State Government

Information Security Workforce Development

A Best Practice Model and Framework

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

FIGURES

Acknowledgements

Development of *The State Government Information Security Workforce Development Model*, a competency-based and functional information security workforce development framework would not have been possible without the support of the U.S. Department of Homeland Security, National Cyber Security Division; and the contributions provided by the information security leaders representing the six (6) pilot states.

Special thanks to:

U.S. Department of Homeland Security
National Cyber Security Division
Brenda Oldfield, Director
Cyber Education & Workforce Development

State of California
Mark Weatherford, Executive Officer
The California Office of Information Security & Privacy Protection

State of Florida
Mike Russo, Chief Information Security Officer
The Agency for Enterprise Information Technology (AEIT)

State of Michigan
Trent Carpenter, Director of Enterprise Security
The Department of Information Technology (DIT)

State of Minnesota
Chris Buse, Chief Information Security Officer
The Office of Enterprise Technology (OET)

State of New York
Laura Iwan, State Information Security Officer
Office of Cyber Security & Critical Infrastructure Coordination (CSCIC)

State of Texas
Bill Perez, Chief Information Security Officer
Department of Information Resources (DIR)

1.0 INTRODUCTION

1.1 OVERVIEW

Computer and information systems permeate all walks of life including home, academia, business and government. Enterprise computer architectures, a networked economy, global use of the Internet, mobile computing, wireless technologies, portable devices, etc. enable easy and immediate access to information. Online access to government information and services are available today, while state governments are increasingly moving more of their core activities to the Internet. Data sharing initiatives within and across state agencies to increase efficiencies pose new risks to data integrity and privacy.

In an ever-changing technological environment, security controls that are state-of-the-art today may be obsolete tomorrow, while new security risks and emerging threats can occur at any time, resulting in potential serious financial and legal impacts to business operations. The most common types of attacks targeting government sectors are denial of service (DoS). Ensuring data protection and maintaining an awareness of security-related risks and vulnerabilities must be addressed and maintained on an ongoing basis at the highest levels of an organization.

Led by executive management, integration of information security is an essential component supporting an organization's ability to achieve its strategic mission. By not aligning information security operations to strategic business goals and objectives, the organization faces increased security risks and the need for higher security budgets to prepare for and mitigate incidents and losses. Ensuring the security of an organization's information is also a business governance responsibility.

State agencies have a unique and critical role as the managers and caretakers of some of the largest collections of high-demand systems, applications and databases.   Data housed in these systems are subject to strict security controls and other protections by law.

In addition, state governments frequently hold data owned by the federal government and this information must be protected in accordance with regulatory requirements of the Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OMB).

FISMA applies to any system operated by or on behalf of a state government that uses federal information or that tracks the use of federal funds. Federal agencies require state agencies to obtain required FISMA documentation and to assess the compliance of state information systems. To satisfy FISMA, state agency systems must be fully FISMA compliant as defined by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB).

An increase in defining and implementing security standards and best practice guidance from the public and private sectors, as well as increased regulatory compliance will continue to affect state government information security and workforce development. Security legislation, regulations and the demand for services, higher levels of accountability, transparency and compliance are increasing, as are requirements for security controls, security awareness, and the critical need for a highly trained information security workforce.

Ensuring state government information security requires a comprehensive information security plan that aligns with organizational strategic goals and objectives, while optimizing business ownership of information security. The development of a comprehensive security program requires business and technology executive management's commitment to:

- Ensure information security is aligned to the organization's strategic mission and integrated as an essential and transparent component of enterprise governance and all organizational processes.
- Support and ensure implementation of annual security awareness training and education.
- Safeguard the integrity, availability and confidentiality of data including classifying and assigning ownership of information.
- Ensure data governance programs define business ownership of information security and include strategic oversight and accountability.
- Require staff to monitor, identify and analyze threats and vulnerabilities, and define remediation solutions in compliance with policies, standards, industry best practices
- Communicate the impacts of potential or actual security incidents in terms of how they affect business operations.
- Endorse, direct and support the management, design, implementation and evaluation of a comprehensive risk-based information security and control framework (people, policies, processes/procedures, and technology).
- Implement management and evaluation of Business Continuity Plans (testing plans in preparation for a potential event or disaster).
- Ensure that information security management has the adequate resources and have achieved the appropriate educational and professional development opportunities to support information security.
- Maximize information security resource management, including balancing technical skills with business, people and process skills.

- Continually review opportunities to improve business processes and implement new technologies to mitigate security vulnerabilities.
- Monitor, measure and report data tracking information assurance performance (in the form of regulatory compliance statistics and performance metrics).

The ability to meet these challenges and provide the infrastructure and workforce capabilities to secure information is critical. However, in today's economy and digital infrastructure, state government budget resources are severely constrained. The budget crisis is forcing many states to reduce services – including services relied upon by the most vulnerable. Across-the-board spending cuts are being imposed, state government workforces are being cut or furloughed several days a month, and hiring freezes are occurring for state government employees and many states cutting healthcare and education programs. State government information technology departments are also bearing increased business demands and government accountability and transparency responsibilities.

Additional state government information security workforce development issues include:

- A lack of information security human resource/civil service-defined position descriptions.
- Position descriptions are linked to a many generic business and/or information technology job classes.
- Lack of attributes associated with information security core competencies.
- Lack of demonstrable career paths.
- Lack of formal training plans, education and certification requirements.
- Information security professional pay is inconsistent from agency to agency.
- Occasionally, critical security functions are not accomplished due to lack of personnel with information security responsibilities.
- Information security roles and responsibilities vary significantly from agency to agency.
- Information security positions are often placed too low in the organization in terms of authority and responsibilities to be effective and sometimes do not exist at all.
- During layoffs, security professionals can be let go and replaced by people without the requisite skills.
- Difficult to assess whether candidates have the requisite information security skills during the hiring process without integration of information security competencies and skills into job descriptions and requirements.

- Difficult to recruit candidates and retain staff without a formal information security career path or professional career development plan
- Changes are needed to provide and promote:
  - Clear and consistent skill requirements
  - A common set of information security roles, responsibilities, competencies and functions to support updating existing and defining new state government information security job class, position/job descriptions and duty statements
  - Pay equity
  - Protection of security talent during layoffs
  - Career planning and professional development to keep pace with rapidly changing security threats and technology advancements
  - Integration of information security workforce development, requirements into state human resource and civil service systems.

To assist state government information security workforce development demands, advance the national information security training and certification landscape, and ensure that state government agencies have the most qualified and appropriately trained information security workforce possible, the U.S. Department of Homeland Security, National Cyber Security Division (DHS-NCSD) supported the development of this State government model for information security and workforce development based upon the DHS/NCSD *IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*.

This effort was initiated at the grassroots level by a *State Government Information Security Workforce Development Advisory Council*, comprised of six (6) pilot states (California, Florida, Michigan, Minnesota, New York and Texas) and the Information Technology Center of Excellence, a non-profit organization supporting technology best practice and education. The Council approached DHS/NCSD to propose development of a State Government Information Security Workforce Development Model utilizing the *DHS IT Security Essential Body of Knowledge (EBK)* http://www.us-cert.gov/ ITSecurity EBK/ . *The State Government Information Security Workforce Development Model* was derived from the EBK as a foundational guideline. The model consists of information security functions, roles, responsibilities, competencies, proficiency levels, education requirements, mapping to commercial “vendor-neutral” IT security certifications, career development and sample job/position descriptions.

Development of *The State Government Information Security Workforce Development Model* included collaboration with the six (6) initial pilot states representing state government information security workforce development from a centralized perspective.

Benefits of *The State Government Information Security Workforce Development Model* include:

- Collaboration with state government peers and the federal government in order to increase the importance to individual state initiatives.
- Support for a government-wide approach to reduce costs and avoidance of isolated curricula and workforce training, thereby reducing duplication of efforts.
- Foster consistency in state government information security missions.

Development of *The State Government Information Security Workforce Development Model* reinforces the benefits of utilizing the *IT Security EBK* as a foundation for information security workforce professional development and workforce management to:

- Articulate the functions that professionals within the state government information security workforce perform.
- Promote uniform competency guidelines to increase the overall efficiency of information security education, training and professional development.
- Provide a content guideline that can be leveraged to facilitate cost-effective professional development of the information security workforce, including future skills training and mappings to certifications and academic curricula.
- Provide a reference (mapping) for comparing the content of information security certifications for career advancement and/or professional development.
- Provide career path development plans aligned to specific needs.

1.2 U.S. DHS IT SECURITY ESSENTIAL BODY OF KNOWLEDGE (EBK) OVERVIEW

Information Technology (IT) Security
Essential Body of Knowledge (EBK:

A Competency and Functional Framework for IT Security Workforce Development

Excerpts from the DHS IT Security EBK:

To assist organizations and current and future members of the information security workforce, the Department of Homeland Security National Cyber Security Division (DHS-NCSD) worked with experts from academia, government and the private sector to develop a high-level framework that establishes a national baseline representing the essential knowledge and skills IT security practitioners should possess to perform - *The IT Security EBK*: *A Competency and Functional Framework for IT Security Workforce* (http://www.us-cert.gov/ITSecurityEBK/)

The federal government developed and launched the IT Security EBK to advance IT security training and certification and to help ensure the most qualified and appropriately trained IT security workforce possible. The IT Security EBK links competencies and functional perspectives to IT security roles fulfilled by personnel in the public and private sectors and builds upon the work of established references and best practices from both the public and private sectors. The EBK is not an additional set of guidelines, and is not intended to represent a standard, directive, or policy by DHS.

The IT Security EBK:

- Articulates functions that professionals within the IT security workforce perform in a common format and language that conveys the work, rather than the context in which the work is performed, i.e. private sector, government, higher education.
- Clarifies key IT security terms and concepts for well-defined uniform competencies to increase the overall efficiency of IT security education, training and workforce development.
- Identifies notional security roles.
- Defines four primary functional perspectives (Manage, Design, Implement, and Evaluate).
- Establishes an IT Security Role, Competency and Function Matrix.
- Provides a reference for comparing the content of IT security certifications and further substantiates the wide acceptance of existing certification as credentials

- Provides uniform competencies that can be utilized to increase the overall efficiency of information security professional development of the IT security workforce, including skills training, academic curricula and other affiliated human resource activities.

