# Air Force Life Cycle Management Center

# Standard Process

# For

# *Cybersecurity*

# *Assessment and Authorization*

Process Owner:  AFLCMC/EZA/EZB/EZC

Date:  21 October 2021

Version:  3.3

## *Cybersecurity Assessment and Authorization*

| Record of Changes | | |
|---|---|---|
| Version | Effective Date | Summary |
| 1.0 | 1 Aug 13 | Standard process approved at 18 Jul 13 S&P Board |
| 2.0 | 15 June 2017 | Updated to align with DoDI 8500.01 and DoDI 8510.01 (Cybersecurity and Risk Management Framework) and to expand the scope of applicability from PIT systems to the entire IT spectrum. Approved at the 15 June 2017 Standards & Process Board. |
| 3.0 | 21 June 2018 | Updated hyperlinks, references, and definitions. Improved various wording and clarified business rules in Table 2.0. Corrected administrative errors. Approved at the 21 June 2018 S&P Board. |
| 3.1 | 17 October 2019 | Annual Review. Aligned with SP for Program Protection Planning and System Security Engineering. Corrected administrative errors. Updated references. Approved at the 17 October 2019 S&P Board. |
| 3.2 | 15 October 2020 | Annual Review. Updated to reflect NIST 800-37 R2. Changed applicability to include SAP. Added ISSM. Corrected administrative errors. |
| 3.3 | 21 October 2021 | Annual Review. Updated references to current versions. Corrected administrative errors. Inputs, process, and customer modified within SIPOC Table 1. Added acquisition intelligence (AIA) roles and responsibilities, e.g. 3.0. Added adversary and threat descriptive information in paragraph 4.1.1. Approved at 21 Oct 2021 SP&P Group. |

# *Cybersecurity Assessment and Authorization*

## 1.0 Description.

This process defines Cybersecurity Assessment and Authorization (A&A) procedures for Information Systems (IS), Platform Information Technology (PIT), Information Technology (IT) Services, and IT products that are or will be assessed or assessed and authorized by Authorizing Officials (AOs) within the Air Force Life Cycle Management Center (AFLCMC) supporting the following DAF authorization boundaries: Aircraft, Command and Control (C2), Rapid Cyber Acquisition (RCA), and Weapons. This process does not apply to any other authorization boundaries. This process applies to Special Access Programs within the above listed boundaries. See the Department of Defense (DoD) Risk Management Framework (RMF) Knowledge Service Collaboration Air Force Component Workspace site for the boundary definitions for each AO:
https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx
This process addresses the Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework for DoD Information Technology*, requirement that systems that receive, process, store, display, or transmit DoD information (unclassified and classified) must receive an authorization in order to test or to operate.

## 2.0 Purpose.

This process applies a risk-based methodology to assess and authorize systems and products acquired and managed by AFLCMC that fall within the authorization boundaries of the Aircraft, C2, RCA, and Weapons AOs in alignment with DoDI 8510.01, Air Force Instruction (AFI) 17-101, Risk Management Framework for AF Information Technology, and. The purpose is to identify and mitigate cybersecurity risks in order to protect systems and products from unauthorized access, use, disclosure, disruption, modification, or destruction. This process details the “assess and authorize” steps from the Risk Management Framework (RMF) as shown in Figure 1 in accordance with 8510.01. For applicable AFLCMC systems, this process supports the implementation of cybersecurity currently prescribed by the Federal Information Systems Management Act (FISMA), as well as DoD and DAF Directives and Instructions. This process does not supersede guidance published at the DAF level or for procedures specific to mission areas, but rather it defines a common assessment and authorization process used by AFLCMC. For Weapon Systems categorized as PIT, refer to AFLCMC Standard Process for Weapon System Program Protection Planning & System Security Engineering (PPP/SSE SP) to help execute RMF steps 0-3, assist in developing Request for Proposals, and develop required A&A artifacts while going through the acquisition lifecycle.

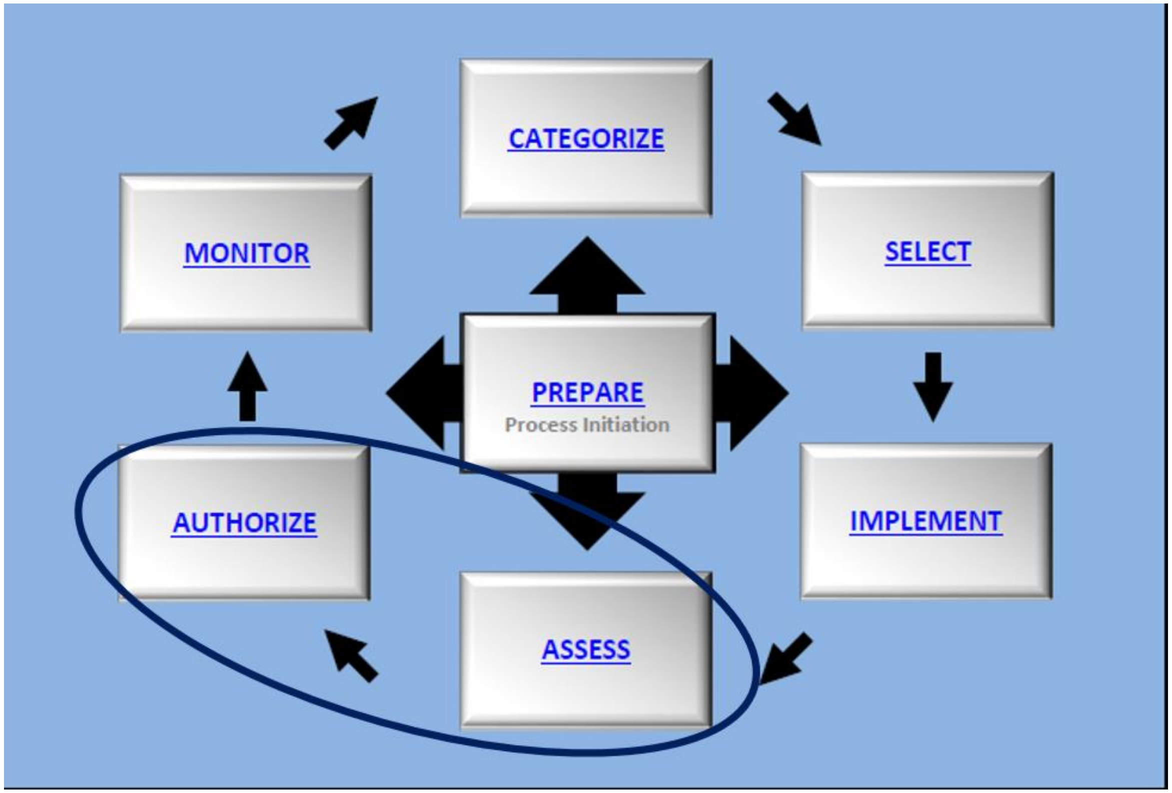


Figure 1 – Risk Management Framework with A&A process steps circled

## 3.0 Entry/Exit Criteria.

3.1 Entry Criteria: Steps 0 to 3 (Prepare, Categorize, Select and Implement) of the RMF process must be completed and the resulting artifacts, identified in Attachment 1 Work Breakdown Structure (WBS) 0-3, must be available before executing this assessment and authorization process. AOs, AO Designated Representatives (AODRs), Security Control Assessors (SCAs) or their representatives, Acquisition Intelligence Analyst (AIA), and Program Managers (PMs) including their Engineers, Information System Security Managers or Information Systems Security Officers all have a role in completing the RMF steps 0-3 that are detailed in other DoD and DAF guidance, such as PM guides, systems security engineering directions/instructions etc. Any systems and products discussed in paragraph 1.0 which require a cybersecurity authorization must execute this process.  Conditions that will initiate execution of this process include requirements for authorization to test or operate, modifications to an authorized system which impact the system's cybersecurity risk posture, expiration of existing authorizations, or Denial of an Authorization to Operate (DATO).

