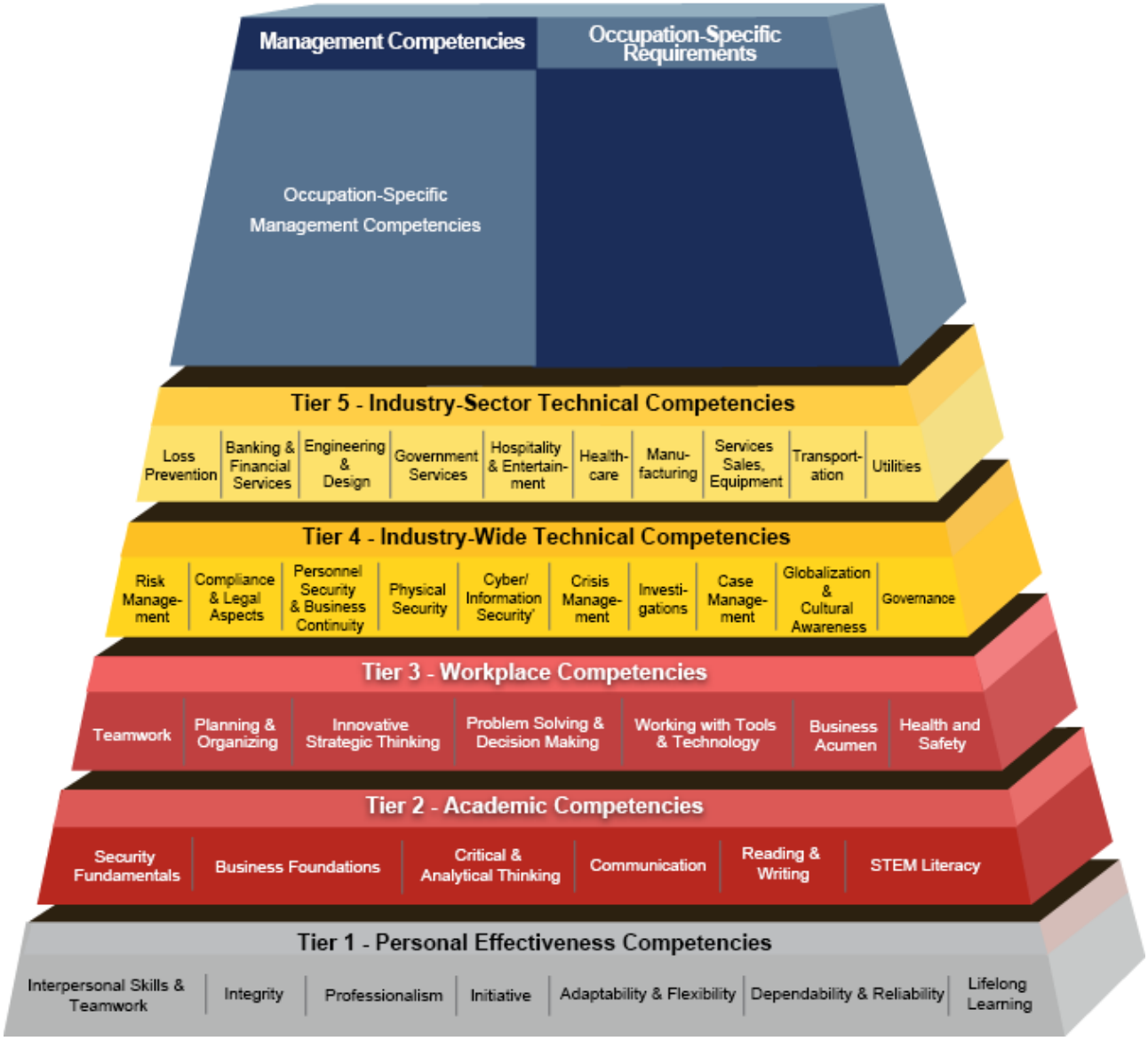
COMPETENCY MODEL CLEARINGHOUSE

Enterprise Security Competency Model



Contents

About the Model

Industry Skills Gap

Enterprise Security is a distinct and sophisticated profession requiring a unique set of competencies and skills for success. Roles in this industry are not a subset or "spin-off" of the criminal justice system. Nonetheless, not all academic and training programs with "security" in their title offer an education with consistent, current, industry-aligned competencies and employability skills. This complication in education contributes to the growing security industry skills gap.

The workforce is also aging, which leads to further shortages of qualified workers, and creates the need to strengthen the industry's talent pipeline. These dynamics, and the absence of industry-endorsed solutions, contribute to large talent deficits that may weaken the security infrastructure of organizations, enterprises, and the larger global economy.

Security Competency Research

To respond to workforce development challenges in enterprise security, the ASIS Foundation[1] engaged in multiple research initiatives to identify the security risks that enterprises are most likely to face over the next five years, and the specific professional competencies and skills[2] that are required to mitigate and respond to those risks. The goal of these research efforts is to promote and maintain a common understanding of the skill sets and competencies that are essential to educate and train a globally competitive security workforce. Establishing consensus on which security competencies are needed across industries and subsectors of the security industry can help to close skills gaps by defining clearer career pathways for tomorrow's professionals.

National Roundtable: In June 2013 the ASIS Foundation convened a national roundtable of senior leaders from the security industry, higher education, and government to identify the top security risks and challenges that the industry will face in the next five years, and the key competencies that security practitioners will require to manage the risks and challenges effectively. The roundtable findings were published in *Enterprise Security Risks and Workforce Competencies*, a report released by the ASIS Foundation and University of Phoenix in fall 2013.[3]

National Survey: The ASIS Foundation conducted a national survey of security industry professionals in fall 2013 to validate the roundtable findings with quantitative data to help verify and prioritize the identified security risks, challenges, and professional competencies. The results of this industry survey were published on August 14, 2014.

---

[1] The ASIS Foundation/University of Phoenix skills gap research, analysis, and collaboration has now led to the application of the U.S. Department of Labor Competency Model Clearinghouse resources, models, and guidance.

[2] A *competency* is the capability to apply or use a set of related knowledge, skills, and abilities required to successfully perform "critical work functions" or tasks in a defined work setting.

[3] University of Phoenix / ASIS Foundation "*Enterprise Security Risks and Workforce Competencies – Findings From An Industry Roundtable on Security Talent Development*" September 2013, http://cdn.assets-phoenix.net/content/dam/altcloud/doc/industry/UOPX-ASISFoundationSecurityRisksandCompetenciesReport.pdf

Enterprise Security Competency Model

The Enterprise Security competency research is formatted into a new Enterprise Security Competency Model, using a framework provided by the U.S. Department of Labor's Employment and Training Administration.[4]

This Enterprise Security Competency Model is designed to encompass the broad baseline skills and competencies needed for the entire industry, not just an industry segment or occupation.[5] The model is intended to reflect the competencies needed for entry-level security professionals and also to serve as a career development tool to help ensure that security practitioners possess foundational competencies that are required as prerequisites for additional education or training that enables them to advance in their careers. The model also serves as a resource to identify the training and education needed to upgrade incumbent workers' skills to adapt to new technologies, emerging industry dynamics, and new work processes.[6]

> A **competency model** is a collection of competencies that together define successful performance in a particular work setting. Competency models are the foundation for important human resource functions such as recruitment and hiring, training and development, and performance management.

Model Publication

The ASIS Foundation, ASIS International, the CSO Roundtable and the Apollo Education Group are working to validate the Enterprise Security Model with subject matter experts, corporations, and other stakeholders. The CSO Roundtable Leadership and Development Committee helped design the validation process and steps necessary to publish the Enterprise Security Competency Model in.

