The ISSPM Competency Model

USDA | aglearn+ adding to your knowledge

AgLearn View of Competencies

Goal: Build an ISSPM Competency Model for the ISSPM role; and use the finalized model for future competency models as part of the IT Working Initiative.

A working group made up of Department and Agency staff (Ted Kaouk, OCIO; Juanita Makuta, Kathleen Fallow, Ivan Jackson, OCFO-NFC, Noah Waters, GIPSA; Eugene Texter, RD; Angela Pompey, ERS; Ortese Parker, ASOC; Greg Schmitz, NITC; Rachel Payne, OCIO; and Vivian Tydings, OCIO) worked together to create the ISSPM Competency Model.

External Awareness	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Collaborates with fellow Federal ISSPMs/CISOs to resolve security issues affecting the Department. Maintains certification(s) with accredited professional associations (i.e. ISC2, SANS, PMP, FITSI, etc.). Develops collection requirements and conducts information collection, ensuring they are translated, tracked and prioritized across the extended enterprise. Collaborates with other cyber counterparts or federal agencies on new or emerging threats and technologies, as required.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Monitors and evaluates external organizations and academic institutions dealing with cybersecurity issues as it relates to a system's compliance with IT security, resilience, and dependability requirements. Regularly researches and studies Federal requirements and Departmental security policies, then assesses/determines applicability to agency, program area, and office level operations. Participates and contributes as an active member of cyber security working groups, at the Department and/or Industry level.

Fully Proficient	**Understands and applies knowledge of identified threats from the Department and/or 3rd-party sources in decision making. Keeps apprised of and analyzes social dynamics of computer attackers in a global context. Maintains knowledge of current events and technologies by acquiring continuous education credits and formal training as needed, or at least annually.**
Basic	Demonstrates an understanding of information collection and collection requirements for a system. Is familiar with cutting edge technology and vendor products. Regularly receives/reviews Cyber Security updates from trusted IT Security entities (i.e.- US-CERT, SANS, etc)
Awareness	Identifies relevant external organizations and academic institutions dealing with cybersecurity issues as it relates to a system's compliance with IT security.

Strategic Planning Policy Development	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Participates in the development of a cybersecurity strategy that aligns with the vision, mission, and goals of the USDA. Develops policy, programs, and guidelines for implementation. Develops and/or implements agency supply chain security/risk management guidance. Serves on agency and interagency policy boards. Writes Information Assurance (IA) policy and instructions. Designs a cybersecurity strategy that that aligns with the vision, mission, and goals of the organization. Develops policy, programs, and guidelines for implementation. Reviews existing and proposed policies with stakeholders, and obtains consensus on policy changes. Supports the Chief Information Officer (CIO) in the formulation of IT-related policies. Translates applicable laws, statues, and regulatory documents into integrated policies.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Translates departmental security policies and federal requirements into directives/procedures at the agency/office level. Develops and maintain a comprehensive set of security policies within their span of management (Agency/Department). Applies assessment data of identified threats in decision making. Assesses policy needs and collaborates with stakeholders to develop policies to govern IT activities. Maintains strategic plans. Ensures established cybersecurity strategy is intrinsically linked to USDA mission objectives. Reviews or conducts audits of IT programs and projects. Translates applicable laws, statues, and regulatory documents into integrated policies. Assesses policy needs and collaborates with stakeholders to develop policies to govern IT activities. Ensures established cybersecurity strategy is intrinsically linked to organizational mission objectives. Identifies and addresses IT workforce planning and management issues, such as recruitment, retention, and training. Monitors the rigorous application of information security/IA policies, principles, and practices in the delivery of planning and management services. Provide policy guidance to IT management, staff, and users.

Fully Proficient	**Reviews Agency information security policy. Defines and/or implements policies and procedures to ensure protection of USDA data and infrastructure (as appropriate). Integrates and implements security policy. Establishes and maintains communication channels with stakeholders. Monitors the rigorous application of information security/IA policies, principles, and practices in the delivery of planning and management services. Promotes awareness of security issues among management and ensures sound security principles are reflected in the agency's vision and goals. Provides policy guidance to IT management, staff, and users. Supports the USDA CIO and Chief Information Security Officer (CISO) in the formulation of IT-related policies. Applies assessment data of identified threats in decision making. Defines and/or implements policies and procedures to ensure protection of critical infrastructure (as appropriate). Promotes awareness of security issues among management and ensures sound security principles are reflected in the organization's vision and goals.**
Basic	Identifies IT resource issues associated with POA&Ms. Obtains input on proposed agency security directives/procedures changes from stakeholders.
Awareness	Demonstrates an understanding of the culture and relevant technology of the current work environment. Is aware of existing security policies.