3.2 Exit Criteria:  Once an authorization has been issued, this assessment and authorization process is complete and is followed by step six, Monitor of the RMF process.  Continuous monitoring of security controls is required for the authorization to remain valid.

## 4.0 Process Workflow and Activities.

4.1 The Suppliers, Inputs, Processes, Outputs, and Customers for this SP are shown in Table 1.

| Suppliers | Inputs | Process | Outputs | Customer |
|---|---|---|---|---|
| **Program Office** | Program Office provides an Architecture Analysis to start the process. Additional inputs required to conduct the process include security assessment plans, risk assessment documents, and other related artifacts (e.g., Intel threat Reporting). | Cybersecurity risks are assessed and presented to the AO for acceptance, approval of POA&M, and operating conditions. | Cybersecurity authorization decision memoranda are issued by the AO then distributed to PMs and ISSMs of systems or products. | AO, Program Office, and MAJCOM user/sponsor. |

Table 1 - Suppliers, Inputs, Process, Outputs, Customers (SIPOC)

4.2 The A&A Process Flow is shown in Figure 2.  Note boxes on a line between two organizations imply shared responsibility.  Refer to the WBS, Attachment 1.

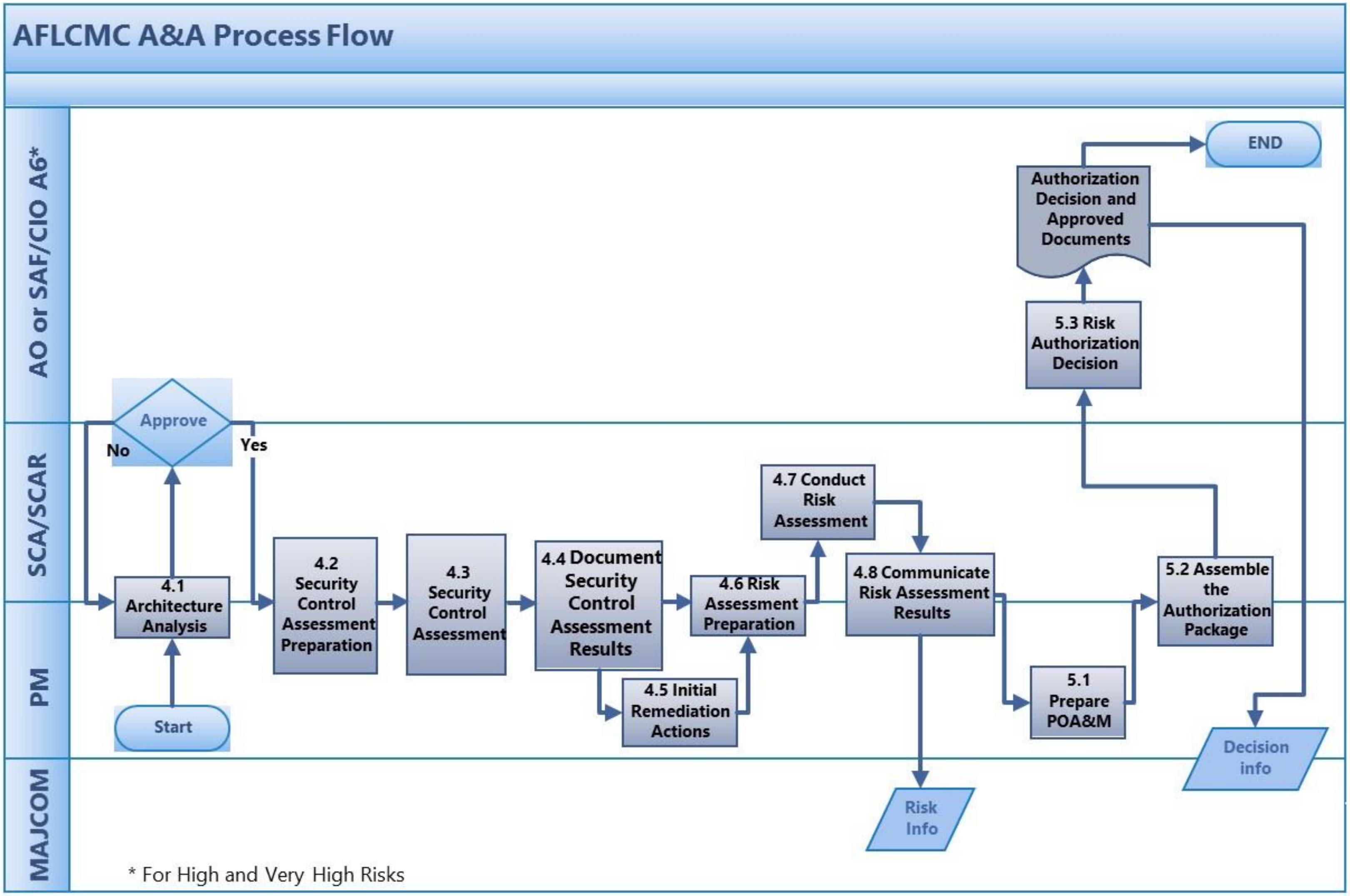

AFLCMC A&A Process Flow
AO or SAF/CIO A6*
SCA/SCAR
PM
MAJCOM
END
Authorization Decision and Approved Documents
5.3 Risk Authorization Decision
Approve
No
Yes
4.7 Conduct Risk Assessment
4.1 Architecture Analysis
4.2 Security Control Assessment Preparation
4.3 Security Control Assessment
4.4 Document Security Control Assessment Results
4.6 Risk Assessment Preparation
4.8 Communicate Risk Assessment Results
5.2 Assemble the Authorization Package
4.5 Initial Remediation Actions
5.1 Prepare POA&M
Start
Decision info
Risk Info
* For High and Very High Risks

Figure 2 – A&A Process Flow

4.3 The WBS shown in Attachment 1, defines activities, descriptions, OPRs, Inputs/Outputs, Supplier and Customers.

4.4 Cybersecurity Risk Assessment and Management, Attachment 2, provides the preferred methodology for risk assessment and management.

**5.0 Measurement.** Table 2 provides details on this standard process metric. SCAs will collect data, perform calculations, and report the metrics for their respective portfolios. Measurement is a mandatory element for all AFLCMC Standard Processes. It serves as a benchmark to gauge the effectiveness of Standard Processes.