Following the publication of the model, the ASIS Foundation will ensure that it will be reviewed to adjust to the changing dynamics of the global security industry. The ASIS Foundation will partner with multiple industry stakeholders to disseminate the model, creating resources and tools to enable security professionals, private organizations, government entities and training and educational institutions to understand and apply the model to their respective workforce development priorities.

U.S. DOL Competency Model Framework

The Enterprise Security Competency Model is depicted in a pyramid graphic with nine tiers. Each tier comprises blocks representing the skills, knowledge, and abilities essential for successful performance in the industry or occupation represented by the model. At the base of the model, the competencies apply to a large number of occupations and industries. As a user moves up the model, the competencies become industry and occupation specific. The pyramid

---

[4] The Enterprise Security Competency Model was written by University of Phoenix & Apollo Education group and validated in partnership with ASIS International, the ASIS Foundation & the CSO Roundtable.

[5] It should be noted, however, that this competency model does not encompass allied professionals in IT-related security fields. IT professionals represent a segment of the security industry that requires a specialized set of competency requirements.

[6] The Enterprise Security Competency Model will be vetted by security industry professionals, security industry associations, industry leaders and subject matter experts, education leaders and governmental entities in the United States and throughout the world. The model will depict the consensus among these global stakeholders for the competencies and skills required for success in the enterprise security industry.

shape does not imply that competencies at the top are at a higher level of skill. Instead, the model's shape represents the increasing specialization and specificity in the application of skills. A table of the competency definitions and associated key behaviors follows.

Foundational Competencies

Tiers 1 through 3 contain Foundation Competencies, which form the foundation needed to be ready to enter the workplace.

> **Competency** – A cluster of related knowledge, skills, and abilities that affects a major part of one's job (a role or responsibility), that correlates with performance on the job, that can be measured against well-accepted standards, and that can be improved via training and development.

- **Tier 1 –Personal Effectiveness Competencies** are shown as the base of the pyramid because they represent personal attributes or "soft skills" that may present some challenges to teach or assess. Essential for all life roles, personal effectiveness competencies generally are learned in the home or community and reinforced at school and in the workplace.
- **Tier 2 – Academic Competencies** are critical competencies primarily learned in a school setting. They include cognitive functions and thinking styles that are likely to apply to most industries and occupations.
- **Tier 3 – Workplace Competencies** represent motives and traits, as well as interpersonal and self-management styles. They generally are applicable to a large number of occupations and industries.

Industry Competencies

Tiers 4 and 5, called Industry Competencies, show competencies that are specific to the *industry or industry sector.* These cross-cutting industry-wide competencies demonstrate the viability of career lattices that allow workers to move easily across industry sub-sectors. As a result, this model supports the development of an agile workforce that does not need to follow a single occupational career ladder.

- **Tier 4 – Industry-Wide Technical Competencies** represent the knowledge and skills that are common across sectors within a broader industry. These technical competencies build on, but are more specific than, competencies represented on lower tiers.
- **Tier 5 – Industry-Sector Technical Competencies** represent a sub-set of industry technical competencies that are specific to an industry sector.

Upper Tiers

Tiers 6 through 9 represent the specialization that occurs within specific *occupations* within an industry. Information on occupational competencies is available through O*NET OnLine (https://www.onetonline.org/).

Tier 1: Personal Effectiveness Competencies

1.1 Interpersonal Skills and Teamwork: Displaying skills to work with others from diverse backgrounds.

1.1.1 Demonstrating concern for others

- 1.1.1.1 Show sincere interest in others and their concerns
- 1.1.1.2 Demonstrate sensitivity to the needs and feelings of others
- 1.1.1.3 Look for ways to help others and deliver assistance

1.1.2 Demonstrating insight into behavior

- 1.1.2.1 Recognize and accurately interpret the verbal and nonverbal behavior of others
- 1.1.2.2 Show insight into the actions and motives of others
- 1.1.2.3 Recognize when relationships with others are strained

1.1.3 Maintaining open communication

- 1.1.3.1 Maintain open lines of communication with others
- 1.1.3.2 Encourage others to share problems and successes
- 1.1.3.3 Establish a high degree of trust and credibility with others

1.1.4 Respecting diversity

- 1.1.4.1 Demonstrate sensitivity and respect for the opinions, perspectives, customs, and individual differences of others
- 1.1.4.2 Value diversity of people and ideas
- 1.1.4.3 Deal with a wide range of people with flexibility and open-mindedness
- 1.1.4.4 Listen to and consider others' viewpoints
- 1.1.4.5 Work well and develop effective relationships with diverse personalities

1.2 Integrity: Displaying accepted social and work behaviors.

1.2.1 Behaving ethically

- 1.2.1.1 Abide by a strict code of ethics and behavior
- 1.2.1.2 Choose an ethical course of action and do the right thing, even in the face of opposition
- 1.2.1.3 Encourage others to behave accordingly

1.2.2 Acting fairly

- 1.2.2.1 Treat others with honesty, fairness, and respect
- 1.2.2.2 Make decisions that are objective and reflect the just treatment of others

1.2.3 Taking responsibility

- 1.2.3.1 Take responsibility for accomplishing work goals within accepted timeframes, or for not accomplishing those goals
- 1.2.3.2 Accept responsibility/accountability for one's decisions and actions and for those of one's group, team, or department
- 1.2.3.3 Understand that past behavior may affect one's ability to obtain occupation or meet occupational requirements
- 1.2.3.4 Attempt to learn from mistakes

1.3 Professionalism: Maintaining a professional demeanor at work.

1.3.1 Demonstrating self-control

1.3.1.1 Demonstrate self-control by maintaining composure and keeping emotions in check

1.3.1.2 Deal calmly and effectively with stressful situations

1.3.2 Maintaining a professional appearance

1.3.2.1 Maintain a professional demeanor

1.3.2.2 Dress appropriately for occupation and its requirements

1.3.2.3 Maintain appropriate personal hygiene

1.3.2.4 Wear appropriate identification, as required

1.3.2.5 Refrain from lifestyle choices which negatively impact the workplace and individual performance

1.3.2.6 Be prepared to represent your organization and effort

1.3.3 Maintaining a positive attitude

1.3.3.1 Project a positive image of oneself and the organization

1.3.3.2 Demonstrate a positive attitude towards work

1.3.3.3 Take pride in one's work and the work of the organization

1.4 Initiative: Demonstrating a willingness to work.

1.4.1 Persisting

1.4.1.1 Pursue work with energy, drive, and a strong accomplishment orientation

1.4.1.2 Persist and expend extra effort to accomplish tasks even when conditions are difficult or deadlines tight

1.4.1.3 Persist at a task or problem despite interruptions, obstacles, or setbacks

1.4.2 Taking initiative

1.4.2.1 Go beyond the routine demands of the job

1.4.2.2 Take initiative in seeking out new work challenges and increasing the variety and scope of one's job

1.4.2.3 Seek opportunities to influence events and originate action

1.4.2.4 Assist others who have less experience or have heavy workloads

1.4.2.5 Seek the information and assistance needed to be successful

1.4.3 Setting challenging goals

1.4.3.1 Establish and maintain personally challenging but realistic work goals

1.4.3.2 Exert effort toward task mastery

1.4.3.3 Bring issues to closure by pushing forward until a resolution is achieved

1.4.4 Working independently

1.4.4.1 Develop and use effective and efficient ways of performing tasks

1.4.4.2 Perform effectively, even with minimal direction, support, approval, or direct supervision

1.4.4.3 Strive to exceed standards and expectations

1.4.4.4 Exhibit confidence in capabilities and an expectation to succeed in future activities

1.5 Adaptability and Flexibility: Displaying the capability to adapt to new, different, or changing requirements.

1.5.1 Employing unique analyses

- 1.5.1.1 Employ unique analyses and generate valuable, innovative ideas
- 1.5.1.2 Integrate related and seemingly unrelated information to develop creative solutions
- 1.5.1.3 Develop innovative methods of obtaining or using information or resources when needed

