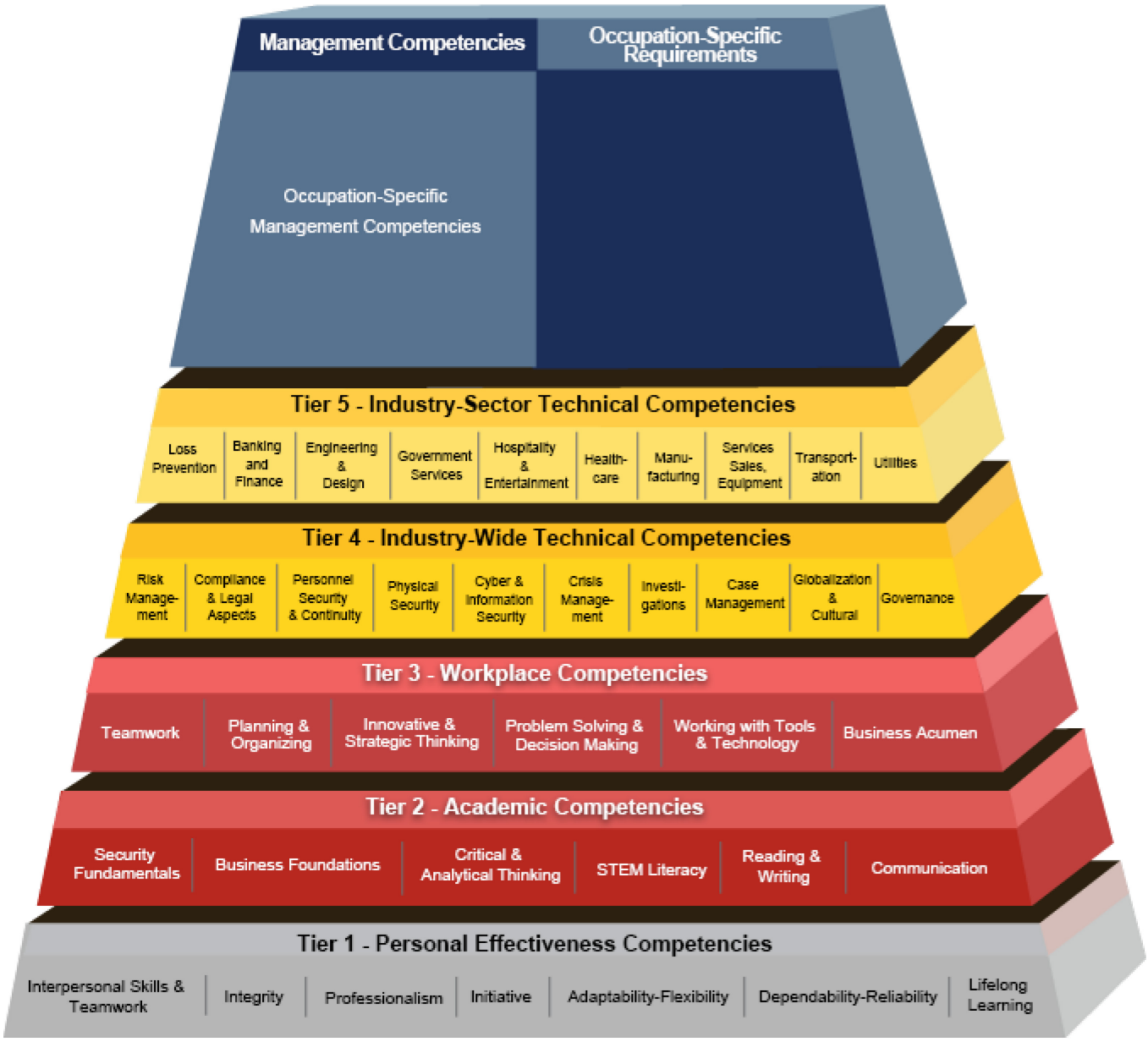
Enterprise Security Competency Model

2015

A collection of broad-based professional skills and competencies needed for successful work performance within the security industry

ASIS FOUNDATION™

Enterprise Security Competency Model



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

[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

prioritize the identified security risks, challenges, and professional competencies. The results of this industry survey were published on August 14, 2014.