| | | Metric Attribute | Description |
|---|---|---|---|
| **Admin Info** | | **APD Ref No** | T02 |
| | | **Process Name** | Cybersecurity Assessment and Authorization |
| | | **Process Owner** | EZA, EZB, EZC |
| | | **Metric POC** | EZA |
| **S** | **Specific** | **Metric Name** | Cybersecurity Assessment and Authorization Process Utilization |
| | | **Metric Description** | Determine the level of process usage across the center. |
| | | **Calculation** | Calculation is the number of systems executing the process vs divided by the total number of known systems that should be executing the process. |
| | | **Business Rules** | The number of systems executing the process are those systems that have completed “WBS 4.1.1, Submit Architecture Analysis Artifacts” or those that have an existing authorization.<br>The total number of known systems that should be executing the process are those that have existing authorization (as counted above) and those that require an authorization that don’t currently have one. |
| **M** | **Measurable** | **Data Source** | AFLCMC AO Tracking Databases |

| | | | |
|---|---|---|---|
| A | Actionable | Decision Maker | AFLCMC/EN-EZ |
| | | Review Forum / Governance Body | Standards & Process (S&P) Board |
| | | Target | Green (80% in Process) |
| | | Threshold (G/Y/R) | > 80% in Process (G)<br>60%-80% in Process (Y)<br><60% in Process (R) |
| | | Baseline Performance | Will be established Semi-Annually (FY) |
| R | Relevance | Enterprise Impact / Process Purpose | Defines Cybersecurity A&A procedures for systems and products. These systems and products are those that will be assessed or assessed and authorized by AOs appointed within the AFLCMC. |
| | | AFLCMC Objective | AFLCMC Objective 2.1: By the end of FY, assess all, complete remaining, and improve standard processes. |
| T | Time Based | Baseline Date | Annually (FY) |
| | | Review Frequency | Semi-Annually (FY) |
| | | Update Frequency | Semi-Annually (FY) |

| | Metric Attribute | Description |
|---|---|---|
| Administrative Info | Process Name | Cybersecurity Assessment and Authorization |
| | Process Lead | EZA, EZB, EZC |
| | Metric POC | EZA |
| | Date Completed | October 2021 |
| S | Metric Name / Description | Cybersecurity Assessment and Authorization Process Utilization |
| | Calculation | Calculation is the number of systems executing the process divided by the total number of known systems that should be executing the process. |
| | Business Rules | The number of systems executing the process are those systems that have completed “WBS 4.1.1, Submit Architecture Analysis Artifacts” or those that have an existing authorization. The total number |

| | | |
|---|---|---|
| | | of known systems that should be executing the process are those that have existing authorization (as counted above) and those that require an authorization that don't currently have one. |
| M | Data Source | AFLCMC AO Tracking Databases |
| A | Process Owner | EZA, EZB, EZC |
| | Decision Maker | AFLCMC/EN-EZ |
| | Review Forum / Governance Body | Standards & Process (S&P) Board |
| | Target | Green (80% in Process) |
| | Thresholds (R/Y/G) | Green: > 80% in Process<br>Yellow: 60%-80% in Process<br>Red: <60% in Process |
| | Baseline Performance | Will be established Semi-Annually (FY) |
| R | Enterprise Impact / Process Purpose | Defines Cybersecurity A&A procedures for systems and products. These systems and products are those that will be assessed or assessed and authorized by AOs appointed within the AFLCMC. |
| T | Baseline Date | Annually (FY) |
| | Review Frequency | Semi-Annually (FY) |
| | Update Frequency | Semi-Annually (FY) |

Table 2 – A&A Process Metric

**6.0 Roles and Responsibilities.** See DoDI 8500.01, DoDI 8510.01, and AFI 17-101 for detailed descriptions of cybersecurity and RMF key personnel roles and responsibilities. The paragraphs below provide top-level roles and responsibilities for key personnel involved in the AFLCMC A&A process.

6.1 Process Owner - AFLCMC/EZA/EZB/EZC:

6.1.1. Maintains and coordinates any changes to this process internally and externally to AFLCMC.

6.1.2. Leads and/or assigns personnel to work on any process improvement.

6.1.3. Coordinates changes to this process with the AFLCMC Standards & Process (S&P) Board.

6.2 AFLCMC S&P Board

6.2.1. Reviews and approves new critical and key processes.

6.2.2. Reviews and approves changes to critical and key processes.

6.3 Authorizing Official (AO)

6.3.1 Appointed by DAF Chief Information Officer (SAF/CIO).

6.3.2. Issues authorizations of systems based on overall risk level, with the exception of systems with unmitigated “Very High” and “High” risk.

6.3.3. If risk is determined to be unacceptable when compared to the mission assurance requirement, then the AO, in collaboration with all system stakeholders e.g., SAF/CIO A6, Chief Information Security Officer (CISO), Information System Owner (ISO), Major Command (MAJCOM), (Program Manager), will issue the authorization decision in the form of a DATO.

6.4. Authorizing Official Designated Representative (AODR)

6.4.1. Appointed by an AO.

6.4.2. Performs all duties designated by the AO with the exception of risk acceptance.

6.5. Security Control Assessor (SCA)

6.5.1. Appointed by DAF CISO.

6.5.2. Makes risk recommendation to AO based on risk assessment (via Security Assessment Plan (SAP) and Report (SAR) and Risk Assessment Report (RAR) and Authorization Briefing).

6.5.3. AFLCMC/EZAS is the SCA for Aircraft.

6.5.4. AFLCMC/EZB is the SCA for Weapons.

6.5.5. AFLCMC/EZC is the SCA for C2 and RCA.

6.6. Security Control Assessor Representative (SCAR)

6.6.1. Appointed by a SCA.

6.6.2. Executes the assessments on behalf of and for the SCA.

6.7. Program Manager (PM)

6.7.1. Responsible for system cybersecurity and for attaining authorizations. Ensures the system has a current authorization.

6.7.2. Develops cybersecurity documents in accordance with Attachment 1.

6.7.3. Ensures risk assessment results and associated mitigations are coordinated across appropriate levels of the program and with the program's stakeholders (e.g. MAJCOM, System Owners, etc.).

6.7.4. Ensures personnel are assigned for the Information System Security Manager (ISSM), Information System Security Officer (ISSO), and Information System Security Engineering (ISSE) functions as required.

6.8. Information System Security Manager (ISSM)

6.8.1. Serves as the primary cybersecurity technical advisor to the AO, PM, and ISO.

6.8.2. Ensures the integration of cybersecurity into and throughout the lifecycle of the IT on behalf of the AO.

6.8.3. Ensures all DAF IT cybersecurity-related documentation is current and accessible to properly authorized individuals.

6.8.4. Continuously monitors the IT, current threats per intelligence analysis, environment for security-relevant events, assess proposed configuration changes for potential impact to the cybersecurity posture, and assess the quality of security controls implementation against performance indicators.

6.8.5. Ensures cybersecurity-related events or configuration changes that impact DAF IT authorization or adversely impact the security posture are formally reported to the AO.

6.9. Information System Security Officer (ISSO)

6.9.1 Serves as the primary cybersecurity technical advisor to the ISSM.

6.9.2 Ensures the integration of cybersecurity into and throughout the lifecycle of the IT on behalf of the ISSM.

6.10. DAF Chief Information Officer / Special Access Program Central Office

6.10.1. Accepts High and Very High cybersecurity risks.

6.10.2. Is informed of all DATO decisions.

## 7.0 Tool.

The DoD maintains an RMF Knowledge Service at the following site: https://rmfks.osd.mil/rmf with an Air Force Component Workspace under the Collaboration menu containing specific DAF information and templates.

The program receives threat information through the acquisition intelligence analyst's utilization of the Community On-Line Intelligence System for End-Users and Managers (COLISEUM) tool.

## 8.0 Training.

8.1 Group training on A&A is available upon request or during AFLCMC Focus Weeks which are scheduled periodically throughout the calendar year.  Contact SCA or SCAR focal points for training opportunities.

8.2 The DoD Cyber Exchange NIPR provides access to cyber training and guidance: https://cyber.mil/.

8.3 The DISA Security Training, Education, and Professionalization Portal (STEPP) provides access to additional cyber and cyber roles training: https://www.cdse.edu/stepp/.

8.4 Numerous AFIT courses such as, SYS 341, Cybersecurity Risk Assessment for Weapon System PIT: Aircraft https://www.afit.edu/ls.

## 9.0 Definitions (Refer to CNSSI 4009).

**Acquisition Intelligence Analyst (AIA)** serves as a focal point for programs to receive threat support from the intelligence community and to assist a program in the identification and satisfying of intelligence requirements.

