

DoD/VA Authority To Operate Reciprocity



ProPath

Office of Information and Technology

Table of Contents

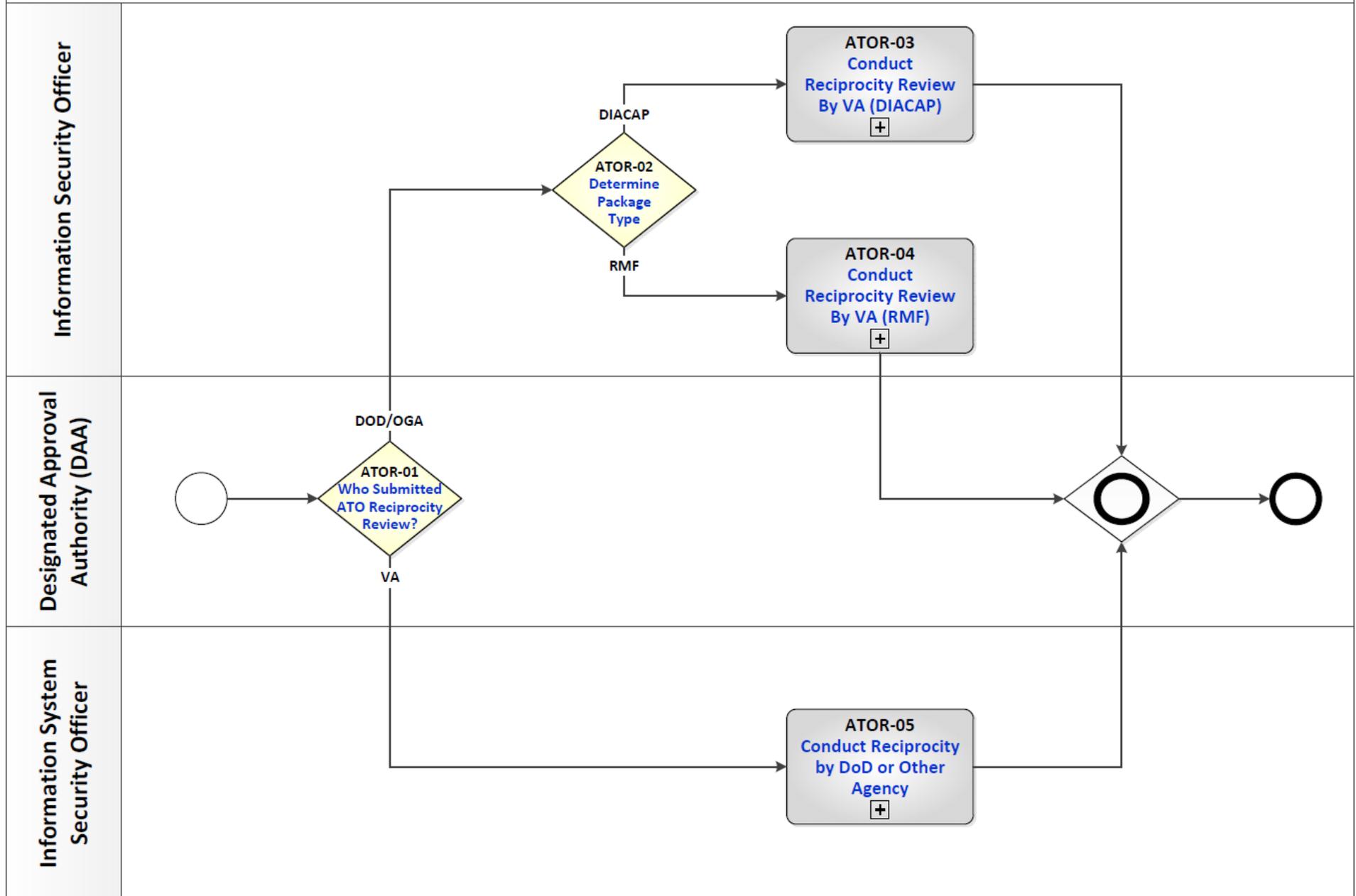
DoD/VA Authority To Operate Reciprocity Process Maps	1
Process: Authority To Operate Reciprocity	5
Authority To Operate Reciprocity Description and Goals.....	6
Description	6
Goals	6
Authority To Operate Reciprocity RACI Information	7
Authority To Operate Reciprocity Associated Artifacts Information	14
Authority To Operate Reciprocity Tools and Web Sites Information	14
Authority To Operate Reciprocity Standards Information	14
Authority To Operate Reciprocity Process.....	15
Process Activity Name: ATOR-01 Who Submitted ATO Reciprocity Review?	15
Process Activity Name: ATOR-02 Determine Package Type.....	15
Process Activity Name: ATOR-03 Conduct Reciprocity Review by VA	
(DIACAP).....	16
Process Activity Name: ATOR-03.01 Deliver DIACAP Package (ATO) to VA	
ISO.....	17
Process Activity Name: ATOR-03.02 Upload DIACAP Package.....	18
Process Activity Name: ATOR-03.03 Notify VA Certification Program Office of	
ATO Package.....	19
Process Activity Name: ATOR-03.04 Additional Information Needed?	20
Process Activity Name: ATOR-03.05 Submit Information Request to VA ISO	
.....	21
Process Activity Name: ATOR-03.06 Communicate ATO Reciprocity Decision	
to DoD ISSO.....	22
Process Activity Name: ATOR-03.07 Provide Required Additional Information	
.....	23
Process Activity Name: ATOR-03.08 Inform ISO of Review Results	23
Process Activity Name: ATOR-03.09 Communicate ATO Reciprocity Decision	
to DoD ISSO.....	24
Process Activity Name: ATOR-04 Conduction Reciprocity by VA (RMF)	25
Process Activity Name: ATOR-04.01 Deliver RMF Package (ATO) to VA ISO	
Process Activity Name: ATOR-04.02 Upload RMF Package.....	27
Process Activity Name: ATOR-04.03 Notify VA Certification Program Office of	
ATO Package.....	28
Process Activity Name: ATOR-04.04 Additional Information Needed?	29
Process Activity Name: ATOR-04.05 Submit Information Request to VA ISO	
.....	30