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

[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.

The Enterprise Security Competency Model depicts the core competencies required for industry practitioners by utilizing the U.S. DOL Competency Model Clearinghouse public toolkit as an organizing framework.[7] To assist businesses, educators, and workforce development professionals in identifying the industry-specific skills and competencies that workers will require, this model consists of a set of building blocks that were created and arranged into nine tiers containing specific sets of related competencies. *"The arrangement of the tiers in a pyramidal shape represents the increasing level of specificity and specialization of content. As a user moves up through the various tiers of the model, the competencies become specific to certain industries and/or occupations*."[8]

Occupation-Related Competencies

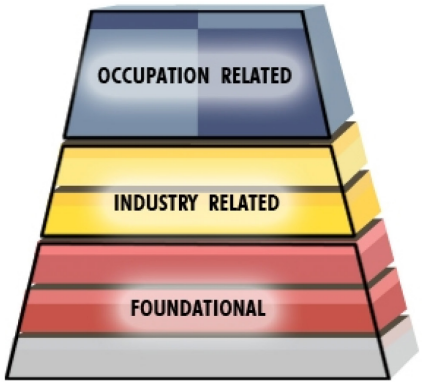
Tier 9 – Management Competencies
Tier 8 – Occupation-Specific Requirements
Tier 7 – Occupation-Specific Technical Competencies
Tier 6 – Occupation-Specific Knowledge Competencies

Industry-Related Competencies

Tier 5 – Industry-Sector Technical Competencies
Tier 4 – Industry-Wide Technical Competencies

Foundational Competencies

Tier 3 – Workplace Competencies
Tier 2 – Academic Competencies
Tier 1 – Personal Effectiveness Competencies



The U.S. DOL defines the three competency levels[9] as follows:

Foundational Competencies

At the base of the model, Tiers 1 through 3 represent competencies that provide the foundation for success in school and in the world of work. Foundational competencies are essential to a large number of occupations and industries. Employers have identified a link between foundational competencies and job performance and have also discovered that foundational competencies are a prerequisite for workers to learn industry-specific skills.

The Foundational Competency Level is organized into three competency tiers representing the "soft-skills" and work readiness skills that most employers demand:

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 through training, development, and experience.

[7] See "Introduction to the Tools," http://www.careeronestop.org/competencymodel/careerpathway/cpwoverview.aspx.
[8] See "Competency Model General Instructions," http://www.careeronestop.org/competencymodel/careerpathway/CPWGenInstructions.aspx.

[9] Ibid.

Tier 1 – Personal Effectiveness Competencies are personal attributes essential for all life roles. Often referred to as "soft skills," personal effectiveness competencies are generally learned in the home or community and honed at school and in the workplace.

Tier 2 – Academic Competencies are primarily learned in an educational setting. They include cognitive functions and thinking styles. Academic competencies are likely to apply to all industries and occupations.

Tier 3 – Workplace Competencies represent motives and traits, as well as interpersonal and self-management styles. They generally apply to a large number of occupations and industries.

Industry-Related Competencies

The competencies shown in Tiers 4 and 5 are referred to as Industry-Related Competencies and are specific to an industry or industry sector. Industry-wide technical competencies cut across industry subsectors, making it possible to create career lattices where a worker can move easily across industry subsectors. Rather than narrowly following a single occupational career ladder, this model supports the development of an agile workforce.

Tier 4 – Industry-Wide Technical Competencies cover the knowledge, skills, and abilities from which workers across the industry can benefit, regardless of the sector in which they operate. These competencies are considered cross-cutting, as they allow a worker to move easily across industry sub-sectors. Because of this mobility, many of the critical work functions on this tier deal with awareness or understanding, rather than performing specific job tasks.