**Architecture Analysis Report (AAR)** documents the system's architecture and cybersecurity concerns.  The AAR provides a description of the system being submitted for authorization.  The document contains an overview of the system including mission and operating environment.  The system description portion shall include architecture drawings and diagrams, description of data flows and types including ports and protocols, external and internal interfaces, hardware and software inventory, and any other system unique characteristics so that the system can be assessed.  It may be considered part of the Security Plan.

**Authorizing Official (AO)** is appointed by the DAF SAF/CIO as the authority to authorize IT systems as specified in their designation memorandum.  The AO has the authority to grant or deny system testing and operation of systems.  The AO balances the total risks and the technical, programmatic, and user requirements in rendering authorization decisions.

**Authorization to Operate (ATO)** is a decision issued after the risk assessment process has been completed.  In addition to being required for system operations, an ATO is also required by the Air Force Operational Test and Evaluation Center prior to the start of Initial Operational Test and Evaluation and by the Joint Interoperability Test Command prior to interoperability certification testing.

**Continuous Monitoring** is used to monitor authorization operating conditions and the effectiveness of security controls employed within or inherited by the system and monitoring of any proposed or actual changes to the system and its environment of operation. The program develops a continuous monitoring strategy that must include a plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor.

**Denial of Authorization to Operate (DATO)** is a decision issued when cybersecurity risks are determined to be unacceptable when compared to a systems' mission assurance requirement.

**Interim Authorization to Test (IATT)** is a special type of authorization decision allowing an IT system to operate for the purpose of testing in order to complete specific test objectives.  An IATT does not authorize operational use of the system.

**Information System Security Manager (ISSM)** serves as a principal advisor on all matters, technical and otherwise, involving the security of information systems under his/her purview. The ISSM shall be appointed in writing by their respective chain of command/leadership (e.g., Commander, Commanding Officer, PM, CIO, PSO, or corporate equivalent). When circumstances warrant, a single individual may fill both the ISSM and the ISSO roles. ISSM responsibilities should not be assigned as collateral duties.

**Plan of Action and Milestones (POA&M)** is a document developed by the program that identifies tasks to mitigate identified risks, issues, or vulnerabilities as directed by the AO.  It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.  The format and/or tool used for a POA&M is determined by the AO.

**Platform Information Technology (PIT)** is a special category of information technology which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real-time to mission performance.  PIT is most often associated with a weapon system but is equally applicable to any host Platform including, but not limited to, command and control, armament, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and Supervisory Control and Data Acquisition systems.

**Program Manager (PM)** is the designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority.

**Risk Assessment** is the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.  As part of risk management, risk assessment incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place, synonymous with risk analysis.

**Risk Assessment Report (RAR)** contains the results of performing a risk assessment or the formal output from the process of assessing risk.

**Security Assessment Plan (SAP)** provides the objectives for the security control assessment. The SAP reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, or assessments subsequent to remediation actions).

**Security Assessment Report (SAR)** provides the results of assessing the implementation of the security controls identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The SAR also contains a list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls.

**Security Authorization Package** consists of the following components:  Security Plan, Security Assessment Report (SAR), Risk Assessment Report (RAR), Plan of Action and Milestones (POA&M), Continuous Monitoring Strategy and the Authorization Decision document.  Each AO may add components as necessary.

**Security Control Assessor (SCA)** is appointed by the Air Force CISO to assess IT as specified in their designation memorandum. The SCA makes risk recommendations based on risk assessments to identify residual risks of operating a system. The SCA makes risk recommendation based on risk assessment to identify residual risk of operating a system.  The SCA is responsible for assessing all technical content of products developed as a result of applying risk management framework process to AFLCMC systems and products.

**SCA Representative (SCAR)** may be assigned by the SCA as necessary. SCAR responsibilities are executed as assigned by the SCA within their designation memorandum.  SCAR appointments may be granted to an individual or organization.

**Security Plan (SP)** is the formal document prepared by the program that provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements.

## 10.0 References to Law, Policy, Instructions or Guidance.

a. AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT), 6 February 2020

b. CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011, Directive Current as of 9 June 2015

c. CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014

d. CNSSI No. 1254, Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems, 31 August 2016

e. DoDI 5000.89, Test and Evaluation, 19 November 2020

f. DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers, 31 December 2020

g. DoDI 8500.01, Cybersecurity, 14 March 2014

h. DoDD 8570.01-M, Information Assurance Workforce Improvement, 10 November 2015

i. AFI 17-1301, Department of the Air Force Guidance Memorandum to AFMAN 17-1301, Computer Security, 6 July 2021

j. AFMAN 17-1303, Air Force Cybersecurity Workforce Improvement Program, 12 May 2020

k. DoDD 5205.07, Special Access Programs Policy, 4 February 2020

l. DoDM 5205.07 - Vol. 1, DoD Special Access Programs Security Manual, 30 September 2020

m. AFI 16-701, Management, Administration, and Oversight of Special Access Programs, 18 February 2014

n. AFI 16-1404, Information Protection, 29 July 2019

o. DoDI 8510.01, Risk Management Framework for DoD IT, 12 March 2014 with Change 2, 28 July 2017, Incorporating Change 3, December 29, 2020

p. DoD Cybersecurity Test and Evaluation Guidebook, 25 April 2018, Version 2.0, Change 1, 10 February 2020

q. Director, OT&E Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, April 03, 2018

r. FISMA, Federal Information Systems Management Act Title III of Public Law 107-347 Sec 301-305, 17 December 2002

s. JSIG Department of Defense Joint Special Access Program (SAP) Implementation Guide, 11 April 2016, and 5 October 2018 Errata Sheet for the JSIG

t. NIST SP 800-53 (see note) Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 Revision 5, September 2020

u. NIST SP 800-30, Guide for Conducting Risk Assessments, Revision 1, 17 September 2012

v. NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Vol 1, November 2016, Includes Updates as of 03-21-2018: Page XIII 21 March 2018, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, Vol 2, 27 November 2019

w. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 2, December 2018 Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37 Revision 2, Dec 2018

x. NIST SP 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, March 2011

y. SAF/AQ, Cybersecurity Security Classification / Declassification Guide for Air Force Weapon Systems, 17 April 2017

z. AFLCMC/EZSP/EZSI IP SP AFLCMC Standard Process for Weapon System Program Protection Planning (PPP) & Systems Security Engineering (SSE), 19 April 2019 16 July 2020, VERSION 2.0 3.0

## 11.0 Acronym List

See Attachment 3.

