

ATO Test Questions

General Process & Overview Questions (Testing Graph Traversal, Direct Lookup, RAG)

1. What is the **overall purpose** of the RMF process, and what kind of approach does it take to risk management?
2. Who are the **key roles** involved in the ATO process, and where can I find their high-level responsibilities?
3. Where can I find the **templates** for the ISSM/ISSO appointment letters?
4. What are the **seven steps** of the RMF, and is the workflow strictly sequential after the initial step?
5. What are some **common pitfalls** or "**Watch Items**" I should be aware of across the entire ATO process to avoid delays?

RMF Step 0: Prepare Questions (Testing Direct Lookup, Procedural, Template Retrieval)

1. Before I even start RMF activities, what are the **prerequisites** my system needs to have fulfilled, such as documentation?
2. What **training** is required before I can request access to eMASS, and where can I find it?
3. What specific **artifacts** are typically produced during the "Prepare" step of the RMF?
4. I need to register my system in ITIPS/DITPR/SNAP. Who is responsible for this, and are there any **reference links** available?

RMF Step 1: Categorize Questions (Testing Specific Requirements, Artifact Details, Cross-Referencing)

1. What is the **ITCSC**, what does it determine, and what happens if I reduce my CIA impact levels from the default?
2. My system is Unclassified but processes Controlled Unclassified Information (CUI). What **CIA levels** should I assign to it, and which DoD memo supports this?
3. What are the "**Watch Items**" for **RMF Step 1**, especially regarding the **Authorization Boundary Topology** and the **Technical Description/Purpose**?
4. If the SCAR doesn't concur with my system's categorization, what is the **next step**?
5. What **external references** (e.g., FIPS, NIST SPs) are relevant to determining information types and CIA levels?

RMF Step 2: Select Questions (Testing Policy Application, Tool Use, Watch Items)

1. After categorizing my system, what's the **first step for the ISSM/ISSO** in eMASS to initiate the Security Plan?
2. How do I determine if my system is a **National Security System (NSS)**, and what are the implications for control selection?
3. When tailoring controls, if I mark a control as "Not Applicable" (N/A), what **justification** must I provide, and which DoDI prohibits certain types of "N/A" justifications?
4. What must be included in my **ISCM Plan/Strategy**, and what external NIST publications should I reference for its development?
5. The SCAR reviews the Security Plan in Select Step 2H. What specific **fields and documents** do they emphasize in their review, particularly concerning End-of-Life (EoL) software?

RMF Step 3: Implement Questions (Testing Procedural, Artifact Management, Policy Specifics)

1. What are the **age requirements** for vulnerability scans and checklists when I'm uploading them as part of the self-assessment in eMASS?
2. What is the **purpose of a POA&M**, and what specific information (e.g., mitigation strategies, milestones) needs to be included for non-compliant controls?
3. If a control in my Implementation Plan is marked as "Planned," what should be its **Estimated Completion Date (ECD)**?
4. What does the eMASS Compelling Evidence section outline, and what are the **consequences** if I fail to provide the indicated evidence for a compliant control?
5. What are the **"dash-one" security control requirements** for policies and procedures, and how do they relate to the SSC S6 provided i-Assure templates?

RMF Step 4: Assess Questions (Testing Definitions, Causal Relationships, Risk Factors)

1. What are some **common reasons** why the A&A Branch might determine my system is "not ready for an assessment"?
2. What is a **Cyber Risk Assessment (CRA)**, and what are its main objectives?
3. During the assessment, what constitutes **"compelling evidence"** for a security control, and how should it be documented in eMASS?
4. If the SCAR or ASCA identifies unmitigated vulnerabilities during the assessment, how are these typically **handled**?

5. What **NIST SPs** are referenced for assessing security and privacy controls in federal information systems?

RMF Step 5: Authorize Questions (Testing Decision Outcomes, Post-Decision Actions)

1. What kind of **authorization decisions** can the AO issue, and what do "ATO with Conditions" or a "DATO" mean for my system?
2. What information is contained within the **Authorization Decision Document (ADD)**, and what is the significance of the **Authorization Termination Date (ATD)**?
3. After receiving the ADD, what are the **ISSM's responsibilities** regarding the terms and conditions and making the document available?
4. What policies or guidelines govern how authorization documents (especially those with vulnerabilities) should be **protected and retained**?
5. If my system receives a **DATO**, what is the expected course of action to achieve authorization?

RMF Step 6: Monitor Questions (Testing Continuous Monitoring, Policy Details, Change Management)

1. What is the **frequency** for reviewing and verifying Red, Yellow, and White Criticality Controls according to the USSF ISCM and ACV Policy?
2. What are the **typical outputs** for continuous monitoring that indicate effective security posture maintenance?
3. When does an **ISSM/ISSO need to notify the SSC S6 SCA/SCAR** regarding changes in the system's risk posture?
4. What is the purpose of the **Annual Control Validation (ACV)**, and what percentage of controls must be selected for it, including specific critical controls?
5. What is a **Security Impact Assessment (SIA)**, what types of changes might trigger it, and what are the different "Levels" of SIA?

Interconnected Systems / Special Cases (Testing Specific Appendices, Relationship to other processes)

1. What defines a "system interconnection," and what are the **four phases** of information exchange management?
2. What is the difference between a **Memorandum of Understanding (MOU/A)** and an **Interconnection Security Agreement (ISA)**, and what key sections does an ISA typically include?

3. When would an **Authority to Connect (ATC)** be required, and what documentation is needed for an external system connecting to a Space system?
4. What are the **specific requirements for a topology diagram** as detailed in Appendix I, especially concerning the authorization boundary, component labeling, and information flow?
5. What types of **Level 2 "Moderate" changes** might trigger an SIA, specifically regarding adding/removing hardware, OS upgrades, or PPS modifications?