Tier 5 – Industry-Sector Functional Areas correspond to workforce roles in a large number of industries, and are 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.

Upper Tiers

The competencies on Tiers 6, 7, 8, and 9 are referred to as Occupation Competencies and are developed to define performance in a workplace, to design competency-based curriculum, or to articulate the requirements for an occupational credential such as a license or certification. (It is important to note that the U.S. DOL emphasizes that the usefulness of the competency model framework is to serve broad industry competency requirements. Accordingly, these top-tier levels of Occupation Competencies are typically not completed on the models available on the U.S. DOL Competency Model Clearinghouse website. The DOL and this model will reference other resources that are available to support profession-specific competency mapping.

Tier 1 – Personal Effectiveness Competencies

1. Interpersonal Skills and Teamwork - Displaying skills to work with others from diverse backgrounds.

Demonstrating concern for others

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

Demonstrating insight into behavior

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

Maintaining open communication

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

Respecting diversity

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

2. Integrity - Displaying accepted social and work behaviors.

Behaving ethically

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

Acting fairly

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

Taking responsibility

- Take responsibility for accomplishing work goals within accepted timeframes, or for not accomplishing those goals

- Accept responsibility/accountability for one's decisions and actions and for those of one's group, team or department
- Understand that past behavior may affect one's ability to obtain occupation or meet occupational requirements
- Attempt to learn from mistakes

3. <u>Professionalism</u> - Maintaining a professional demeanor at work.

Demonstrating self-control

- Demonstrate self-control by maintaining composure and keeping emotions in check
- Deal calmly and effectively with stressful situations

Maintaining a professional appearance

- Maintain a professional demeanor
- Dress appropriately for occupation and its requirements
- Maintain appropriate personal hygiene
- Wear appropriate identification, as required
- Refrain from lifestyle choices which negatively impact the workplace and individual performance
- Be prepared to represent your organization and effort

Maintaining a positive attitude

- Project a positive image of oneself and the organization
- Demonstrate a positive attitude towards work
- Take pride in one's work and the work of the organization

4. <u>Initiative</u> - Demonstrating a willingness to work.

Persisting

- Pursue work with energy, drive, and a strong accomplishment orientation
- Persist and expend extra effort to accomplish tasks even when conditions are difficult or deadlines tight
- Persist at a task or problem despite interruptions, obstacles, or setbacks

Taking initiative

- Go beyond the routine demands of the job
- Take initiative in seeking out new work challenges and increasing the variety and scope of one's job
- Seek opportunities to influence events and originate action
- Assist others who have less experience or have heavy workloads
- Seek the information and assistance needed to be successful

Setting challenging goals

- Establish and maintain personally challenging but realistic work goals
- Exert effort toward task mastery
- Bring issues to closure by pushing forward until a resolution is achieved

Working independently

- Develop and use effective and efficient ways of performing tasks
- Perform effectively, even with minimal direction, support, approval, or direct supervision
- Strive to exceed standards and expectations
- Exhibit confidence in capabilities and an expectation to succeed in future activities

5. Adaptability and Flexibility - Displaying the capability to adapt to new, different, or changing requirements.

Employing unique analyses

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

Entertaining new ideas

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

Dealing with ambiguity

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

6. Dependability and Reliability - Displaying responsible behaviors at work.

Fulfilling obligations

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

Attending to details

- Understand team or organizational goals, efforts, and requirements sufficiently to be able to assess and understand the purpose and appropriateness of detail work

- Check work to ensure that all essential details have been considered
- Notice errors or inconsistencies that others have missed, and take prompt, thorough action to correct errors

Complying with policies and procedures

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

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

Demonstrating an interest in learning

- Demonstrate an interest in personal learning and development
- Seek feedback from multiple sources about how to improve, develop, and modify behavior based on feedback and/or self-analysis of past mistakes
- Use newly learned knowledge and skills to complete specific tasks