# ATTACHMENT 1

Work Breakdown Structure (WBS) for Cybersecurity A&A

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | **Prepare** | Assign risk management roles. Identify system for assessment. | PM/SCA/AO | Organizational and system information | PM | Cybersecurity role assignments and system description (AAR, SSP) | PM |
| 1 | 1.0 | **Categorize** | Develop and approve IT Categorization and Selection Checklist | PM/SCA/AO | IT Categorization and Selection Checklist | PM | Signed IT Categorization and Selection Checklist | PM |
| 1 | 2.0 | **Select** | Select and document security controls | PM/SCA | AAR, System design artifacts, CONOPS, Program Protection Plan, CSS, specifications, Intel reports (if available), Domain Specific Security Control Overlays | PM | Draft Security Plan and Continuous Monitoring Strategy | PM |
| 1 | 3.0 | **Implement** | Implement and document security controls | PM | Security Plan, test results, and verification reports | PM | Updated Security Plan | PM |
| 1 | 4.0 | **Assess** | | | | | | |
| 2 | 4.1 | **Architecture Analysis** | | | | | | |
| 3 | 4.1.1 | **Submit Architecture Analysis artifacts** | Document the system's architecture, subsystems, authorization boundary, system baseline (hardware, software, and firmware), interfaces, | PM | Design artifacts, DoD Architecture Framework (DoDAF) views, Configuration Management documents, CONOPS, | PM | Architecture Analysis Report | SCA |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| | | | data types and flows, and threats | | system/subsystem criticality, system operating environments, classification, system users and access to the system, system components (hardware, software, firmware, networking, ports protocols, and services), data types and flows, system interfaces, and changes/modification from prior architecture analysis | | | |
| 3 | 4.1.2 | **Approve AAR (optional as required by SCA/AO)** | Review the system architecture | SCA/ AO | Architecture Analysis Report | SCA | Approved Architecture Analysis Report | PM |
| 3 | 4.1.3 | **Conduct Cyber threat/mission analysis (optional as required by SCA/AO)** | Review threat/vulnerability/mission analysis data for the purposes of discovering cyber threats, vulnerabilities, risks, and mitigations | PM | Threat information, vulnerability information, system architecture documents, mission description/information | PM | Threat/vulnerability/mission analysis data results (SAR - vulnerabilities, RAR - threats) | SCA/AO |
| 2 | 4.2 | **Security Control Assessment Preparation** | Develop, review, and approve a plan to assess the security controls | PM/SCA | AAR, program documentation, Overlay(s), Security Plan | PM | Approved Security Assessment Plan, Security Requirements Traceability Matrix (SRTM) | SCA/AO |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| 2 | 4.3 | **Security Control Assessment** | Assess the security controls in accordance with the assessment procedures defined in the security assessment plan | PM/SCA | Security Assessment Plan, Security Plan, Test Results/Reports, and supporting artifacts | PM/SCA | Security Assessment Results and Draft Security Assessment Report | SCA |
| 2 | 4.4 | **Document Security Control Assessment Results** | Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment | PM/SCA | Security Assessment Plan, Security Plan, Test Results/Reports, Security Assessment Report (draft) | PM | Updated Security Plan, updated draft Continuous Monitoring Strategy and Security Assessment Report | PM/ AO |
| 2 | 4.5 | **Initial Remediation Actions** | Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report, reassess remediated control(s), as appropriate, and document results | PM | Findings and recommendations from Approved Security Assessment Report, Test Results/Reports | PM/SCA | Updated Security Assessment Report (as required by AO) and initial POA&M | PM/AO/SCA |
| 2 | 4.6 | **Risk Assessment Preparation** | | | | | | |
| 3 | 4.6.1 | **Identify Purpose** | Identify purpose for risk assessment (initial authorization, re-authorization, in response to incident or system change) | PM/SCA/AO | Security Assessment Report, existing authorization documentation, Incident Reports, system change documentation | PM | Purpose of Risk Assessment (reauthorization, initial, response to incident, etc.) | PM |
| 3 | 4.6.2 | **Identify Scope** | Identify the scope of the risk assessment in terms of organizational applicability, time frame | PM/SCA | Security Assessment Report, existing authorization | SCA | Scope of the Risk Assessment | PM |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| | | | supported, and architectural/technology considerations | | documentation, applicable AFIs. | | | |
| 3 | 4.6.3 | **Assumptions and Constraints** | Identify the specific assumptions and constraints under which the risk assessment is conducted | PM/SCA | Documented assumptions for: Threat Sources, Threat Events, Vulnerabilities and Predisposing Conditions, Likelihood, Impacts, Risk Tolerance and Uncertainty, Analytic Approach | PM | Documented Assumptions | SCA |
| 3 | 4.6.4 | **Information Sources** | Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment | PM/SCA | AAR, Threat and vulnerability information | PM | Documented list of information sources used in risk assessment | SCA |
| 3 | 4.6.5 | **Risk Model and Analytic Approach** | Identify the risk model and analytic approach to be used in the risk assessment | PM/SCA | AO specific guidance | SCA | Documented Risk Model and Analytic Approach | PM |
| 2 | 4.7 | **Conduct Risk Assessment** | | | | | | |
| 3 | 4.7.1 | **Identify Threat Sources & Events** | Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.<br>Identify potential threat events, relevance of the | SCA | Intel data, AAR, Test report(s), Threat and mission data analysis results, Adversary Cyber Threat Assessment (ACTA), Validated On-Line Lifecycle Threat (VOLT), other intel products | SCA (with PM, Intel, and Office of Special Investigations (OSI) support as required by AO) | Threats Identified in draft Risk Assessment Report | SCA |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| | | | events, and the threat sources that could initiate the events. | | | | | |
| 3 | 4.7.2 | **Identify Vulnerabilities and pre-disposing conditions** | Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts | SCA | AAR, SAR, Test report(s), Threat and mission data analysis results, VOLT, other intel products | SCA (with PM support as required by AO) | Vulnerabilities identified against threat events identified in draft Risk Assessment Report | SCA |
| 3 | 4.7.3 | **Determine Likelihood of Occurrence** | Determine the likelihood that threat events of concern result in adverse impacts, considering the characteristics of the threat sources means and opportunities to initiate the events | SCA | AAR, SAR, Test report(s), Threat and mission data analysis results, VOLT, other intel products | SCA (with PM support as required by AO) | Likelihood of occurrence for threat events identified in draft Risk Assessment Report | SCA |
| 3 | 4.7.4 | **Determine Impact** | Determine the magnitude of impact based on severity and criticality criteria | SCA | Criticality analysis, mission severity analysis | SCA (with PM support as required by AO) | Magnitude of impact for threat events identified in draft Risk Assessment Report | SCA |
| 3 | 4.7.5 | **Determine Risk** | Create a risk statement and quantify the risk to the system/mission from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring | SCA | Likelihood of occurrence and magnitude of impact for threat events identified in draft Risk Assessment Report | SCA (with PM support as required by AO) | Risk Assessment Report | SCA |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| 3 | 4.7.6 | **Determine DATO need** | If risk is determined to be unacceptable when compared to the mission assurance requirement, then the AO, in collaboration with all system stakeholders (e.g. SAF/CIO A6, CISO, MAJCOM, Program Manager), will issue the authorization decision in the form of a DATO. | SCA | Risk Assessment Report | SCA | DATO Recommendation | PM/AO |
| 2 | 4.8 | **Communicate Risk Assessment Results** | Communicate risk assessment results to organizational decision makers to support risk responses and share results | PM/SCA | Risk Assessment Report | PM | Risk Assessment Report Summary | MAJCOM/SCA/AO |
| 1 | 5.0 | **System Authorization** | | | | | | |
| 2 | 5.1 | **Prepare POA&M** | Develop and select mitigation options based on the threat and vulnerability, limit the vulnerability, or stop the threat in turn reducing the likelihood or impact | PM/SCA | Program artifacts, Tech Orders and design documents | PM | POA&M | AO |
| 3 | 5.1.1 | **Justification to accept risk(s)** | Justify risk acceptance. If risk remains high or very high - the risk must be coordinated with MAJCOM, the SAE, and accepted by SAF/CIO A6 | PM/SCA | Risk Assessment Results | PM | POA&M update | AO/MAJCOM, SAE, and SAF/CIO A6 |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
| 2 | 5.2 | **Assemble the Authorization Package** | The security authorization package contains: (i) the security plan; (ii) the security assessment and risk assessment reports; and (iii) the POA&M | PM/SCA | Security Plan, RAR, SAR, POA&M, AAR, Continuous Monitoring Plan, draft Authorization Decision, and other relevant artifacts per AO. | PM | Authorization Package | SCA/AO |
| 3 | 5.2.1 | **SCA Risk Recommendation** | SCA documents recommendations based on risks and mitigations; operating conditions will be developed to limit exposure to risks | SCA | Authorization Package | SCA | Coordinated Authorization Package | AO |
| 3 | 5.2.2 | **Program Coordination** | PM coordinate the authorization package with the system stakeholders (as required by AO) | PM | Authorization Package | PM | Coordinated Authorization Package | AO |
| 2 | 5.3 | **Risk Authorization Decision** | The AO renders an authorization decision. If high/very high then the SAF/CIO A6 accepts the risk | AO or SAF/CIO A6 | Coordinated Authorization Package | AO or SAF/CIO A6 | Signed Authorization and Security Plan | SCA |
| 3 | 5.3.1 | **Implement Authorization** | SCA/SCAR provides signed authorization (e.g., IATT, ATO, DATO) to the PM. Program distributes the authorization and conditions to the users and testers. | SCA | Signed Authorization | SCA | Signed Authorization and Security Plan | PM |
| 1 | 6.0 | **Monitor Security Controls** | PM ensures all system changes are reviewed for cybersecurity impact prior to implementation. The PM must report any Security Incident to the | PM/SCA/ AO | Reauthorizations, change requests, incidents, system level Continuous Monitoring Plan, etc. | PM | Authorizations, updated RAR, etc. (depends on the results of the monitoring) | PM |