Development of the competency and functional framework involved close collaboration with subject-matter experts from academia, industry and government, as represented below:

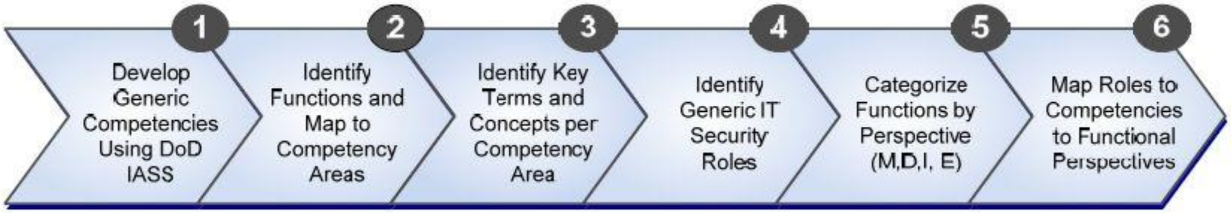

1
Develop Generic Competencies Using DoD IASS
2
Identify Functions and Map to Competency Areas
3
Identify Key Terms and Concepts per Competency Area
4
Identify Generic IT Security Roles
5
Categorize Functions by Perspective (M,D,I, E)
6
Map Roles to Competencies to Functional Perspectives

Figure 1-1 US DHS IT Security EBK Competency and Functional Framework Development Process

1. **<u>Develop Generic Competencies Using DoD Information Assurance Skills Standard (IASS</u>**)

   DHS-NCSD participated in working groups conducted by DoD to "define a common language for describing IA work and work components in order to provide commercial certification providers and training vendors with targeted information to enhance their learning efforts." (*DoD Information Assurance Skill Standard (IASS) – part of DoD 8570.1-M*)

   The DoD IASS defines information assurance (IA) work within DoD according to critical work functions (CWF), each of which contains multiple tasks. DHS-NCSD reverse-engineered the DoD IASS document to obtain the set of technical competency areas to which these CWFs and tasks were aligned. Each area was given a functional statement/definition to clarify what it would include

2. **<u>Identify Functions and Map to Competency Areas</u>**

   Once competency areas were developed, DoD IASS CWFs were mapped to them. Other IT Security documents were also analyzed to identify the functions associated with each area (*National Institute of Standards and Technology (NIST) standards, Committee on National Security Systems (CNSS) standards, International Organization for Standardization (ISO) standards, private sector models – Control Objectives for Information and Related Technology (COBIT®), and Systems Security Engineering Capability Maturity model (SSE CMM)*). Data were captured as functions rather than job tasks to allow the terminology and procedural specificity of the sectors from which the data originated to be replaced by more general language that would apply to all sectors.

   The EBK emphasized the functional statements. Training and education opportunities should be pursued to an IT security professional's knowledge of a competency

3. Identifies Key Terms and Concepts per Competency Area

Key terms and concepts from all of the IT Security competency areas make up the “essential body of knowledge” that is needed by a generalist in the IT security field. Because the scope of professional responsibility of practitioners performing IT security functions varies widely, knowledge of key terms and concepts is fundamental to performance. At a minimum, individuals should know the key terms and concepts that correspond with the competencies mapped to their role. The DHS EBK identified the following Key Terms and Conepts:

The competency areas identified by the EBK are:

- Data Security
- Digital Forensics
- Enterprise Continuity
- Incident Management
- IT Security Training and Awareness
- IT Systems Operations and Maintenance
- Network and Telecommunications Security
- Personnel Security
- Physical and Environmental Security
- Procurement
- Regulatory and Standards Compliance
- Security Risk Management
- Strategic Security Management
- System and Application Security

4. Identify Generic IT Security Roles

After competencies were adequately populated with functions, and key terms and concepts were recognized, a set of generic roles performed by professionals in the IT security field were identified. Roles, rather than job titles were chosen to eliminate IT sector-specific language and accurately capture the multitude of IT security positions in a way that would allow a practitioner to easily identify his or her role. The notional roles identified by the EBK:

The notional roles identified by the EBK are:

- Chief Information Officer
- Digital Forensics Professional
- Information Security Officer
- IT Security Compliance Officer
- IT Security Compliance Officer
- IT Security Engineer
- IT Systems Operations and Maintenance Professional
- IT Security Professional
- Physical Security Professional
- Privacy Professional
- Procurement Professional

5. Categorize Functions by Perspective: Manage (M), Design (D), Implement (I), Evaluate (E)

Once roles were identified, competencies were revisited. Specifically, the CWFs within each competency were categorized into one of the four functional perspectives of Manage, Design, Implement, or Evaluate.

> ***Note:*** *These perspectives do **not** convey a lifecycle concept of task or program execution as is typical of a traditional system development lifecycle, but are used to sort functions of a similar nature.*

- **Manage**: Functions that encompass overseeing a program or technical aspect of a security program at a high-level and ensuring currency with changing risk and threat environments.

- **Design**: Functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.

- **Implement**: Functions that encompass putting programs, processes, or policies into action with an organization.

- **Evaluate**: Functions that encompass assessing the effectiveness of a program, policy, process or security service in achieving its objectives.

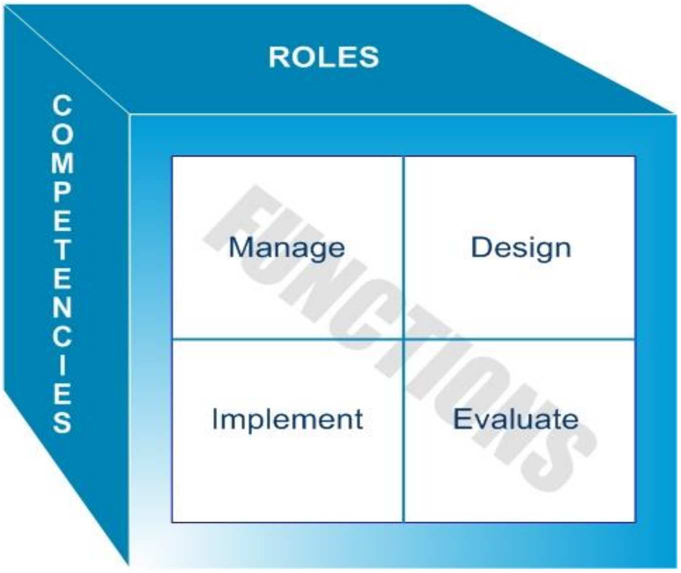


Figure 1-3 Mapping Diagram: Roles to Competencies to Functions

6. Map Roles to Competencies to Functional Perspectives

The final step involved mapping the roles to appropriate sets of competencies and identifying the specific functional perspective that described work performed in that role.   This activity also created the *IT Security Role, Competency and Functional Matrix*. When a role is mapped to a competency, and to a functional perspective within that competency, the role performs *all* of the functions within the perspective.

Work conducted by the IT security workforce is complex and not all work in a given area is performed by a single role. This work – from creating the strategy for a portion of the IT security program, to developing a program's procedures and scope, to performing hands-on implementation work, to evaluating the work's effectiveness – is performed by a team of individuals with different responsibilities and spans of control. Rather than all roles being responsible for knowing all areas of IT security and having the ability to perform all job tasks, individual roles are associated with a subset of competencies to represent the work performed as part of the IT security team. The type of work performed is resolved by role through the four functional perspectives across a series of technical competency areas. It is on these functions that an individual should be evaluated if a role-based certification truly measures the individual's ability to perform.

1.3 Review Cycle

The State Government Information Workforce Development Model first draft was completed in December 2009. DHS-NCSD, in collaboration with the State Information Security Advisory Council presented the model to the Multi-State Information Sharing and Analysis Center (MS-ISAC) which is coordinating the model's introduction to state governments for review and comment.

The State Government Information Security Workforce Development Model will be re-evaluated periodically to ensure that the content and overall structure remains relevant to state government information security workforce development goals and objectives.

1.4 Model Organization

The remaining sections of this document are organized as follows:

- **Section 2.0 – State Government Information Security Model**

  (Model Methodology, Information Security Competency Model, Competency-Based HR Model, Information Security Competencies, Competency Structure, Individual/Core Attributes, Proficiency Levels, Individual Competencies)
- **Section 3.0 – Information Security Roles and Functional Perspectives** (Chief *(Information Security Officer, Privacy Officer, Information Security Officer or Manager, Compliance Officer (Information Assurance), Information Security Engineer, Information Security Professional, Information Security Operations and Maintenance, Information Security System Administration Professional)*
- **Section 4.0 – State Government Information Security Competency and Functional Matrix**
- **Section 5.0 – State Government Information Security Job/Position Descriptions**
- **Section 6.0 – Information Security Career Planning**
- **Appendices**
  - ***Appendix I - State Government Information Security Competencies***
  - ***Appendix II - State Government Information Security Position/Job Descriptions***
  - ***Appendix III - Information Security Certification Dictionary and Mapping Matrices***
  - ***Appendix IV - Glossary of Key Terms and Concepts***

2.0 STATE GOVERNMENT INFORMATION SECURITY MODEL

The State Government Information Security Competency Model creates a common foundation and consistent framework to integrate information security roles and competencies into existing and new job classifications, and the specification of job/position descriptions/duty statements, etc.

Competency management supports alignment of individual performance to strategic business objectives and goals. Individual state government human resource management processes define the way the competency model will be used to support other initiatives throughout the enterprise (e.g., knowledge management, professional training and education, and workforce management).

2.1 INFORMATION SECURITY MODEL DEVELOPMENT METHODOLOGY

The methodology utilized in competency development for *The State Government Information Security Model* is defined below:

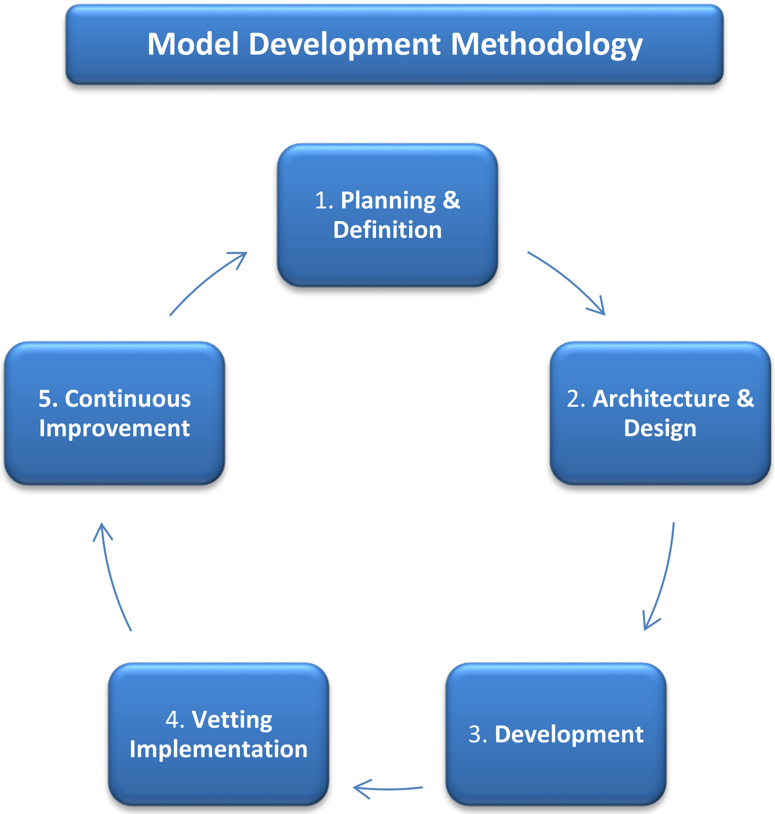

Model Development Methodology
1. Planning & Definition
2. Architecture & Design
3. Development
4. Vetting Implementation
5. Continuous Improvement

Figure 2-1 Information Security Model Development Methodology

1. Planning and Definition

- Planning Purpose - Tied to supporting state government information security workforce development and management requirements.
- In collaboration with the U.S. Department Homeland Security/National Cyber Security Division, established the State Government Information Security Advisory Group consisting of six (6) pilot states (California, Florida, Michigan, Minnesota, New York, and Texas).
- Defined project vision and supporting work (project) plan.