Process Activity Name: ATOR-04.06 Communicate ATO Reciprocity Decision to DoD ISSO.....	31
Process Activity Name: ATOR-04.07 Provide Required Additional Information	31
Process Activity Name: ATOR-04.08 Inform ISO of Review Results	32
Process Activity Name: ATOR-04.09 Communicate ATO Reciprocity Decision to Agency ISSO	33
Process Activity Name: ATOR-05 Conduct Reciprocity by DoD or Other Agency	34
Process Activity Name: ATOR-05.01 Submit ATO Package for Reciprocity Review.....	35
Process Activity Name: ATOR-05.02 Register System and Import ATO Package	36
Process Activity Name: ATOR-05.03 Review and Prepare RMF Package for Workflow.....	37
Process Activity Name: ATOR-05.04 Notify DoD SCA of RMF Package in eMASS.....	38
Process Activity Name: ATOR-05.05 Review Package and Provide Assessment.....	39
Process Activity Name: ATOR-05.06 Review SCA's Assessment	40
Process Activity Name: ATOR-05.07 Issues?.....	41
Process Activity Name: ATOR-05.08 Resolve Issues	42
Process Activity Name: ATOR-05.09 Provide Recommendation to Authorizing Official	43

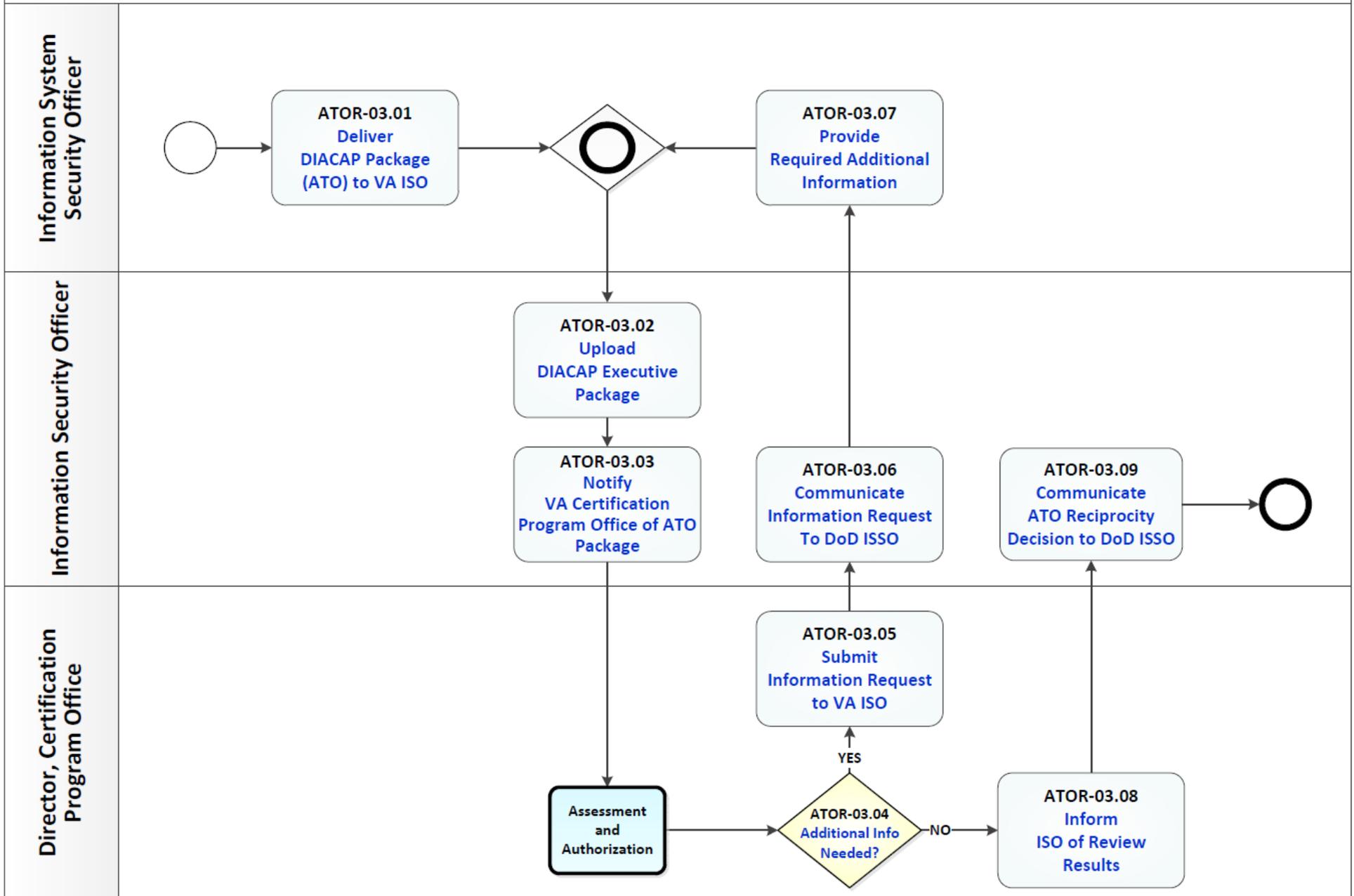
DoD/VA Authority To Operate Reciprocity Process Maps

Authority To Operate Reciprocity (ATOR)

