SLF4J, Version 1.7.6, http://www.slf4j.org/. Simple Logging Façade for Java, serves as a simple facade or abstraction for various logging frameworks (e.g. java.util.logging, logback, log4j) allowing the end user to plug in the desired logging framework at deployment time.

- Xerces, Version 2.11.0, http://xerces.apache.org/xerces-j/. XML Document Object Model (DOM) parsing library for Java.

3.3.2 milCloud

RMK will be deployed in milCloud. As previously stated, milCloud is a DISA offering and uses VMware technologies, to provide the underlying infrastructure services to enable a virtual private cloud that will provision on-demand, elastic, and measured computing resources. milCloud provisions virtualized processing, storage, network, and other fundamental computing resources where the consumer is able to deploy and run approved software, which can include operation systems and applications.

RMK will implement the DISA Cloud Ecosystem Management Service (CEMS), based on the commercial CONS3RT cloud orchestration tool, to provide additional tools to manage virtualized resources within the milCloud environment. CEMS significantly reduces the server administrator burden by allowing preconfigured and templated STIG-compliant virtual server instances into the virtual data center.

The Risk Management Knowledgebase server administrators will be responsible for operating system maintenance. This is a departure from previous DISA-provisioned hosting environments in which DISA, the hosting service provider, assumed risk for the server and operating system. That said, RMK coordinated closely with and is in full compliance with the DISA Ports, Protocols, and Service Management (PPSM) Program office.

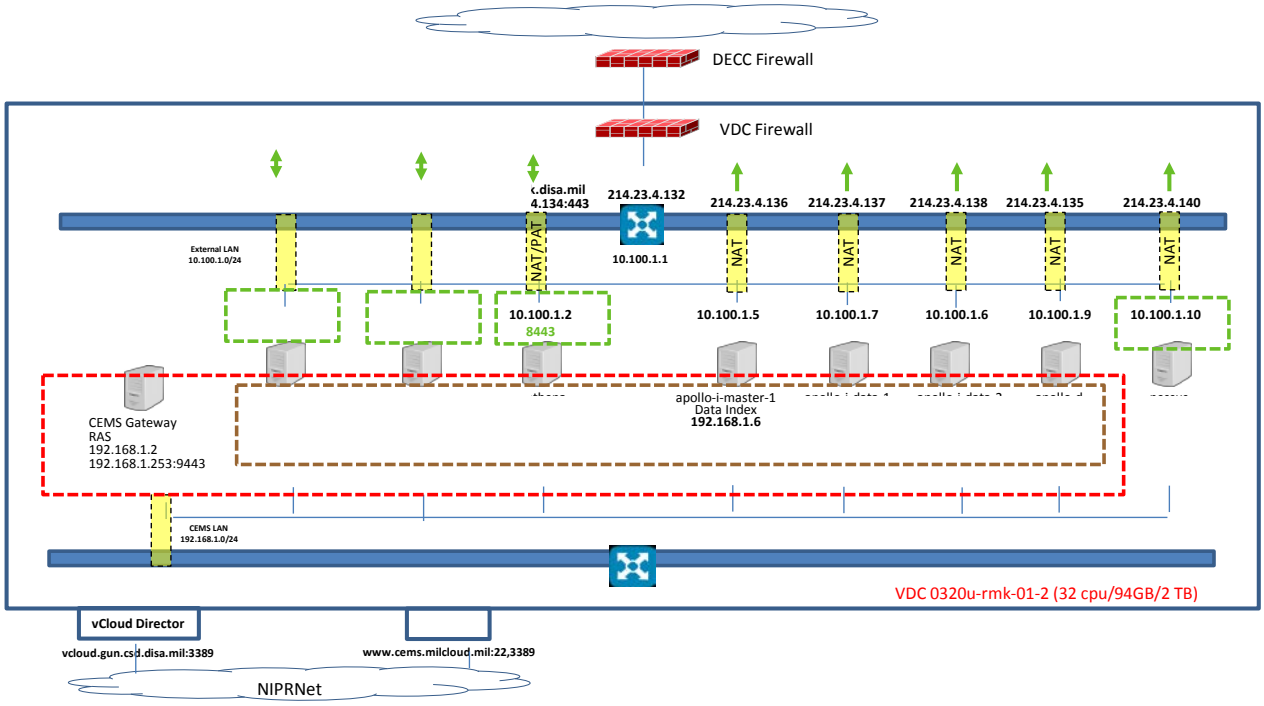
DISA's PPSM develops and implements DoD guidance and procedures that govern the use, configuration, and management of applications, protocols, and services (with their associated ports) in DoD Information Systems. The PPSM program does this by creating fundamental and definitive PPSM standards to maintain strong, secure, uninterrupted access to government resources and critical applications, in a manner that promotes network security, interoperability, and the evolution of net-centric operations across the DoD Information Networks.

The Virtual Data Center uses vCloud Director to manage the infrastructure to include the network and network protections. vCloud Edge Gateways are employed to control access into and out of the Virtual Data Center to external networks. There are two Edge Gateways established for the RMK Virtual Data Center, one external Edge Gateway for communications to the NIPRNet and Internet and one CEMS Edge Gateway for exclusive connectivity to CEMS for server management. The internal LANS within the Virtual Data Center use private, non-routable IP addresses and non-standard TCP port addresses to provide additional network-layer protections.

The External Edge Gateway is used to control traffic with separate inbound and outbound traffic rules. For inbound traffic, traffic is permitted only to the three external facing servers, Hyperion, Athena, and Hercules, and only on TCP port 443 (HTTPS). Port Address Translation (PAT) and Network Address Translation (NAT) is conducted on the External Edge Gateway so that internal IP addresses and TCP ports are not known. Inbound traffic from the outside the NIPRNet, such as from the Internet, is not permitted because the Virtual Data Center exists in the Demilitarized Zone (DMZ) Private Zone and that traffic is blocked by NIPRNet boundary protections. Outbound traffic is permitted for all servers only on TCP ports 80 (HTTP), TCP port 443 (HTTPS), and UDP port 53 (DNS). All servers can communicate externally over TCP port 80 and TCP port 443 to NIPRNet and Internet destinations. All servers can communicate externally over UDP port 53 to the local DNS servers at 152.229.110.11 and 152.229.110.12.
The CEMS Edge Gateway is used for management access from the CEMS Remote Access Server. This Internal Edge Gateway is part of CEMS security architecture and allows for web-based access to server remote terminal sessions that is controlled and accessed via the CEMS web site. Through the establishment of this DISA PPSM program-approved architecture, RMK has eliminated all unnecessary and nonsecure ports, protocols, and services. The utilization of these bare-minimum ports and protocols will be reviewed annually as the SDD is reviewed.

The Virtual Data Center employs two LANs, a production LAN (10.100.1.0/24) that is connected the External Edge Gateway, and a management LAN (192.168.1.0/24) that is connected to the CEMS Edge Gateway. All RMK server-to-server communications occur over the management LAN. Each server runs the Linux Firewall-Daemon that further divides network communications to enhance security via segregated zones each with specific controls for inbound traffic. All servers are configured with a Work zone that permits inbound traffic from other servers over the management LAN through the specific ports required for each application. All servers are configured with an Internal zone that permits communications from the CEMS Remote Access Server over TCP port 22 (SSH). Finally, the three externally facing servers,

Hyperion, Athena, and Hercules, are configured with a Public zone that allows inbound traffic over TCP port 9443 for Hyperion, and TCP port 8443 for Athena and Hercules. These ports are initially received on TCP port 443 by the External Edge Gateway but then translated using Port Address Translation to the appropriate port.



3.4 Software Architecture

The Risk Management Knowledgebase is an operational data store designed to provide rapid return of data from a large data set. It is based on commercial software specifically designed for the ingestion, disambiguation, indexing, storage, and retrieval of disparate data from multiple data sources. The Risk Management Knowledgebase consists of several interdependent software service modules that are implemented on different servers to improve system performance, although it may be possible to implement the software modules on a single server for smaller datasets.

