FISMA A&A Roles and Responsibilities

The role descriptions below, which can be used to identify appropriate staff to fulfill key roles, are based on definitions found in NIST Special Publication 800-37 rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

Information Owner (also known as the Federal Business Owner)

The Information Owner (also synonymous with Federal Business Owner), is a Federal official with the statutory, management, or operational authority to safeguard specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. A single information system may contain data from multiple information owners, who also can provide input to IT system owners regarding security requirements and controls. The Information Owner has a governance role to ensure Information System Owner(s) working on their behalf are meeting the operational interests of the user community and maintaining compliance with security requirements. The role of Information Owner is an inherently governmental one and cannot be delegated to non-government staff.

Note: NIST combines both of the Information (aka Business) Owner and Information System Owner roles into a single role called “System Owner.” NCI split the NIST-defined “System Owner” role into two separate roles as described on this page, so that we can better distinguish their unique features and roles. The former must be filled by a federal staff member, the latter can be filled by federal or contractor staff. When NIST calls for a system owner role, NCI normally associates that with our Information/Business Owner role.

Information System Owner

The Information System Owner (commonly referred to as System Owner) is an official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. System owners are also responsible for addressing the operational interests of the user community and for ensuring compliance with security requirements.

Information System Security Officer (ISSO)

The ISSO is the individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and works in close collaboration with the IS owner. Security posture refers to the presence of effective security controls including technical, operational, and managerial that, together, ensure the system and its information are adequately protected against threats. The ISSO also serves as a principal advisor on matters involving security.

Security Control Assessor (SCA)

The SCA is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls inside an information system to determine the overall effectiveness of the controls. SCAs can also assess severe weaknesses or deficiencies in the IS and its operational environment. They usually recommend ways to fix these problems.

The required level of assessor independence is determined by the specific conditions of the assessment. Assessor independence is an important factor in:

- preserving the unbiased nature of the assessment process
- determining the credibility of security-assessment results
- ensuring that authorizing officials receive the most objective information possible

Authorizing Official (AO)

An AO is a senior federal official with the authority to assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, or the country. AOs oversee budgets for information systems, and they may be responsible for the mission or business operations supported by a system. They are also accountable for the security risks associated with information-system operations. AOs have primary responsibility for ensuring adequate resources (e.g., funding and staffing) are made available to address POA&M items. The role of AO is an inherently governmental one.

NCI Security Teams

All NCI security teams are organizationally located within Center for Biomedical Informatics and Information Technology (CBIIT) supporting the NCI ISSO.

Cyber Governance, Risk, and Compliance Team (CGRC)

The CGRC Team is responsible for the cyber governance and compliance of all NCI information systems. In performing these functions, the EST works with Information Owners, System Owners, and their support teams to establish their system's categorization (Step 1 of the RMF), complete their Starter Kit (Step 2 of the RMF), and also finalizes the ATO package for the system and works with the Federal A&A Lead and AO to issue the system's authorization to operate (ATO) (Step 5 of the RMF).

IT Security Advisor (ITSA)

The ITSA works with Information Owners, System Owners, and their support teams to provide guidance during the implementation of security controls (Step 3 of the RMF) and completing the required documentation for the system to receive an ATO.

Security Control Assessor (SCA)

The SCA performs the independent security control assessment for internal NCI systems (Step 4 of the RMF).