1.5.2 Entertaining new ideas

- 1.5.2.1 Remain open to considering new ways of doing things
- 1.5.2.2 Actively seek out and carefully consider the merits of new approaches to work
- 1.5.2.3 Embrace new approaches when appropriate and discard approaches that are no longer working

1.5.3 Dealing with ambiguity

- 1.5.3.1 Take appropriate action without having all facts or permissions, when necessary
- 1.5.3.2 Change plans, goals, action, or priorities in response to changing, unpredictable, or unexpected events, pressures, situations, and job demands

1.6 Dependability and Reliability: Displaying responsible behaviors at work.

1.6.1 Fulfilling obligations

- 1.6.1.1 Behave consistently and predictably
- 1.6.1.2 Fulfill obligations reliably, responsibly, and dependably
- 1.6.1.3 Diligently follow through on commitments and consistently meet deadlines
- 1.6.1.4 Demonstrate regular and punctual attendance

1.6.2 Attending to details

- 1.6.2.1 Understand team or organizational goals, efforts, and requirements sufficiently to be able to assess and understand the purpose and appropriateness of detail work
- 1.6.2.2 Check work to ensure that all essential details have been considered
- 1.6.2.3 Notice errors or inconsistencies that others have missed, and take prompt, thorough action to correct errors

1.6.3 Complying with policies and procedures

- 1.6.3.1 Follow written and verbal directions
- 1.6.3.2 Comply with organizational rules, policies, and procedures
- 1.6.3.3 Resolve uncertainties with rules, policies, and procedures to assure compliance

1.7 Lifelong Learning: Displaying a willingness to learn and apply new knowledge and skills.

1.7.1 Demonstrating an interest in learning

- 1.7.1.1 Demonstrate an interest in personal learning and development
- 1.7.1.2 Seek feedback from multiple sources about how to improve, develop, and modify behavior based on feedback and/or self-analysis of past mistakes

1.7.1.3 Use newly learned knowledge and skills to complete specific tasks

1.7.2 Participating in training

1.7.2.1 Take steps to develop and maintain the knowledge, skills, and expertise necessary to perform one's role successfully

1.7.2.2 Participate fully in relevant training and professional development programs

1.7.2.3 Broaden knowledge and skills through technical expositions, seminars, professional groups, reading publications, job shadowing, certification, and continuing education

1.7.3 Anticipating changes in work

1.7.3.1 Anticipate changes in work demands and search for and participate in assignments or training that address these changing demands

1.7.3.2 Treat unexpected circumstances as opportunities to learn

1.7.4 Identifying career interests

1.7.4.1 Take charge of personal career development by identifying occupational interests, strengths, options, and opportunities

1.7.4.2 Make insightful career planning decisions based on integration and consideration of others' feedback, and seek out additional training to pursue career goals

Tier 2: Academic Competencies

2.1 Security Fundamentals: Understands and can apply basic security principles to the security of the enterprise or a specific structure, system, or process.

2.1.1 Plan, organize, direct, and manage the organization's security program to avoid/control losses and apply the process to provide a secure work environment.

2.1.2 Develop, manage, or conduct threat/vulnerability analyses to determine the probable frequency and severity of natural and man-made disasters, criminal activity, counterproductive and risk behaviors and risk categories on the organization's profitability, function, safety, and or ability to deliver products/services.

2.1.3 Evaluate methods to improve security and loss prevention and information loss prevention systems on a continuous basis through auditing, review, and assessment.

2.1.4 Develop and present employee security awareness programs to achieve organizational goals and objectives.

2.1.5 Conducts pre-employment background screening for the unit, organization, operation, or enterprise.

2.2 Business Foundations: Understand basic business principles, trends, and economics.

2.2.1 Develop and manage budget and financial controls to achieve fiscal responsibility

2.2.2 Develop, implement, and manage policies, procedures, plans and directives to achieve organizational objectives.

2.2.3 Develop procedures/techniques to measure and improve organizational productivity

2.2.4 Develop, implement, and manage staffing, leadership, training, and management programs in order to achieve organizational objectives

2.2.5 Monitor and ensure a sound ethical climate in accordance with the laws and the organization's directives and standards to support and promote proper enterprise practices.

2.3 Critical and Analytical Thinking: Using logic, reasoning, and analysis to address problems.

2.3.1 Reasoning

2.3.1.1 Possess sufficient logic, inductive, and deductive reasoning ability to perform job successfully

2.3.1.2 Critically review, analyze, synthesize, compare, and interpret information

2.3.1.3 Draw conclusions from relevant and/or missing information

2.3.1.4 Understand the principles underlying the relationship among facts and apply this understanding when solving problems

2.3.1.5 Be able to differentiate between fact and opinion

2.3.1.6 Be able to effectively and efficiently present logic, reasoning, and analysis to others

2.3.2 Mental agility

2.3.2.1 Identify connections between issues

2.3.2.2 Quickly understand, orient to, and learn new assignments

2.3.2.3 Shift gears and change direction when working on multiple projects or issues

2.4 Communication: Giving full attention to what others are saying, and communicating in English well enough to be understood by others.

2.4.1 Listening

- 2.4.1.1 Receive, attend to, interpret, understand, and respond to verbal messages and other cues
- 2.4.1.2 Pick out important information in communications
- 2.4.1.3 Understand complex instructions
- 2.4.1.4 Acknowledge feelings and concerns of communications

2.4.2 Communication

- 2.4.2.1 Express relevant information appropriately to individuals or groups taking into account the audience and the nature of the information (e.g., technical or controversial)
- 2.4.2.2 Communicate clearly and confidently
- 2.4.2.3 Communicate using common English conventions including proper grammar, tone, and pace
- 2.4.2.4 Track listener responses and react appropriately to those responses
- 2.4.2.5 When possible, effectively use eye contact and non-verbal expression
- 2.4.2.6 Ask questions or report problems or concerns to people in authority when information or procedures are unclear or need improvement, or when feeling unsafe or threatened in the workplace

2.4.3 Two-way communication

- 2.4.3.1 Practice meaningful two-way communication (i.e., communicate clearly, pay close attention, and seek to understand others, and clarify information)
- 2.4.3.2 Be able to demonstrate good listening by summarizing or repeating communication back to other speakers
- 2.4.3.3 As appropriate, effectively use eye contact, posture, and other nonverbal cues
- 2.4.3.4 Be able to effectively answer questions of others or communicate an inability to do so and suggest other sources of answers

2.4.4 Persuasion/influence

- 2.4.4.1 Persuasively present thoughts and ideas
- 2.4.4.2 Gain commitment and ensure support for proposed ideas

2.5 Reading and Writing: Understanding written sentences and paragraphs in work-related documents. Using standard English to compile information and prepare written reports.