The Risk Management Knowledgebase service modules consists of a presentation service (codename “Hyperion”), an application service (codename “Athena”), and a data service (codename “Apollo”). These service modules are designed to operate using DISA’s approved version of Red Hat Enterprise Linux, which currently is Version 6.

3.4.1 Hyperion Presentation Service

The Hyperion Presentation Service retrieves interacts with the web-user to accept user requests, communicate with the Athena Application Service, retrieve requested data, and present that data

to the web-user in an understandable and contextualized format. Hyperion is a Jetty web server with customized pages and scripts to support RMK.

3.4.2 Athena Application Service

The Athena Application Service provides application logic to correlate data and to coordinate data transfers between the other RMK service modules. It implements the cybersecurity risk assessment algorithms that result in cybersecurity scores for enclaves and assets. Athena is an enterprise scale java application designed to support RMK.

3.4.3 Apollo Data Service

The Apollo Data Service is a non-SQL database management system that inputs, indexes, stores, and retrieves data collected from various information security systems. For all identified cybersecurity data sources, an ingest correlator will be configured to map the data source to the Apollo data format. The use of non-SQL database structures allow for a more direct physical mapping between data elements in the database, resulting in scalability and faster retrieval times. Additionally, the Apollo data Service is designed to accommodate the scale of data associated with cybersecurity risk management and does not require that older data be removed or cached, thus making the data readily available for historical analysis.

Apollo is the key to supporting the Enterprise Data Bus functionality of the Risk Management Knowledgebase. It is designed to support automated machine-to-machine data exchanges using a variety of industry-standard formats. Furthermore, Apollo will expose its data via Application Program Interfaces that can be accessed via web service calls.

4 METHODOLOGY

4.1 Business Process Engineering

While the emphasis of the RMK is the development of a data integration capability, part of the development effort includes increased customer engagement in broader cybersecurity assessment activities. These activities will support better understanding and visibility of cybersecurity assessment requirements and also facilitate system implementation. Customer engagement includes providing regular awareness updates of enterprise level cybersecurity risk management activities, meetings, maintaining awareness of cybersecurity assessment and staff business processes. The updates and engagements will also support the reassessment and development of cybersecurity assessment policy and procedures.

Business Process Engineering will be conducted in coordination with the development of the RMK in order to ensure successful implementation as a DISA enterprise system. Many information security systems throughout the enterprise were developed piecemeal without any over-arching Business Process Engineering System resulting in the current Information Security Ecosystem by which many redundant systems exist to perform similar functions. Furthermore, the lack of Business Process Engineering has resulted in the implementation of business

processes solely to support the implementation and operation of information security systems, rather than using information security systems to support DISA's business processes.

Business Process Engineering will be used to continually inventory both formal and informal processes used to support Information Security Risk Management. Those processes will be mapped against existing Information Security Systems and an analysis will be conducted to determine gaps and redundancies. Recommendations for changes to existing policies, processes, and procedures will be brought up to the RME for guidance and decisions.

4.2 Agile Development

In order to minimize cost, schedule, and performance risks for the RMK, the system will be developed in an iterative manner, known as Agile development methodology that acknowledges the complexity and high degree of unknowns as evident in the current system-centric and manual-process driven approach to risk management. This development methodology, based on industry best practices, seeks to deliberately explore and understand discrete elements of the problem space. Capability is accordingly released in discrete increments on a short-term cycle. This is in sharp contrast to the traditional waterfall methodologies that emphasize up-front requirements analysis, but in practice tend to produce software that was delivered late, over cost, and failed to meet customer expectations.

The Agile development methodology is particularly useful for systems where the complete requirements and specifications are unknown. All development activities (requirements, design, development, testing, and release) occur in increments, referred to as sprints or spirals, and build upon the previous increment. Rather than expending time and resources to uncover, analyze, and document a complete set of requirements and specifications, the Agile development methodology seeks to manage complexity by using development sprints for a finite and known capability requirement. The value is that having a working capability, even a small limited subsystem, provides a useful foundation upon which additional requirements, design, and development can occur.

The Agile development methodology does not negate the need for system requirements, but rather allows for those system requirements to be developed over a longer period of time and to be refined as both customer and developer become more acquainted with the project, product requirements, technical possibilities, business processes, and corporate context. Throughout this process, different DISA stakeholders have been approached, and even more will need to be engaged during the requirements development. Any lack of input and cooperation from DISA stakeholders could represent project risk.

5 SECURITY

5.1 Identification and Authentication (IA)

To access the RMK system requires certain prerequisites that necessitate identification and authentication. To access the mere outside web interface of RMK requires the use of a DoD / DISA certified and issued laptop or desktop from the NIPRNet. To access the DISA NIPRNet,

requires the use of a DoD Common Access Card (CAC) utilizing PKI. Assuming an individual has a Government CAC, authenticates that CAC, and is utilizing authorized Government equipment, then the individual must register for an RMK account prior to access. Part of this registration is the requirement of a DD Form-2875 that must be filled out (on-line) and approved by the requesters' Supervisors prior to being granted access. All the above strictly follows:

- DoD I 8500.01 Cybersecurity, March 14, 2014, section 8. Use of DoD approved identify credentials,
- DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
- DoDI 8520.03 Identify Authentication for Information systems, 13 May 2011.

Through the above mentioned requirements, RMK is able to:

- Follow identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Follow procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls
- Implement multifactor authentication for network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access
- Implement replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- Provide single sign-on capability for information system accounts
- Implement multifactor authentication for privileged and non-privileged accounts
- Accept and electronically verify Personal Identity Verification (PIV) credentials
- Benefit from hardware enforced security safeguards

5.2 Access Control (AC)

Access control within RMK is done by different process to support different functionality. Functions such as application programmer privileges to change production code and software development are one form of required access control that is conducted. Another is administrative privileges to support the introduction of new data. Then there are the end-users, which require a completely different level of access and privileges to support their needed functionality within RMK.

Not only is access control a function of type of privileges, but of levels of privileges and access as well. At the most basic level of access is the requirement of a common access card (CAC). Without this access control, no user can even access at the enterprise-level - the NIPRNet, much less RMK within the DISA-milCloud. Then there are the privileges as assigned once inside the RMK information system infrastructure. RMK uses a very strict Role-Based Access Control (RBAC) authorization system. Within RMK's RBAC system are administrative-level privileges. There are also machine-to-machine privileges allowing for the introduction of new data into

RMK. Additionally, there are the user-level privileges. Within this band of user-level privileges are another set of even more refined privileges.

Proper access control does many things at many levels. It prevents unauthorized programs or modifications to authorized programs from being implemented by unauthorized personnel. Proper RBAC allows for review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel only and are properly implemented.

The RMK team has configured RMK to enforce all applicable authorizations for logical access to the information and the system resources. For all applicable RMK components that have applicable STIGs or SRGs, RMK has configured the information system to comply with the applicable STIGs and SRGs pertaining to CCI 213: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

It is also worth reiterating that, as RMK is a virtual network operating inside the DISA milCLoud, run inside DISA's DECCS Montgomery, that all physical access controls are inheritable by RMK and beyond the capability of RMK. This is also applicable to possible BIOS manipulation as that is outside the scope of the RMK accreditation boundary.

RMK RBAC levels and privileges are reviewed at least annually during the standard annual review of this document.