2. Architecture and Design

- Conducted on-site visits with each of the above six (6) states. Captured information security organizational goals and objectives from a centralized perspective including current snapshot-in-time, key job roles/responsibilities and validation of critical information security competencies required for job success.
- Compared results to industry best practice (public/private), information security standards, and the DHS/NCSD IT Security Essential Body of Knowledge (EBK).
- Utilizing the DHS/NCSD IT Security Essential Body of Knowledge (EBK) as a foundational guideline, designed the architecture of the State government information security competency framework to support:
  - Mapping to existing job classifications and job/position descriptions/duty statements
  - Creation of new job classifications and job/position descriptions/duty statements that are information security specific
- Mapped competencies to existing preferred state government information security certifications.

  Note: Certification mappings included vendor-neutral information security certifications. Vendor product-specific certifications are not included.
- Designed information security career paths from entry-level (basic knowledge) to two (2) perspectives:
  1. Functional (Technical)
  2. Executive (Managerial)

3. Construction

- Incorporated DHS/NCSD IT Security Essential Body of Knowledge (EBK) competencies elements into competency model detail.
- Incorporated additional competencies identified by state government pilot states.
- Incorporated proficiency levels, education, and work experience.
- Mapped competencies to state government pilot states' job roles/descriptions.
- Initial Publication – Draft.
- Draft Model Refinement.

4. Implementation

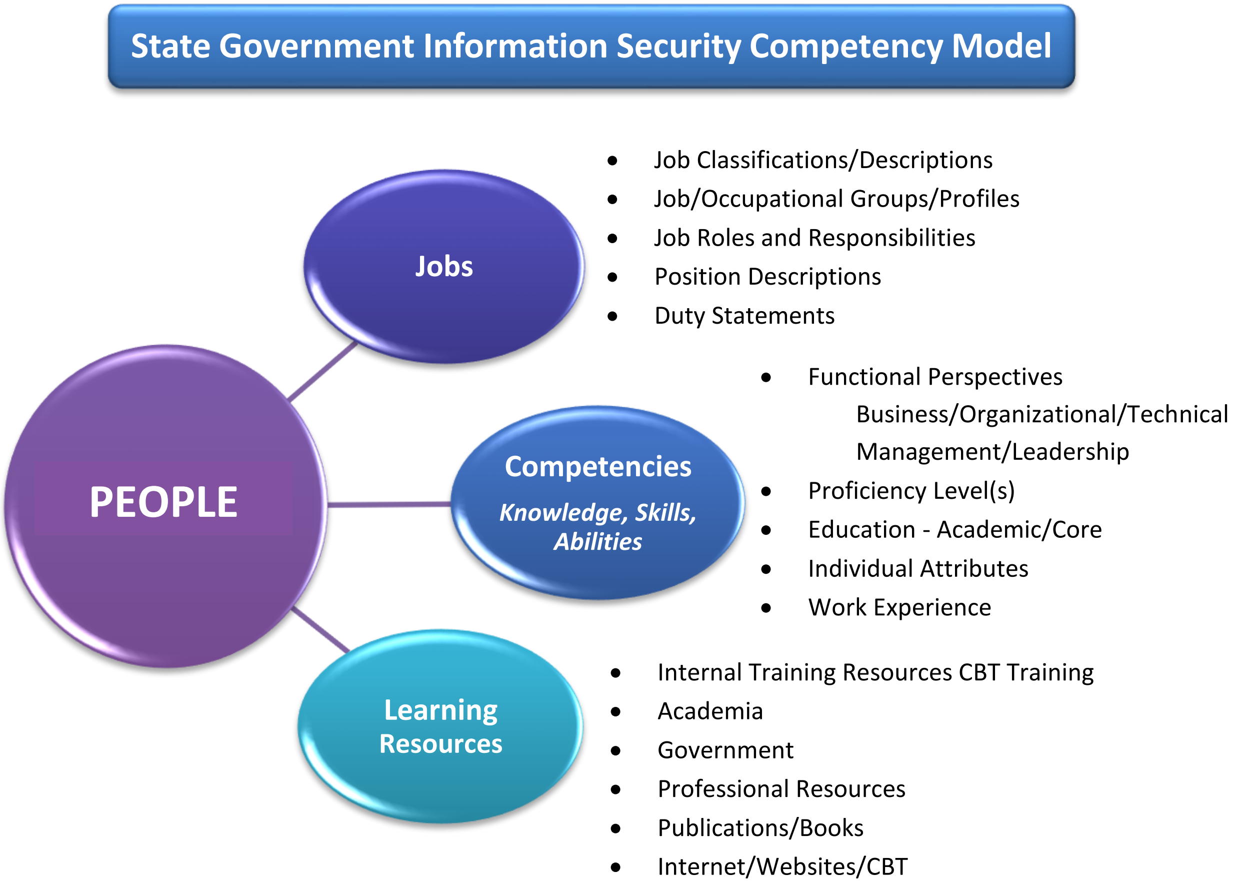
- Ensure Refined and Approved Model Design is Relevant and Usable.
- Vet Model – All State Governments via coordination by U.S. Department Homeland Security (e.g., MS-ISAC, NASCIO, etc.).
- State Government Information Security Website - Upon completion of vetting *The State Government Information Security Model* and updating/editing appropriately to represent comments/recommendations from all states., the model will be reflected in an interactive website providing access to the best practice model and a forum to support model continuous improvement.
- Support state implementation.

5. Maintenance

- Implement Continuous Improvement via the established feedback mechanism (*State Government Information Security Model* website).
- Repeat Steps 1-4.

2.2 INFORMATION SECURITY COMPETENCY MODEL

The State Government Information Security Competency Model taxonomy is derived from core state government information security roles and responsibilities (job classifications/descriptions/ profiles, position descriptions, duty statements, etc.) represented by the State Government Information Security Advisory Group and integration of the U.S. Department Homeland Security IT Security Essential Body of Knowledge (EBK).


State Government Information Security Competency Model
Jobs
PEOPLE
Competencies
Knowledge, Skills, Abilities
Learning Resources

- Job Classifications/Descriptions
- Job/Occupational Groups/Profiles
- Job Roles and Responsibilities
- Position Descriptions
- Duty Statements

- Functional Perspectives
  Business/Organizational/Technical
  Management/Leadership
- Proficiency Level(s)
- Education - Academic/Core
- Individual Attributes
- Work Experience

- Internal Training Resources CBT Training
- Academia
- Government
- Professional Resources
- Publications/Books
- Internet/Websites/CBT

Figure 2-2 State Government Information Security Competency Model

JOBS

Current state government HR information technology job classifications/descriptions are generic and do not represent information security specificity. Associated job descriptions/position descriptions/duty statements support providing the detail required to communicate required information security roles, responsibilities, functions, skills, and education. Many state government information security organizations desire to update existing or develop new job classifications and associated job descriptions/position descriptions, etc. to represent information security as an independent occupational group that accurately reflects information security roles and responsibilities.
Many states have moved forward to adopt a best-practice human resource model that defines the work performed in various occupations by competency (knowledge, skills, abilities and personal characteristics) and proficiency levels. In order to represent a State government information security workforce development best practice competency-based model, organizational state government human resources/civil service workforce policies, regulations, statutes, guidelines, etc. must be addressed. <u>Any changes to or development of new job classifications, job descriptions/position descriptions, etc. must be in compliance to human resource and collective bargaining policies and procedures, as they apply to each state and existing or new occupational groups</u>.

COMPETENCIES

Competencies are a combination of the knowledge, skills and abilities required to perform a job successfully (functions, proficiencies, education, individual attributes and work experience). Developing individuals who can both master individual competencies and apply them are critical success factors. Competencies support definitions of job classifications/occupational group profiles, roles and responsibilities, position descriptions, duty statements, etc.

LEARNING RESOURCES

Learning resources support competency achievement, future professional development, certifications, etc. Providing a supporting training and skills development process in concert with access to learning resources, both internally and externally will reinforce continuous learning and professional development providing a clear link to achievement of defined proficiency levels and career path opportunities.

2.3 COMPETENCY-BASED HUMAN RESOURCE (HR) MODEL

The State government best practice competency-based HR model is comprised of:

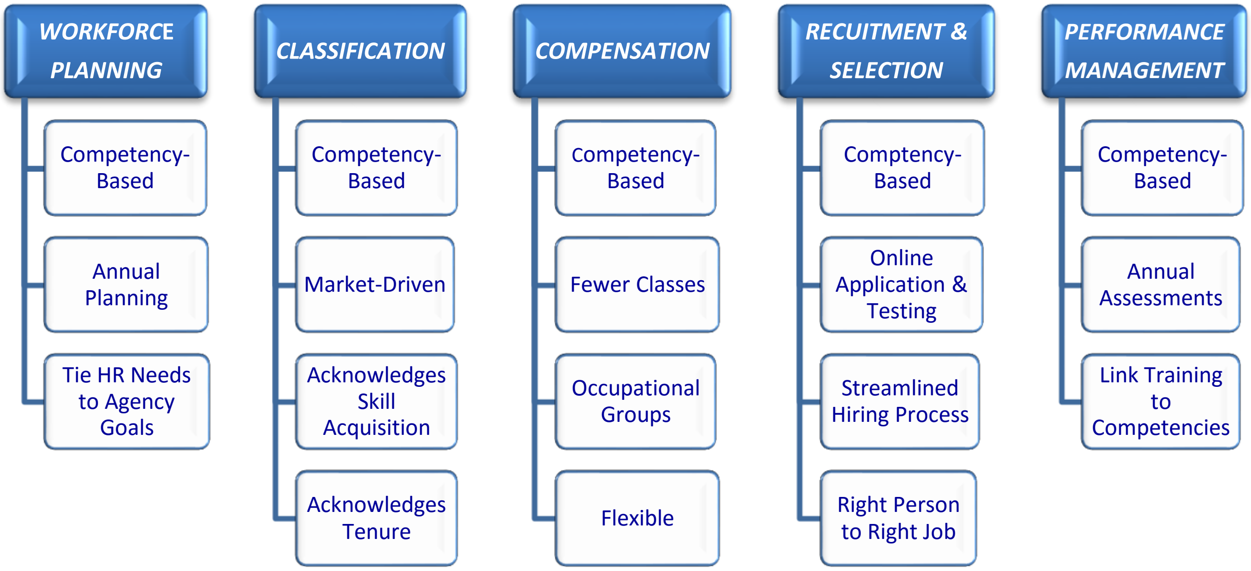


Figure 2-3 Competency-Based Human Resource (HR) Model

The information security workforce will be the drivers and end-users of this competency model. They provide the organizational knowledge, functions, and roles and responsibilities representing state government information security and are an essential resource to support competency model continuous improvement.