2.5.1 Comprehension

- 2.5.1.1 Locate, understand, and interpret written information in prose and in documents such as manuals, reports, memos, letters, forms, graphs, charts, tables, calendars, schedules, signs, notices, applications, and directions
- 2.5.1.2 Understand the purpose of written materials
- 2.5.1.3 Attain meaning and comprehend core ideas
- 2.5.1.4 Learn definitions of unfamiliar terms
- 2.5.1.5 Critically evaluate and analyze information in written materials
- 2.5.1.6 Integrate and synthesize information from multiple written materials

2.5.2 Attention to detail

2.5.2.1 Identify main ideas, implied meaning and details, missing information, biases, differing perspectives, sources, and reliability of written materials

2.5.2.2 Note details, facts, and inconsistencies

2.5.3 Application

2.5.3.1 Integrate what is learned from written materials with prior knowledge

2.5.3.2 Apply what is learned from written material to follow instructions and complete specific tasks

2.5.3.3 Apply what is learned from written material to future situations

2.5.4 Organization and development

2.5.4.1 Prepare reports that are easy to understand using proper terminology

2.5.4.2 Communicate thoughts, ideas, information, messages, and other written information which may contain technical material, in a logical, organized, efficient, and coherent manner

2.5.4.3 Present ideas that are well developed with supporting information and examples

2.5.5 Mechanics

2.5.5.1 Use standard syntax and sentence structure

2.5.5.2 Use correct spelling, punctuation, and capitalization

2.5.5.3 Use appropriate grammar (e.g., correct tense, subject-verb agreement, no missing words)

2.5.5.4 Write legibly

2.5.5.5 Proof read finished documents for errors

2.5.5.6 Distribute written materials appropriately for intended audiences and purposes

2.5.6 Tone

2.5.6.1 Write in a manner appropriate for the industry and organization

2.5.6.2 Use language appropriate for the target audience

2.5.6.3 Use appropriate tone and word choice (e.g., writing is professional and courteous)

2.6 STEM Literacy (Science, Technology, Engineering, Mathematics): Understand and apply science, technology, engineering, and mathematics to work within individual roles and responsibilities and in collaborating with allied workers.

2.6.1 Science: Using scientific rules and methods to solve problems.

2.6.1.1 Scientific Method

- Understand the scientific method (identify problems, collect information, form and validate hypotheses, draw conclusions) and apply basic scientific research
- Apply the scientific method to testing, measuring, and troubleshooting security functions

2.6.1.2 Scientific Investigation

- Formulate scientifically investigable questions, construct investigations, collect and evaluate data, and develop scientific recommendations based on findings

- Evaluate scientific constructs including: conclusions, conflicting data, controls, data, inferences, limitations, questions, sources of errors, and variables

2.6.1.3 Applications

- Apply basic scientific principles to work-related responsibilities
- Physical
- Environmental
- Technological
- Compliance and Quality Assurance

2.6.2 Technology: Using technology tools such as software, computers, communication devices and related applications to input, retrieve, monitor, measure and communicate information.

2.6.2.1 Understand terminology and demonstrate familiarity with the function and capabilities of common computer, software, information and communication technology devices, communication systems, information systems, components, and concepts, including wired and wireless telephones, wearable computing, audio conferences, videoconferences, and online collaboration tools

2.6.2.2 Understand and efficiently use common computer hardware (e.g., desktops, laptops, tablets, PC components, cabling, wearable computing), software (e.g., operating systems, applications, communication, collaboration, and productivity software) and communication devices (e.g., telephony, wireless devices, network, and wireless systems) to perform tasks and communicate effectively

2.6.2.3 Use word processing applications to compose, organize, and edit simple documents and other business communications, and produce accurate outputs to print or share electronically

2.6.2.4 Use standard formulas and functions, format and modify content, and demonstrate competence in creating and formatting spreadsheets, graphs, or charts

2.6.2.5 Use spreadsheet, database, and presentation software both independently and in an integrated fashion

2.6.2.6 Use audio and video recording equipment and software to produce digital audio and video records and communications

2.6.2.7 Manage file storage: use functions to store, retrieve, and sort documents

2.6.2.8 Understand social media and their appropriate workplace uses and risks

2.6.2.9 **Define:** Be able to define a problem that needs information in order to be solve

2.6.2.10 **Access:** Search, find and retrieve appropriate information relative to the task

2.6.2.11 **Manage:** Apply an organizational or classification system to organize retrieved information

2.6.2.12 **Evaluate:** Be able to judge the quality, relevance, usefulness, efficiency, and adequacy of information and information sources for the defined purpose (including the authority, bias, and timelines of information)

2.6.2.13 **Integrate:** Interpret and represent data and information gathered, using quality management tools to organize, compare, contrast, summarize and synthesize information from multiple sources

2.6.2.14 **Create:** Adapt, apply, design or author information resulting from the research that describes the research and its analysis and findings, facilitates decision-making, and develops conclusions and recommendations

2.6.2.15 **Communicate:** Communicate that research and its findings effectively and efficiently in person and through written, visual, and digital media in a way that is appropriate for the intended audience

2.6.2.16 Understand new and emerging technologies that present solutions and risk

2.6.2.17 Demonstrate skill in applying and incorporating technologies into proposed solutions

2.6.2.18 Understand industry indicators useful for identifying technology trends and applications that can be applied to enhance the security of an enterprise, division or function of a group, asset, or person

2.6.3 Engineering: Using applications of scientific, economic, social, and practical knowledge in order to enhance, design, plan and inspect the security of systems, processes, and the physical structures.

2.6.3.1 Design, Application, and Integration of Physical Security Systems

- Understands the basics of systems engineering, IT fundamentals, communications systems basics to help bridge the gaps across disciplines, facilitation security integrations in designs and avoid engineering re-designs.
- Establish security system requirements and performance specifications.
- Understands security legislative and regulatory functions and their impact on the design and construction physical structures, systems, and processes.
- Applies physical security measures and select appropriate system components.
- Is able to clearly and effectively communicate with corporate managers, end customers and engineers from other departments
- Develop and documents system design and pre-implementation plans.
- Identifies problems or opportunity to enhance security through the collection and analysis of data
- Helps determine the specifications for the solution and develops conceptual design for facilities security, systems, and processes, collaborates with others to reach consensus, and issues opinions for security designs
- Reviews, evaluates, and implements new technologies that support best practices in areas that include, but are not limited to compliance, work management, outage restoration, and the planning and scheduling of work.
- Uses logical thought processes to analyze information and draw conclusions
- Identifies inconsistent or missing information
- Critically reviews, analyzes, synthesizes, compares, and interprets information
- Tests possible hypotheses to ensure the security infrastructure, process or system is correctly analyzed or problems are properly diagnosed and the best solution is found

2.6.3.2 Project Planning

- Determines project requirements and estimates resources
- Conducts economic analyses to determine optimum plan
- Creates an effective project plan
  - Prioritize tasks
  - Create milestones
- Anticipates project constraints and creates alternative plans
- Monitors project status against the plan and reports on the results
- Provides input for requests for proposal (RFP's) and assists in the analysis of responses
- Provides input into the preparation of contracts and participates in the negotiation of revisions, changes, and additions to contractual agreements with consultants, clients, suppliers, and subcontractors.
- Acts independently on technical matters in the assigned field of expertise and recommends approval of professional services, materials & construction procurement contracts as related to the security of physical structures, processes, and systems.

2.6.4 Mathematics: Using mathematics to express ideas, implement metrics, create fiscal projections, and solve problems.

2.6.4.1 Quantification

- Read and write numbers
- Count and place numbers in sequence
- Understand relationships between numbers

2.6.4.2 Computation

- Add, subtract, multiply, and divide with whole numbers, fractions, decimals, and percentages
- Calculate averages, ratios, proportions, and rates
- Convert decimals to fractions and fractions to decimals
- Convert fractions to percentages and percentages to fractions

2.6.4.3 Measurement and estimation

- Take and understand measurements of time, temperature, distances, length, width, height, perimeter, area, volume, weight, velocity, and speed
- Use and report measurements correctly, including units of measurement
- Convert from one measurement to another (e.g., from English to metric or International System of Units (SI), or Fahrenheit to Celsius)

2.6.4.4 Application

- Perform basic math computations accurately
- Translate practical problems into useful mathematical expressions
- Use appropriate mathematical formulas and techniques

Tier 3: Workplace Competencies

3.1 Teamwork: Working cooperatively with others to complete work assignments.

3.1.1 Acknowledging team membership and role

- 3.1.1.1 Accept membership in the team
- 3.1.1.2 Identify the roles of each team member
- 3.1.1.3 Show loyalty to the team
- 3.1.1.4 Determine when to be a leader and when to be a follower depending on what is needed to achieve the team's goals and objectives
- 3.1.1.5 Encourage others to express their ideas and opinions
- 3.1.1.6 Identify and draw upon team members' strengths and weaknesses to achieve results
- 3.1.1.7 Learn from other team members

