Module 11

Tips to succeed as an ISSO

@2023 Confidential and Proprietary

Being Successful as an ISSO

To Be Successful as an ISSO you will:

- Mission/Business functions of the organization
- How the system supports the mission of the organization
- System details:
  - Architecture
  - System components (HW/SW)
  - Location
  - Data flow
  - Interconnections (internal and external)
  - Security Categorization
  - Security Requirements
  - Configuration management process and procedures
  - Users (how many?, location of users (remote/on prem))
  - Key personnel by name

@2023 Confidential and Proprietary

ISSO Reoccurring Tasks

Periodic items ISSOs should preform: (Note: will vary based on the org)

- Ongoing Activities
  - Continuous monitoring and controlled testing
  - Review and update the Security Authorization Process document
  - Review and remediate findings in the POA&M
  - Maintain Cybersecurity Certifications
  - Report Incidents to the ISSM & ISO
- Weekly Activities
  - Attend System scrum meetings
  - Review Audit Logs (e.g. Splunk or ArcSight SIEM Reviews)
  - Attend Change Control Board (CCB) meetings
  - Review Account Management activity
- Monthly Activities
  - Perform Vulnerability Scan Analysis and provide the report to admins (Weekly/Monthly)
  - Review inactive accounts on the system
  - Update information in the System of Record (eMASS, CSAM, XACTA)

@2023 Confidential and Proprietary

ISSO Reoccurring Tasks….cont.

Periodic items ISSOs should preform: (Note: will vary based on the org)

- Annual Activities
  - Training: ensure all system users with security responsibilities receive their annual training (e.g., Role-based, Incident Response and Security Awareness Training, Computer Awareness Training)
  - Review, approve, and validate user access rights/permissions
  - Conduct the Contingency Plan Testing
  - Update Security Documentation (SP, CP, CPT, FIPS 199, Privacy PIA/PTA/SORN)
- As Required Activities
  - Update SSP
  - Participate in the Change Request process (i.e., Conduct Security Impact Analysis, review/approve CRs)
  - Ensure all system users sign the Rules of Behavior (RoB) before granting access
  - Ensure the decommissioning procedures are followed to dispose of system components

@2023 Confidential and Proprietary