Participating in training

- Take steps to develop and maintain the knowledge, skills, and expertise necessary to perform one's role successfully
- Participate fully in relevant training and professional development programs
- Broaden knowledge and skills through technical expositions, seminars, professional groups, reading publications, job shadowing, certification and continuing education

Anticipating changes in work

- Anticipate changes in work demands and search for and participate in assignments or training that address these changing demands
- Treat unexpected circumstances as opportunities to learn

Identifying career interests

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

1. Security Fundamentals - Understands and can apply basic security principles to the security of the enterprise or a specific structure, system or process.
▪ Plan, organize, direct and manage the organization's security program to avoid/control losses and apply the process to provide a secure work environment. ▪ 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 organizations profitability, function, safety, and or ability to deliver products/services. ▪ Evaluate methods to improve security and loss prevention and information loss prevention systems on a continuous basis through auditing, review and assessment. ▪ Develop and present employee security awareness programs to achieve organizational goals and objectives. ▪ Conducts pre-employment background screening for the unit, organization, operation or enterprise.
2. Business Foundations - Understand basic business principles, trends, and economics.
▪ Develop and manage budget and financial controls to achieve fiscal responsibility ▪ Develop, implement, and manage policies, procedures, plans and directives to achieve organizational objectives. ▪ Develop procedures/techniques to measure and improve organizational productivity ▪ Develop, implement, and manage staffing, leadership, training, and management programs in order to achieve organizational objectives ▪ 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.
3. Critical and Analytical Thinking - Using logic, reasoning, and analysis to address problems.
Reasoning ▪ Possess sufficient logic, inductive, and deductive reasoning ability to perform job successfully ▪ Critically review, analyze, synthesize, compare, and interpret information ▪ Draw conclusions from relevant and/or missing information ▪ Understand the principles underlying the relationship among facts and apply this understanding when solving problems ▪ Be able to differentiate between fact and opinion

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

Mental agility

- Identify connections between issues
- Quickly understand, orient to, and learn new assignments
- Shift gears and change direction when working on multiple projects or issues

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

Listening

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

Communication

- Express relevant information appropriately to individuals or groups taking into account the audience and the nature of the information (e.g., technical or controversial)
- Communicate clearly and confidently
- Communicate using common English conventions including proper grammar, tone, and pace
- Track listener responses and react appropriately to those responses
- When possible, effectively use eye contact and non-verbal expression

Two-way communication

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

Persuasion/influence

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

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

Comprehension

- 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
- Understand the purpose of written materials
- Attain meaning and comprehend core ideas
- Learn definitions of unfamiliar terms
- Critically evaluate and analyze information in written materials
- Integrate and synthesize information from multiple written materials

Attention to detail

- Identify main ideas, implied meaning and details, missing information, biases, differing perspectives, sources, and reliability of written materials
- Note details, facts, and inconsistencies

Application

- Integrate what is learned from written materials with prior knowledge
- Apply what is learned from written material to follow instructions and complete specific tasks
- Apply what is learned from written material to future situations

Organization and development

- Prepare reports that are easy to understand using proper terminology
- Communicate thoughts, ideas, information, messages, and other written information which may contain technical material, in a logical, organized, efficient, and coherent manner
- Present ideas that are well developed with supporting information and examples

Mechanics

- Use standard syntax and sentence structure
- Use correct spelling, punctuation, and capitalization
- Use appropriate grammar (e.g., correct tense, subject-verb agreement, no missing words)
- Write legibly
- Proof read finished documents for errors
- Distribute written materials appropriately for intended audiences and purposes

Tone

- Write in a manner appropriate for the industry and organization
- Use language appropriate for the target audience
- Use appropriate tone and word choice (e.g., writing is professional and courteous)

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.

Science: Using scientific rules and methods to solve problems.