| WBS Level | WBS | Activity | Description | OPR | Input | Supplier | Output | Customer |
|---|---|---|---|---|---|---|---|---|
|  |  |  | SCA/SCAR.  The PM must maintain the system authorization.  The PM must initiate an updated risk assessment and authorization prior to the expiration of the current authorization. |  |  |  |  |  |

## ATTACHMENT 2

## Cybersecurity Risk Assessment and Management

**1.0 Purpose.** Cybersecurity risk assessment is the part of risk management that incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Cybersecurity risk is a function of the likelihood of a given threat exploiting a potential vulnerability and the resulting impact. There are three components of cybersecurity risk:

- A future root cause (manifested by a specific threat and vulnerability), which, if eliminated or corrected, would prevent a potential event from occurring
- A likelihood assessed at the present time of that future root cause occurring
- The impact of that future occurrence

A threat is any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. A vulnerability is a weakness in a system, system security procedures, internal controls, or implementation that could be exploited by a threat source. A threat does not present a risk to a system when there is no vulnerability that can be exploited and conversely, vulnerability does not present a risk if there is no threat. There may be many threats associated with a single vulnerability and many vulnerabilities associated with a single threat.

In particular, this document provides a risk assessment methodology for planning, identifying, analyzing, handling, and monitoring cybersecurity risks which agree with the suggested five-step management process defined in the *Department of Defense Risk, Issue and Opportunity (RIO) Management Guide for Defense Acquisition Programs*, 9 January 2017. Specific tasks for Cybersecurity Risk Assessments are provided in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments.* NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Appendix E – Summary of RMF Tasks describes the tasks, responsibilities, and supporting roles required to apply the Risk Management Framework (RMF) to systems. Many of these tasks are relevant to this cybersecurity risk assessment methodology. NIST SP 800-39, *Managing Information Security Risk*, may also be consulted for guidance on an integrated program for managing information security risk to operations to complement an overall risk management program.

**2.0 Risk Planning (WBS 4.6). (Reference NIST SP 800-30 Tasks 1-1, 1-2, 1-3, 1-4, and 1-5).** Since the DoD RIO Guide does not attempt to address specialized risks, such as cybersecurity, programs should utilize this guidance to map cybersecurity risks into their overall risk management processes.  The purpose, scope, assumptions, and constraints of the risk assessment should be identified.  For assessing cybersecurity risks, it is recommended that the program form a specialized cybersecurity risk assessment team.  The purpose of this team is to bring system stakeholders together to provide a forum for continually identifying and assessing cybersecurity risk throughout system design and operation.  This team will recommend solutions to the PM and should include all the necessary stakeholders, internal and external.  Each program can choose its own team members, but the team should include program engineering, system security engineering, information protection, program protection, intelligence representatives, using MAJCOM, test organizations, the SCA or SCAR, ISSM, and ISSO.

**3.0 Risk Identification (WBS 4.7).  (Reference NIST SP 800-30 Task 1-5)**.  The objective of risk identification is to produce a list of cybersecurity risks that can be prioritized by risk level and used to inform risk response decisions.  It includes the identification of cybersecurity threats against the system and the identification of cybersecurity vulnerabilities within the system.

**3.1 Threat Identification (WBS 4.7.1).  (Reference NIST SP 800-30 Tasks 2-1 and 2-2).**  The cybersecurity threats to the system and its operational environment must be understood.  Threats can be categorized as internal or external.  Internal threats are the result of individuals with malicious intent or just erroneous actions in operating the system.  External threats are the result of outside sources trying to disrupt DoD operations.  The external threat is generally an orchestrated attempt by a foreign government.  Threat sources may also be adversarial or non-adversarial.  The result of this action should be clear and concise threat statements that capture circumstances or events with the potential to intentionally or unintentionally cause an incident affecting the availability, integrity, and confidentiality of a system.  This may be achieved by attack path analysis modeling, review of threat assessments, and review of intelligence reports.

**3.2 Vulnerability Identification and Analysis (WBS 4.7.2).  (Reference NIST SP 800-30 Task 2-3; NIST SP 800-37 Task A-3).**  A cybersecurity vulnerability refers to the inability of the system to withstand the effects of a hostile environment open to attack or damage.  A flaw or weakness exists in the system that an attacker can access and exploit.  Non-compliant security controls may be used as a basis to identify system vulnerabilities as well as results from cybersecurity penetration testing, attack path analysis, and any cybersecurity relevant results from the Test & Evaluation Community.

The system should be assessed against each requirement or control to determine its level of compliance.  If non-compliant, this security weakness should be further evaluated to determine if it represents a system vulnerability.  If a threat statement cannot be linked to at least one vulnerability, a root cause does not exist, and the threat should be removed from further consideration.  Similarly, if a threat-vulnerability relationship cannot be established for each non-compliant requirement, then the non-compliant requirement does not pose a risk to the system and should be removed from further evaluation.

The results of these actions are clear and concise vulnerability statements describing a flaw or weakness in design or implementation, including security procedures and controls, and the linkage of each vulnerability to at least one threat.

**3.3 Write Risk Statements (WBS 4.7.5).** Capturing a statement of risk involves considering and recording the conditions that are causing concern for a potential loss to the system. Risk statements must be neutral, clear, quantifiable statements. The objective of capturing a statement of risk is to arrive at a concise description of risk, which can be understood and acted upon. The components and description of a statement of risk are:

- Potential Event: a single phrase or sentence that briefly describes the key circumstances, situations, etc., causing concern, doubt, anxiety, or uncertainty
- Consequence: a single phrase or sentence that describes the key, possible negative outcome(s) of the current conditions

Risk statements must be linked to specific threats and vulnerabilities and documented in the Risk Assessment Report (RAR). The combination of a specific threat and vulnerability may result in one or many risk statements. The result of this action will be a number of unique risk statements, each specifically mapped to a threat and vulnerability pairing. Risk statements should also be associated with their cybersecurity control/requirement identified in the Security Assessment Report (SAR). The combination of a threat and vulnerability often results in information that is classified, and the program's security classification guide should be consulted for correct classification of risk information. The SAF/AQ Cybersecurity Security Classification / Declassification Guide for Air Force Weapon Systems, dated 17 April 2017, should also be consulted for additional instructions to classify DAF Weapon Systems cybersecurity information.

As a result of the actions under *Risk Identification*, the Risk team should have generated a list of system specific threats, identified system vulnerabilities linked to specific threats, and developed corresponding risk statements that are documented in the RAR.

**4.0 Risk Analysis.** Risk analysis involves determining and assigning a likelihood of occurrence and impact to each of the identified risks from the risk identification activity. The following subsections provide an exemplary model for risk analysis. Other models may be approved by the AO.