2.4 INFORMATION SECURITY COMPETENCIES

2.4.1 INFORMATION SECURITY COMPETENCY STRUCTURE

The structure of each state government information security competency includes:

- ✓ **Competency Name -** Name of the information security competency area.
- ✓ **Definition** – Competency core definition.
- ✓ **Key Terms and Concepts** - List of terms and concepts associated to a competency that identifies the basic knowledge that professionals should have to be conversant in the field of information security and to perform the required work functions.
- ✓ **Core/Individual Attributes and Competencies** – Common to all information security competencies. *(Refer to Section 2.4.2)*
- ✓ **Proficiency Levels** –Required to achieve competency. Applied to meet individual job position roles and responsibilities. *(Refer to Section 2.4.3)*
    - Not Applicable
    - Entry-Level (Basic Knowledge)
    - Intermediate (Practical Application)
    - Advanced (Applied Theory/Recognized Authority).
- ✓ **Certifications** – Represents the associated information security vendor-neutral certification(s).
- ✓ **Sample Job Titles** - Represents state government job title examples.
- ✓ **Functional Perspectives - Manage/Design/Implement/Evaluate:** (For each functional perspective)
    - Definition – Functional Perspective
    - Proficiency Level – Required to achieve competency
    - Work Experience – Required to achieve competency.
    - Education: Academic/Core Requirements – Required core academic education requirements to achieve competency.

2.4.2 INDIVIDUAL/CORE ATTRIBUTES

All individual/core competencies are provided for each competency. Selection of individual /core attributes are based on individual state government information security job/position descriptions or duty statements.

- **Leadership/Management** - Supervision, direction and guidance to individuals and groups in completion of tasks and goals. Competencies support the adaptive behaviors required to support strategic vs. tactical goals and objectives, and potential shifting organizational demands.

- **Human Relationship/Collaboration** – Interpersonal skills to support collaboration and to resolve conflicts.

- **Consulting/Research** – Specific knowledge and ability to conceptualize research and plan future needs and solutions for meeting those needs.

- **Communication** – Skills to support effective and results-oriented communication.

- **Computing/Internet** – Basic computer and Internet/Intranet knowledge and skills

- **Organizational Awareness** – Knowledge specific to the organization, and position in the organization with respect to subject domain.

- **Basic Skills**– Day-to-day skills that assist in promoting effective production and work satisfaction.

- **Personal Attributes** - Represent the knowledge, skills and abilities that result in personal effectiveness, successful achievements and effective interactions with others. Competencies reside on a foundation of behavioral success factors that align to different types of environmental drivers. These basic, but critical requirements comprise the set of personnel attributes.

Leadership/ Management	Human Relationship/ Collaboration	Consulting/ Research	Communication	Computing/ Internet	Organizational Awareness	Basic Skills	Personal Attributes
Global Perspective	Assess Needs	Needs Analysis/ Assessment	Writing Effectively & Concisely	Knowledge of Subject Domain	Knowledge of Organization's Goals and Objectives	Day-to-Day Skills that Assist in Promoting Effective Production and Work Satisfaction	Ethics & Integrity
Vision & Strategic Planning	Understand Enterprise Goals & Objectives	Research	Speaking Effectively	Working Knowledge of Computer/ Internet, Operating Systems, Hardware	Knowledge of Role within Organization	Customer Focus	Personal Credibility
Creative & Innovative Thinking	Understand Organization Structure	Organization Awareness	Presentation	Knowledge of Internet Technology, Web-Services/ Applications, E-Business, etc.	Understanding Subject Domain Impact on Organization	Decision-Making & Implementation	Personal Confidence
Risk Management	Relationship Building	Project Planning	Listening		Understanding Business Processes	Cooperation	Self-Discipline
Delegation	Listening	Negotiation	Facilitation		Understanding Business Division/ Department Interrelationships	Enforce Policies	Analytical & Creative Thinking
Setting and Monitoring Goals and Objectives to Organizational Goals	Motivation	Teamwork	Interviewing			Punctuality	Thoroughness

Leadership/ Management	Human Relationship/ Collaboration	Consulting/ Research	Communication	Computing/ Internet	Organizational Awareness	Basic Skills	Personal Attributes
Group / Project Management	Problem Resolution	Maintaining Confidentiality	Communication Styles			Time Management	Quest for Learning
Teamwork	Ability to Share Credit	Listening	Negotiation/ Persuading/ Influencing			Flexibility	Optimism
Resource Management	Foster Diversity	Analytical	Representing Security Incidents in Business & Technology Language			Attending to Detail	High Level of Energy
Presentation	Foster Cooperation	Presentation	Conflict Resolution			Meeting Goals	Accepts Responsibility
Evaluation	Delegating with Respect	Monitoring				Enlisting Help when Needed	Commitment
Planning and Organization	Mentoring	Evaluation				Accepting Responsibility	Dependability
Forecasting	Representing Others	Resource Management				Setting and Meeting Deadlines	Organization
Negotiation/ Problem Resolution	Respect Values of Others					Organization	Teamwork
Change Leadership	Verbal, Non-Verbal					Decision-Making	Effective Communication Skills
Financial Management	Writing Effectively						
Monitoring Compliance	Maintaining Confidentiality						

Leadership/ Management	Human Relationship/ Collaboration	Consulting/ Research	Communication	Computing/ Internet	Organizational Awareness	Basic Skills	Personal Attributes

2.4.3 INFORMATION SECURITY PROFICIENCY LEVELS

Information Security Proficiency Levels	
Not Applicable	Not required to apply or demonstrate this competency. This competency is not applicable to the position.
Entry-Level ***(Basic Knowledge)***	Limited Experience, basic knowledge. Level of experience has been gained in a classroom and/or experimental scenarios or as a trainee on-the-job. Help or mentoring will be needed in performing this skill. Demonstrates basic understanding of information security concepts, common knowledge and its application to computer systems architecture. Ability to understand and discuss terminology, concepts and principles, and issues related to this competency. Focus is on learning and development of on-the-job experience.
Intermediate ***(Practical Application)***	Practical Application. Demonstrates solid information security knowledge and possesses the ability to apply the competency with minimal or no guidance in the full range of typical situations. Would require guidance to handle novel or more complex situations. Able to successfully complete tasks in this competency as requested. Competency has been applied to situations occasionally while needing minimal guidance to perform successfully. Help or mentoring from an expert may be required from time-to-time, but the skills can be performed independently. Focus is on applying and enhancing knowledge and skill sets. Ability to understand and discuss competency context and implications of changes to processes, policies, and procedures in this area.
Advanced ***(Applied Theory, Recognized Expert)***	Applied Theory. Recognized Authority. Demonstrates expert understanding, knowledge and a broad advanced understanding, knowledge and ability in multiple information security subjects. Can apply the competency in new or complex situations. Demonstrates expert knowledge of law, regulation, policies and procedures, and information security standards including the ability to interpret and translate subject matter to various audiences. Actions can be performed associated with this skill without assistance. Recognized within organization as knowledgeable and a "person to ask" when difficult questions arise regarding this competency. Focus in on broad organizational/professional issues. Provide consistent, practical, and relevant ideas and perspectives on process or practice improvements which may easily be implemented. Capable of coaching and mentoring others in the application of this competency by translating complex nuances relating to this competency into easy to understand terms in a business and/or technology context. Participate in senior and executive level discussions regarding this competency. Assists in development of reference and resource materials related to this competency.

Information Security Proficiency Levels	

2.4.4 INFORMATION SECURITY COMPETENCIES

The fifteen (15) information security competencies defined below comprise *The State Government Information Security Model* competency areas.

Detailed competency information including Competency Key Terms and Concepts, Core/Individual Attributes, Proficiency Levels, Certifications, Sample Job Titles, and Functional Perspective Statements are provided in -

APPENDIX I

State Government Information Security Competencies

1. **Data (Information) Security**

   Refers to the application of the principles, policies and procedures necessary to ensure the confidentiality, integrity, availability and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle.

2. **Digital Forensics**

   Refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating and analyzing electronic data to reconstruct events related to security incidents. Such activities require building a digital knowledge base. The investigative process is composed for our (4) phase: Prepare, Acquire, Analyze and Report.

3. **Enterprise Architecture**

   Refers to the practice of applying security design principles to applications, and architecting enterprise-scale security solutions, infrastructure, processes and business activities.

4. **Enterprise Continuity (Disaster Recovery)**

   Refers to the application of the principles, policies and procedures to ensure than an enterprise continuous to perform essential business functions after the occurrence of a wide range of potential catastrophic events.

5 Incident Management

Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate and recover, and the ability to apply lessons learned from incidents impacting the mission of an organization.

6. Information Security Training and Awareness

Refers to the principles, practices and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills and abilities. Training activities are designed to instruct workers about their security responsibilities and teach them about information security processes and procedures to ensure duties are performed optimally and securely within related environments. Awareness activities present essential information security concepts designed for the workforce and to affect user behavior.

7. IT Systems Operations and Maintenance

Refers to the ongoing application of principles, policies and procedures to maintain, monitor, control and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended.

8. Network and Telecommunications Security

Refers to application of the principles, policies and procedures involved in ensuring the security of basic network and telecommunications services and data, and in maintaining the hardware layer on which it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

9. Physical and Personnel Security

Physical Security - Refers to methods and controls used to proactively protect an organization from natural or manmade threats to physical facilities and buildings, as well as to the physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations). Physical and environmental security protects an organization's personnel, electronic equipment and data/information.

Personnel Security - Refers to methods and controls used to ensure than an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information and non-compliance. These controls include organization/ functional design elements such as separation of duties, job rotation and classification.

10. Privacy

Refers to the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

State and federal law require state agencies to collect, display, retain, destroy, and dispose of records that contain personal identifying information of the residents of this state.