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

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

- 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
- 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
- Use word processing applications to compose, organize, and edit simple documents and other business communications, and produce accurate outputs to print or share electronically
- Use standard formulas and functions, format and modify content, and demonstrate competence in creating and formatting spreadsheets, graphs, or charts
- Use spreadsheet, database, and presentation software both independently and in an integrated fashion
- Use audio and video recording equipment and software to produce digital audio and video

records and communications

- Manage file storage: use functions to store, retrieve, and sort documents
- Understand social media and their appropriate workplace uses and risks
- Define: Be able to define a problem that needs information in order to be solve
- Access: Search, find and retrieve appropriate information relative to the task
- Manage: Apply an organizational or classification system to organize retrieved information
- 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)
- Integrate: Interpret and represent data and information gathered, using quality management tools to organize, compare, contrast, summarize and synthesize information from multiple sources
- 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
- 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
- Understand new and emerging technologies that present solutions and risk
- Demonstrate skill in applying and incorporating technologies into proposed solutions
- 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

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.

- 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

- 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.

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

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

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

Tier 3 – Workplace Competencies

1. **Teamwork** - Working cooperatively with others to complete work assignments.
Acknowledging team membership and role ▪ Accept membership in the team ▪ Identify the roles of each team member ▪ Show loyalty to the team ▪ 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 ▪ Encourage others to express their ideas and opinions ▪ Identify and draw upon team members' strengths and weaknesses to achieve results ▪ Learn from other team members **Establishing productive relationships** ▪ Develop constructive and cooperative working relationships with others ▪ Exhibit tact and diplomacy and strive to build consensus ▪ Show sensitivity to the thoughts and opinions of other team members ▪ Deliver constructive criticism and voice objections to others' ideas and opinions in a supportive, non- accusatory manner ▪ Cooperate with others and contribute to the group's effort ▪ Respond appropriately to positive and negative feedback **Identifying with the team and its goals** ▪ Identify the goals, norms, values, and customs of the team ▪ Use a group approach to identify problems and develop solutions based on group consensus ▪ Effectively communicate with all members of the group or team to achieve goals and objectives ▪ Participate on virtual teams and use tools for virtual collaboration **Resolving conflicts** ▪ Bring others together to reconcile differences ▪ Handle conflicts maturely by exercising "give and take" to achieve positive results for all parties ▪ Reach formal or informal agreements that promote mutual goals and interests, and obtain commitment to those agreements from individuals or groups

2. <u>Planning and Organizing</u> - Planning and prioritizing work to manage time effectively and accomplish assigned tasks.

Planning

- Approach work in a methodical manner
- Plan and schedule tasks so that work is completed on time
- Keep track of details to ensure work is performed accurately and completely
- Work concurrently on several tasks
- Anticipate obstacles to project completion and develop contingency plans to address them
- Takes necessary corrective action when projects go off-track
- Apply lessons learned from previous tasks to more efficiently execute current tasks

Prioritizing

- Prioritize various competing tasks and perform them quickly and efficiently according to their urgency
- Find new ways of organizing work area or planning work to accomplish work more efficiently

Allocating resources

- Determine personnel and other resources required for achieving project deliverables
- Allocate time and resources effectively and coordinate efforts with all affected parties

Project Management

- Develop, communicate, and implement a plan for a project
- Develop a timeline for sequencing the activities of a project
- Keep track of time, resources, assignments, and deliverables
- Anticipate obstacles and develop contingency plans
- Document plans, assignments, changes, and deliverables
- Understand and plan for dependencies (e.g., step A must be completed before step B)
- Manage activities to meet plans and adjust plans and communicate changes as needed
- Keep all parties informed of progress and all relevant changes to project timelines
- Engage in effective time management to keep multiple tasks moving forward

3. <u>Innovative Strategic Thinking</u> - Generating innovative and creative solutions.