**4.1 Calculate Likelihood (WBS 4.7.3). (Reference NIST SP 800-30 Task 2-4).** Assign a likelihood of occurrence based on a relative scale, taking into account an estimation of the means and opportunity of a potential adversary.

**4.1.1 Means.** Means represents an estimation of an adversary's capability in creating the conditions necessary for a risk occurrence, considering cost, time, and skill needed to execute a successful attack. Threat is very similar to adversary, but a threat is the specific source of harm, for example a known hacker, a specific employee, whereas the adversary is the collection or group of threat, for example a hacker collective or nation state. Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events. An attack is an action intended to compromise the confidentiality, integrity, and/or availability of a system. There are many types of attacks including intrusions, reconnaissance, tampering, implantation, denial of service, corruption of data, ex-filtration of data, etc. Each risk is assessed for Means and assigned a Means level according to the criteria in Table 1.

**Table 1. Means**

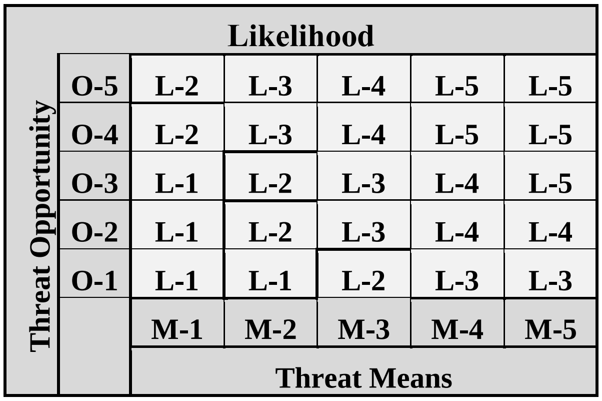
| Level | Description |
|---|---|
| M-5 | Threat has a very high capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is almost certain to succeed. |
| M-4 | Threat has a high capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is highly likely to succeed. |
| M-3 | Threat has a moderate capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is likely to succeed. |
| M-2 | Threat has a low capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is has a low likelihood to succeed. |
| M-1 | Threat has a very low capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it has a very low likelihood to succeed. |

**4.1.2 Opportunity.** Opportunity represents an estimation of an adversary’s likelihood to attack the system. A system’s attack surface is the set of methods and interfaces through which an adversary can enter the system and conduct an attack. Each risk is assessed an Opportunity level according to the criteria in Table 2.

**Table 2. Opportunity**

| Value | Description |
|---|---|
| O-5 | Adversary is almost certain to initiate the threat event. The threat event/actor or Tactic, Technique or Procedure (TTP) has been seen by the system or mission area. |
| O-4 | Adversary is highly likely to initiate the threat event. The threat event/actor or TTP has been seen by the organization's peers. |
| O-3 | Adversary is somewhat likely to initiate the threat event. The threat event/actor or TTP has been reported by a trusted source. |
| O-2 | Adversary is unlikely to initiate the threat event. The threat event/actor or TTP has been predicted by a trusted source. |
| O-1 | Adversary is highly unlikely to initiate the threat event. The threat event/actor or TTP has been described by a somewhat credible source. |

**4.1.3 Likelihood.** With the aid of the Likelihood Matrix (Figure 1), individual means and opportunity levels are used to determine an overall Likelihood level for each risk.



| Threat Opportunity | | Likelihood | | | | |
|---|---|---|---|---|---|---|
| | O-5 | L-2 | L-3 | L-4 | L-5 | L-5 |
| | O-4 | L-2 | L-3 | L-4 | L-5 | L-5 |
| | O-3 | L-1 | L-2 | L-3 | L-4 | L-5 |
| | O-2 | L-1 | L-2 | L-3 | L-4 | L-4 |
| | O-1 | L-1 | L-1 | L-2 | L-3 | L-3 |
| | | M-1 | M-2 | M-3 | M-4 | M-5 |
| | | Threat Means | | | | |

**Figure 1. Likelihood Matrix**

**4.2 Calculate Impact (WBS 4.7.4). (Reference NIST SP 800-30 Task 2-5).** Assign an impact of occurrence based on a relative scale, taking into account an estimation of the criticality of the system and the severity of system damage.

**4.2.1 Criticality.** Criticality represents an estimation of adverse effects to the mission, organization, assets, individuals, or nation due to system/capability/information loss or compromise. Each risk is assessed for Criticality and assigned a Criticality level according to the criteria in Table 3.

**Table 3. Criticality**

| Level | Description |
|---|---|
| C-5 | Loss of the system/subsystem/function/capability results in Severe or total mission failure and/or compromise or loss of information results in exceptionally grave damage to national security. |
| C-4 | Loss of the system/subsystem/function/capability results in significant/unacceptable mission degradation and/or compromise or loss of information results in grave damage to national security. |
| C-3 | Loss of the system/subsystem/function/capability results in moderate or partial mission degradation and/or compromise or loss of information results in damage to national security. |
| C-2 | Loss of the system/subsystem/function/capability results in minor mission degradation and/or compromise or loss of information results in limited damage to national security. |
| C-1 | Loss of the system/subsystem/function/capability results in minimal mission degradation and/or compromise or loss of information results in negligible damage to national security. |

**4.2.2 Severity.** Severity represents an estimation of the damage to the system resulting from exploitation of a vulnerability by an adversary, stated in terms of loss of capability, disruptive system change or loss of information. Each risk is assessed for severity and assigned a *Vulnerability Severity* level according to the criteria in Table 4.

**Table 4. Severity**

| Level | Description |
|---|---|
| S-5 | The vulnerability is of severe/catastrophic concern. Vulnerability exploitation results in severe/catastrophic system performance impact, and/or severe compromise or modification of the system information. |
| S-4 | The vulnerability is of significant concern. Vulnerability exploitation causes significant unacceptable system capability impact and/or significant compromise or modification of the system/system information. |
| S-3 | The vulnerability is of moderate concern. Vulnerability exploitation causes partial system performance impact and/or partial compromise or modification of the system/system information. |
| S-2 | The vulnerability is of minor concern. Vulnerability exploitation causes minor system capability impact and/or minor compromise or modification of the system/system information. |
| S-1 | The vulnerability is of minimal concern. Vulnerability exploitation causes minimal system performance impact and/or no compromise or modification of the system/system information. |

**4.2.3 Impact.** With the aid of the Impact Risk Factor Matrix (Figure 2), individual Severity and Criticality levels are used to determine an overall Impact Risk Factor Level for each risk.

| Impact | | | | | | |
|---|---|---|---|---|---|---|
| Vulnerability Severity | S-5 | I-2 | I-3 | I-4 | I-5 | I-5 |
| | S-4 | I-2 | I-3 | I-3 | I-4 | I-5 |
| | S-3 | I-1 | I-2 | I-3 | I-4 | I-5 |
| | S-2 | I-1 | I-1 | I-2 | I-3 | I-4 |
| | S-1 | I-1 | I-1 | I-1 | I-2 | I-3 |
| | | C-1 | C-2 | C-3 | C-4 | C-5 |
| | | Mission Criticality | | | | |

**Figure 2. Impact Risk Factor Matrix**

**4.3 Determine Risk (WBS 4.7.5). (Reference NIST SP 800-30 Task 2-6).** The Likelihood and Impact levels are used to determine an Overall Risk Factor for each risk using the Overall Risk Factor Matrix (Figure 3).

| | | | | | | |
|---|---|---|---|---|---|---|
| Likelihood | L-5 | Very Low | Low | Moderate | High | Very High |
| | L-4 | Very Low | Low | Moderate | High | Very High |
| | L-3 | Very Low | Low | Moderate | Moderate | High |
| | L-2 | Very Low | Low | Low | Low | Moderate |
| | L-1 | Very Low | Very Low | Very Low | Low | Low |
| | | I-1 | I-2 | I-3 | I-4 | I-5 |
| Impact | | | | | | |

**Figure 3. Overall Risk Factor Matrix**

**4.4 Communicate Results (WBS 4.8). (Reference NIST SP 800-30 Tasks 3-1 and 3-2; NIST SP 800-37 Tasks R-2 and R-5).** The results of the risk analysis are captured in a RAR. The RAR should include the complete risk analysis results including specific justification of all risk assessment values and the analysis that led to their selection.