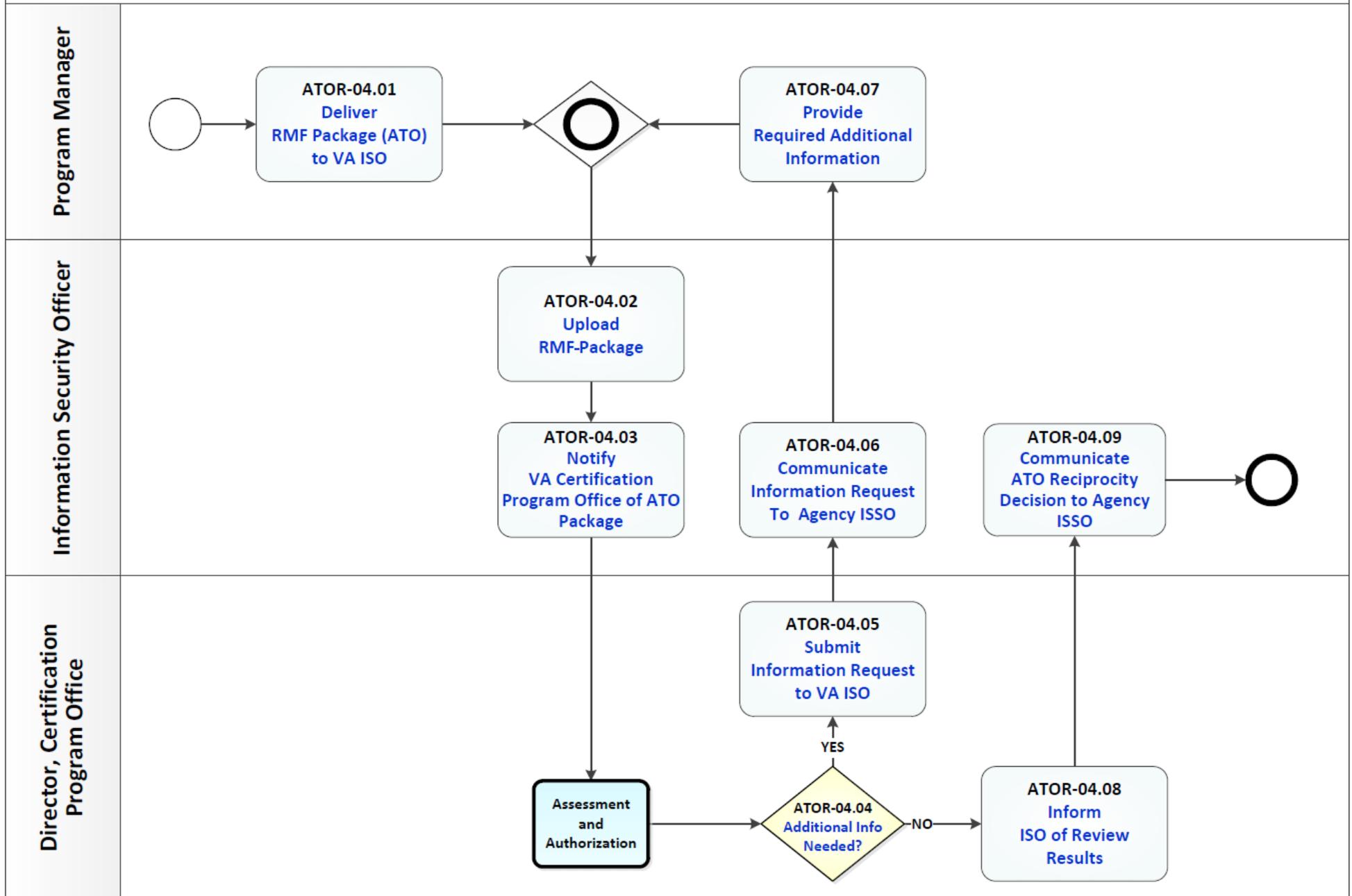
[Home](#) [Overview](#) [RACI](#) [Help](#)



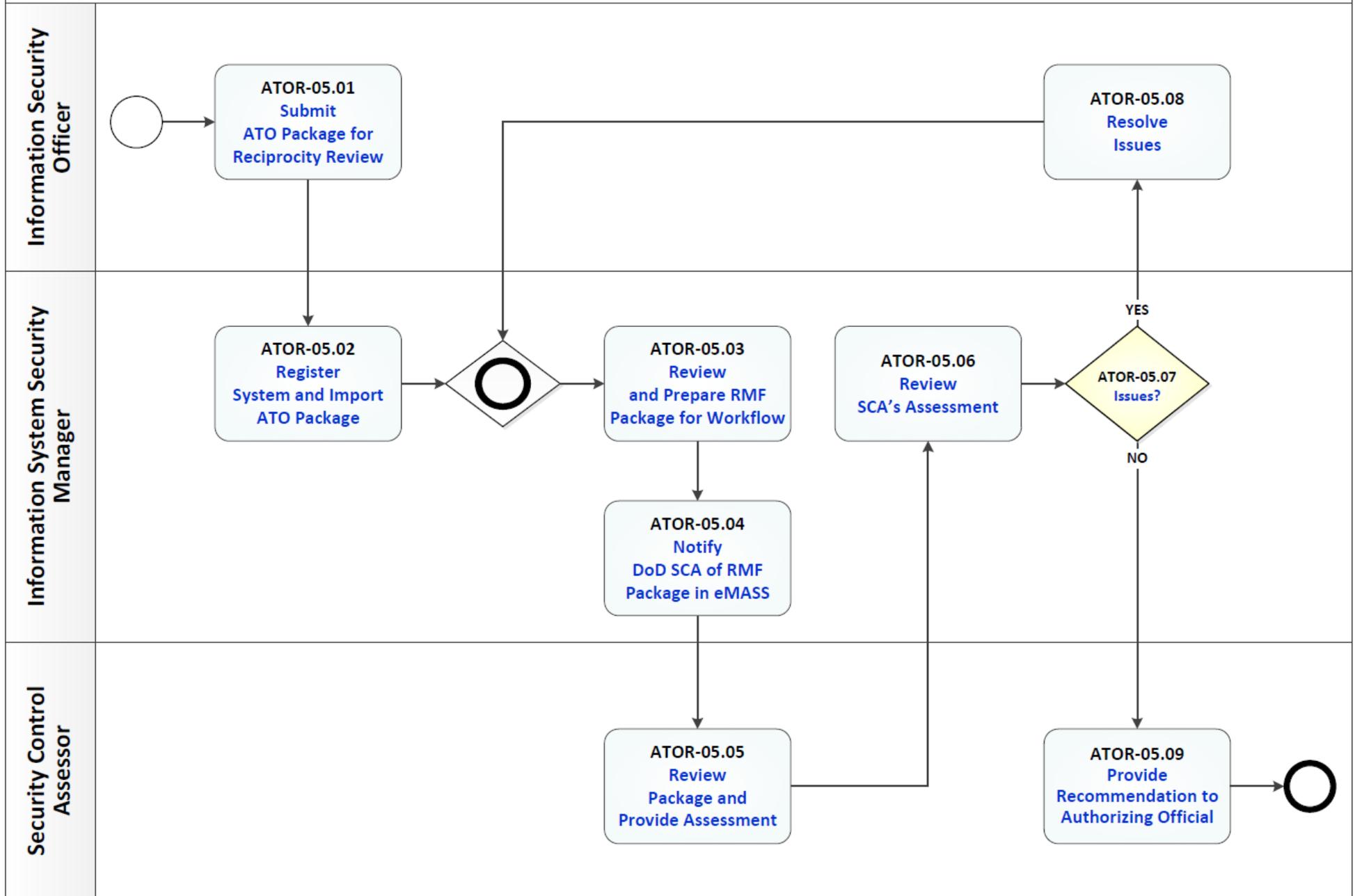
Authority To Operate Reciprocity: ATOR-03 Conduct Reciprocity by VA (DIACAP)



Authority To Operate Reciprocity: ATOR-04 Conduct Reciprocity by VA (RMF)



Authority To Operate Reciprocity: ATOR-05 Conduct Reciprocity by DoD or Other Agency



Process: Authority To Operate Reciprocity

Overview: The process map for Authority To Operate Reciprocity cycles through the following process and review activities:

- ATOR-01 Who Submitted ATO Reciprocity Review?
- ATOR-02 Determine Package Type
- ATOR-03 Conduct Reciprocity Review by VA (DIACAP)
 - ATOR-03.01 Deliver DIACAP Package (ATO) to VA ISO
 - ATOR-03.02 Upload DIACAP Package
 - ATOR-03.03 Notify VA Certification Program Office of ATO Package
 - ATOR-03.04 Additional Information Needed?
 - ATOR-03.05 Submit Information Request to VA ISO
 - ATOR-03.06 Communicate ATO Reciprocity Decision to DoD ISSO
 - ATOR-03.07 Provide Required Additional Information
 - ATOR-03.08 Inform ISO of Review Results
 - ATOR-03.09 Communicate ATO Reciprocity Decision to DoD ISSO
- ATOR-04 Conduction Reciprocity by VA (RMF)
 - ATOR-04.01 Deliver RMF Package (ATO) to VA ISO
 - ATOR-04.02 Upload RMF Package
 - ATOR-04.03 Notify VA Certification Program Office of ATO Package
 - ATOR-04.04 Additional Information Needed?
 - ATOR-04.05 Submit Information Request to VA ISO
 - ATOR-04.06 Communicate ATO Reciprocity Decision to DoD ISSO
 - ATOR-04.07 Provide Required Additional Information
 - ATOR-04.08 Inform ISO of Review Results
 - ATOR-04.09 Communicate ATO Reciprocity Decision to Agency ISSO
- ATOR-05 Conduct Reciprocity by DoD or Other Agency
 - ATOR-05.01 Submit ATO Package for Reciprocity Review
 - ATOR-05.02 Register System and Import ATO Package
 - ATOR-05.03 Review and Prepare RMF Package for Workflow
 - ATOR-05.04 Notify DoD SCA of RMF Package in eMASS
 - ATOR-05.05 Review Package and Provide Assessment
 - ATOR-05.06 Review SCA's Assessment
 - ATOR-05.07 Issues?
 - ATOR-05.08 Resolve Issues
 - ATOR-05.09 Provide Recommendation to Authorizing Official

Authority To Operate Reciprocity Description and Goals

Description

The Authority to Operate (ATO) Reciprocity Process defines a set of common repeatable procedures that assures the necessary due care has been performed and controls are implemented commensurate with information security and privacy risks. The ATO Reciprocity process adjudicates ATO packages submitted by the Department of Defense (DoD) or Other Governmental Agencies (OGA) to VA, or for ATO packages submitted by VA to DoD/OGA for review and adjudication.

Goals

The overall goal of this process is to establish a common framework to facilitate reciprocity of ATOs for system interactions between VA and DoD or Other Governmental Agencies (OGA) in a timely manner. Specific objectives of this process are:

- To establish a common process framework for reciprocity of ATOs between DoD/OGA and VA based on the Federal Information Security Management Act of 2002 (FISMA);
- To verify the necessary due care has been performed based on the established security authorization process from respective agencies; and
- To achieve the necessary level of trust between DoD/OGA and VA by verifying the necessary information security and privacy controls have been implemented.

Authority To Operate Reciprocity RACI Information

The following describes the RACI information for this process:

ATOR-01 Who Submitted ATO Reciprocity Review?

Responsible Role: Designated Approval Authority

Accountable Role: None Listed

Consulted Role: None Listed

Informed Role: None Listed

ATOR-02 Determine Package Type

Responsible Role: Designated Approval Authority

Accountable Role: None Listed

Consulted Role: None Listed

Informed Role: None Listed

ATOR-03.01 Deliver DIACAP Package (ATO) to VA ISO

Responsible Role: Information System Security Officer

Accountable Role: Information System Security Manager

Consulted Role: None Listed

Informed Role: Information Security Officer

ATOR-03.02 Upload DIACAP Package

Responsible Role: Information Security Officer

Accountable Role: Certification Agent

Consulted Role: None Listed

Informed Role: Director, Certification Program Office

ATOR-03.03 Notify VA Certification Program Office of ATO Package

Responsible Role: Information Security Officer

Accountable Role: Certification Agent
Consulted Role: None Listed
Informed Role: Director, Certification Program Office

ATOR-03.04 Additional Information Needed?

Responsible Role: Director, Certification Program Office
Accountable Role: None Listed
Consulted Role: None Listed
Informed Role: None Listed

ATOR-03.05 Submit Information Request to VA ISO

Responsible Role: Director, Certification Program Office
Accountable Role: Director, Office of Cyber Security
Consulted Role: None Listed
Informed Role: Information Assurance Manager

ATOR-03.06 Communicate ATO Reciprocity Decision to DoD ISSO

Responsible Role: Information Security Officer
Accountable Role: Certification Agent
Consulted Role: None Listed
Informed Role: Information Assurance Manager; Director, Certification Program Office

ATOR-03.07 Provide Required Additional Information

Responsible Role: Information System Security Officer
Accountable Role: Certification Agent
Consulted Role: None Listed
Informed Role: Director, Certification Program Office

ATOR-03.08 Inform ISO of Review Results

Responsible Role: Director, Certification Program Office

Accountable Role: Director, Office of Cyber Security

Consulted Role: None Listed

Informed Role: Information Security Officer

ATOR-03.09 Communicate ATO Reciprocity Decision to DoD ISSO

Responsible Role: Information Security Officer

Accountable Role: Certification Agent

Consulted Role: None Listed

Informed Role: Director, Certification Program Office

ATOR-04.01 Deliver RMF Package (ATO) to VA ISO

Responsible Role: Program Manager

Accountable Role: Program Manager

Consulted Role: None Listed

Informed Role: None Listed

ATOR-04.02 Upload RMF Package

Responsible Role: Information Security Officer

Accountable Role: Certification Agent

Consulted Role: None Listed

Informed Role: None Listed

ATOR-04.03 Notify VA Certification Program Office of ATO Package

Responsible Role: Information Security Officer

Accountable Role: Certification Agent

Consulted Role: None Listed

Informed Role: Information System Security Officer

ATOR-04.04 Additional Information Needed?