3.1.2 Establishing productive relationships

- 3.1.2.1 Develop constructive and cooperative working relationships with others
- 3.1.2.2 Exhibit tact and diplomacy and strive to build consensus
- 3.1.2.3 Show sensitivity to the thoughts and opinions of other team members
- 3.1.2.4 Deliver constructive criticism and voice objections to others' ideas and opinions in a supportive, non- accusatory manner
- 3.1.2.5 Cooperate with others and contribute to the group's effort
- 3.1.2.6 Respond appropriately to positive and negative feedback

3.1.3 Identifying with the team and its goals

- 3.1.3.1 Identify the goals, norms, values, and customs of the team
- 3.1.3.2 Use a group approach to identify problems and develop solutions based on group consensus
- 3.1.3.3 Effectively communicate with all members of the group or team to achieve goals and objectives
- 3.1.3.4 Participate on virtual teams and use tools for virtual collaboration

3.1.4 Resolving conflicts

- 3.1.4.1 Bring others together to reconcile differences
- 3.1.4.2 Handle conflicts maturely by exercising "give and take" to achieve positive results for all parties
- 3.1.4.3 Reach formal or informal agreements that promote mutual goals and interests, and obtain commitment to those agreements from individuals or groups

3.2 Planning and Organizing: Planning and prioritizing work to manage time effectively and accomplish assigned tasks.

3.2.1 Planning

- 3.2.1.1 Approach work in a methodical manner
- 3.2.1.2 Plan and schedule tasks so that work is completed on time
- 3.2.1.3 Keep track of details to ensure work is performed accurately and completely
- 3.2.1.4 Work concurrently on several tasks

3.2.1.5 Anticipate obstacles to project completion and develop contingency plans to address them

3.2.1.6 Takes necessary corrective action when projects go off-track

3.2.1.7 Apply lessons learned from previous tasks to more efficiently execute current tasks

3.2.2 Prioritizing

3.2.2.1 Prioritize various competing tasks and perform them quickly and efficiently according to their urgency

3.2.2.2 Find new ways of organizing work area or planning work to accomplish work more efficiently

3.2.3 Allocating resources

3.2.3.1 Determine personnel and other resources required for achieving project deliverables

3.2.3.2 Allocate time and resources effectively and coordinate efforts with all affected parties

3.2.4 Project management

3.2.4.1 Develop, communicate, and implement a plan for a project

3.2.4.2 Develop a timeline for sequencing the activities of a project

3.2.4.3 Keep track of time, resources, assignments, and deliverables

3.2.4.4 Anticipate obstacles and develop contingency plans

3.2.4.5 Document plans, assignments, changes, and deliverables

3.2.4.6 Understand and plan for dependencies (e.g., step A must be completed before step B)

3.2.4.7 Manage activities to meet plans and adjust plans and communicate changes as needed

3.2.4.8 Keep all parties informed of progress and all relevant changes to project timelines

3.2.4.9 Engage in effective time management to keep multiple tasks moving forward

3.3 Innovative Strategic Thinking: Generating innovative and creative solutions.

3.3.1 Employ unique analyses and generate new, innovative ideas in complex areas

3.3.2 Reframe problems in a different light to find fresh approaches

3.3.3 Entertain wide-ranging possibilities to develop unique approaches and useful solutions

3.3.4 Seek out and entertain diverse perspectives, including those from other fields and roles

3.3.5 Understand the pieces of a system as a whole and possess a big picture view of the situation

3.3.6 Integrate seemingly unrelated information to develop creative solutions

3.3.7 Develop innovative methods of obtaining or using resources when insufficient resources are available

3.3.8 Demonstrate innovative thinking by using new and existing technology in new ways

3.3.9 Find new ways to add value to the efforts of a team and organization

3.4 Problem Solving and Decision Making: Applying critical-thinking skills to solve problems by generating, evaluating, and implementing solutions.

3.4.1 Identifying the problem

- 3.4.1.1 Anticipate or recognize the existence of a problem
- 3.4.1.2 Identify the true nature of the problem by analyzing its component parts
- 3.4.1.3 Evaluate the importance of the problem
- 3.4.1.4 Use all available reference systems to locate and obtain information relevant to the problem
- 3.4.1.5 Recall previously learned information that is relevant to the problem
- 3.4.1.6 Document the problem and any corrective actions already taken and their outcomes

3.4.2 Locating, gathering, and organizing relevant information

- 3.4.2.1 Effectively use both internal resources (e.g., internal computer networks, manuals, policy, or procedure guidelines) and external resources (e.g., internet search engines) to locate and gather information relevant to the problem
- 3.4.2.2 Examine information obtained for rigor, relevance, and completeness
- 3.4.2.3 Recognize important gaps in existing information and take steps to eliminate those gaps
- 3.4.2.4 Organize/reorganize information as appropriate to gain a better understanding of the problem
- 3.4.2.5 Refer the problem to appropriate personnel when necessary

3.4.3 Generating alternatives

- 3.4.3.1 Integrate previously learned and externally obtained information to generate a variety of high-quality alternative approaches to the problem
- 3.4.3.2 Use logic and analysis to identify the strengths and weaknesses, the costs and benefits, and the short- and long-term consequences of different approaches

3.4.4 Choosing a solution

- 3.4.4.1 Choose the best solution after contemplating available approaches to the problem, environmental factors, and conducting cost/benefit analyses
- 3.4.4.2 Make difficult decisions even in highly ambiguous or ill-defined situations
- 3.4.4.3 Implementing the solution
- 3.4.4.4 Commit to a solution in a timely manner, and develop a realistic approach for implementing the chosen solution
- 3.4.4.5 Observe and evaluate the outcomes of implementing the solution to assess the need for alternative approaches and to identify lessons learned
- 3.4.4.6 Document issues, plans, and solutions; get appropriate permissions; and communicate appropriately to impacted stakeholders

3.4.5 Implementing the solution

- 3.4.5.1 Commit to a solution in a timely manner, and develop a realistic approach for implementing the chosen solution
- 3.4.5.2 Observe and evaluate the outcomes of implementing the solution to assess the need for alternative approaches and to identify lessons learned
- 3.4.5.3 Document issues, plans, and solutions; get appropriate permissions; and communicate appropriately to impacted stakeholders

3.5 Working with Tools and Technology: Selecting, using, and maintaining tools and technology to facilitate work activity.