5.2.1 Account Management

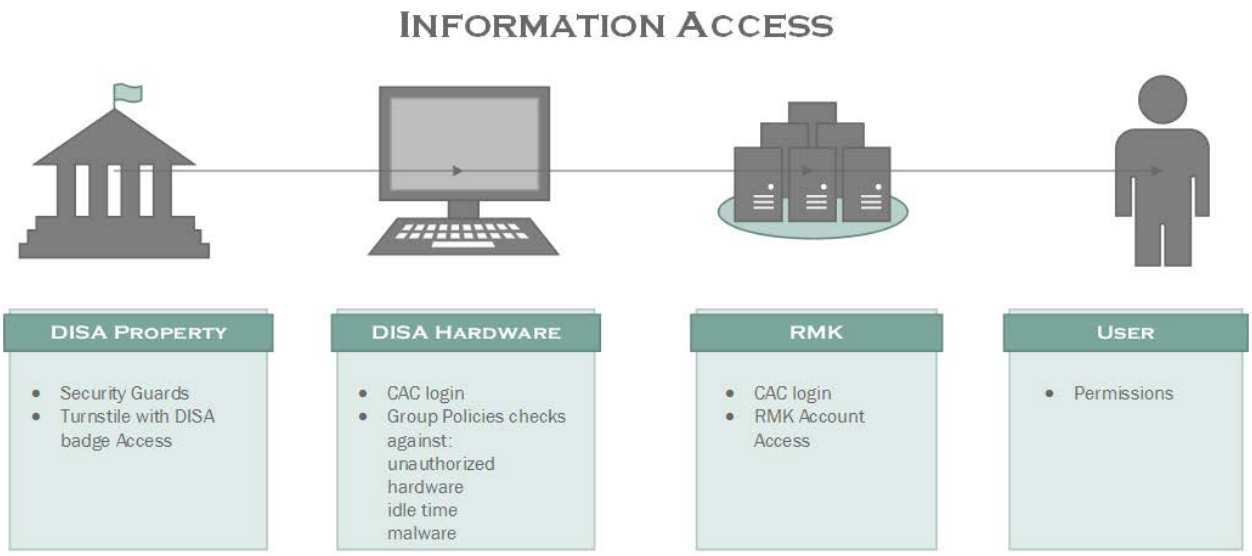
RMK implements the requirement for dual-authentication for implementing changes to core software. The different roles shared/groups utilized in RMK are listed below along with the permissions associated with that particular role or group. These listed below as well as all standard users are still required to complete a DD Form-2875 that must be approved by their immediate Supervisor prior to being authorized access at any level. These groups are reviewed at least annually to ensure any members that have left are purged from the group-permissions, ensuring a clean, updated, and vetted group listings.

Role	Permissions
Admin	Allowed to perform all user actions and some special actions.
Contributor	Can view, write, delete and make comments.
Reviewer	Can view, comment and approve/disapprove workflows.
Workflow	Can create or modify workflows

5.2.2 Access Enforcement

A strength of RMK is that it integrates seamlessly with the current security infrastructure that DISA has in place. DISA offers layers of security that must be passed in order to view any information on the system. The reliance on DISA systems and security extends the already

robust system of policies, scanners and safeguards to RMK. When a system does not comply with DISA polices, that system will not have access to the DISA network and therefore no access to RMK. These layers of security are detailed below.



Once the outer layers of security have been exhausted, RMK utilizes a role based access control system. (Please see account management for description of roles). Unlike many other systems RMK does not rely on session cookies for access enforcement or access control. Alternatively, every request made to the server is filtered based on the permissions granted to the user's certificate. These permissions are determined by the user's role. This feature requires the user to be logged in with their Common Access Card (CAC). If the personal certificate from the CAC cannot be accessed, the user will not be able to interact with or even view the information from the system. Likewise, because the permissions are granted based on the user's certificate, the user will only be able to view information to which they are given access.

5.2.3 Other Access Control

Part of the RMK authorized access program is the DISA Ports and Protocols' Services Management (PPSM) program. Again, DISA's PPSM develops and implements DoD guidance and procedures that govern the use, configuration, and management of applications, protocols, and services (with their associated ports) in DoD Information Systems.

DISA's intent is to deploy ACAS passive scanners to do an analysis. This scanning ensures that registered systems are in fact utilizing only the PPSM-authorized ports and protocols as was initially approved by the systems' respective AO.
RMK utilizes a Deny-All and Allow-by-Exception only policy in restricting software execution by unauthorized personnel. This is to be reviewed annually in conjunction with the SDD as a whole.

5.3 Auditing (AU)

RMK shall maintain audit records (also referred to as “logs”) in accordance with NIST SP 800-29 and other applicable policies.

5.3.1 Logging Mechanism

RMK shall use the open-source Simple Logging Façade for Java (SLF4J) (http://slf4j.org)

RMK shall send audit records to the UNIX/Linux-standard syslog mechanism (via SLF4J) as its primary logging record. This mechanism has extensive native and FLOSS/commercial third-party support for log management, analysis, and other functions.

RMK may be configured to use an alternate logging mechanism, such as the popular open-source logback mechanism (http://logback.qos.ch/) at run-time.

5.3.2 Audit Events

RMK shall generate audit/log records for the following events as required by NIST SP 800-53:

- Successful and unsuccessful attempts to access, modify, or delete security objects, specifically defined as user principals, groups, roles, and permissions.
- Successful and unsuccessful attempts to log-in.
- Three or more unsuccessful attempts to log-in
- Users explicitly logging out of the system.
- Users attempting to access the system after their session has timed out.
- Concurrent log-ins from multiple Web browsers.
- Any attempted actions that are denied by the application’s authorization mechanisms.
- Successful and unsuccessful attempts to access system-level functions, specifically including the user interface or underlying Web services for the accounts and workflow functions.
- Program start-up and shutdown.
- Actual or attempted efforts to change code.
- Interactions with the application via the application console.

In addition, RMK shall generate audit/log records for the following additional events, which are important to monitoring the secure and reliable operation of the system and troubleshooting any issues that may occur:

- Application exceptions.
- HTTP requests for resources that do not exist/cannot be found (HTTP status code 404: not found).

- HTTP requests that client errors (HTTP status code 4xx, including 401: unauthorized and 403: forbidden).
- HTTP requests that resulted in a server error (HTTP status code 5xx, including 500: internal server error and 503: service unavailable).

By default, all audit events are enabled. Specific audit events, specified by event code, may be suppressed using the RMK configuration files, although this is not recommended.

5.3.3 Audit Record Contents

All audit records generated by RMK shall include the following information:

- A five-character alphanumeric identification code for the event, of the form *Cnnn*, where *C* is a two-character alphabetic character sequence identifying the category of the event and *nnn* is a three-digit numeric code identifying the specific event within the category. Currently-defined values for *C* are "S" for security and "D" for data access. As an example, event code "S001" is a successful login.
- A brief human-readable description of the event including success or failure (e.g., "Successful log-in" or "Unsuccessful log-in attempt.")
- An ISO 8601-compliant representation of the date and time that the event occurred, in Universal Coordinated Time (UTC) (also referred to as "ZULU time"). This date/time stamp shall include the year, month, day,
- The IP address of the client machine from which the event was initiated.
- The URL of the incoming HTTP request (if applicable).
- The full name of the authenticated user, if any.

5.3.4 Log Access Control

File access controls for the log directory and individual log files shall be set as follows:

Item	User	Group	All
Log Directory	RMK application account	RMK group (application account + administrators)	
	Read Write Execute	Read Execute	None
Log Files	RMK application account	RMK group (application account + administrators)	
	Read Write	Read	None

- Owner: Application account; read and write permissions, plus execute permissions for directories.
- Group: Application administrators; read permission only, plus execute permission for directories.

5.3.5 Log Management

RMK shall use the UNIX/Linux-standard log rotation facilities to maintain a rolling 30-day window of on-line logs. Logs that are older than 30 days shall be compressed and archived in the event that they are needed, for example in support of incident response activities. Archived logs that are older than one year shall be deleted.

The host platforms for RMK shall be configured to automatically notify the DevOps team via a system-generated email message when available disk space (for any purpose, including logging) reaches 10% or less. Per the default behavior of syslog, if there is insufficient disk space for new log records, the oldest logs will be deleted. Prior to deletion of any audit log files or records, there will be a two-person concurrence and record kept of what logs were deleted and by whom.