Incident Management	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Administers low profile methods to lure and contain attacker (i.e. - treasures, honeypots, etc.). Identifies and avoids software code that is compromised or that does not meet a certain level of security. Leads the Incident Response Team, serving as the incident commander and responsible for directing the response.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Performs initial, forensically sound collection of images and inspects to discern possible mitigation/remediation on enterprise systems. Writes and publishes Computer Network Defense guidance and reports on incident findings to appropriate constituencies. Prescribes the proper containment and recovery operations commensurate with the incident type. Organizes post-mitigation analysis meetings with stakeholders; articulates lessons learned and implements approved actions. Trains the Incident Response Team regarding their roles and responsibilities.
Fully Proficient	Performs real-time Computer Network Defense Incident Handling (e.g., system image, intrusion correlation/tracking, threat analysis, and directs system remediation) tasks to support deployable Incident Response Teams (IRTs). Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts. Serves as liaison to law enforcement personnel and explains incident details as required. Tracks and documents Computer Network Defense incidents from initial detection through final resolution.

Basic	**Identifies the factors that determine incident response capability. Matches phases of an incident response plan with their corresponding descriptions. Recognizes examples of individuals who may require notification in case of a serious security incident. Matches members of response and recovery teams with their corresponding responsibilities. Recognizes the types of security controls that are in place during a security incident. Determines the appropriate type of recovery site given examples of requirements. Recognizes methods for recovering communication and computing systems. Recognizes examples of metrics used for testing incident response and recovery plans. Identifies important aspects of executing incident response and recovery plans.**
Awareness	Orders the steps in the incident management process. Recognizes the elements of an incident management plan; matches causes of challenges in developing an incident management plan with corresponding solutions. Identifies the roles that make up an incident response team, matching key incident management roles with their corresponding responsibilities. Recognizes examples of personal skills and technical knowledge required by members of an incident response team. Recognizes the activities that are performed during a business impact analysis.

Enterprise Architecture	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Assesses and designs key management functions (as related to IA). Designs system architecture or system components required to meet user needs. Develops IA designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). Employs secure configuration management processes.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Analyzes user requirements to plan system architecture. Collaborates with system developers and users to select appropriate design solutions or ensure the compatibility of system components. Defines and prioritizes essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. Defines appropriate levels of system availability based on critical system functions and ensures system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over, backup, and material supportability requirements. Documents and addresses organization's information security, IA architecture, and systems security engineering requirements throughout the acquisition lifecycle. Ensures that acquired or developed systems and architectures are consistent with organization's IA architecture guidelines. Performs security reviews, identifies gaps in security architecture, and develops a security risk management plan. Provides advice on project costs, design concepts, or design changes. Provides input on security requirements for statements of work and other procurement documents. Provides input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).

Fully Proficient	**Collects user needs and requirements for the analysis to plan system or enterprise architecture. Defines, documents and coordinates how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. Manages or supports an enterprise technical risk register, documenting, prioritizing, and managing technical risks throughout the system lifecycle. Ensures all definition and architecture activities (system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials, etc.) are properly documented and updated as necessary. Identify the protection needs (i.e., security controls) for the information systems and networks and document appropriately.**
Basic	Defines documentation and diagrams for a system's business, technical, data and security processes throughout the System's Development Life Cycle (SDLC). Documents design specifications, installation instructions, and other system-related information.
Awareness	Develops understanding on documenting and diagramming system business, technical, data, and security processes. Defines the process and approach, the intended use, the lifecycle and the scope of the Enterprise Architecture.