3.5.1 Selection and application

- 3.5.1.1 Identify, evaluate, select, and apply hardware or software tools or technological solutions appropriate to the task at hand (e.g., use statistical tools to show reliability of data)
- 3.5.1.2 Identify potential hazards or risks related to the use of tools and equipment
- 3.5.1.3 Present and obtain approval from decision-makers for acquiring tools and solutions
- 3.5.1.4 Negotiate with and manage relationships with vendors of tools and technologies
- 3.5.1.5 Operate tools and equipment in accordance with established operating procedures and safety standards
- 3.5.1.6 Document tools and technologies and how they are used in the organization

3.5.2 Keeping current

- 3.5.2.1 Seek out and continue learning about new and emerging tools, technologies, and methodologies that may assist in streamlining work and improving productivity
- 3.5.2.2 Take charge of your own personal and professional growth

3.6 Business Acumen: Understand basic business principles, trends, and economics.

3.6.1 Situational awareness

- 3.6.1.1 Understand business mission and goals: impact, profit, market share, and/or reputation
- 3.6.1.2 Understand the industry, trends in the industry, and the company's position in the industry and market
- 3.6.1.3 Recognize one's role in the functioning of the company and understand the potential impact one's own performance can have on the success of the organization
- 3.6.1.4 Stay current on organizational strategies to maintain competitiveness
- 3.6.1.5 Understand relevant legal and regulatory requirements of the operation

3.6.2 Business practices

- 3.6.2.1 Apply effective people and project management skills
- 3.6.2.2 Understand fundamental and relevant business customer and supplier relationships
- 3.6.2.3 Use product improvement techniques
- 3.6.2.4 Comply with the norms of conventional business etiquette
- 3.6.2.5 Protect intellectual property and proprietary information
- 3.6.2.6 Demonstrate understanding of the importance of adding value to the enterprise

3.6.3 Business ethics

- 3.6.3.1 Act in the best interest of the company, the community, and the environment
- 3.6.3.2 Comply with applicable laws and rules governing work and report loss, waste, or theft of company property to appropriate personnel

3.6.3.3	Demonstrate professional ethics to protect the privacy of the client, the integrity of the profession, and the privacy and integrity of you as an individual
3.7 Health and Safety: Supporting a safe and healthy workplace.	
3.7.1 Maintaining a healthy and safe environment	
3.7.1.1	Take actions to ensure the safety of self and others, in accordance with established personal and jobsite safety practices
3.7.1.2	Anticipate and prevent work-related injuries and illnesses
3.7.1.3	Comply with federal, state, and local regulations, and company health and safety policies
3.7.1.4	Recognize common hazards and unsafe conditions that occur at work, their risks, and appropriate controls to address them
3.7.1.5	Follow organizational procedures and protocols for workplace emergencies, including safe evacuation and emergency response
3.7.1.6	Maintain a sanitary and clutter-free work environment
3.7.1.7	Administer first aid or CPR, if trained, and summon assistance as needed
3.7.1.8	Properly handle and dispose of hazardous materials
3.7.2 Safeguarding one's person	
3.7.2.1	Engage in safety training
3.7.2.2	Use equipment and tools safely
3.7.2.3	Use appropriate personal protective equipment
3.7.2.4	Recognize how workplace risks can affect one's life and one's family
3.7.2.5	Understand the legal rights of workers regarding workplace safety and protection from hazards
3.7.2.6	Report injuries, incidents, and workplace hazards to a supervisor as soon as safely possible
3.7.2.7	Contribute to discussions of safety concerns in the workplace, making suggestions as appropriate

Tier 4: Industry-Wide Technical Competencies

4.1 Risk Management: Demonstrate ability to identify threats/risks and vulnerabilities taking into account the frequency, probability, speed of development, severity, and reputational impact to achieve a holistic view of risk across the entity.

4.1.1 Demonstrate ability to classify risks.

- 4.1.1.1 Classify risks according to relevant criteria under the entity's control
- 4.1.1.2 Classify risks according to relevant criteria beyond the entity's control
- 4.1.1.3 Classify risks according to relevant criteria with prior warnings (such as human behaviors, tornadoes, and hurricanes)
- 4.1.1.4 Classify risks according to relevant criteria with no prior warnings (such as human behaviors, earthquakes)

4.1.2 Demonstrate ability to identify the organization's risk exposures from both internal and external sources.

- 4.1.2.1 Demonstrate ability to identify the organization's nature disaster risks
- 4.1.2.2 Demonstrate ability to identify the organization's technological risks
- 4.1.2.3 Demonstrate ability to identify the organization's human risks (e.g., workplace violence, theft, fraud, counterfeit products and services, accidental, negligent behaviors, reckless behaviors and intentional behaviors and services etc.)
- 4.1.2.4 Demonstrate ability to identify the organization's controllable exposures/risks versus those beyond the entity's control
- 4.1.2.5 Demonstrate ability to identify the organization's resilience to events with prior warnings versus those with no prior warnings

4.1.3 Demonstrate ability to assess an organizations risk exposure over multiple assets

- 4.1.3.1 Facility
- 4.1.3.2 Security (both physical and logical)
- 4.1.3.3 Reputational / Brand
- 4.1.3.4 Legal
- 4.1.3.5 Customer
- 4.1.3.6 Procedural
- 4.1.3.7 IT (including enterprise infrastructure)
- 4.1.3.8 People
- 4.1.3.9 Supply Chain (including transportation and outsourcing)
- 4.1.3.10 Compliance
- 4.1.3.11 Availability of personnel
- 4.1.3.12 Network Communications technology

4.1.4 Explain the proper use of penetration testing and vulnerability scanning for vulnerability assessments

4.1.5 Explain the rationale of and adhere supply chain security/risk management policies, requirements, and procedures

4.1.6 Explain the need for security products and services used in an organization's operations and the need for continuous metrics on their ability to effectively address current and foreseeable risks

4.1.7	Explain the need to track/control/prevent/correct installation and execution of security products and services for the enterprise based on an asset inventory of approved procurements
4.1.8	Explain the importance of training an organization's workers to use sensitive business information, access to facilitates and other behaviors properly and to protect the organization's and its stakeholders' resources
4.1.9	Describe and practice safe behaviors and avoid counterproductive or risk generating worker behaviors
4.1.10	Explain the risks associated with social media and the countermeasures available to address them
4.1.11	Explain the impact and proper use of environmental controls
4.1.12	Explain the need for security audit logging and analysis
4.2 Compliance and Legal Aspects: Develop and maintain security policies, procedures and practices that comply with relevant elements of criminal, civil, administrative, and regulatory law to minimize adverse legal consequences.	
4.2.1	Provide coordination, assistance, and evidence such as documentation and testimony to support actual or potential proceedings
4.2.2	Provide advice and assistance to management and others in developing performance requirements and contractual terms for security vendors/suppliers and establish effective monitoring processes to ensure that organizational needs and contractual requirements are being met
4.2.3	Develop and maintain security policies, procedures, and practices that comply with relevant laws regarding investigations, personnel security, information security and other areas
4.3 Personnel Security and Business Continuity: Develop, implement, and manage systems and security practices that protect people and practices to ensure enterprise continuity and risk resilience.	
4.3.1	Develop, implement, and manage background investigations to validate individual for hiring, promotion, or retention
4.3.2	Develop, implement, manage, and evaluate policies, procedures, and programs, and methods to protect individuals in the workplace against harassment, threats, and violence
4.3.3	Identify critical business practices (such as complex supply chain strategies implemented on a regional or global scale) that may adversely impact the entity's ability to recover following a disaster event
4.3.4	Clearly define resource requirements for the Business Continuity Plan and solicit management support and commitment for required resources
4.3.5	Present and obtain management/leadership support, approval, and sponsors of Business Continuity Plan
4.3.6	Work with management and any risk management/enterprise risk management groups within the entity to gain agreement on a clear and standardized risk assessment methodology and to gain understanding of the entity's tolerance for risk
4.3.7	Design a crisis communications plan that addresses the need for effective and timely communication between the entity and all the stakeholders impacted by an event or involved during the response and recovery efforts