5.3.6 Log Review

The RMK DevOps team shall review the system and application logs on a weekly basis for indications of attempts to bypass or circumvent security measures, unauthorized attempts to access or modify data, attempts to gather large amounts of information for which a user does not have a need-to-know, or conduct a Denial of Service (DOS) attack. Key items of interest in reviews are:

- Repeated failed user logins.
- Successful user logins far outside of normal working hours.
- User account change or deletion.
- Service failure.
- Attempts to access non-existent files (HTTP status code 404).
- Code (SQL, HTML) seen as part of the URL
- Access to extensions you have not implemented.
- Web service stopped/started/failed messages
- Successful operations on HTTP
- Failed user authentication (HTTP status code 401 and 403)
- Invalid HTTP requests (HTTP status code 400).
- Repeated attempts to access non-existent URLs, resulting in HTTP status code 404: not found. This could indicate probing for vulnerabilities.
- Attempts to use disallowed HTTP methods (for example, an HTTP POST request for a URL where only GET is allowed), resulting in HTTP status code 405: method not allowed
- Internal server errors (HTTP status code 500)

If it is necessary to time-correlate multiple logs (for example, Linux system logs and RMK application logs), concatenate the log files together (with the standard Linux **cat** command) and

then open the concatenated log file and sort by date/time in GNOME System Log Viewer or a similar tool.

5.3.7 Log Viewing and Analysis Tools

The RMK DevOps team shall deploy and use the open-source GNOME System Log Viewer (in the RHEL 7 gnome-system-log package) to view and analyze log files. This tool can be used to view, filter, search, and extract subsets of syslog records.

More information on this tool is available at https://help.gnome.org/users/gnome-system-log/stable/.

5.4 Security Assessment and Authorization (CA)

Within the Certification and Accreditation role, RMK develops, documents, and disseminates to applicable authority, security assessments and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Additionally, RMK has developed procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessments and authorization controls.

RMK will conduct self-assessments on a monthly basis to include vulnerability scanning and compliance checking, using available tools within the DISA-milCloud library of applications. Formal security control assessment will be conducted by RE5 as part of their Security Assessment Plan and will include announced vulnerability scanning reports. Security control assessments will be conducted as part of the certification and re-certification process, but not to exceed once every three years.

RMK has adopted a continuous monitoring strategy and implements a continuous monitoring program. This program includes the establishment of regular scanning and ongoing security control assessments. The scans are to be done at least monthly but shall also include unannounced scans to ensure variability. Scan will also be done whenever a new vulnerability is announced which may even remotely affect the RMK system. The scan results will be monitored in accordance with the organizational continuous monitoring strategy. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy do occur along with the correlation and analysis of security-related information generated by assessments and monitoring. The response actions to address results of the analysis of security-related information and reporting the security status of the RMK VDC and the information system are laid out in the RMK Information System Contingency Planning document.

5.5 Planning (PL)

Security planning for the Risk Management Knowledgebase (RMK) is conducted by DISA in accordance with DoD policies for the entirety of the DISA enterprise. The Risk Management Knowledgebase leverages the DISA-milCloud infrastructure practices and procedures. RMK also

leverages DECC-Montgomery, where the DISA-milCloud is housed, to support security requirements in providing many of the controls required for operation. Not only in network security instances does RMK leverage these existing security requirements, but also in reference to physical requirements. Lastly, the RMK system leverages the DISA infrastructure, practices, and policies in the screening of individuals prior to authorizing access to the information system. RMK also leverages DISA policies in the rescreening of individuals according to DISA policies where rescreening is so indicated, the frequency of such rescreening also based on DISA procedures. RMK does not require exception, and is otherwise fully compliant and compatible with existing security plans, architectures, and Concept of Operations.

6 MAINTENANCE (MA)

As the Risk Management Knowledgebase (RMK) information system is virtual network architecture, there are no physical hardware maintenance requirements of the RMK team. As per the DISA milCloud Virtual Data Center Administrative Guide (version 1.0, October 20, 2015), the DISA Enterprise Virtualization Team (EVT) is responsible for maintaining the VMware virtualization infrastructure at all DECCs. In addition to supporting virtual environments for the traditional DECC hosting, the EVTs are also the systems administrators for milCloud's vCloud implementations.

In terms of implementing a process for ensuring that plans of action and milestones (POA&M) for the security program and associated organizational information systems are developed and maintained, RMK has an assigned ISSM who will be responsible for these actions. The assigned system ISSM will also be documenting the remedial information and security actions to ensure that RMK is adequately responding to risks. The assigned ISSM will also be reviewing applicable POA&Ms for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

DISA's Centralized Communication Center (CCC) is the physical manager of the milCloud and all its dependent virtual data centers. The CCC manages the physical network infrastructure, e.g. routers/switches, and a variety of network services. Some of the network services include DNS, SMTP, F5 proxy, DECC Firewall, and certain VPN concentrators. Provisioning of most assets under CCC control is performed manually via service desk ticket.

RMK implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed and maintained during annual review of Security and Training Requirements as per DISA designated training cycle. This training cycle is not to exceed annual training, review, and documentation cycle.

7 CONFIGURATION MANAGEMENT (CM)

Configuration Management establishes the overall approach for the Configuration Management requirements and Change Control Board (CCB) of the Risk Management Knowledgebase (RMK) system. In order to better incorporate input and feedback from DISA concerning

configuration management and modifications to the RMK baseline and future capabilities, the RMK CMP and CCB has been formed. That document defines and identifies the roles, responsibilities, and processes necessary to track and document configuration changes and operations of the RMK CCB. The RMK CCB will make recommendations on whether or not changes should be made to RMK capabilities.

7.1 Configuration Management Execution

The execution of CM for the RMK program involves configuration identification, change control, status accounting, and verification and auditing of the products and processes.[1] These are the key functions required to manage system configurations. An overview of the three key activities is provided below.

- *Configuration Identification* – establish a structure for system products and system configurations; select, define, document, and baseline system attributes; and assign unique identifiers to each CI.
- *Baseline Management* - define a basis for further system life cycle process activity and allow reference to, control of, and traceability among configuration items and to requirements
- *Change Management* – ensure that changes to a configuration baseline are properly identified, recorded, evaluated, approved or disapproved, and implemented and verified.

7.2 Configuration Management Goals and Objectives

CM Program Goals:

- Ensure that Configuration Items (CI) are identified.
- Ensure that CIs are controlled and managed throughout the life-cycle.
- Ensure CI status is recorded and reported to all stakeholders.
- Ensure integrity of baselines and work products is assured.
- Ensure cost for CM is controlled, duplication of effort is prevented, and efficiency is maintained.

CM Program Objectives:

- Establish a CM strategy.
  - Establish roles and responsibilities for the application of CM activities.
- Identify and baseline CIs.
  - Identify CIs that will be baselined or placed under configuration control and baseline them.
- Establish and maintain a repository for CIs and configuration baselines.
  - Establish and maintain a repository to store and control CIs and baselines.

---

[1] *Defense Acquisition Guidebook, "Configuration Management" (Chapter 4.3.7)*

- Control changes.
  - Control changes to CIs and baselines throughout the project life-cycle.
- Record and report configuration status.
  - Record and report status and change information about the baselined CIs.
- Conduct configuration audits and inspections.
  - Conduct configuration audits and inspections to verify integrity of the baselines and CIs.

7.3 Change Management

One of the responsibilities of the CCB is to evaluate Change Requests (CR) as per the Change Request Form in Appendix C, and determine the standards for effectiveness, interoperability, suitability and the security assurance requirements of the submitting organization. Examples of change requests include:

- Version upgrade proposed by the RMK Team
- Enhancements to address a new requirement or operational need
- Change to an existing requirement

The RMK CCB will also ensure that DISA operational needs are addressed throughout the lifecycle of the capability. The RMK CCB will conduct an impact analysis for all proposed changes as prescribed within the CCB Change Request Form. Based on the impact analysis, the Change Control Board can then choose to:

- Approve the changes
- Reject the changes
- Request additional information
- Recommend adjustments to the change
- Postpone the decision pending some other decisions

Proposed changes must receive CCB approval before being included in a new release or capability. The RMK CCB will verify that any related project documentation is updated to ensure program integrity is maintained.

8 Risk Assessment (RA)

A Risk Assessment is done initially as one of the first steps towards systems development. Security Categorization is conducted, in consultation with security assessors from DISA RE5. The Risk Management Knowledgebase is assessed with a Security Categorization of Confidentiality=High, Integrity=Medium, and Availability=Medium.