The collection, display, retention, destruction, and disposal of records containing the personal identifying information of state residents exposes the state and its residents to security risks, including, but not limited to, identify theft and other privacy violations.

Federal privacy law, including, but not limited to, the Privacy Act of 1974, Public Law 93-579, 5 USC 552a; the Right to Financial Privacy Act of 1978, Public Law 95-630, 12 USC 3401; and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 42 USC 1320d, impose restrictions on the collection, display, retention, destruction, and disposal by government agencies of records containing an individual's personal identifying information.

The Identity Theft Protection Act, 2004 PA 452, MCL 445.72, as amended by 2006 PA 566, requires that state departments and agencies that own or license personal information included in a database or that maintain a database of personal information notify residents of this state of the unauthorized access and acquisition of that information if the department or agency determines that the security breach is likely to cause substantial loss or injury, or result in identity theft to that resident.

State government is firmly committed to ensuring not only that government is accountable for the personal information and personal identifying information of state residents for which it is responsible, but that the residents of the state understand the manner in which their personal identifying information is collected, displayed, retained, destroyed, and disposed of by state government and understand their rights when that information is used or accessed without authorization.

11. **Policies, Standards and Compliance (Information Assurance)**

Refers to the application of the principles, policies and procedures that enable an enterprise to meet applicable information security laws, standards and policies to satisfy statutory requirements, perform industry-wide best practices and achieve information security program goals.

Information Assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability and non-repudiation.

12. **Procurement**

Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements (SLA), justifications required by policies or procedures, and contract administration plans.

13. **Security Risk Management**

Refers to the policies, processes, procedures and technologies used by an organization to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment and to manage mitigation strategies that achieve the security needed at an affordable cost.

14. **Strategic Security Management**

Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic security management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints.
The goal of these analyses is to ensure that an organization’s IT security principles, practices, and system design are in line with its mission statement.

15. Systems and Application Security

Refers to the principles, policies and procedures pertaining to integrating information security into an IT system or application during the SDLC prior to the Operations and Maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation and software security standards compliance.

3.0 INFORMATION SECURITY ROLES, COMPETENCIES AND FUNCTIONAL PERSPECTIVES

Eight roles have been identified to segment the many job titles within the state government information security workforce into manageable functional groups. Each of these roles represents a cluster of organizational positions/job titles that perform similar functions in the workplace with the appropriate information security competencies.

3.1 CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer (CISO) specializes in the information and physical security strategy within an organization supporting the strategic use and management of information, information systems and information technology. The CISO is charged with the development and subsequent enforcement of the organization's security policies and procedures, security awareness and education programs, business continuity and disaster recovery plans, and all security-related regulatory compliance issues.

Competencies:

- **Data (Information) Security**: *Manage, Evaluate*
- **Digital Forensics**: *Manage, Evaluate*
- **Enterprise Architecture**: *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Manage*
- **Incident Management**: *Manage*
- **Information Security Training and Awareness**: *Manage*
- **IT Systems Operations and Maintenance**: *N/A*
- **Network and Telecommunications Security**: *Evaluate*
- **Physical and Personnel Security**: *Manage*
- **Policies, Standards and Compliance (Information Assurance:)** *Manage, Evaluate*
- **Privacy**: *Manage, Design, Evaluate*
- **Procurement**: *Manage, Design, Evaluate*
- **Security Risk Management**: *Manage, Design, Implement, Evaluate*
- **Strategic Security Management**: *Manage, Design, Implement, Evaluate*
- **System and Application Security**: *Manage, Evaluate*

Example Job Titles :

- **Chief Information Security Officer (CISO)**

- **Executive Director, Information Security**
- **Director, Information Security**

3.2 PRIVACY OFFICER

The Privacy Officer is responsible for developing and managing an organization's privacy compliance program. Privacy implementation is the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. The Privacy Officer establishes a risk management framework and governance model to assure the appropriate handling of Personally Identifiable Information (PII) and ensures that PII is managed throughout the information life cycle from collection to disposal. Included is integration of the appropriate privacy security controls and technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

Competencies:

- **Data (Information) Security**: *Manage, Design, Evaluate*
- **Digital Forensics**: *Evaluate*
- **Enterprise Architecture**: *N/A*
- **Enterprise Continuity (Disaster Recovery)**: *Evaluate*
- **Incident Management**: *Manage, Design, Implement, Evaluate*
- **Information Security Training and Awareness**: *Design, Evaluate*
- **IT Systems Operations and Maintenance**: *N/A*
- **Network and Telecommunications Security**: *N/A*
- **Physical and Personnel Security**: *Design, Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Design, Implement, Evaluate*
- **Privacy**: *Manage, Design, Implement, Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Manage, Design, Implement, Evaluate*
- **Strategic Security Management**: *N/A*
- **System and Application Security**: *Evaluate*

Example Job Titles :

- **Chief Privacy Officer (CPO)**
- **Privacy Officer (PO)**

- **Privacy Specialist**

3.3 INFORMATION SECURITY OFFICER OR MANAGER

The Information Security Officer (ISO) or Information Security Manager (ISM) specializes in the information and physical security strategy within an organization. The ISO or ISM is charged with the development and subsequent enforcement of the organization's policies and procedures, security awareness program, business continuity and disaster recovery plans, and all industry and governmental compliance issues. The ISO or ISM reports to the Agency Director (Secretary, Commissioner, etc.). The ISO or ISM:

- Manages an agency's information security program by overseeing and ensuring agency compliance with policies and procedures regarding the security of information assets.
- Must be of a sufficiently high-level job classification and/or position/job description that can execute the responsibilities of the office in an effective and independent manner.
- Establishes security policies and procedures.
- Understand the business process needs.
- Assesses internal and external risks and the respective business impact.
- Provide appropriate mitigation strategies.
- Stay current on state statutes, state/federal laws and regulations.
- Provide oversight responsibility at the agency level for ensuring the integrity and security of automated files, databases, and computer systems.
- Provides approval of proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data
- Determine aforementioned proposals meet all provisions of agency information security and risk management policies
- Approves the use of alternatives to support encryption for the protection of confidential, personal and sensitive information stored on portable electronic storage media and portable computing devices
- Approves any business use of peer-to-peer technologies

Competencies:

- **Data (Information) Security**: *Manage, Design, Evaluate*
- **Digital Forensics**: *Implement*
- **Enterprise Architecture**: *N/A*

- **Enterprise Continuity (Disaster Recovery)**: *Evaluate*
- **Incident Management**: *Design, Implement, Evaluate*
- **Information Security Training and Awareness**: *Design, Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *N/A*
- **Network and Telecommunications Security**: *N/A*
- **Physical and Personnel Security**: *Manage, Design, Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Manage, Design, Implement, Evaluate*
- **Privacy**: *Implement*
- **Procurement**: *N/A*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Evaluate*

Example Job Titles :

- **Information Security Officer**
- **Information Security Manager**
- **Information Security Agency Lead**

3.4 COMPLIANCE OFFICER (INFORMATION ASSURANCE)

The Compliance Officer is responsible for overseeing, evaluating and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Compliance Office provides guidance and autonomous evaluation of the organization to management.

Information Assurance practitioners ensure, verify and validate the protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and protection against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Competencies:

- **Data (Information) Security**: *Evaluate*

- **Digital Forensics**: *Evaluate*
- **Enterprise Architecture**: *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Evaluate*
- **Incident Management**: *Evaluate*
- **IT Security Training and Awareness**: *Design, Evaluate*
- **IT Systems Operations and Maintenance**: *Evaluate*
- **Network and Telecommunications Security**: *Evaluate*
- **Physical and Personnel Security**: *Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Manage, Design, Implement, Evaluate*
- **Privacy**: *Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Implement, Evaluate*
- **Strategic Security Management**: *Evaluate*
- **System and Application Security**: *Evaluate*

Example Job Titles :

- **Compliance Officer**
- **Inspector General**
- **Certification and Accreditation Engineer**
- **Information Assurance Engineer**
- **Analyst**
- **Specialist**
- **Risk Assurance Specialist**
- **Software Quality Assurance Analyst**
- **Computer Systems Validation Engineer**
- **Cyber Security Analyst**
- **Project Director**
- **Project Manager**

3.5 INFORMATION SECURITY ENGINEER

The Information Security Engineer applies cross-disciplinary IT and information security knowledge to build technology systems that remain dependable in the process of conducting business and in the face of malice, error and mischance.

Competencies:

- **Data (Information) Security**: *Design, Implement, Evaluate*
- **Digital Forensics**: *Design, Evaluate*
- **Enterprise Architecture**: *Manage, Design, Implement*, *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement, Evaluate*
- **Incident Management**: *Design, Implement, Evaluate*
- **IT Security Training and Awareness**: *Design, Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Design, Implement, Evaluate*
- **Network and Telecommunications Security**: *Manage, Design, Implement*, *Evaluate*
- **Physical and Personnel Security**: *Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance)**: *Implement*
- **Privacy**: *Design, Evaluate*
- **Procurement**: *Design, Evaluate*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **Information Security Engineer**
- **Information Security Architect**
- **Systems Engineer**
- **Technology (Data) Center Operations Engineer or Manager**
- **Operations Manager**
- **Systems Analyst**
- **Digital Forensics Manager**
- **Risk, Security and Facilities Specialist**
- **Information Technology Infrastructure Analyst**
- **Systems Analyst**
- **Information Security Analyst**
- **Requirements Analyst**
- **Software Architect**

3.6 INFORMATION SECURITY PROFESSIONAL

The Information Security Professional concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.

The Information Security Professional also includes the Information Security Procurement Professional. The Information Security Procurement Professional is responsible for purchasing and negotiating for products (e.g., software and hardware) and services (e.g., contractor support) in support of an organization's IT strategy. In the information security context, they must ensure that security requirements are specified within solicitation and contract documents (Sarbanes-Oxley, FISMA, etc.) and that only products and services meeting requirements are procured. Information Security Procurement Professionals must be knowledgeable about their industry and their own organization, and must be able to effectively communicate with supplies and negotiate terms of service.

Competencies:

- **Data (Information) Security**: *Design, Implement*
- **Digital Forensics**: *Implement, Evaluate*
- **Enterprise Architecture**: *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement, Evaluate*
- **Incident Management**: *Design, Implement,, Evaluate*
- **IT Security Training and Awareness**: *Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Evaluate*
- **Network and Telecommunications Security**: *Evaluate*
- **Physical and Personnel Security**: *Design, Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance)**: *Implement, Evaluate*
- **Privacy**: *Design, Implement, Evaluate*
- **Procurement**: *Design, Implement, Evaluate*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement, Evaluate*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **Information Security Professional**
- **Information Technology Security Analyst**
- **IT Security Analyst**
- **Systems Analyst**

- **IT Security Technical Analyst**
- **Research Specialist**
- **Digital Forensics Analyst**
- **Purchasing Manager**
- **Acquisition Manager**
- **Buyer**
- **Contracting Officer**
- **Contract Specialist**
- **Purchasing Specialist**
- **Facility Security Officer**
- **Physical Security Administrator**
- **Personnel Security Officer**

3.7 INFORMATION SECURITY OPERATIONS & MAINTENANCE PROFESSIONAL

The IT Security Operations and Maintenance Professional ensures the security of information and information systems during the operations and maintenance phases of the software development lifecycle (SDLC).