Responsible Role: Director, Certification Program Office

Accountable Role: None Listed

Consulted Role: None Listed

Informed Role: None Listed

ATOR-04.05 Submit Information Request to VA ISO

Responsible Role: Director, Certification Program Office

Accountable Role: Director, Office of Cyber Security

Consulted Role: None Listed

Informed Role: None Listed

ATOR-04.06 Communicate ATO Reciprocity Decision to DoD ISSO

Responsible Role: Information Security Officer

Accountable Role: Certification Agent

Consulted Role: None Listed

Informed Role: None Listed

ATOR-04.07 Provide Required Additional Information

Responsible Role: Program Manager

Accountable Role: Program Manager

Consulted Role: None Listed

Informed Role: None Listed

ATOR-04.08 Inform ISO of Review Results

Responsible Role: Director, Certification Program Office

Accountable Role: Director, Office of Cyber Security

Consulted Role: None Listed

Informed Role: Information Security Officer

ATOR-04.09 Communicate ATO Reciprocity Decision to Agency ISSO

Responsible Role: Information Security Officer

Accountable Role: Certification Agent

Consulted Role: None Listed

Informed Role: Information System Security Officer

ATOR-05.01 Submit ATO Package for Reciprocity Review

Responsible Role: Program Manager

Accountable Role: Program Manager

Consulted Role: None Listed

Informed Role: None Listed

ATOR-05.02 Register System and Import ATO Package

Responsible Role: Information System Security Manager

Accountable Role: Information System Security Manager

Consulted Role: None Listed

Informed Role: Information Security Officer; Director, Certification Authority Office

ATOR-05.03 Review and Prepare RMF Package for Workflow

Responsible Role: Information System Security Manager

Accountable Role: Information System Security Manager

Consulted Role: None Listed

Informed Role: Authorizing Official; Information System Security Officer

ATOR-05.04 Notify DoD SCA of RMF Package in eMASS

Responsible Role: Information System Security Manager

Accountable Role: Information System Security Manager

Consulted Role: None Listed

Informed Role: Information System Security Manager; Security Control Assessor

ATOR-05.05 Review Package and Provide Assessment

Responsible Role: Director, Security Control Assessor

Accountable Role: Director, Security Control Assessor

Consulted Role: None Listed

Informed Role: None Listed

ATOR-05.06 Review SCA's Assessment

Responsible Role: Information System Security Manager

Accountable Role: Information System Security Manager

Consulted Role: None Listed

Informed Role: None Listed

ATOR-05.07 Issues?

Responsible Role: Information System Security Manager

Accountable Role: None Listed

Consulted Role: None Listed

Informed Role: None Listed

ATOR-05.08 Resolve Issues

Responsible Role: Information Security Officer

Accountable Role: Program Manager

Consulted Role: None Listed

Informed Role: None Listed

ATOR-05.09 Provide Recommendation to Authorizing Official

Responsible Role: Security Control Assessor

Accountable Role: Security Control Assessor

Consulted Role: None Listed

Informed Role: None Listed

Authority To Operate Reciprocity Associated Artifacts Information

There are no artifacts associated with this process.

Authority To Operate Reciprocity Tools and Web Sites Information

The Tools and Web Sites associated with this process (including hyperlinks) include:

Agilience RiskVision National Release GRC Instance

Enterprise Mission Assurance Support Service (eMASS)

Interagency ATO Crosswalk Checklist

TRICARE Management Activity (TMA) Large Attachment File System

Veterans Affairs Intranet Quorum (VAIQ)

Authority To Operate Reciprocity Standards Information

Standards associated with this process (including hyperlinks) include:

DoDI 8500.01, Cybersecurity

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems

NIST Special Publication 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

Authority To Operate Reciprocity Process

Process Activity Name: ATOR-01 Who Submitted ATO Reciprocity Review?

Previous Activities

Process Begins

Next Activities

If "DOD/OGA":

ATOR-02 Determine Package Type

Or

If "VA":

ATOR-05 Conduct Reciprocity by DoD or Other Agency

Description

The Designated Approval Authority determines who has submitted the ATO reciprocity package to review. If submitted by Department of Defense (DoD) or any Other Governmental Agency (OGA) then the next step is to determine if the package is a Risk Management Framework or DoD Information Assurance Certification and Accreditation Process (DIACAP) Package for Authority to Operate (ATO), the package is routed accordingly. Otherwise, the package is submitted to the Department of Veterans Affairs for review and adjudication.

Responsible Role

Designated Approval Authority

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: ATOR-02 Determine Package Type

Previous Activities

ATOR-01 Who Submitted ATO Reciprocity Review?

Next Activities

If "DIACAP":

ATOR-03 Conduct Reciprocity Review by VA (DIACAP)

Or

If "RMF":

ATOR-04 Conduction Reciprocity by VA (RMF)

Description

The Designated Approval Authority determines the type of package being submitted and to which agency it needs to be submitted.

Responsible Role

Designated Approval Authority

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: ATOR-03 Conduct Reciprocity Review by VA (DIACAP)

Previous Activities

ATOR-02 Determine Package Type

Next Activities

ATOR-03.01 Deliver DIACAP Package (ATO) to VA ISO

Description

The sub-process Conduct Reciprocity Review by VA (DIACAP), addresses how a DIACAP ATO package is submitted to VA for adjudication:

- Deliver DIACAP Package (ATO) to VA ISO
- Upload DIACAP Package
- Notify VA Certification Program Office of ATO Package
- Additional Information Needed?
- Submit Information Request to VA ISO
- Communicate ATO Reciprocity Decision to DoD ISSO
- Provide Required Additional Information
- Inform ISO of Review Results
- Communicate Information Request to DoD ISSO

Process Activity Name: ATOR-03.01 Deliver DIACAP Package (ATO) to VA ISO

Previous Activities

ATOR-03 Conduct Reciprocity Review by VA (DIACAP)

Next Activities

ATOR-03.02 Upload DIACAP Package

Description

The Department of Defense (DoD) Information System Security Officer delivers DoD Information Assurance Certification and Accreditation Process (DIACAP) Package for Authority to Operate (ATO) to Department of Veterans Affairs (VA) assigned Information Security Officer.

Input

DoD Information Assurance Certification and Accreditation Process (DIACAP) Package (for ATO)

Output

DoD Confirmation of Delivery of DIACAP ATO Package

Associated Artifacts

None Listed

Responsible Role

Information System Security Officer

Accountable Role

Information System Security Manager

Consulted Role

None Listed

Informed Role

Information Security Officer

Tools and Websites

None Listed

Standards

None Listed

More Info

DIACAP Package (ATO) includes Vulnerability Matrix, DIACAP Scorecard, Accreditation Memo, and Plan of Action and Milestones.

Process Activity Name: ATOR-03.02 Upload DIACAP Package

Previous Activities

ATOR-03.01 Deliver DIACAP Package (ATO) to VA ISO

Or

ATOR-03.07 Provide Required Additional Information

Next Activities

ATOR-03.03 Notify VA Certification Program Office of ATO Package

Description

The assigned VA Information Security Officer (ISO) initiates the Assessment & Authorization review by uploading the Assessment and Authorization (AAA) documents into the RiskVision Tool. The ISO ensures all required documents from the artifact checklist are uploaded into RiskVision.