Information Assurance Compliance	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Develops methods to monitor and measure risk, compliance, capital planning, POA&M management, and assurance efforts. Develops security compliance processes and/or audits for noncompliance, including external services (e.g., cloud service providers, data centers, system inventory and networks). Develops specifications to ensure risk, compliance, and assurance efforts conform to security, resilience, and dependability requirements at the software application, system, and network environment level. Correlates business needs, financial requirements (i.e., ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and ensures that information security resources are available for expenditure as planned). Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed and maintained; documents the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; ensures these are reported in accordance with OMB FISMA reporting requirements. Manages organization's enterprise information security program.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Develops statements of preliminary or residual security risks for system operation. Manages and evaluates Accreditation Packages (e.g., ISO/IEC 15026-2) for submission. Performs validation steps, analyzing the differences between actual results with expected results to identify impact and risks. Provides a technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant IA compliances. Recommends new or revised security, resilience, and dependability measures based on the results of reviews. Verifies that application software/network/system security postures are implemented as stated, documents deviations, and recommends required actions to correct those deviations. Performs Security Assessment and Authorization process. Performs Security management. Plans, designs, and develops organization's enterprise information security architecture system. Plans, designs, and develops security controls based on IA principles and tenets.

Fully Proficient	**Detects and proposes solutions for basic and mid-tier issues that have immediate resolutions to minimize risk to the enterprise, local or physical level. Ensures the development and implementation of system/network backup and recovery procedures, as applicable. Analyzes security compliance processes in conformity with federal or departmental requirements and industry best practices. Describes or reports on identified risks for system operation (e.g. physical, system, code) as required. Inspects continuous monitoring results and deploys mitigation strategies to ensure that the level of risk is within acceptable limits for the software application, network, or system. Maintains information systems assurance and accreditation materials and updates as needed.**
Basic	Monitors a system's compliance with IT security, resilience, and dependability requirements. Verifies that the software application/network/system accreditation and assurance documentation is current. Analyzes how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. Assists in developing, testing, and implementing network infrastructure contingency and recovery plans. Assists in performing damage assessments.
Awareness	Demonstrates an understanding of IA principles used to manage risks related to the use, processing, storage, and transmission of information or data. Demonstrates an understanding of confidentiality, integrity, and availability principles. Demonstrates an understanding of vulnerabilities and associated attacks.

Network Services	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Evaluates strategic implications of network architecture options. Plans, designs, develops, and manages or enhances new highly efficient network systems in response to business requirements. Ensures rigorous application of information security/information assurance policies, principles, and practices to the delivery of network services. Manages network systems including end-to-end systems performance monitoring.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Plans, designs, develops, and integrates network systems consistent with existing or planned network infrastructures. Applies network architecture, topography, and protocols to provide network services. Performs network capacity planning against existing network infrastructure.

Fully Proficient	**Reviews new system design procedures, test procedures, and quality standards, as applicable. Ensures new systems are integrated into existing network architecture. Ensures network vulnerabilities are patched to ensure information is safeguarded against outside parties. Provides feedback on network requirements, including network architecture and infrastructure, as applicable.** **Applies network standards, protocols, and procedures to assist in development, configuration, installation, and maintenance of networked systems including local area networks and wide area networks. Performs routine network configuration management functions. Understands capabilities and applications of network equipment (e.g., hubs, routers, switches). Assists in planning, designing, developing, and integrating network systems consistent with existing or planned network infrastructures.**
Basic	Participates in the continuous monitoring of network capacity and performance, as applicable. Operates network diagnostic tools. Gathers and analyzes basic network information and performance metrics. Performs network configuration tasks on network equipment.
Awareness	Builds awareness of organizational IT network policies and procedures. Assists in collecting information regarding network inventory. Learns about existing network architecture and concepts.

Education and Training	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Plans organization's training program to ensure instructional objectives align with mission objectives, information is current and accurate; ensures content meets the system security requirements of the organization. Authors specialized training material that addresses current threats or results from recent incidents.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Identifies appropriate security awareness and role based training for employees tailored to their security responsibilities. Writes instructional materials (e.g. standard operating procedures) to provide detailed guidance to relevant security program. Develops communication vehicles to ensure employee awareness regarding current or emergent threats from external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus).
Fully Proficient	Ensures awareness and specialized training addresses mission requirements. Tracks and reports monthly on specialized training for security related roles to ensure completion. Supports the design and execution of contingency, disaster recovery, and incident response exercise scenarios.
Basic	Demonstrates an understanding of the annual security awareness and specialized training requirements.
Awareness	Recognizes security awareness and specialized training requirements for the organization.

Systems Security Architecture	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Analyzes USDA needs and requirements to plan system architecture. Defines appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Evaluates current or emerging technologies to consider factors such as cost, security, compatibility, or usability, as appropriate. Identifies and prioritizes critical business functions in collaboration with USDA stakeholders, as appropriate. Plans system implementation to ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware.