Competencies:

- **Data (Information) Security**: *Implement, Evaluate*
- **Digital Forensics**: *Implement*
- **Enterprise Architecture**: *Implement, Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement*
- **Incident Management**: *Design, Implement, Evaluate*
- **IT Security Training and Awareness**: *Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Manage, Design, Implement, Evaluate*
- **Network and Telecommunications Security**: *Manage, Design, Implement, Evaluate*
- **Physical and Personnel Security**: *Evaluate*
- **Policies, Standards and Compliance (Information Assurance)**: *Implement, Evaluate*
- **Privacy**: *Implement, Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Implement*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **IT Security Engineer**
- **Operations and Maintenance Engineer**
- **Operations and Maintenance Manager or Supervisor**
- **Information Technology Specialist**
- **Database Administrator**
- **Directory Services Administrator**
- **Network Administrator**
- **Service (Help) Desk Representative**
- **Technical Support Personnel**

3.8 INFORMATION SECURITY SYSTEM ADMINISTRATION PROFESSIONAL

The Information Security System Administration Professional supports the application of the principles, policies and procedures, and compliance with laws, regulations, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes the integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

Competencies:

- **Data (Information) Security**: *Design, Implement, Evaluate*
- **Digital Forensics**: *Implement*
- **Enterprise Architecture**: *Implement, Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement, Evaluate*
- **Incident Management**: *Design, Implement, Evaluate*
- **IT Security Training and Awareness**: *Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Manage, Design, Implement, Evaluate*
- **Network and Telecommunications Security**: *Manage, Design, Implement, Evaluate*
- **Physical and Personnel Security**: *Design, Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Implement, Evaluate*
- **Privacy**: *Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement*

- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **System Administrator**
- **Database Administrator**

4.0 STATE GOVERNMENT INFORMATION SECURITY COMPETENCY & FUNCTIONAL MATRIX

Work conducted by the information security workforce is complex and not all work in a given competency area is performed by a single role. Work performed by a team of individuals with different responsibilities and spans of control ranges from creating the strategy for a component of the Information Security Program, to development of the program's scope and procedures, to performing hands-on implementation work, and to evaluating the work's efficiency and effectiveness. Rather than all roles being responsible and knowledgeable in all areas of information security and having the ability to perform all job tasks, individual roles are associated with a subset of competencies to represent the work performed as part of an Information Security team. The type of work performed is resolved by role through the four (4) functional perspectives (Manage, Design, Implement, and Evaluate) across a series of technical competency areas. It is on these functional perspectives that an individual should be evaluated if a role-based certification truly measures his or her ability to perform.

To present a visual depiction of the relationship among state government information security roles, competencies and functional perspectives that describe work performed in that role, the *State Government Information Security Competency & Functional Matrix* is provided on the following page.

Information security roles are broadly grouped into Executive (Managerial), and Functional (Technical) categories. When a role is mapped to a competency, and to a functional perspective within that competency, it defines *all* of the functions the role performs within the functional perspective.

> Example:
>
> An Information Security Officer who develops procedures related to "Incident Management" is mapped to the "Design", "Implement", and "Evaluate" functional perspectives within the "Incident Management" competency area and would perform work within these functional perspectives.

STATE GOVERNMENT INFORMATION SECURITY
Competency & Functional Framework

Functional Perspectives:

M - Manage
D - Design
I - Implement
E - Evaluate

		STATE GOVERNMENT INFORMATION SECURITY ROLES															
		Executive (Managerial)								***Functional (Technical)***							
	INFORMATION SECURITY COMPETENCIES	**Chief Information Security Officer**		**Privacy Officer**		**Information Security Officer or Manager**		**Compliance Officer (Information Assurance)**		**Information Security Engineer**		**Information Security Professional**		**Information Security Operations & Maintenance Professional**		**Information Security System Administration Professional**	
1	Data (Information) Security	M		M	D	M	D				D		D				D
			E		E		E		E	I	E	I		I	E	I	E
2	Digital Forensics	M									D						
			E		E	I			E		E	I	E	I		I	
3	Enterprise Architecture									M	D						
			E						E	I	E		E	I	E	I	E
4	Enterprise Continuity (Disaster Recovery)	M									D		D		D		D
					E		E		E	I	E	I	E	I		I	E
5	Incident Management	M		M	D		D				D		D		D		D
				I	E	I	E		E	I	E	I	E	I	E	I	E
6	Information Security Training and Awareness	M			D		D		D		D						
					E	I	E		E	I	E	I	E	I	E	I	E
7	IT Systems Operations and Maintenance										D			M	D	M	D
									E	I	E		E	I	E	I	E
8	Network and Telecommunications Security									M	D			M	D	M	D
			E						E	I	E		E	I	E	I	E
9	Physical and Personnel Security	M			D	M	D						D				D
				I	E		E		E	I	E	I	E		E	I	E
10	Policies, Standards and Compliance (Information Assurance)	M			D	M	D	M	D								
			E	I	E	I	E	I	E	I		I	E	I	E	I	E
11	Privacy	M	D	M	D						D		D				
			E	I	E	I			E		E	I	E	I	E		E
12	Procurement	M	D								D		D				
			E		E				E		E	I	E		E		E
13	Security Risk Management	M	D	M	D		D				D		D				D
		I	E	I	E	I	E	I	E	I	E	I	E	I		I	E
14	Strategic Security Management	M	D														
		I	E			I			E	I		I	E	I		I	
15	System and Application Security	M									D		D		D		D
			E		E		E		E	I	E	I	E	I	E	I	E

Figure 4-1 State Government Information Security Competency and Functional Matrix

5.0 STATE GOVERNMENT INFORMATION SECURITY JOB/POSITION DESCRIPTIONS

The following sample information security job/position descriptions from the six (6) pilot states are provided. Additional examples will be added as other states contribute to the model framework.

- Chief Information Security Officer (CISO)
- Director, Division Information Security
- Privacy Officer
- Information Security Officer (ISO)
  - Also Included:
    - *"Implementing an Effective State Government Information Security Program"* - Explains ISO/ISM roles and responsibilities.
    - Information Security Officer (ISO) Survey
- Information Security Manager (ISM)
- Technology Center Operations – Systems Analyst – Risk, Security & Facilities Specialist
- Information Technology Security Analyst – Information Security Policy Analyst
- Information Security Analyst – Enterprise Information Security Analyst
- Research Specialist
- Systems Analyst – Information Security Technical Analyst
- Information Security Administration
  - Information Technology Specialist I
  - Information Technology Specialist II
  - Information Technology Specialist III

Detailed information on each of the above job/position descriptions is provided in -

APPENDIX II

State Government Information Security Job/Position Descriptions

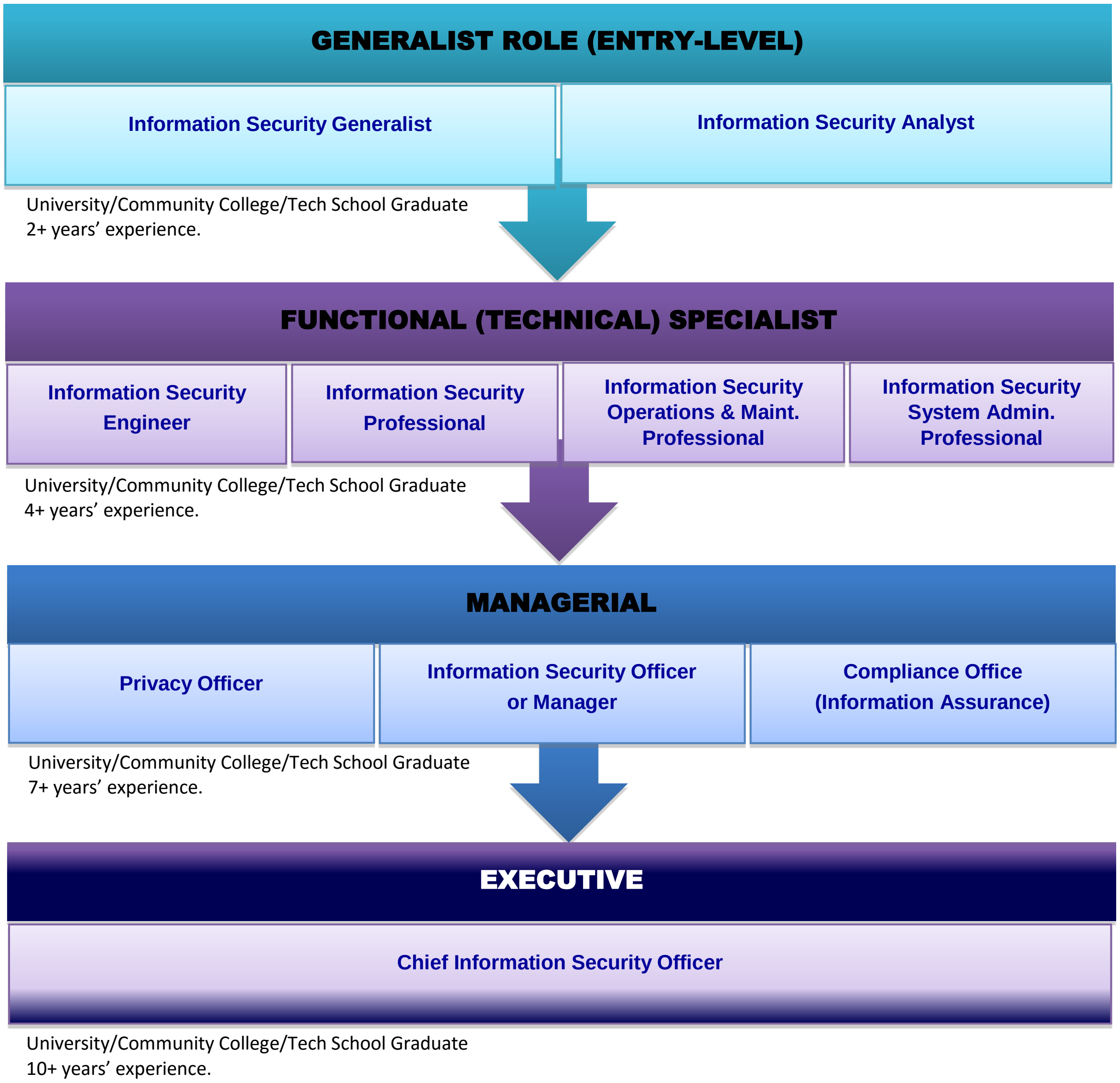
6.0 STATE GOVERNMENT INFORMATION SECURITY CAREER PLANNING

Demand for information security professionals is increasing continuously at a high rate. The Global Information Security Workforce Study (2008), conducted by $(ISC)^2$, advises that the number of information security professionals worldwide will likely rise from 1.6 million in 2009 to 2.7 million by 2012. Survey data indicated a switch from protecting organizational networks to protecting organization data.