After the Security Categorization, a Risk Assessment is conducted and periodically updated. Finally, vulnerability scanning is routinely conducted with the Nessus scanner that is part of the system architecture. Should a new or unique vulnerability or software threat be discovered, RMK will share this information from the scanning results, and subsequent report, with all applicable organizations and their designated personnel to ensure the minimization of this threat affecting other systems.

9 System and Services Acquisition (SA)

RMK determines information security requirements for the information system or information system service in mission process planning. While RMK determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process, many of these costs are accounted for in the monthly payments to DISA-milCloud and for the internal security measures included in the monthly price.

RMK management requires the RMK developers to demonstrate the use of proper Agile development life cycle best practices. Agile best practices also encompass security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes.

10 DevOps

10.1 Physical and Environmental Protection (PE)

RMK is a virtual network housed within a DISA-milCloud infrastructure, surrounded by a DECC-Montgomery groundwork base. As such, all physical security, environmental, and other appropriate physical security concerns are inherited and covered under the aforementioned organizations, as applicable.

10.2 Systems and Communications Protection (SC)

The system and communication protections are implemented for the RMK through various configurations of system components. The system is implemented as a virtual data center by the milCloud service provider, which provides logical isolation of the servers from other servers that may be physically collocated at DECC Montgomery. Within the virtual data center, individual servers can only be configured and deployed from pre-configured and pre-authorized configuration templates. Many hardware configuration options are simply not available with virtualized hardware. The system architecture also isolates specific functions into distinct application processes or layers that further adds protection.

Communications between server components and with end-users is through authenticated, authorized, and encrypted communications. DoD Public Key Infrastructure is used to authenticate and valid users. Furthermore, firewalls at the server, virtual data center, milCloud, and DECC Montgomery layers, as well as the NIPRNet CNDSP network protections, ensure transmission confidentiality and integrity.

In order to remain up-to-date on security issues with third-party components, the RMK system administrators shall subscribe to security bulletins or mailing lists produced by the following third-party vendors: Red Hat, Oracle Java Runtime Environment, OrientDB, Elasticsearch, Jetty, and Restlet. These subscriptions are managed via the vendor’s public websites and ensure that the RMK system administrators receive security updates from the vendors as soon as they are

made available to the public. These subscriptions also ensure compliance with STIG ID #APP6040, SV-17835r1_rule.

10.3 Personnel

10.3.1 Personnel Security (PS)

Through strict adherence and by abiding by all DISA and DOD rules, regulations, policies, and procedures, RMK ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system. Through these same processes, RMK ensures that individuals accessing the RMK information system processing, storing, or transmitting capabilities, acquire through DISA and DoD policy, formal indoctrination for all of the relevant types of information to which they have access on the system. RMK also fully inherits and utilizes DISA and DoD policy in ensuring all applicable individuals have valid access authorizations as demonstrated by assigned official government duties. This involves the consideration of physical threat and restricted access. In the event of a personnel threat, the offending account is immediately deprecated.

10.3.2 Awareness and Training (AT)

RMK fully leverages and utilizes the DoD and DISA training requirements in support of all security training prerequisites required by the organization.

10.4 Maintenance

RMK is a virtual network located within the DISA-milCloud, hosted within the DECC-Montgomery infrastructure. As such, all scheduled, performed, documented, and record reviews of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements, are executed in accordance with milCloud Terms of Agreement and in accordance with CJCSM 6510.01B. RMK complies with requirements to report incident and spillage should either occur. RMK responsibility is to notify milCloud/DISA and coordinate an appropriate response.

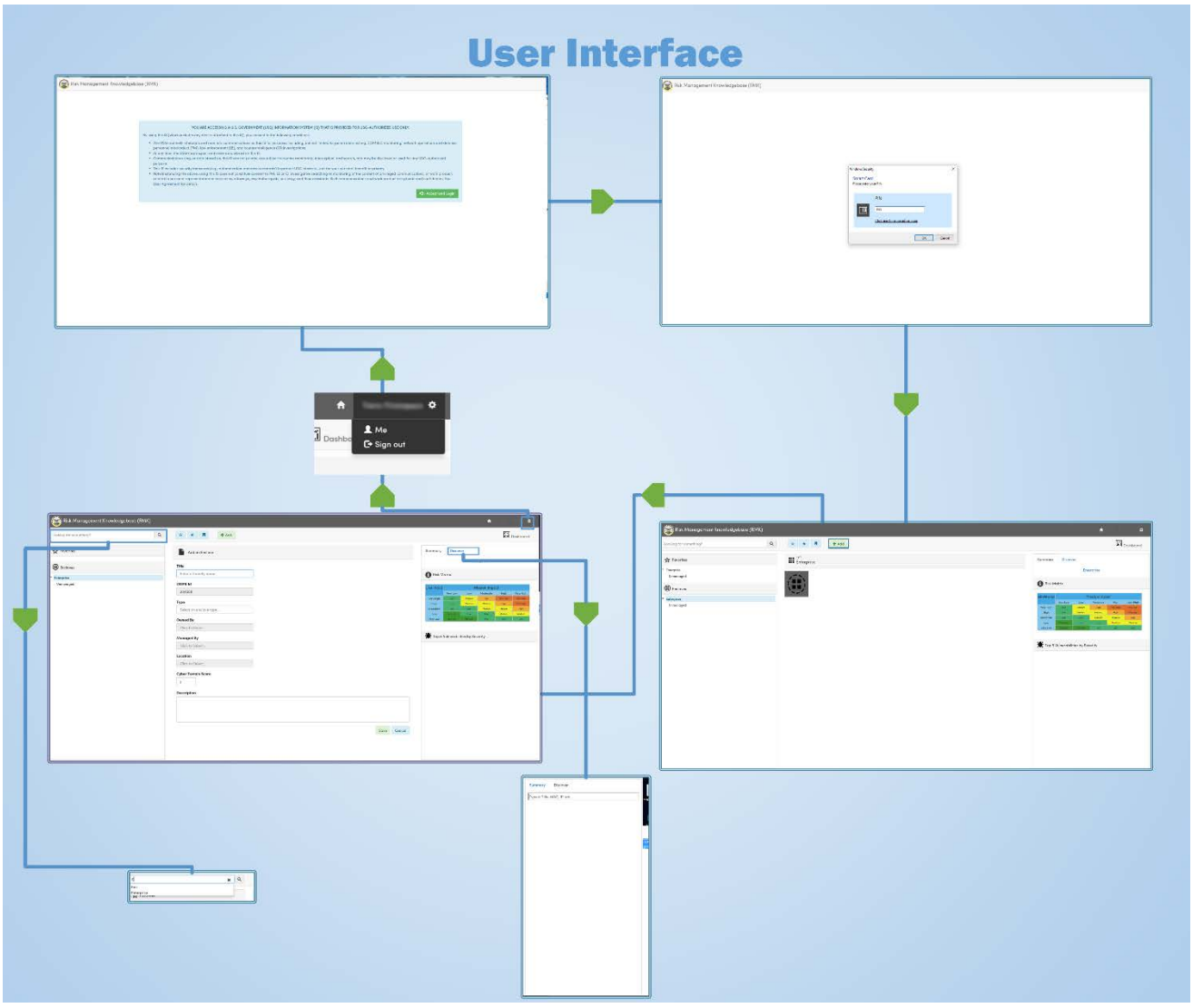
All maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location is covered by the milCloud Terms of Agreement and the DISA milCloud Virtual Data Center Administrative Guide Version 1.0, dated October 20, 2015. Also covered under these agreements are:

- The requirements to explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs,
- sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs, and
- the requirement to check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
- To ensure all physical equipment maintenance-related information is recorded properly in the DISA milCloud PMO maintenance records.