4.3.8	Provide guidance within the plan to determine frequency of communications needed to each stakeholder before an event, during the event itself, and following an event.
4.3.9	Identify and establish relationships with the internal departments and personnel and external agencies, contractors, and others with responsibility for emergency preparedness and response
4.3.10	Develop an incident response strategy and plan to limit incident effect and to repair incident damage
4.3.11	Identify trigger points for key service and support areas to identify, escalate and execute strategies selected to take advantage of key risks
4.3.12	Develop formal reports and presentations focused on increasing the awareness and potential impact of risks to the organization from a business continuity perspective
4.3.13	Define organizational titles, roles, lines of authority, succession of authority, and responsibilities for internal and external resources (e.g., corporate/business unit, departments, managers, supervisors, public agencies, contractors, etc.)
4.3.14	Establish an exercise, testing, maintenance, and audit program for the Business Continuity Plan to establish confidence in a predictable and repeatable performance of recovery activities throughout the organization
4.3.15	Coordinate, conduct, and or participate in training, drills, and exercises with first responders to comply with regulations, as needed to establish required capabilities, and or as requested by first responders
4.3.16	Conduct a debrief meeting immediately following training, drills and exercises and document actions to be taken to improve emergency preparedness and response capabilities
4.3.17	Design framework and define document structure for the plan documentation
4.3.18	Define and obtain approval for criteria to be used to assess the impact on the entity's operations including but not limited to: customer impact; financial impact; regulatory impact (fines, penalties, required to pull product off market due to loss of safety information); operational impact; reputational impact; human impact
4.4 Physical Security: Measures that are designed to deny unauthorized access to facilities, equipment, and resources, and to protect personnel and property from damage or harm, involving the use of multiple layers of interdependent systems and techniques.	
4.4.1	Survey facilities in order to manage and or evaluate the current status of physical security, emergency and or restoration capabilities
4.4.2	Select, implement, and manage security processes to reduce the risk of loss
4.4.3	Assess the effectiveness of security measures by testing and monitoring
4.4.4	Identify assets to determine their value loss impact and criticality
4.4.5	Assess the nature of threats so that scope of the problem can be determined
4.4.6	Conduct a physical security survey in order to identify the vulnerability of the organization
4.4.7	Perform risk analysis so that appropriate countermeasures can be developed
4.4.8	Establish security system requirements and performance specifications
4.4.9	Apply physical security measures and select appropriate system components
4.4.10	Develop and conduct system design and pre-implementation plans
4.4.11	Outline criteria for pre-bid meeting to ensure comprehensiveness of implementation
4.4.12	Procure physical security measures, implement recommended quality assurance plan(s)

4.4.13	Conduct commissioning acceptance testing, and delivery of the physical security measure
4.5 Cyber/Information Security: The practice of protecting physical and electronic information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.	
4.5.1	Survey information facilities, processes, and systems to evaluate current status of: physical security, procedural security, information systems security, employee awareness, and information destruction and recovery capabilities.
4.5.2	Develop and implement policies and standards to ensure information is evaluated and protected against all forms of unauthorized inadvertent access, use, disclosure, modification, destruction, or denial.
4.5.3	Develop and manage a program of integrated security controls and safeguards to ensure confidentiality, integrity, availability, authentication, non-repudiation, accountability, recoverability, and audit ability of sensitive information and associated information technology resources, assets, and investigations.
4.5.4	Evaluate the effectiveness of the information security program's integrated security controls, to include related policies, procedures, and plans, to ensure consistency with organization strategy, goals, and objectives.
4.5.5	Risk mitigation applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the internet.
4.5.6	Secure processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction, and is of growing importance in line with the increasing reliance on computer systems of most societies worldwide.
4.6 Crisis Management: The process by which an enterprise deals with a critical incident or major event that threatens to harm the organization, its property, assets, systems, continuity and or people.	
4.6.1	Assess and prioritize risks to mitigate potential consequences of incidents.
4.6.2	Prepare and plan how the organization will respond to incidents.
4.6.3	Respond to and manage an incident.
4.6.4	Recover from incidents by managing the recovery and resumption of operations.
4.7 Investigations: The methodology the enterprise undertakes to collect and preserve information in reports to enable the enterprise to make reliable decisions in response to situations effectively interface with all stakeholders.	
4.7.1	Develop and manage investigation programs.
4.7.2	Manage or conduct the collection and preservation of evidence to support post-investigation actions (employee discipline, criminal or civil proceedings, arbitration and or other processes).
4.7.3	Manage or conduct surveillance processes.
4.7.4	Manage or conduct specialized investigations.
4.7.5	Manage or conduct investigative interviews.

4.8 Case Management: A system to manage, analyze, report and present findings from investigations for internal enterprise stakeholders and external systems.
4.8.1 Analyze case for applicable ethical conflicts 4.8.2 Analysis and assess case elements and strategies 4.8.3 Determine need and develop strategy by reviewing procedural options 4.8.4 Prepare reports to substantiate investigative findings 4.8.5 Prepare and present business case, testimony, or other case presentation by reviewing case files, meeting with stakeholders, and presenting relevant facts.
4.9 Globalization and Cultural Awareness: Integrating cultures and global dynamics into security systems, metrics, and responses.
4.9.1 Understand how security supports and is affected by globalization. 4.9.2 Understand the impact of globalization on the business model. 4.9.3 Interpret and adhere to global standards and standardization. 4.9.4 Integrates cultural aspects into security applications and functions.
4.10 Governance: Specialty areas providing leadership, management, direction, and or development and advocacy so that individual and organization may effetely conduct security work.
4.10.1 Leading security policy and decision-making for the enterprise. 4.10.2 Accountability with budgets, finance, and security decisions. 4.10.3 Managing employment decisions, qualifications, and related policies. 4.10.4 Leading communication with executive decision makers and external representations.

Tier 5: Industry-Sector Functional Areas

NOTE: The 'Industry-Sector Functional Areas' tier corresponds to workforce roles in a large number of industries and is meant to represent roles frequently aligned with the indicated specialty area. Please note, specialty areas reflect work that is highly specialized in diverse industries. At times, these roles may be assigned to a specific role or co-mingled with multiple enterprise security responsibilities in the industry it serves.

Many competency models published with the U.S. Department of Labor do not populate the 4th Tier. The research, industry validation and guidance received by the Executive Steering Committee indicate distinct competencies utilized in a distinct number of industry segments. Although each segment is outlined in this section, the research on the specific competencies utilized by each segment will continue with the involvement of aligned ASIS International Councils and allied organizations that offer specialized expertise in each segment herein.

1. Loss Prevention: Is a set of practices employed by retail companies and other corporate sectors reducing preventable losses and secure corporate systems, policies, and procedures to mitigate losses caused by deliberate or inadvertent human actions.
2. Banking and Financial Services: Is a specialized security field including retail banking, mortgage, credit/debit cards, internet banking, commercial and consumer lending to stock brokerages, insurance companies, and other financial institutions requiring a sophisticated application of various regulatory agencies.
3. Engineering & Design: Is a specialized field of engineering that focuses on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts.
4. Government Services: Government/industrial security professionals provide a variety of services from the protection of classified information in accordance with the National Industrial Security Program (NISP) to the protection of buildings, people, and assets.
5. Hospitality & Entertainment: Security specialists operate in the hospitality, hotel, lodging, entertainment, event, and gaming applying risk and personnel management, budgeting and finance, and a host of other areas in this specialized security segment.
6. Healthcare: Security in the healthcare industry involves in a work environment oriented toward patient protection and service, and may also include safety and community emergency management, supply chain security, pharmaceutical security, and other areas of specialization.
7. Manufacturing: The security of manufacturing and industrial, as well as food and beverage production and processing and warehouse and distribution, facilities and operations includes industry specific risks and security risks.
8. Services Sales, Equipment: Is a specialized area of security-related products and services have resulting from emerging threats and evolving high technology.
9. Transportation: Specialized security segment that includes shipping, carrying, railroads, highways, freight, trucking, tourism, air cargo, ports, and other transportation domains with unit standards for security within the industry.
10. Utilities: Utilities refers to the security operations within telecommunications, water, electric, and nuclear power plants, and related private corporations. Even though sources of power differ, there are common facilities to all utility operations.