Input

Accreditation Memo

DoD Information Assurance Certification and Accreditation Process (DIACAP) Executive Package (for ATO)

Plan of Action and Milestones

Scorecard

Vulnerability Matrix

Output

Record of Notification

VA DoD Information Assurance Certification and Accreditation Process (DIACAP) Artifact Checklist

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Director, Certification Program Office

Tools and Websites

Agilience RiskVision National Release GRC Instance

Standards

None Listed

More Info

The Vulnerability Matrix refers to VA's Authorizing Official Designated Representative (AODR) Risk Analysis artifact.

The Information Security Officer verifies if there is a RiskVision account created for the submitted package, and if not ensures an account is created. For further information on how to request for a package account of RiskVision please refer to the Assessment and Authorization process.

Process Activity Name: ATOR-03.03 Notify VA Certification Program Office of ATO Package

Previous Activities

ATOR-03.02 Upload DIACAP Package

Next Activities

Assessment and Authorization Process

Description

The assigned VA Information Security Officer sends notification email to the Certification Program Office to notify that the DoD Information Assurance Certification and Accreditation Process (DIACAP) ATO package is ready for review. The Certifying Agent follows the Assessment and Authorization sub-process Obtain Approval to obtain adjudication of the ATO package.

Input

VA DoD Information Assurance Certification and Accreditation Process (DIACAP) Artifact Checklist

Output

Notification of DoD Information Assurance Certification and Accreditation Process (DIACAP) ATO Package

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Director, Certification Program Office

Tools and Websites

Agiliance RiskVision National Release GRC Instance

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-03.04 Additional Information Needed?**Previous Activities**

Assessment and Authorization Process

Next Activities

If "YES":

ATOR-03.05 Submit Information Request to VA ISO

Or

If "NO":

ATOR-03.08 Inform ISO of Review Results

Description

If additional information is needed, then the VA Information Security Officer is asked to request the additional required information. If additional information is not needed, then the VA Information Security Officer is notified of the results of the review.

Responsible Role

Director, Certification Program Office

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: ATOR-03.05 Submit Information Request to VA ISO

Previous Activities

ATOR-03.04 Additional Information Needed?

Next Activities

ATOR-03.06 Communicate ATO Reciprocity Decision to DoD ISSO

Description

The VA Director, Certification Program Office submits an email request for the required information to complete the Risk Management Framework Package as needed to make Authority To Operate (ATO) Reciprocity decision to the VA Information Security Officer (ISO).

Input

Risk Management Framework Package

Output

Information Request

Associated Artifacts

None Listed

Responsible Role

Director, Certification Program Office

Accountable Role

Director, Office of Cyber Security

Consulted Role

None Listed

Informed Role

Information Assurance Manager

Tools and Websites

None Listed

Standards

NIST Special Publication 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: ATOR-03.06 Communicate ATO Reciprocity Decision to DoD ISSO

Previous Activities

ATOR-03.05 Submit Information Request to VA ISO

Next Activities

ATOR-03.07 Provide Required Additional Information

Description

The VA Information Security Officer sends a formal communications email to the DoD Information System Security Officer to notify them of the final results of the reciprocity review and the decision to approve or deny ATO Reciprocity.

Input

Approved Authority to Operate (ATO)

Output

Notification of Final Results

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Information Assurance Manager; Director, Certification Program Office

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-03.07 Provide Required Additional Information

Previous Activities

ATOR-03.06 Communicate ATO Reciprocity Decision to DoD ISSO

Next Activities

ATOR-03.02 Upload DIACAP Package

Description

The Department of Defense (DoD) Information System Security Officer fulfills information request received from the VA Information Security Officer.

Input

Notification of Information Required

Output

Information Response

Associated Artifacts

None Listed

Responsible Role

Information System Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Director, Certification Program Office

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-03.08 Inform ISO of Review Results

Previous Activities

ATOR-03.04 Additional Information Needed?

Next Activities

ATOR-03.09 Communicate ATO Reciprocity Decision to DoD ISSO

Description

Upon completion of the Assessment and Authorization (AAA) process, the Director, Certification Program Office sends an email to the VA Information Security Officer (ISO) to notify them of the results of the review and uploads the DIACAP ATO authorization artifact into Governance Risk and Compliance (GRC) RiskVision Tool and VA Intranet Quorum (VAIQ).

Input

Approved Authority to Operate (ATO)

Output

Notification of Completion

Associated Artifacts

None Listed

Responsible Role

Director, Certification Program Office

Accountable Role

Director, Office of Cyber Security

Consulted Role

None Listed

Informed Role

Information Security Officer

Tools and Websites

Agilience RiskVision National Release GRC Instance

Veterans Affairs Intranet Quorum (VAIQ)

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-03.09 Communicate ATO Reciprocity Decision to DoD ISSO

Previous Activities

ATOR-03.08 Inform ISO of Review Results

Next Activities

Process Ends

Description

The VA Information Security Officer sends a formal communications email to the DoD Information System Security Officer to notify them of the final results of the reciprocity review and the decision to approve or deny ATO Reciprocity.

Input

Information Request

Output

Notification of Information Required

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Director, Certification Program Office

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-04 Conduction Reciprocity by VA (RMF)

Previous Activities

ATOR-02 Determine Package Type

Next Activities

ATOR-04.01 Deliver RMF Package (ATO) to VA ISO

Description

The sub-process map Conduct Reciprocity Review by VA (RMF) cycles through the following dependent activities:

- Deliver RMF Package (ATO) to VA ISO

- Upload RMF Package
- Notify VA Certification Program Office of ATO Package
- Additional Information Needed?
- Submit Information Request to VA ISO
- Communicate ATO Reciprocity Decision to DoD/OGA ISSO
- Provide Required Additional Information
- Inform ISO of Review Results
- Communicate ATO Reciprocity Decision to Agency ISSO

Process Activity Name: ATOR-04.01 Deliver RMF Package (ATO) to VA ISO

Previous Activities

ATOR-04 Conduction Reciprocity by VA (RMF)

Next Activities

ATOR-04.02 Upload RMF Package

Description

The Other Government Agency (OGA) program manager or designee delivers the agency's Risk Management Framework Package for Authority to Operate (ATO) to Department of Veterans Affairs (VA) assigned Information Security Officer.