10.5 System and Information Integrity (SI)

RMK undergoes both automated and manual reviews of the system. The flaws are reported within a central repository and are corrected before being implemented within production. Updates to system components are manually implemented. Security updates are implemented immediately. Through this process, the organization is able to identify, report, and correct information system flaws. RMK also tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. RMK installs security-relevant software and firmware updates within the DISA prescribed time requirements and initiates flaw remediation into the organizational configuration management process.

10.5.1 UI Flow



10.5.2 Error Messages

RMK balances the error messages within the system to make sure they are helpful for the system administrator yet discrete for security. The majority of error messages concerning the system are sent to logs that are presented to System Administrators only. There error messages, while not specifying particular elements or actual data, provide enough detail for accurate and directed debugging. Those messages presented within the browser tend to be more generic in nature and useful for identifying higher level network issues. The more generic messages partnered with the logs, which can only be viewed by system administrators, are very helpful when debugging without being a security risk.

10.6 Media Protection (MP)

RMK is a virtual network that has no hardware and does not operate within a classified system. As such, there are no requirements to:

- Develop policy on hardware media protection that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities
- Develop procedures to facilitate the implementation of the media protection policy and associated media protection controls
- Restrict access to any media
- Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of the information
- Physically control and securely store any media
- Protect information system media until the media is destroyed or sanitize
- Employ access restrictions to media storage areas
- Protect and control media during transport outside of controlled areas
- Document activities associated with the transport of information system media

10.7 Incident Response (IR)

The Risk Management Knowledgebase Security Incident Response Capability is implemented in accordance with DoDD 8500.01E, DoD 8570.01-M, CJCSI 6510.01B, milCloud Admin Guide, and milCloud Terms and Conditions. milCloud is the cloud service provider that provisions the virtual data center within which the Risk Management Knowledgebase operates. The Risk Management Knowledgebase Security Incident Response Capability is focused on ensuring that System Administrators are properly trained to know the proper reporting process of security incidents to the milCloud Service Desk, which then formally manages security incidents as a service provider.

10.8 Contingency Planning (CP)

Through the use and utilization of DoD I 8500.01 March 14, 2014, section 13.r (pg24) DoD contingency plans and NIST SP 800-34 Contingency Planning Guide for Federal Information Systems, May 2010, RMK maintains compliance with applicable contingency planning policy

requirements that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Additionally, RMK has developed its own Information Systems Contingency Planning (ISCP) document. Through its ISCP, RMK:

- Coordinates contingency plan development with organizational elements responsible for related plans
- Plans for the resumption of all missions functions
- Coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied
- Identifies critical information system assets supporting essential mission functions
- Provides contingency training to information system users consistent with assigned roles and responsibilities

All back-up site requirements are covered by either the DISA milCloud Virtual Data Center Administrative Guide Version 1.0, or the DECC-Montgomery site COOP program.

THIS PAGE BLANK

Appendix A REFERENCES

Executive Order, Making Open and Machine Readable the New Default for Government Information, 9 May 2013.

Office of Management and Budget Memorandum M-13-13, Open Data Policy – Managing Information as an Asset, 9 May 2013.

DoD instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, 5 August 2013.

DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, 3 August 2015.

DoD Instruction 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), 21 May 2014.

DoD Instruction 8500.01, Cybersecurity, 14 Aug 2014

DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology, 12 Mar 2014

Department of Defense Net-Centric Services Strategy, March 2007.

Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary, 26 April 2010

DISA Policy Letter (draft) Open Sharing of Cybersecurity Data

The Department of Defense Cyber Strategy, Apr 2015

United States Cyber Command Joint Enterprise Risk Assessment Model (JERAM) User Guide, Version 5.0, 20 Oct 2014

Department of Defense Net-Centric Services Strategy, March 2007.

DoD Manual 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification, 24 Feb 2014

THIS PAGE BLANK

Appendix B ACRONYMS

ACAS	Assured Compliance Assessment Solution
API	Application Program Interface
ATO	Authority to Operate
CCC	Consolidated Communications Center
CCE	Common Configuration Enumeration
CCI	Control Correlation Identifier
CCRI	Command Cyber Readiness Inspection
CCSS	Common Configuration Scoring System
CDC	Core Data Center
CIO	Chief Information Officer
CMDB	Configuration Management Database
CMRS	Continuous Monitoring and Risk Scoring
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
COAMS	Cyber Operational Attribute Management System
COTS	Commercial Off-The-Shelf
CPE	Common Platform Enumeration
CSAAC	Cyberspace Situational Awareness Analytic Cloud
CVE	Common Vulnerability and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CyTS	Cyber Terrain Score
DCCB	DISANet Change Configuration Board

DECC	Defense Enterprise Computing Centers
DIACAP	DoD Information Assurance Certification and Accreditation
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	DoD Information Technology Portfolio Repository
DMS	Data Management Service
DMZ	Demilitarized Zone
DODIN	DoD Identification Number, formerly EDIPI (q.v.)
DoDIN	Department of Defense Information Networks
DNS	Domain Name System
DPAS	Defense Property Accountability System
DPMS	Digital Policy Management Service
DoD	Department of Defense
DOS	Denial of Service
DDOS	Distributed Denial of Service
EDIPI	Electronic Data Interchange Personal Identifier, now referred to as DODIN (q.v.)
eMASS	Enterprise Mission Assurance Support Service
ESB	Enterprise Service Bus
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FLOSS	Free/Libre Open-Source Software; q.v. *FOSS*.
FOC	Full Operational Capability
FOSS	Free and Open-Source Software; q.v., *FLOSS*.
FY	Fiscal Year
GRE	Governance, Risk Management, Compliance

HBSS	Host Based Security System
IA	Information Assurance
IaaS	Infrastructure as a Service
IAP	Internet Access Point
IATO	Interim Authority to Operate
IATT	Interim Authority to Test
IAVM	Information Assurance Vulnerability Management
IP	Internet Protocol
IPsec	Internet Protocol Security
ISCM	Information Security Continuous Monitoring
ISSM	Information System Security Manager
IT	Information Technology
JERAM	Joint Enterprise Risk Assessment Model
JRSS	Joint Regional Security Stack
KCT	Key Cyber Terrain
NCCM-R	Network Change and Configuration Management – Replacement
NIST	National Institute of Science and Technology
NVD	National Vulnerability Database
OSS	Operational Support System
OV	Operational View
OVAL	Open Vulnerability and Assessment Language
PICE	Pre-Ingest Correlation Engine
POA&M	Plan of Actions and Milestones
RME	Risk Management Executive
RMF	Risk Management Framework

RMK	Risk Management Knowledgebase
SA	System Administrator
SCA	Security Configuration Assessment
SCAP	Security Content Automation Protocol
SCCM	Systems Center Configuration Manager
SCM	Secure Configuration Management
SDD	System Design Document
SIEM	Security Information and Event Management
SRG	Security Requirements Guide
SRR	Security Readiness Review
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guide
SV	Systems Viewpoint
USGCB	U.S. Government Configuration Baseline
VA	Vulnerability Assessment
VAR	Vulnerability Assessment Report
VMS	Vulnerability Management System
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

Appendix C GLOSSARY

Application Programming Interfaces (API). A set of programming instructions and standards for accessing a web-based software application.

Asset. A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. (CNSSI No. 4009)

Compute Asset. An asset that possesses an Operating System.

Domain. An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. (CNSSI No. 4009)

Enclave. Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. (CNSSI No. 4009)

Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (44 U.S.C., Sec 3542)

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C., Sec 3502)

Information Security System. An Information System dedicated to performing a function related to Information Security.

Information Security Data. Data that is produced from an Information Security System.

Non-compute Asset. An asset that does not possess an Operating System.

Risk Management. Risk Management is the program and supporting processes used to manage information security risk to organizational operations (including mission, functions, image, and reputation), organization assets, individuals, or the organizations and the Nation. This Risk Management also includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. NIS TSP 800-39

Risk Management Knowledgebase (RMK). An enterprise data bus capable of uniquely-structuring data from multiple organizational systems for more effective correlating, processing, and publishing of information security data in order to support risk management at the enterprise level. The RMK also employs operationalized ontologies that have been tailored for the DISA Information Security domain to distinctively reveal new data relationships that directly contribute to improved Risk Management activities.

