NIST RMF
Step 5: Authorize

Managing Cybersecurity Risk

Dr. Ibrahim Waziri Jr.

Step 5 - Authorize

- Authorizing Official (AO) authorizes based on outcome of the assessment and recommendation of security officials (including ISSO, SO etc.)
- Security Officials review the ATO package, and AO signs the ATO memo.
- AO is often a senior management official (such as CISO, etc.)
- Authorization requires submitting the Authority to Operate (ATO) request memo and package.

Authorizations: (IATT/ATO/ATU)

- IATT – Interim Authority to Test – Before Production
- ATO – Authority to Operate - Systems owned and operated internally
- ATU – Authority to Use - systems owned by external organizations and operated as a service.

Step 5 - Authorize

Minimum Authorization Package:

- Step 1 – FIPS 199 Memo
- Step 2 – Approved Selected Controls
- Step 3 – SSP
- Step 4 – SAR, POA&Ms
- Step 5 – ATO Memo Template
- Step 6 – Information Security Continuous Monitoring Plan

Other additional documents (as agreed):

- E-Authentication
- Config Mgt Plan (CMP)
- Contingency Plan (CP)
- Business Impact Analysis (BIA)
- Contingency Plan
- Risk Assessment
- Incident Response Plan (IRP)
- System of Record Notice (SORN)
- Privacy Documents (PTA & PIA)
- Memorandum of Agreement (MOU/MOA)
- Interconnection Security Agreement (ISA)
- Operations and Maintenance (O&M)
- Rules of Engagement etc.

ATO Memo Template available on Canvas

Activity: Build an ATO Package; and fill out the ATO Memo Template