Input

OGA Risk Management Framework Package for Authority to Operate (ATO)

Output

OGA Confirmation of Delivery of RMF ATO Package

Associated Artifacts

None Listed

Responsible Role

Program Manager

Accountable Role

Program Manager

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-04.02 Upload RMF Package

Previous Activities

ATOR-04.01 Deliver RMF Package (ATO) to VA ISO

Or

ATOR-04.07 Provide Required Additional Information

Next Activities

ATOR-04.03 Notify VA Certification Program Office of ATO Package

Description

The VA Information Security Officer (ISO) initiates the Assessment & Authorization review by uploading the Assessment and Authorization (AAA) documents into the RiskVision Tool. The ISO ensures all required documents from the artifact checklist are uploaded into RiskVision.

Input

Accreditation Memo

Additional Information Responses from ISSO

Agency Risk Framework Management Package (for ATO)

Plan of Action and Milestones, if applicable

Scorecard

Vulnerability Matrix

Output

Record of Notification

VA Risk Framework Management Package Artifact Checklist

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision National Release GRC Instance

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

The Vulnerability Matrix refers to VA's Authorizing Official Designated Representative (AODR) Risk Analysis artifact.

The Information Security Officer verifies if there is a RiskVision account created for the submitted package, and if not ensures an account is created. For further information on how to request for a package account of RiskVision please refer to the Assessment and Authorization process.

Process Activity Name: ATOR-04.03 Notify VA Certification Program Office of ATO Package**Previous Activities**

ATOR-04.02 Upload RMF Package

Next Activities

Assessment and Authorization Process

Description

The VA Information Security Officer sends notification email to the Certification Program Office to notify that the Risk Management Framework ATO package is ready for review.

Input

Risk Management Framework ATO Package

Output

Notification of Risk Management Framework ATO Package

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Information System Security Officer

Tools and Websites

Agilience RiskVision National Release GRC Instance

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-04.04 Additional Information Needed?**Previous Activities**

Assessment and Authorization Process

Next Activities

If "YES":

ATOR-04.05 Submit Information Request to VA ISO

Or

If "NO":

ATOR-04.08 Inform ISO of Review Results

Description

If additional information is needed, then the VA Information Security Officer is asked to request the additional required information. If additional information is not needed, then the VA Information Security Officer is notified of the results of the review.

Responsible Role

Director, Certification Program Office

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: ATOR-04.05 Submit Information Request to VA ISO

Previous Activities

ATOR-04.04 Additional Information Needed?

Next Activities

ATOR-04.06 Communicate ATO Reciprocity Decision to DoD ISSO

Description

The VA Director, Certification Program Office submits an email request for the required information to complete the Risk Management Framework Package as needed to make Authority To Operate (ATO) Reciprocity decision to the VA Information Security Officer (ISO).

Input

Required Information

Output

Information Request

Associated Artifacts

None Listed

Responsible Role

Director, Certification Program Office

Accountable Role

Director, Office of Cyber Security

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

None Listed

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: ATOR-04.06 Communicate ATO Reciprocity Decision to DoD ISSO

Previous Activities

ATOR-04.05 Submit Information Request to VA ISO

Next Activities

ATOR-04.07 Provide Required Additional Information

Description

The VA Information Security Officer sends a formal communications email to the external Information System Security Officer to provide the requested information.

Input

Requested Information

Output

Notification of Information Required

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-04.07 Provide Required Additional Information

Previous Activities

ATOR-04.06 Communicate ATO Reciprocity Decision to DoD ISSO

Next Activities

ATOR-04.02 Upload RMF Package

Description

The agency Program Manager, or designee, fulfills information request received from the VA Information Security Officer.

Input

Notification of Information Required

Output

Information Response

Associated Artifacts

None Listed

Responsible Role

Program Manager

Accountable Role

Program Manager

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-04.08 Inform ISO of Review Results**Previous Activities**

ATOR-04.04 Additional Information Needed?

Next Activities

ATOR-04.09 Communicate ATO Reciprocity Decision to Agency ISSO

Description

Upon completion of the Assessment and Authorization (AAA) process, the Director, Certification Program Office sends an email to the VA Information Security Officer (ISO) to notify them of the results of the review.

Input

Approved Authority to Operate (ATO)

Output

Notification of Completion

Associated Artifacts

None Listed

Responsible Role

Director, Certification Program Office

Accountable Role

Director, Office of Cyber Security

Consulted Role

None Listed

Informed Role

Information Security Officer

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-04.09 Communicate ATO Reciprocity Decision to Agency ISSO

Previous Activities

ATOR-04.08 Inform ISO of Review Results

Next Activities

Process Ends

Description

The VA Information Security Officer sends a formal communications email to the external Information System Security Officer to notify them of the final results of the reciprocity review and the decision to approve or deny the Authority to Operate.

Input

Information Request

Output

Notification of Information Required

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

Information System Security Officer

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-05 Conduct Reciprocity by DoD or Other Agency**Previous Activities**

ATOR-01 Who Submitted ATO Reciprocity Review?

Next Activities

ATOR-05.01 Submit ATO Package for Reciprocity Review

Description

The sub-process map Conduct Reciprocity Review by DoD or Other Agency cycles through the following activities:

- Submit ATO Package for Reciprocity Review
- Register System and Import ATO Package
- Review and Prepare RMF Package for Workflow
- Notify DoD SCA of RMF Package in eMASS

- Review Package and Provide Assessment
- Review SCA's Assessment
- Issues?
- Inform Program Management Office of Review Results
- Resolve Issues

Process Activity Name: ATOR-05.01 Submit ATO Package for Reciprocity Review

Previous Activities

ATOR-05 Conduct Reciprocity by DoD or Other Agency

Next Activities

ATOR-05.02 Register System and Import ATO Package

Description

The VA Information Security Officer develops Authority to Operate (ATO) package and upon completion, submits the compiled ATO package to the Department of Defense (DoD) for their reciprocity review.

Input

Authority to Operate (ATO) or Temporary ATO (TATO) Memorandum (Authorization Decision Document)

Authority to Operate Determination Report

Plan of Action and Milestones

Risk Assessment Report (RAR)

Security Assessment Report (SAR)

System Security Plan (SSP)

Vulnerability Matrix

Output

Notification of Record to Review

Associated Artifacts

None Listed

Responsible Role

Program Manager

Accountable Role

Program Manager

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Interagency ATO Crosswalk Checklist

TRICARE Management Activity (TMA) Large Attachment File System

Standards

NIST Special Publication 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations

More Info

The Interagency ATO Crosswalk Checklist contains the names of the respective artifacts between the DoD and the VA.

Process Activity Name: ATOR-05.02 Register System and Import ATO Package

Previous Activities

ATOR-05.01 Submit ATO Package for Reciprocity Review

Next Activities

ATOR-05.03 Review and Prepare RMF Package for Workflow

Description

The Department of Defense (DoD) Information System Security Manager (ISSM) provides a formal, written response back to the VA to inform VA that their Authority to Operate (ATO) package has been received and the review will be initiated.