THIS PAGE BLANK

Appendix D INVENTORY OF INFORMATION SECURITY SYSTEMS AND PROCESSES

Access, Security, and Configuration Control (ASCC): a cross-platform server automation tool based on the BMC BladeLogic product.

Assured Compliance Assessment Solution (ACAS): an integrated software solution that is scalable to an unlimited number of locations. ACAS provides automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery. Further, the product suite generates the required reports and data, with a centralized console, and is SCAP compliant

Continuous Monitoring and Risk Scoring (CMRS): a web based system that visualizes the cybersecurity risk of the Department of Defense (DoD) based on published asset inventory and compliance data. CMRS supports the risk-management approach to cybersecurity oversight by quantitatively displaying an organization's security posture through the use of risk dashboards. Using the risk dashboards, users can gather actionable direction, implement prioritized mitigation decisions, and ensure effectiveness of security controls in order to support their cybersecurity risk management duties. (The risk state of the DoD Enterprise security controls for software inventory, antivirus configuration, Security Technical Implementation Guide (STIG), and Information Assurance Vulnerability Management (IAVM) vulnerability and patch compliance are measured and reported.)

Cyber Operational Attribute Management System (COAMS)

Cyberspace Situational Awareness Analytic Cloud (CSAAC)

DoD Information Technology Portfolio Repository (DITPR): the DoD's inventories of IT systems. DITPR is a web-based IT system which contains basic overview information regarding all DoD IT systems. This includes information such as system names, acronyms, descriptions, sponsoring component, approval authority, points of contact, and other basic information required for any analysis of Departmental inventory, portfolios, or capabilities. DITPR supports IT Portfolio Management capabilities. DITPR also enables the Portfolio Managers with IT investments and Components to accomplish IT Portfolio Management (PfM).

Domain Name System (DNS): a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information with domain names assigned to each of the participating entities. It translates domain names, easily memorized by humans, to the numerical IP addresses needed in support of computer services and devices worldwide.

Defense Property Accountability System (DPAS): a Property System that provides accountability for: Real Property/Stewardship Land; Military property; Heritage Assets; Personal Property; Government Furnished Equipment

Digital Policy Management Service (DPMS)

Element Management System (EMS): responsible for all systems that provide direct control and management of DISN elements. The EMS is implemented through a flexible and globally distributed architecture to support network operations at the Global and Theater NetOps Centers. The EMS collects, consolidates, and normalizes fault, performance, and configuration data from network elements and transmits the data to the Network Management System (NMS)

Enterprise Mission Assurance Support Service (eMASS): a service-oriented computer application that supports Information Assurance (IA) program management and automates the DoD Information Assurance Certification and Accreditation Process (DIACAP). eMASS is managed by DISA to help the DoD maintain IA situational awareness, manage risk, and comply with the Federal Information Security Management Act (FISMA).

Enterprise Security Posture System (ESPS): a comprehensive security compliance tool created by DECC Montgomery which leverages the use of FSO/SCAP content with increased automation. ESPS provides the situational awareness of the security posture of all servers regardless of platform.

Host Based Security System (HBSS): is the DoD's commercial-off-the-shelf (COTS) suite of software applications used to monitor, detect, and counter attacks against the DoD computer networks and systems.

Information Assurance Vulnerability Management (IAVM): employs positive control mechanisms to mitigate potentially critical software vulnerabilities, through the rapid development and dissemination of actions to all Combatant Commands/Services/ Agencies /Field Activities (CC/S/A/FAs). The US CYBER COMMAND, subordinate to the United States Strategic Command (STRATCOM), and the Defense Information Systems Agency (DISA) jointly manage the IAVM and Computer Network Directives.

Joint Enterprise Risk Assessment Model (JERAM): is a framework that provides a standardized assessment across the DoD that enhances situational awareness and informs commanders regarding risk to their military operations. The JERAM is a risk assessment tool that assesses threats and vulnerabilities against DoD Information Networks (DoDIN)

Cyber Terrain: a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

Microsoft® Systems Center Configuration Manager (SCCM): a commercial product for inventorying, auditing, administrating, and updating Microsoft platforms

Network Change and Configuration Management-Replacement (NCCM-R): a strategic approach to minimizing the impact of change on a network or IT ecosystem. The goal is to create a company-wide standardized method to implementing both self-motivated, internal change, such as upgrades and troubleshooting; as well as externally required change, such as government regulations on data.

Operational Support System (OSS)

Pre-Ingest Correlation Engine (PICE)

Secure Configuration Management (SCM): the integration and optimization of enterprise IA applications, tools, and data standards to support automated processes for risk management. SCM is supposed to deliver capabilities that enable continuous monitoring, enterprise vulnerability exposures, and awareness.

Security Information and Event Management (SIEM)

Security Requirements Guide (SRG): a compilation of Control Correlation Identifiers (CCIs) grouped into more applicable, specific technology areas at various levels of technology and product specificity. An SRG provides DoD specificity to CCI requirements (organizationally defined parameters). An SRG is used by DISA FSO and vendor guide developers to build Security Technical Implementation Guides (STIGs). There are basically two types of SRGs. The first group are the four CORE SRGs which deal with Applications, Networking Devices, Operating Systems, and Policy. The second group is the Technology specific SRGs. A Technology specific SRG is a child of a CORE SRG. For example, the Database SRG was derived from the requirements in the Application SRG.

Security Readiness Review (SRR): the audit performed at designated sites to review compliance with DISA STIGs.

Security Technical Implementation Guide (STIG): contains technical guidance to lock-down information systems / software that might otherwise be vulnerable to a malicious computer attack (or greater than three [3] unsuccessful log-in attempts).

RMK also complies with STIG requirements to lock-down an account for unsuccessful log-in attempts and STIG-compliant timed-out account lock-out: 20-minutes.

Serialized Asset Management / Serialized Asset Lifecycle Tool (SAM/SALT): Reports on exceptions between DPAS and what is auto-discovered on the network

Vulnerability Management System (VMS): is a web-based database interface to process data generated by DoD Enterprise tools and assist CC/S/A/FAs in identifying and tracking security vulnerabilities throughout their lifecycle. VMS monitors the compliance of CC/S/A/FAs regarding Information Assurance Vulnerability Management (IAVM) notices issued by USCYBERCOM. VMS tracks the potential existence of all vulnerabilities based on the posture (configuration, installed software, etc.) of an asset.

THIS PAGE BLANK

Appendix E CYBER TERRAIN SCORE

One aspect of the Risk Management Knowledgebase that distinguishes it from other risk management methodologies is the application of the Cyber Terrain Score (CyTS) to quantify operational impact of enclaves. The Cyber Terrain Score is derived by applying a scoring rubric. The intent is for the DISA Center for Operations to maintain custody of the Cyber Terrain Score for all DISA systems and to update the scores based on their assessment of any operational impacts caused by system loss or degradation.

The following scoring rubric breaks down assessment factors in order to assign a cyber-terrain score, based on an understanding of factors and importance of the system on completing the organization's mission. It is important to note that a cyber-terrain score may be adjusted over time (temporarily or permanently) based on the emergence of new missions or the elevated importance of a current mission (whether based on updated intelligence, geographic importance, scope, or applicability).

The following chart gives the person scoring any given system "hints" as to where certain impact factors should be scored. The chart is not intended to be all inclusive and should only be considered as a guideline to the individual assigning a cyber-terrain score. Judgement and experience are also two essential factors that an individual should use to guide the assignment of appropriate cyber-terrain scores.