Information Security has become one of the most "in-demand" career opportunities in information technology. However, for those entering this field, determining the best path can be difficult. According to a recent economic impact survey conducted by $(ISC)^2$ in April – May 2009 to gain insight into the impact that the economic downturn is having on its certified membership and their employers, of the more than 2,800 professionals participating in the survey, 775 had hiring responsibilities, with 44 percent of those looking to hire additional information security staff this year and over 11 percent planning to add more than three people. Despite economic conditions, over 80 percent of hiring managers identified that they are challenged in their efforts to find the right candidate. The range of concerns included a lack of desired skills or lack of available professionals within a local area, and salary demands that are too high for available budgets, particularly from people who had previously worked within the troubled financial services sector. Information security professionals can look forward to a future with new job opportunities within the market and fewer budget cuts. Most hiring managers are struggling to fill positions as the pool of qualified candidates is too low and salary expectations are too high due to budget constraints.

Recommended career progression for state government information security professionals includes the following roles: Generalist (entry-level), Functional (Technical) Specialist, Managerial and Executive. The typical state government information security job path is represented on the following page in *Figure 6.1 Recommended Information Security Career Progression.*

6.1 INFORMATION SECURITY CAREER PROGRESSION



GENERALIST ROLE (ENTRY-LEVEL)

Information Security Generalist

Information Security Analyst

University/Community College/Tech School Graduate
2+ years' experience.

FUNCTIONAL (TECHNICAL) SPECIALIST

Information Security Engineer

Information Security Professional

Information Security Operations & Maint. Professional

Information Security System Admin. Professional

University/Community College/Tech School Graduate
4+ years' experience.

MANAGERIAL

Privacy Officer

Information Security Officer or Manager

Compliance Office (Information Assurance)

University/Community College/Tech School Graduate
7+ years' experience.

EXECUTIVE

Chief Information Security Officer

University/Community College/Tech School Graduate
10+ years' experience.

Figure 6-1 Recommended Information Security Career Progression

6.2 CREATING CAREER PATHS

Creating career paths for information security professionals will support an overwhelming impact to the success of the organization. Utilizing an internal information security workforce and augmenting with training and professional development can help establish, support and maintain a successful information security program. Career planning will facilitate growing the internal team and creating job satisfaction, increasing retention and aiding recruiting.

Information Security career planning should take into account, both the professional's and practitioner's aspects of security and ensure that there is both a career path for each and a combination of the two.

Development of the *State Government Information Security Career Planning Model* involved research of best practice models from the public and private sectors in order to provide the most effective and efficient Career Planning guideline to support state government's information security workforce professional development.

Research included the "Information Technology (IT) Workforce Development Roadmap", a career development tool for current and prospective Federal IT workers. The IT Roadmap allows IT professionals to conduct self-assessments to determine where skill gaps exist and to tailor career development plans to meet their specific needs. Individuals are able to select developmental opportunities from a wide variety of educational formats (i.e., web-based training, seminars, classrooms, certifications, and eventually, experiential opportunities). Training sources are linked to specific competencies.

6.3 CAREER PLANNING RESOURCES/TOOLS

There are a multitude of career planning resources, tools and software available to state government to help motivate, develop and support information security professionals in progressing their careers.

Managers and employees should collaborate to establish dynamic career development plans to meet both organizational and individual goals.

Effective career planning should address:

- **Goals / Action Plans** - Setting career goals and create action plans (career ladders/lattices)
- **Matching Goals to Objectives** - Matching individual goals to business objectives
- **Resource Availability** - Accessing information security career professional development resources (education/training (internal/external), certification support)
- **Workforce Planning**
  - Position Management
  - Talent Resource Planning
- **Performance Management**
  - Integrate a complete evaluation process to include competency management, job profiling, assessment, reviews, goals and objective setting
  - Plan individual efforts in support of organizational goals and objectives
  - Evaluate outcomes, performance and core competencies
  - Create specific, measurable, achievable, realistic and time-based performance goals
  - Track competencies
  - Implement weighting, rating measures and measurement scales
  - Separate workflows
  - Utilize Executive Dashboards and Employee Scorecards
  - Measure performance against financial, customer, business processes and learning indicators
  - Document employee appraisals

- **Succession Planning**
  - Create organization's view of employees' careers
  - Create individual career plans and match to organizational plans
  - Identify and track high performers
  - Track employee skills, competencies and career desires
  - Match skills to open positions

- **Career Planning and Development**
  - Set career goals and create action plans
  - Enable employees to create role-based career plans (highlighting gaps and suggestions for competency improvement)
  - Match individual goals to business objectives
  - Track professional development and achievements
  - Access career/professional development resources
  - Conduct personality and values assessments

- **Transition/Outplacement**
  - Job Search
  - Psychometric Tools
  - Resume design/distribution
  - Career research

6.4 INFORMATION SECURITY CAREER PLANNING ROADMAP

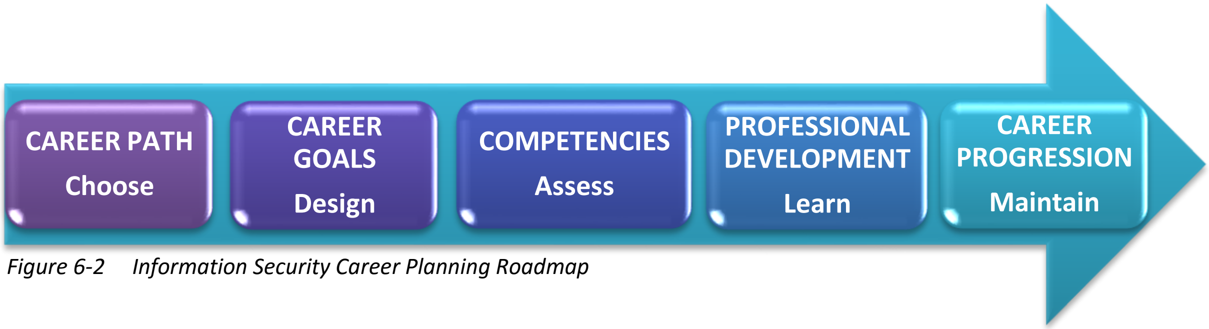


Figure 6-2 Information Security Career Planning Roadmap

- ✓ **1. Career Path: Choose**
  - – Identify and Set Career Goals
  - – Choose Career Path
  - – Consider Time Frame
  - – Identify Career Coach
- ✓ **2. Career Goals: Design**
  - – Choose appropriate job title(s) to meet your career goal
  - – Choose appropriate anticipated experience (performance) level(s)
  - – Identify core and recommended competencies for selected job titles/performance levels
- ✓ **3. Competencies**
  - – Complete assessment of general and technical competencies to assigning appropriate "current proficiency"
  - – Identify competency gaps for selected job title(s)
- ✓ **4. Professional Development**
  - – Select appropriate developmental opportunities from course catalogs to develop competencies and mitigate gaps
  - – Select appropriate IT security certifications
  - – Include additional "personal attributes" developmental opportunities
- ✓ **5. Career Progression**
  - – Track/edit individual career development plans for each career development scenario
  - – Add desired education/training courses and certifications to plan, as appropriate
  - – Periodically check progress against development plan, integrating competency and education/training achievements

6.5 BUILDING A COMPETENCY MODEL CAREER LADDER/LATTICE

Best Practice – CareerOneStop – Sponsored by the U.S. Department of Labor

*Best Practice - The Occupational Information Network (O*NET)*

CareerOneStop is a U.S. Department of Labor-sponsored website that offers career resources and workforce information to job seekers, students, businesses and workforce professionals to foster talent development in a global economy. (http://www.careeronestopo.org).

O*NET – The O*NET program is the nation's primary source of occupational information comprised of the O*NET database, containing information on hundreds of standardized and occupation-specific descriptors, developed under the sponsorship of the US Department of Labor/Employment and Training Administration (USDOL/ETA) through a grant to the North Carolina Employment Security Commission. The database, which is free to the public, is continually updated by surveying a broad range of workers from each occupation. The database also provides Career Exploration Tools. (http://www.onetcenter.org)

Information Security Competency Model – Identifies the information security knowledge, skills and abilities needed to perform successfully. To build model tiers, the appropriate competencies and key behaviors must be defined.

Career Ladder and Lattice – Outline critical experiences individuals in a particular career must successfully achieve.

- Career ladders and lattices are devices that help people visualize and learn about the job options available as they progress through their career. Career ladders consist of a group of related jobs that comprise a career and should be utilized in conjunction with and aligned to career competencies. Included is a pictorial representation of job progression in a career as well as detailed descriptions of the jobs and experiences that facilitate movement between jobs

- Career ladders display only vertical movement between jobs. Career lattices contain both vertical and lateral movement between jobs and may reflect more closely the career paths of today's workforce.

Utilizing the State Government Information Security Workforce Development Model to serve as a foundational guideline, the following steps support creation of a Career Ladder/Lattice:

1. **Job Information** - Important job characteristics (Resource: Occupational Information Network (O*NET) Database, America's Career InfoNet, State-Specific Departments of Labor
   a. Job Title, Job Level (Functional Perspective)
   b. Job Description – Roles/Responsibilities/Functions
   c. Education - Supporting Competencies Achievement
   d. Workforce Preparation/Duration – Specific training requirements
   e. Work Experience - Can work experience and education substitute for each other?
   f. Licensure/Certification – Associated to Achieved Competencies
   g. Salary/Wages (Derived from employment statistics, benchmarking, etc.).
   h. Employment Outlook (Derived from HR/employment statistics)
   i. References

2. **Place and Link Jobs** – How people may progress through the defined jobs.
   a. Arrange job titles and map to relationships between jobs in the career.