Fully Proficient	**Documents business impact assessments for all major systems and correlate BIAs to help identify recovery priorities. Ensures appropriate system documentation identifies system design specifications, installation instructions, and other system-related information. Ensures secure configuration management processes are in place and implemented. Ensures all definition and architecture activities (system lifecycle support plans, acquisitions, concept of operations, operational procedures, and maintenance training materials, etc.) are properly documented and updated as necessary. Ensures that acquired or developed systems and architectures are consistent with USDA's IA security architecture guidelines. Participates to identify the protection needs (i.e., security controls) for the information systems and networks and document appropriately. Provides input on security requirements to be included in statements of work and other appropriate procurement documents. Provides input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).**
Basic	Assists in identifying key management functions (as related to IA). Review documentation on how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. Assists in documenting and addressing USDA's information security, IA architecture, and systems security engineering requirements throughout the acquisition lifecycle, as appropriate. Assists in documenting and managing an enterprise technical risk register, prioritizing and managing technical risks throughout the system lifecycle.
Awareness	Demonstrates a knowledge of products and applications with the capability to enforce security controls.

Vulnerability Assessment and Management	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Designs site/enterprise cyber defense strategy. Develops and implements agency-wide risk assessment and mitigation strategy. Fully documents attack plan (rules of engagement), taking a holistic approach in coordinating activities among key stake holders.
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Provides analysis of Cyber Defense policies and configurations to evaluate compliance with regulations and enterprise directives. Recommends long-term risk mitigation approach. Weighs and evaluates findings/weaknesses and discriminates between actual findings and false positives. Completes detailed analysis and recommend appropriate risk mitigation. Analyzes and prioritizes vulnerability findings (from tools, reviews, pen-testing, technical/non-technical assessments). Manages the Risk Based Decision(RBD)/Waiver Process and reviews RBD/waiver on a regular basis. Leads the agency in compliance with Homeland Security and OMB's CDM (continuous diagnostics mitigation) strategy.

Fully Proficient	**Assists with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes). Assists with the cost-benefit analysis of risk mitigation handling options. Performs analysis of pen-testing results and places in order of criticality. Performs technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (i.e., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure). Participates in required reviews as appropriate within environment (e.g., Technical Surveillance Countermeasure Reviews (TSCM), TEMPEST countermeasure reviews). Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas. Prepares audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions. Compares vulnerability findings with the NIST vulnerability database, (CVE/CVSS). .**
Basic	Deploys and configures defense components. Classifies risk/vulnerabilities and applies pre-identified rating criteria. Performs predefined attack scripts and uses associated tool sets (e.g. metasploit). Completes vulnerability scan using tool set (Nessus, Core Impact, Nexpose, etc.).
Awareness	Identifies current computer network defense components. Defines the five Risk Mitigation handling options (Assume/Accept, Avoid, Control, Transfer, Watch/Monitor). Describes key elements of a penetration attack. Review risk assessment reports. Defines principles of vulnerability assessment. Identify HW/SW assets.