Score	Description of Impact
10	Loss of Life
9	Inability to execute or complete mission
9-7	Degradation of C2
9, 7, 5	Mission Performance Degradation (Limited, Moderate, Severe)
8	Compromise of Personal Health or Privacy Data
8	Inability to complete full mission
8	OPSEC Violation
8-6	Loss of Logistical support
8-6	International impact
8, 6, 4	Economic Impact (Organizational, DoD, National)
7	Complete Loss of a System / Application / Infrastructure for greater than 14 days
7	Federal Regulation or Law Non-Compliance (other than Privacy & HIPAA/HITECH)
6	Adversaries' capabilities increased
6	Loss or effect on associated systems
5	Effect on Future Capabilities
4	Contractual Non-Compliance
3	Public Affairs (Public Incident)

Table 1. Cyber Terrain Score Description

Value	IMPACT Score Description	Data Compromise	Mission Impact	System / Network Operational Dependencies	Effect on Future Capabilities	Departmental Affect
10	The event or loss of confidentiality, integrity, or availability would be expected to have catastrophic adverse effects on the mission leading to loss of life and complete mission failure.	Data is of a classification & operational nature as to catastrophically affect the mission. Data protections under the Privacy, HIPAA , and HITECH Acts (PII & PHI)	Loss of life	Compromise of operationally critical system	Immediate and lasting effect will be recognized	International effect and impact can be expected
9	The event or loss of confidentiality, integrity, or availability would be expected to have catastrophic adverse effects on the mission leading to complete mission failure.		Inability to perform or complete the mission [whether based on type of system(s) affected, number of users, or targeted user(s)]	Compromise of a system(s) that advisedly affects other / multiple vital systems		
8	The event or loss of confidentiality, integrity, or availability could be expected to have multiple severe or catastrophic adverse effects on the mission. A severe or catastrophic adverse effect may mean, the threat could cause several severe degradations in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or catastrophic harm to individuals involving loss of life or serious life threatening injuries.					
7	The event or loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on the mission. A severe or catastrophic adverse effect may mean the threat could cause a severe degradations in or loss of mission capability to an extent and duration that the organization is not able to perform one of its primary functions.	Data protected by Federal Statutes and Department of Defense Regulation	Inability to execute primary objective of the mission [whether based on type of system(s) affected, number of users, targeted user(s)]	Compromise of a system that advisedly affects or potentially affects another system (e.g.: IDS, IPS, Firewalls)	Potential for lasting effect is very high	National-level impact can be expected (e.g.: media, DHS, etc.)
6	The event or loss of confidentiality, integrity, or availability could be expected to have multiple serious adverse effects on the mission. A serious adverse effect means that the threat event may cause significant degradation in mission capability to an extent and duration that the organization is not able to effectively perform one or more of its primary functions; the effectiveness of the functions are significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or significant harm to individuals that does not involve loss of life or serious life threatening injuries.					
5	The event or loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on the mission. A serious adverse effect means that the threat event may cause significant degradation in mission capability to an extent and duration that the organization is not able to effectively perform one of its primary functions; the effectiveness of the function is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or significant harm to individuals that does not involve loss of life or serious life threatening injuries.					

4	The event or loss of confidentiality, integrity, or availability could be expected to have multiple limited adverse effects on the mission. The limited effect may be in the form of mission capability degradation, but the organization is able to perform its primary functions with minor degradation in effectiveness.	Data protected by local regulations	Primary mission objective can still be performed with over-all varying degrees of minor degradation (Regardless of number of systems or users)	Any cursory system affected is of a non-critical nature	Minimal to no future effect will be felt.	Internal-only departmental effects can be expected
3	The event or loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on the mission. The limited effect may be in the form of mission capability degradation, but the organization is able to perform its primary functions with minor degradation in effectiveness.					
2	The event or loss of confidentiality, integrity, or availability, could be expected to have minor and negligible adverse effects on the mission, organizational operations, organizational assets, individuals, or other organizations.					No noticeable effect outside immediate team can be expected.
1	The event or loss of confidentiality, integrity, or availability, could be expected to have none or negligible adverse effects on the mission, organizational operations, organizational assets, individuals, or other organizations.			Stand-Alone System	No effect can be anticipated	

Table 2. Cyber Terrain Score Rubric

THIS PAGE BLANK

Appendix F PLAN OF ACTION AND MILESTONES

DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology, requires the DISA Chief Information Officer to implement processes and procedures to manage Plans of Action and Milestones (POA&Ms) for known vulnerabilities in assets. While these POA&Ms do not mitigate cybersecurity risks, they help provide visibility of vulnerabilities and ensure that responsible individuals have specific plans in place to eventually mitigate those risks.

While the focus of RMK capability is to support executive decision making on how to best mitigate cybersecurity risks, a POA&M feature will be provided in RMK to allow visibility on those cybersecurity risks that remain unmitigated and assumed by DISA. POA&Ms will be linked to asset vulnerabilities that are identified through various enterprise scanning tools. For each asset vulnerability, a POA&M will be developed by the Information Systems Security Manager that describes basic information on why the vulnerability remains unmitigated and a projected date of when the vulnerability will be mitigated. The POA&Ms will be compiled for a given enclosure and routed through the Directorate SES, Authorizing Official Representative, and Senior Information Security Officer before being accepted by the DISA Authorizing Official who assumes the vulnerability risk until it is properly mitigated. Figure 1 provides an overview of the RMK POA&M functionality.

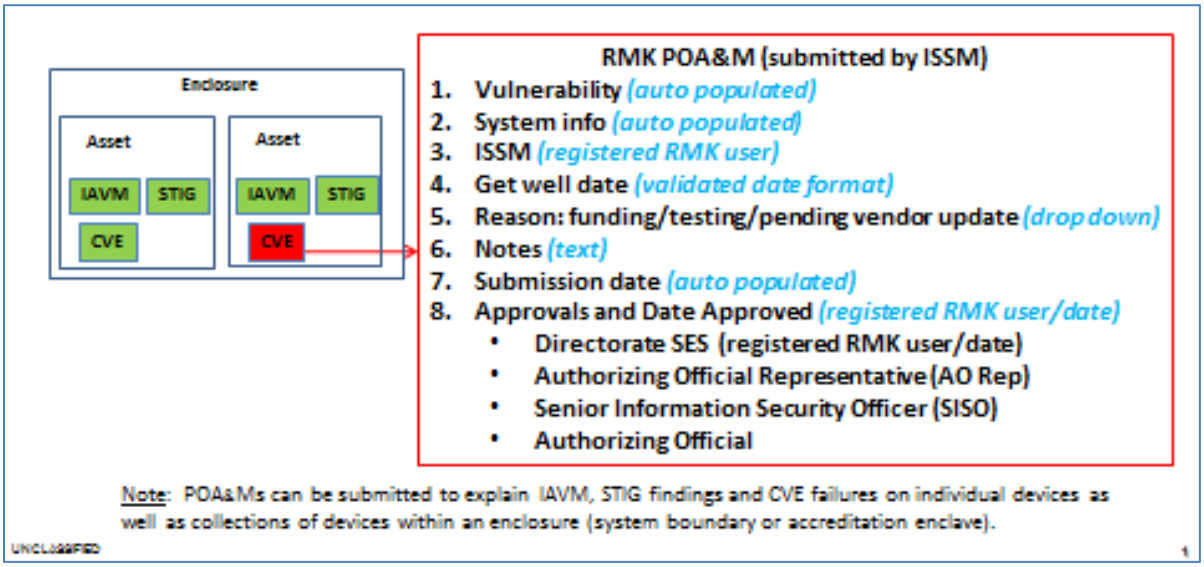


Figure 7. RMK POA&M Overview

THIS PAGE BLANK

Appendix G DISA ORGANIZATION

The Risk Management Knowledgebase is being developed specifically for DISA and organize enclaves into appropriate DISA centers, directorates, and divisions as appropriate. The following list provides those DISA organizations that own systems for which the DISA Risk Management Executive is responsible for.

- Workforce Management Directorate (MP)
- Financial Management Directorate (DC)
- Operations Center (OPC)
- Engineering and Solutions Analysis Directorate (EE)
- Services Development Directorate (SD)
- Test and Evaluation Executive (TED)
- Infrastructure Development Directorate (ID)
- 5th Estate (FEC)
- Infrastructure Directorate (IE)
- Services Directorate (SE)
- White House Communications Agency (WHCA)
- White House Support Staff (WHSS)
- COMSATCOM
- JFHQ-DODIN