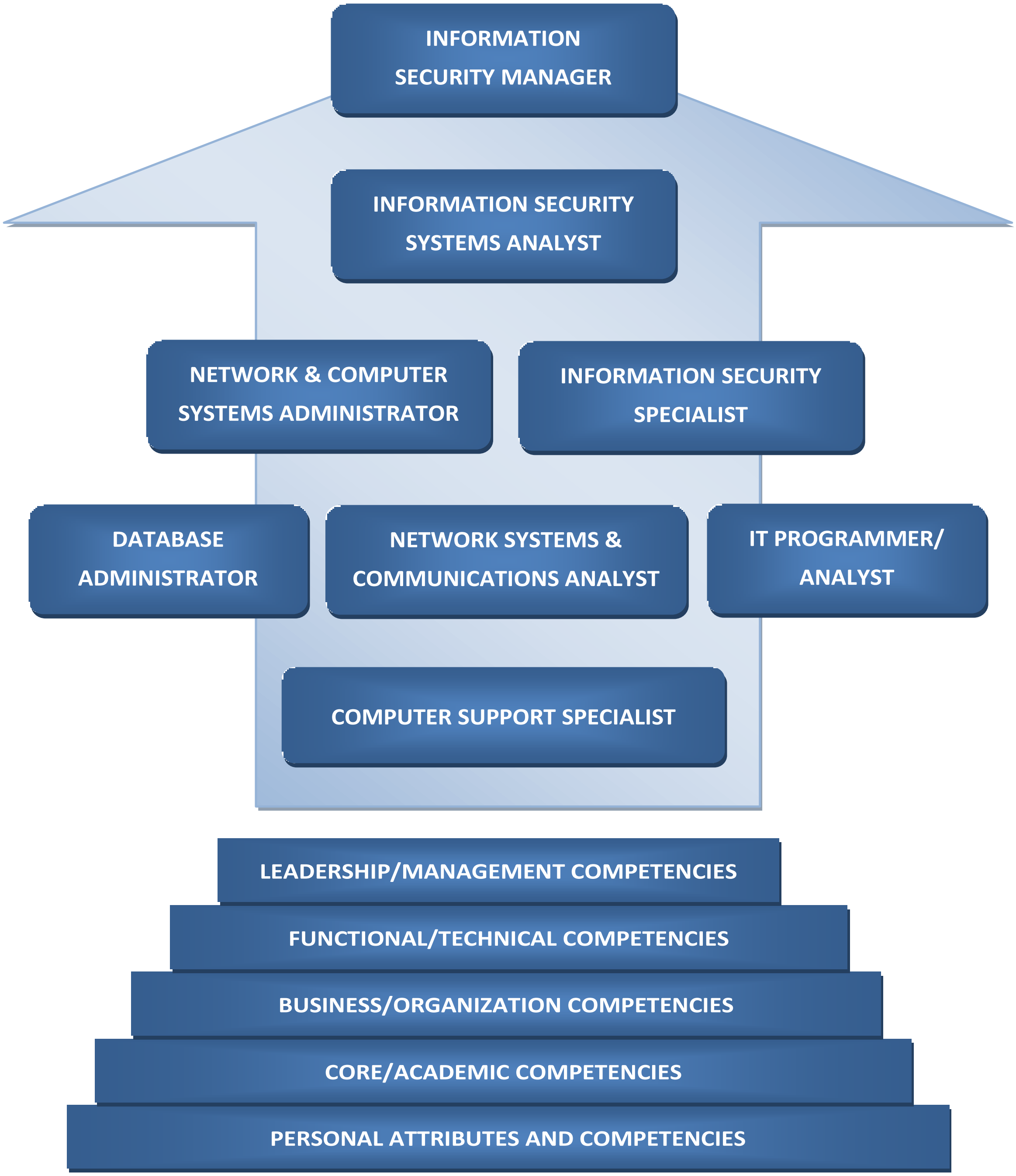
3. **Add Critical Development Experiences** – Describe key differences between jobs in this career.
   a. Identify the critical development experiences (CDEs) that individuals should pursue as they make preparations to move from one job to another.
   b. CDEs will also represent differences between jobs (i.e., educational requirements, work-related experience requirements (training, OJT, years of experience), licensure/certification requirements, skills to develop or tasks to perform to prepare for a new position).

   When developing CDEs:
   1. Identify differences between linked jobs and which of the differences are critical experiences promoting career progression.
   2. Interview incumbents in the target job to identify experiences obtained during their career that contributed to their development.
   3. Interview supervisors of individuals in the target job to identify the experiences they advise are relevant when considering prospective employees
   4. Examine tasks for the current position and desired position. What are the differences? What actions should the employee take to prepare for target position tasks?

4. **Track and Maintain**

a. Track and maintain to support continuous improvement and success metrics.

SAMPLE INFOMRATION SECURITY CARREER LADDER



INFORMATION SECURITY MANAGER
INFORMATION SECURITY SYSTEMS ANALYST
NETWORK & COMPUTER SYSTEMS ADMINISTRATOR
INFORMATION SECURITY SPECIALIST
DATABASE ADMINISTRATOR
NETWORK SYSTEMS & COMMUNICATIONS ANALYST
IT PROGRAMMER/ ANALYST
COMPUTER SUPPORT SPECIALIST
LEADERSHIP/MANAGEMENT COMPETENCIES
FUNCTIONAL/TECHNICAL COMPETENCIES
BUSINESS/ORGANIZATION COMPETENCIES
CORE/ACADEMIC COMPETENCIES
PERSONAL ATTRIBUTES AND COMPETENCIES

Figure 6-3 Sample Information Security Career Ladder

6.6 CAREER PLANNING SWOT ANALYSIS

A typical Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis can be applied to information security career planning from either an "employer" or "employee" perspective. Results from both perspectives can be compared to help design a Career Plan Roadmap.

INTERNAL	☑	Strengths	☑	Weaknesses
		Goals and Positive Traits to Leverage for Career Planning		Lack of Goals and Negative Traits That Need Improving
		Work Experience		Lack of Work Experience
		Education – Credentials, Certifications		Lack of Appropriate Education, Credentials, Certifications
		Business Knowledge		Weak Business Knowledge
		Strong Knowledge of Job Role and Responsibilities within Organization		Weak Job Role and Responsibilities Knowledge
		Strong Technical Knowledge, Applies Technical Skills to Tasks		Weak Technical Knowledge
		Information Security Technology Knowledge, Applies Technology Skills to Tasks		Weak Information Security Technology Skills
		Transferrable (Soft) Skills Sets **<u>Communication Sills</u>** *Skillful Expression, Transmission and Interpretation of Knowledge and Ideas* Speaking Effectively, Written Communication - Writing Concisely, Listening, Expressing Ideas, Facilitation, Team Leadership, Conflict Management & Resolution / Negotiation, Persuading/Influencing Others, Representing Security Incidents to Business and Technical Communities, Interviewing		Weak Communication Skills Indicate Communication skill sets needing improvement

	☑	Strengths	☑	Weaknesses
		Personal Characteristics *Strong Ethics, Self-Discipline, Ability to Work Under Pressure* Ethics & Integrity, Personal Credibility, Personal Confidence, Forward Thinking, Analytical Thinking, Creative Thinking, Thoroughness, Learning, Optimism, High Level of Energy, Initiative for Continuing Professional Development		Weak Personal Characteristics Skills Indicate Personal Characteristics skill sets needing improvement
		Research and Planning *Research Specific Knowledge and Ability to Conceptualize and Plan Future Needs and Solutions for Meeting those Needs* Organizational Awareness, Planning and Organizing, Diagnostic Information Gathering, Forecasting, Predicting, Creating Ideas, Identifying and Solving Problems Identifying Alternative Solutions, Identifying Resources, Gathering Information, Setting Goals, Defining Needs, Analyzing, Developing Evaluation Strategies		Weak Research and Planning Skills Indicate communication skill sets needing improvement
		Human Relations *Interpersonal Skills to Resolve Conflict,* *Relating to and Helping People* Relationship Building, Sensitivity, Listening, Conveying Perceptions, Providing Support, Motivating, Sharing Credit, Developing and Empowering Others, Fostering Diversity, Mentoring, Counseling, Cooperation, Delegating with		Weak Human Relations Skills Indicate Human Relations skill sets needing improvement

	Respect, Representing Others, Assertion		
☑	**Strengths**	☑	**Weaknesses**
	Organizational Management and Leadership *Supervision, Direction and Guidance to Individuals and Groups in Completion of Tasks and Goals* Global Perspective, Vision and Strategic Thinking, Risk Management, Stress Management, Teamwork, Initiating New Ideas, Handling Details, Coordinating Tasks, Managing Groups, Delegating Responsibility, Teaching, Coaching, Counseling, Promoting Change, Selling Ideas, Decision Making, Managing Conflict, Change Leadership, Negotiation, Results Orientation		Weak Organizational Management and Leadership Skills Indicate Organizational and Management skill sets needing improvement
	Work Survival *Day-to-Day Skills that Assist in Promoting Effective Production and Work Satisfaction* Customer Focus, Decision-Making and Implementation, Cooperating, Enforcing Policies, Being Punctual, Managing Time, Flexibility, Attending to Detail, Meeting Goals, Enlisting Help, Accepting Responsibility, Setting and Meeting Deadlines, Organizing, Workforce/Resource Management, Making Decisions		Weak Work Survival Skills Indicate Work Survival skill sets needing improvement
	Interaction with Professional Organizations to Promote Continuous Professional Development		Lack of Interaction with Professional Organizations to Promote Continuous Professional Development

EXTERNAL	☑	Opportunities	☑	Threats
		Positive External Information Security Conditions or Trends to Leverage		Threats Negative Trends in the Information Security Industry Out of Your Control
		Career Opportunities are Available by Enhancing Education and/or Achieving Certification		Competitor Applicants with Superior Skills, Experience and Knowledge
		Information Security Industry Demand has Increased for Skill Sets		Demand for Skill Sets Have Dropped
		Opportunities Available for Access to Education and Increased Knowledge Aligned with Specific Job Goals		Limitations, Obstacles to Advanced Education/Training
		Information Security Advancement Opportunities		Limited Advancement Opportunities, Advancement is Too Competitive
		Information Security Professional Development		Limited Professional Development
		Job Requirements Providing Opportunities for Professional Development and Advancement		Job Requirements Changing with No Opportunities for Professional Development and Advancement
		Changing Technology is Providing New Opportunities that Align with Job Roles and Responsibilities, Professional Development and Advancement		Changing Technology Threatens Career Plans with No Opportunities to Align with Job Roles and Responsibilities, Professional Development and Advancement
		The Economy has Increased Career Plans and Opportunities		The Economy has and is Negatively Affecting Career Plans and Opportunities

7.0 APPENDICES

The following *State Government Information Security Model* Appendices are contained in separate documents.

- *Appendix I – State Government Information Security Competencies*
- *Appendix II – State Government Information Security Position/Job Descriptions*
- *Appendix III – State Government Information Security Matrix*

8.0 DOCUMENT MANAGEMENT

Version	*Date*	*Description*
1.0	June 2010	Final Version for Release to Multi-State ISAC (MS-ISAC)