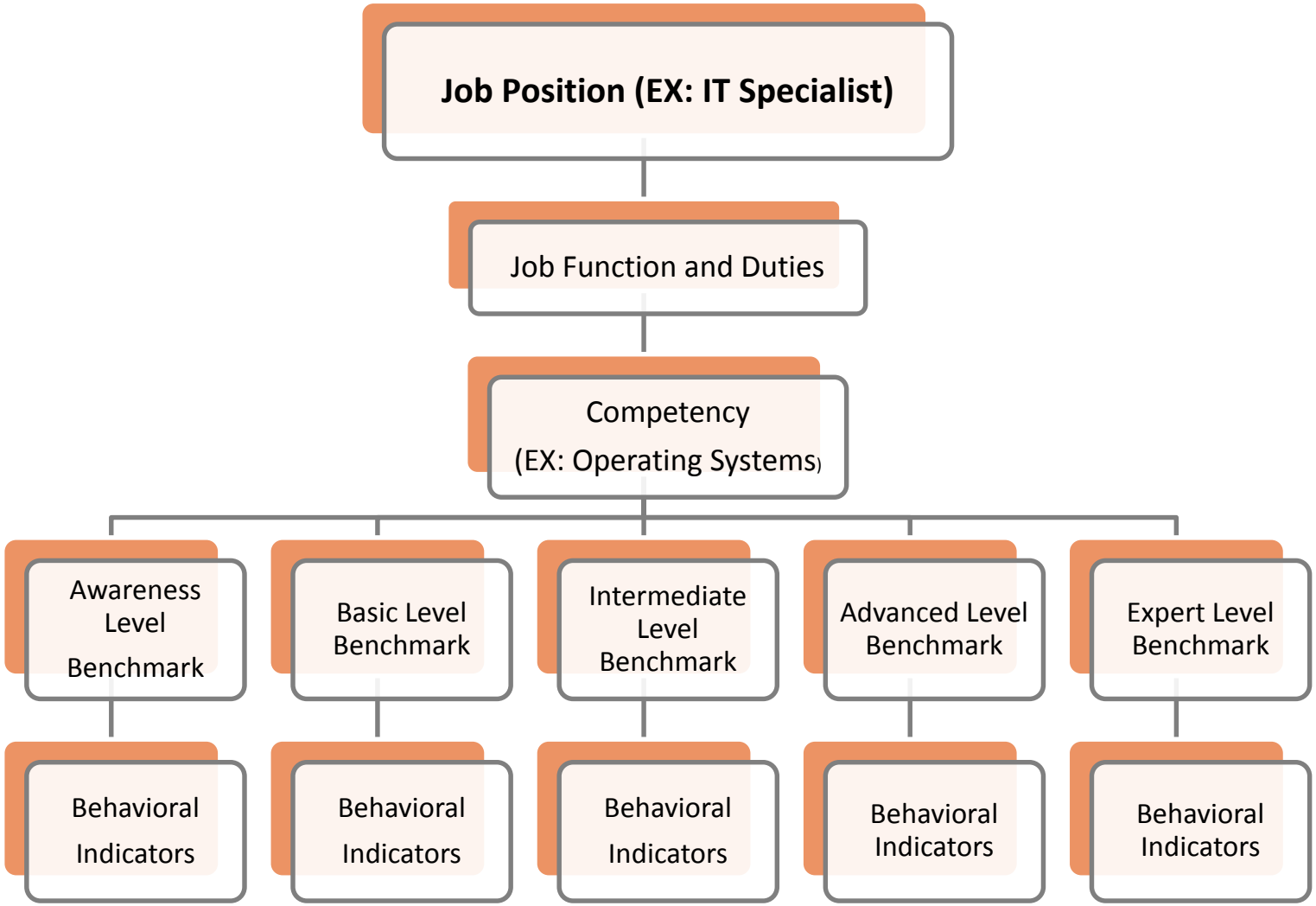
Legal Advice and Advocacy	Proficiency Level
Master	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Understands and articulates statutory considerations to be applied during investigations leading to possible criminal charges and/or Personnel Action (i.e.- 1st and 4th Amendments, Freedom of Information Act (FOIA), etc.)
Advanced	In certain environments, it may be more important to supervise or manage the tasks listed in the following behaviors. Consider each statement to include, wherever appropriate, the supervision of a task in place of the actual performance of these tasks. Evaluates contracts to ensure compliance with funding, legal, and program requirements, as appropriate. Evaluates the effectiveness of laws, regulations, policies, standards, or procedures. Evaluates, monitors, and ensures compliance with information communication technology (ICT) security policies and relevant legal and regulatory requirements. Interprets and applies laws, regulations, policies, standards, or procedures to specific issues (i.e.- SOWs, Security Incident post-mitigation, Acquisitions, etc). Ensures that contractual language is compliant with departmental requirements. Ensures that privacy documentation is accurate and current. (PIA, PTA, SORN, etc.).
Fully Proficient	Acquires and maintains a working knowledge of incident handling, including chain of evidence, and other relevant laws, regulations, policies, standards, or procedures, such that potential criminal investigations are not jeopardized by mishandling. Conducts framing of allegations to determine proper identification of applicable law, regulation, policy or guidance. Articulates applicable laws, regulations, policies, standards, and/or procedures to specific issues, formal documents or when specifying vendor requirements (i.e.- SOWs, Security Incident post-mitigation, Acquisitions, etc).
Basic	Assists to resolve conflicts in laws, regulations, policies, standards, or procedures, as appropriate.
Awareness	Distinguishes between the major categories of security incidents. Identifies laws related to information security and privacy. Recognizes the investigative considerations involved in dealing with security incidents. Categorizes laws according to the security incident they protect against.