As a result of the actions under *Risk Analysis*, the risk team has completed a comprehensive risk analysis taking into account the Means and Opportunity of an adversary to attack the system as well as the Criticality and Severity of such an attack. An overall Risk Factor has been generated for each individual risk.

**5.0 Handling. (Reference NIST SP 800-37 Tasks A-6 and R-3).** Once risks have been identified and quantified, the question of what to do about the risk must be answered. This is accomplished by identifying, evaluating, and selecting management strategies to set risk at an acceptable level. Results are documented in the RAR and should include the specifics of what should be done, when it should be accomplished, and who is responsible, and required resources to implement. Risk management strategies that require future implementation should be documented in a Plan of Action and Milestones (POA&M). For each risk, one or more of the following management strategies may apply:

a. Avoiding risk by eliminating threat and/or the impact. This includes not performing an activity that could carry risk. This could be accomplished by modifying program requirements. This adjustment could be accommodated by change in funding, schedule, or technical requirements. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on an increased capability that accepting the risk may have allowed.

b. Controlling and/or reducing system vulnerability. This adjustment could be accommodated by any number of methods including changing the system's design, implementing additional procedures, or increasing user training. It is synonymous with the term risk mitigation (mitigation - the action of lessening in severity or intensity).

c. Transferring the Risk. Reassign organizational accountability, responsibility, and authority. The conditions of this transfer must be documented in the Security Plan.

d. Accepting the level of risk. Cybersecurity risk acceptance must be clearly documented in an Authorization Decision Memorandum before a system may commence testing or operations. The AO is the only authority able to accept risk, except for High and Very Risks, which are accepted by the SAF/CIO A6.

**6.0 Monitor (WBS 6.0). (Reference NIST SP 800-30 Tasks 4-1 and 4-2; NIST SP 800-37 Tasks M-1, M-2, M-3, M-4, M-5 and M-6).** The intent of risk monitoring is to ensure continued risk management throughout the system's operational life. The need to monitor and maintain risk assessment results over time overlaps with the continuous monitoring step in the RMF and should be documented in a continuous monitoring plan. The plan should cover change management, incident reporting, updated threat and/or vulnerability assessments, POA&M updates, and updated risk assessments supporting cybersecurity authorizations.

**7.0 Program Risk.** A method to map cybersecurity risks into a program's overall risk management process may be desirable. A key factor is to ensure that the correct risk level is presented when going from five levels of cybersecurity risk (Very High, High, Moderate, Low, and Very Low) to three levels of program risk (High, Moderate, and Low).

If cybersecurity risk levels Very Low and Low are equivalent to Low program risk, and High and Very High cybersecurity risk levels are equivalent to High program risk, then there are five potential risk cells that may be misrepresented when converting cybersecurity risk to program risk. These risk cells, numbered 1-5, require extra consideration when translating cybersecurity risk to program risk. Since each risk cell goes from a lower cybersecurity risk level to a higher program risk level, if translated directly, the resultant cybersecurity risks for the program may be overstated (Figure 4). Cybersecurity risk can impact program risk.

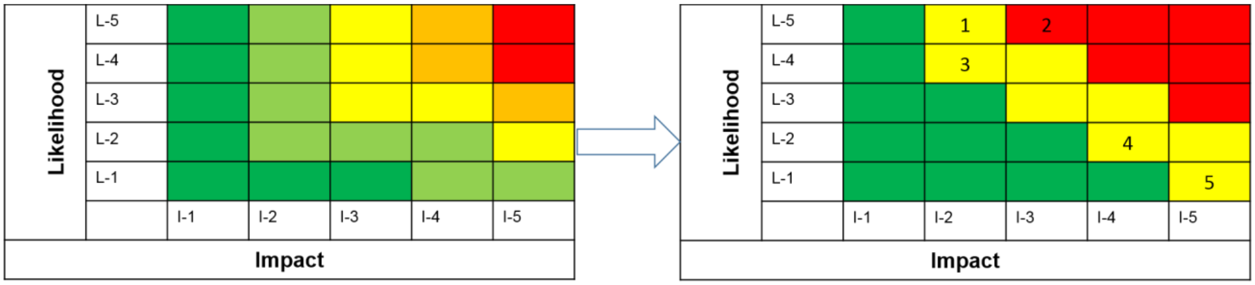


**Figure 4. Cybersecurity Risk translated to Program Risk**

# Attachment 3
# Acronym List

| | |
|---|---|
| AAR | Architecture Analysis Report |
| ACTA | Adversary Cyber Threat Assessment |
| AFI | Air Force Instruction |
| AIA | Acquisition Intelligence Analyst |
| A&A | Assessment and Authorization |
| AFLCMC | Air Force Life Cycle Management Center |
| AO | Authorizing Official |
| AODR | Authorizing Official Designated Representative |
| ATO | Authorization to Operate |
| C2 | Command and Control |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CJCSI | Chairman of the Joint Chiefs of Staff Instruction |
| CND | Computer Network Defense |
| CNSSI | Committee on National Security Systems Instruction |
| CONOPS | Concept of Operations |
| CSS | Cybersecurity Strategy |
| DAF | Department of the Air Force |
| DATO | Denial of Authorization to Operate |
| DISA | Defense Information Systems Agency |
| DoD | Department of Defense |
| DoDAF | DoD Architecture Framework |

| | |
|---|---|
| DoDI | Department of Defense Instruction |
| FISMA | Federal Information Systems Management Act |
| FY | Fiscal Year |
| IA | Information Assurance |
| IATT | Interim Authorization to Test |
| IS | Information Systems |
| ISO | Information System Owner |
| ISSE | Information System Security Engineering |
| ISSM | Information System Security Manager |
| ISSO | Information Systems Security Officer |
| IT | Information Technology |
| JSIG | Joint Special Access Program (SAP) Implementation Guide |
| MAJCOM | Major Command |
| NIPRNet | Non-Classified Internet Protocol Router Network |
| NIST | National Institute of Standards and Technology |
| OSI | Office of Special Investigations |
| OT&E | Operational Test and Evaluation |
| PIT | Platform Information Technology |
| PM | Program Manager |
| POA&M | Plan of Action & Milestones |
| POC | Point of Contact |
| PPP | Program Protection Plan |
| RAR | Risk Assessment Report |
| RCA | Rapid Cyber Acquisition |
| RIO | Risk, Issue and Opportunity |

| | |
|---|---|
| RFP | Request for Proposal |
| RMF | Risk Management Framework |
| SAE | Service Acquisition Executive |
| SAP | Security Assessment Plan |
| SAP | Special Access Program |
| SAR | Security Assessment Report |
| SCA | Security Control Assessor |
| SCAR | Security Control Assessor Representative |
| SIPOC | Suppliers, Inputs, Process, Outputs, Customers |
| SP | Standard Process |
| SP | Security Plan |
| SRTM | Security Requirements Traceability Matrix |
| SSE | System Security Engineering |
| STEPP | Security Training, Education, and Professionalization Portal |
| S&P | Standards and Process |
| VOLT | Validated On-Line Lifecycle Threat |
| WBS | Work Breakdown Structure |