Input

Authority to Operate (ATO) or Temporary ATO (TATO) Memorandum

Authority to Operate (ATO) Determination Report

Plan of Action and Milestones

Requirements Traceability Matrix (RTM)

Vulnerability Matrix

Output

Mapped Requirements Traceability Matrix to DoD Information Assurance Controls

Mapped Vulnerability Matrix to DoD Information Assurance Controls

System Registration in Enterprise Mission Assurance Support Service (eMASS)

Associated Artifacts

None Listed

Responsible Role

Information System Security Manager

Accountable Role

Information System Security Manager

Consulted Role

None Listed

Informed Role

Information Security Officer; Director, Certification Authority Office

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Standards

DoDI 8500.01, Cybersecurity

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

NIST Special Publication 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations

More Info

None Listed

Process Activity Name: ATOR-05.03 Review and Prepare RMF Package for Workflow**Previous Activities**

ATOR-05.02 Register System and Import ATO Package

Or

ATOR-05.08 Resolve Issues

Next Activities

ATOR-05.04 Notify DoD SCA of RMF Package in eMASS

Description

The Department of Defense (DoD) Information System Security Manager (ISSM) reviews and translates VA's Authority to Operate (ATO) Package into Risk Management Framework (RMF) Package for Enterprise Mission Assurance Support Service (eMASS).

Input

Authority to Operate (ATO) Determination Report

Authority to Operate (ATO) or Temporary ATO (TATO) Memorandum

Plan of Action and Milestones

Requirements Traceability Matrix

Vulnerability Matrix

Output

DoD Security Controls

Associated Artifacts

None Listed

Responsible Role

Information System Security Manager

Accountable Role

Information System Security Manager

Consulted Role

None Listed

Informed Role

Authorizing Official; Information System Security Officer

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Interagency ATO Crosswalk Checklist

Standards

DoDI 8500.01, Cybersecurity

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

More Info

The Interagency ATO Crosswalk Checklist contains the names of the respective artifacts between the DoD and the VA.

Process Activity Name: ATOR-05.04 Notify DoD SCA of RMF Package in eMASS

Previous Activities

ATOR-05.03 Review and Prepare RMF Package for Workflow

Next Activities

ATOR-05.05 Review Package and Provide Assessment

Description

The Department of Defense (DoD) Information System Security Manager notifies the Certification Authority and Security Control Assessor (SCA) via Enterprise Mission Assurance Support Service (eMASS) for review of Risk Management Framework (RMF) for DoD Information Technology (IT) Package.

Input

DoD Security Controls

RMF Package in Enterprise Mission Assurance Support Service (eMASS)

Output

Notification to Review

Associated Artifacts

None Listed

Responsible Role

Information System Security Manager

Accountable Role

Information System Security Manager

Consulted Role

None Listed

Informed Role

Information System Security Manager; Security Control Assessor

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Standards

DoDI 8500.01, Cybersecurity

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

More Info

None Listed

Process Activity Name: ATOR-05.05 Review Package and Provide Assessment**Previous Activities**

ATOR-05.04 Notify DoD SCA of RMF Package in eMASS

Next Activities

ATOR-05.06 Review SCA's Assessment

Description

The Department of Defense (DoD) Director, Security Controls Assessor reviews the Risk Management Framework (RMF) for DoD Information Technology (IT) Package in eMASS in order to provide an assessment. If there are any issues with the Package, questions are communicated to the DoD Information System Security Manager; otherwise, the package is recommended for approval.

Input

RMF Package in Enterprise Mission Assurance Support Service (eMASS)

Output

DoD Certification Statement

Information Request

Associated Artifacts

None Listed

Responsible Role

Director, Security Control Assessor

Accountable Role

Director, Security Control Assessor

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Standards

DoDI 8500.01, Cybersecurity

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

More Info

None Listed

Process Activity Name: ATOR-05.06 Review SCA's Assessment**Previous Activities**

ATOR-05.05 Review Package and Provide Assessment

Next Activities

ATOR-05.07 Issues?

Description

The Department of Defense (DoD) Information System Security Manager (ISSM) reviews the Security Control Assessor's (SCA) assessment and works with VA Information Security Officer (ISO) to resolve any potential issues. If issues are found, the VA ISO is informed of the issues and the package is returned for refinement; otherwise, the DoD ISSM provides the Recommendation for Approval.

Input

Information Request

RMF Package in Enterprise Mission Assurance Support Service (eMASS)

Output

Recommendation for Approval

Associated Artifacts

None Listed

Responsible Role

Information System Security Manager

Accountable Role

Information System Security Manager

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Standards

DoDI 8500.01, Cybersecurity

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

More Info

None Listed

Process Activity Name: ATOR-05.07 Issues?**Previous Activities**

ATOR-05.06 Review SCA's Assessment

Next Activities

If "Yes":

ATOR-05.08 Resolve Issues

Or

If "No":

ATOR-05.09 Provide Recommendation to Authorizing Official

Description

If issues are found (Yes), the VA Information Security Officer is informed of the issues and the package is returned for refinement.

If issues are not found (No), the Department of Defense (DoD) Information System Security Manager provides the Recommendation for Approval.

Responsible Role

Information System Security Manager

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: ATOR-05.08 Resolve Issues**Previous Activities**

ATOR-05.07 Issues?

Next Activities

ATOR-05.03 Review and Prepare RMF Package for Workflow

Description

The VA Information Security Officer reviews the issues raised by the Department of Defense (DoD) and submits additional information to satisfy the need for required information which is used to make the reciprocity decision.

Input

Information Request

Output

Information Response with Additional Artifacts

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Program Manager

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

TRICARE Management Activity (TMA) Large Attachment File System

Standards

None Listed

More Info

None Listed

Process Activity Name: ATOR-05.09 Provide Recommendation to Authorizing Official**Previous Activities**

ATOR-05.07 Issues?

Next Activities

Process Ends

Description

If no issues with the Risk Management Framework (RMF) package are determined, the Department of Defense (DoD) Security Control Assessor (SCA) provides a formal, written recommendation to the Authorizing Official (AO).

Input

RMF Package in Enterprise Mission Assurance Support Service (eMASS)

Output

Recommendation to Department of Defense Authorizing Official (AO)

Associated Artifacts

None Listed

Responsible Role

Security Control Assessor

Accountable Role

Security Control Assessor

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Mission Assurance Support Service (eMASS)

Standards

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

More Info

None Listed

END OF PROCESS