Resources Reviewed

Developer	Resource	Resource URL
ASIS International and the Institute of Finance & Management (IOFM)	*The United States Security Industry: Size and Scope, Insights, Trends, and Data*, 2013.	
University of Phoenix/ASIS Foundation	*Enterprise Security Risks and Workforce Competencies – Findings From An Industry Roundtable on Security Talent Development,* September 2013	http://cdn.assetsphoenix.net/content/dam/altcloud/doc/industry/UOPX-ASISFoundationSecurityRisksandCompetenciesReport.pdf
University of Phoenix/ASIS Foundation	*Security Industry Survey of Risks and Professional Competencies*, August, 2014	http://cdn.assets-phoenix.net/content/dam/altcloud/doc/industry/ASIS-Security-report-WEB.pdf
University of Phoenix/ASIS Foundation	*Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals*, September, 2014	http://cdn.assets-phoenix.net/content/dam/altcloud/doc/industry/cybersecurity-report.pdf
Security Executive Council	Corporate Governance and Compliance Hotline Benchmark Report, 2007	
ASIS International	Board Certification, Certified Protection Professional (CPP) (2014)	
ASIS International	Board Certification, Professional Certified Investigator (PCI), 2014	
ASIS International	Board Certification, Physical Security Professional (PSP), 2014	
ASIS Foundation, Justice & Safety Center, Eastern Kentucky University, and the National Institute of Justice	Scope and Emerging Trends, ASIS Foundation Security Report, 2005	
ASIS Foundation, National Counterintelligence Executive, ASIS Information Asset Protection Council	Trends in Proprietary Information Loss, Survey Report, 2007	
ASIS Foundation	ASIS Foundation CRISP Report: Lost Laptops = Loss Data Measuring Costs, Managing Threats, by Glen Kitteringham, CPP, (2008)	

Developer	Resource	Resource URL
ASIS Foundation	ASIS Foundation CRISP Report: Situational Crime Prevention and Supply Chain Security, Theory For Best Practice, Harland Haelterman, PhD 2013	
ASIS Foundation	ASIS Foundation CRISP Report: Tackling the Insider Threat, Nick Catrantzos, CPP, 2010	
ASIS International	Business Continuity Guidelines, A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, 2005	
ASIS International	Business Continuity Management Systems: Requirement with Guidance for Use, ASIS International/BSI BCM.01-2010, American National Standard	
ASIS International	General Security Risk Assessment Guideline, 2006	
ASIS International	Chief Security Office (CS0) Organizational Standard, ASIS CSO1.-2008, American National Standard	
ASIS International	Facilities Physical Security Measures, ASIS GLD FPSM-2009 Guideline	
	Organizational Resilience: Security, Preparedness, and Continuity Management Systems	
ASIS International	Requirements with Guidance for Use, ASIS SPC 1-2009, American National Standard	
ASIS International	Information Asset Protection, Guideline, 2007	
ASIS International	Pre-employment Background Screening, ASIS GDL PBS 2009, Guideline	
ASIS International	Workplace Violence Prevention and Intervention, ASIS/SHRM WVPI.1-2011, American National Standard	

Developer	Resource	Resource URL
ASIS International	Workplace Violence Prevention and Response, Guideline, 2005	
O*NET Online	2013 O*NET Summary Reports for category: Security Managers 11-9199.07	http://www.onetonline.org/link/summary/11-9199.07
O*NET Online	2013 O*NET Summary Reports for category: Security Management Specialists 13-1199.02	http://www.onetonline.org/link/summary/13-1199.02
O*NET Online	2013 O*NET Summary Reports for category: Security Officers 33-9032.00	http://www.onetonline.org/link/summary/33-9032.00
O*NET Online	2013 O*NET Summary Reports for category: Gaming Surveillance Officers and Gaming Investigators 33-9031.00	http://www.onetonline.org/link/summary/33-9031.00
O*NET Online	2013 O*NET Summary Reports for category: Loss Prevention Managers 11-9199.08	http://www.onetonline.org/link/summary/11-9199.08
O*NET Online	Retail Loss Prevention Specialists 33-9099.02	http://www.onetonline.org/link/summary/33-9099.02
O*NET Online	2013 O*NET Summary Reports for category: Security Guards 33-9032.00	http://www.onetonline.org/link/summary/33-9032.00
O*NET Online	2013 O*NET Summary Reports for category: Private Detectives and Investigators 33-9021.00	http://www.onetonline.org/link/summary/33-9021.00
O*NET Online	2013 O*NET Summary Reports for category: Occupational Health and Safety Specialists 29-9011.00	http://www.onetonline.org/link/summary/29-9011.00
O*NET Online	2013 O*NET Summary Reports for category: Occupational Health and Safety Technicians 29-9012.00	http://www.onetonline.org/link/summary/29-9012.00
O*NET Online	2013 O*NET Summary Reports for category: Information Security Analysts 15-1122.00	http://www.onetonline.org/link/summary/15-1122.00

Developer	Resource	Resource URL
O*NET Online	2013 O*NET Summary Reports for category: Intelligence Analysts 33-3021.06	http://www.onetonline.org/link/summary/33-3021.06
O*NET Online	2013 O*NET Summary Reports for category: Business Continuity Planners 13-1199.04	http://www.onetonline.org/link/summary/13-1199.04
O*NET Online	2013 O*NET Summary Reports for category: Risk Management Specialists 13-2099.02	http://www.onetonline.org/link/summary/13-2099.02
O*NET Online	2013 O*NET Summary Reports for category: Emergency Management Directors 11-9161.00	http://www.onetonline.org/link/summary/11-9161.00
O*NET Online	2013 O*NET Summary Reports for category: Industrial Safety and Health Engineers 17-2111.01	http://www.onetonline.org/link/summary/17-2111.01
O*NET Online	2013 O*NET Summary Reports for category: Supply Chain Managers 11-9199.04	http://www.onetonline.org/link/summary/11-9199.04
O*NET Online	2013 O*NET Summary Reports for category: Industrial Safety and Health Engineers 17-211.01	http://www.onetonline.org/link/summary/17-2111.01
Loss Prevention Foundation	Loss Prevention Qualified Certification (LPQ)	
Loss prevention Foundation	Loss Prevention Certified Certification (LPC)	
American Hotel & Lodging Educational Institute	Certified Lodging Security Director (CLSD)	
American Bankers Association (ABA)	Institute Certified Financial Services Security Professional (CFSSP)	
International Information Systems Security Certification Consortium ((ISC)2)	Certified Information Systems Security Professional (CISSP)	
North American Electric Reliability Corporation (NERC)	System Operator Certification (SOC)	
EC-Council	Certified Ethical Hacker (CEH)	
Information Systems Audit and Control Association (ISACA)	Certified information Security Auditor (CISA)	

Developer	Resource	Resource URL
ISACA	Certified Information Security Manager (CISM)	
ISACA	Certified in Risk and Information Systems Control (CRISC)	
Global Information Assurance Certification (GIAC)	Certified Incident Handler (GCIH)	
GIAC	Certified Intrusion Analyst (GCIA)	
GIAC	Penetration Tester (GPEN)	
GIAC	Web Application Penetration Tester (GWAPT)	
International Association for Healthcare Security and Safety (IAHSS)	Basic Certification for the Healthcare Security Officer	
IAHSS	Advanced Certification for the Healthcare Security Officer	
IAHSS	Supervisory Certification for the Healthcare Security Professional	
IAHSS	Certified Healthcare Protection Administrator for the Healthcare Security Manager/Director	
Association of Certified Fraud Examiners	Certified Fraud Examiner (CFE)	
IAHSSP	Certified Healthcare Protection Administrator (CHPA)	
(ISC)2	Certified Information Systems Security Professional (CISSP)	
Educational Institute of the American Hotel and Lodging Association (AH&LA)	Certified Lodging Security Supervisor (CLSS) and Certified Lodging Security Director (CLSD)	
SANS Institute	Global Information Assurance Certificate (GIAC)	
National Classification Management Society (NCMS)	Industrial Security Professional (ISP)	