Defining Competencies

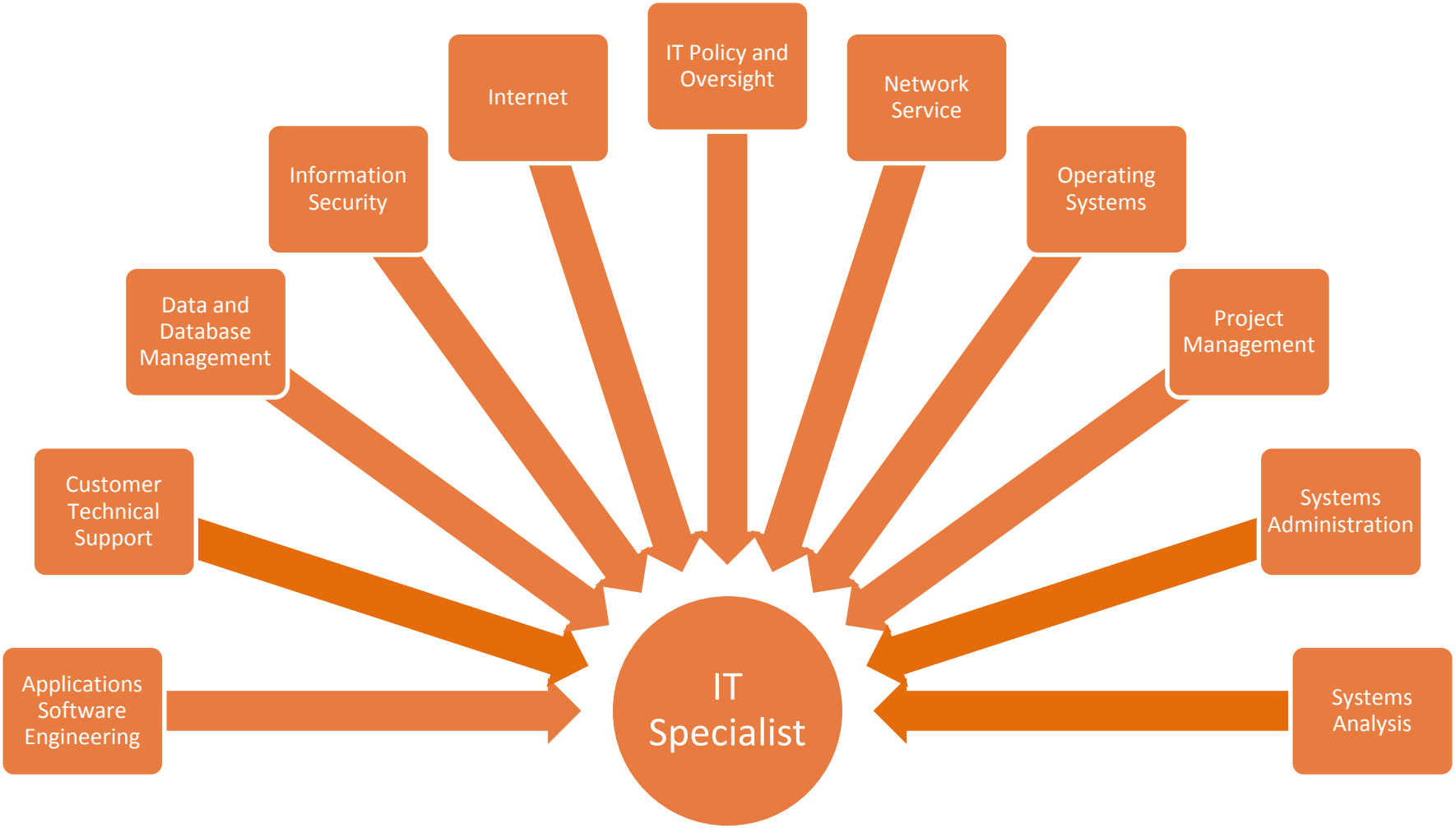
- Competency
  - A measurable pattern of knowledge, skills, abilities, or other characteristics
  - Needed to successfully perform work roles or functions
  - Differentiate performance
- Competency model
  - Collection of required competencies in an occupation or organization

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Competency Structure in AgLearn



Competency Profiles



NEXT STEPS:

- Present to the CIOs, Human Resources and the IT Workforce Working Group;
- Align to ISSPM (INFOSEC) Specialist positions;
- Establish training in AgLearn to assist in meeting identified competencies;
- Align competencies with IDPs for ISSPMs;
- Identify working groups to develop other competencies models for identified IT Workforce positions.

- Questions?


aglearn+
adding to your knowledge