- Employ unique analyses and generate new, innovative ideas in complex areas
- Reframe problems in a different light to find fresh approaches
- Entertain wide-ranging possibilities to develop unique approaches and useful solutions
- Seek out and entertain diverse perspectives, including those from other fields and roles
- Understand the pieces of a system as a whole and possess a big picture view of the

situation

- Integrate seemingly unrelated information to develop creative solutions
- Develop innovative methods of obtaining or using resources when insufficient resources are available
- Demonstrate innovative thinking by using new and existing technology in new ways
- Find new ways to add value to the efforts of a team and organization

4. <u>Problem Solving and Decision Making</u> - Applying critical-thinking skills to solve problems by generating, evaluating, and implementing solutions.

Identifying the Problem

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

Locating, gathering, and organizing relevant information

- 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
- Examine information obtained for rigor, relevance, and completeness
- Recognize important gaps in existing information and take steps to eliminate those gaps
- Organize/reorganize information as appropriate to gain a better understanding of the problem
- Refer the problem to appropriate personnel when necessary

Generating alternatives

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

Choosing a solution

- Choose the best solution after contemplating available approaches to the problem, environmental factors, and conducting cost/benefit analyses
- Make difficult decisions even in highly ambiguous or ill-defined situations
- Implementing the solution
- Commit to a solution in a timely manner, and develop a realistic approach for

implementing the chosen solution

- Observe and evaluate the outcomes of implementing the solution to assess the need for alternative approaches and to identify lessons learned
- Document issues, plans, and solutions; get appropriate permissions; and communicate appropriately to impacted stakeholders

Implementing the solution

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

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

Selection and Application

- 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)
- Identify potential hazards or risks related to the use of tools and equipment
- Present and obtain approval from decision-makers for acquiring tools and solutions
- Negotiate with and manage relationships with vendors of tools and technologies
- Operate tools and equipment in accordance with established operating procedures and safety standards
- Document tools and technologies and how they are used in the organization

Keeping Current

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

6. Business Acumen - Understand basic business principles, trends, and economics.

Situational Awareness

- Understand business mission and goals: impact, profit, market share, and/or reputation
- Understand the industry, trends in the industry, and the company's position in the industry and market
- 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
- Stay current on organizational strategies to maintain competitiveness

- Understand relevant legal and regulatory requirements of the operation

Business Practices

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

Business Ethics

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

Tier 4 – Industry-Wide Technical Competencies

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.

- Demonstrate ability to classify risks.
  - Classify risks according to relevant criteria under the entity's control
  - Classify risks according to relevant criteria beyond the entity's control
  - Classify risks according to relevant criteria with prior warnings (such as human behaviors, tornadoes and hurricanes)
  - Classify risks according to relevant criteria with no prior warnings (such as human behaviors, earthquakes)
- Demonstrate ability to identify the organization's risk exposures from both internal and external sources.
  - Demonstrate ability to identify the organization's nature disaster risks
  - Demonstrate ability to identify the organization's technological risks
  - 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.)
  - Demonstrate ability to identify the organization's controllable exposures/risks versus those beyond the entity's control
  - Demonstrate ability to identify the organization's resilience to events with prior warnings versus those with no prior warnings
- Demonstrate ability to assess an organizations risk exposure over multiple assets
  - Facility
  - Security (both physical and logical)
  - Reputational / Brand
  - Legal
  - Customer
  - Procedural
  - IT (including enterprise infrastructure)
  - People
  - Supply Chain (including transportation and outsourcing)
  - Compliance
  - Availability of personnel
  - Network Communications technology
- Explain the proper use of penetration testing and vulnerability scanning for

vulnerability assessments

- Explain the rationale of and adhere supply chain security/risk management policies, requirements, and procedures
- 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
- 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
- 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
- Describe and practice safe behaviors and avoid counterproductive or risk generating worker behaviors
- Explain the risks associated with social media and the countermeasures available to address them
- Explain the impact and proper use of environmental controls
- Explain the need for security audit logging and analysis

2. Compliance & 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.

- Provide coordination, assistance, and evidence such as documentation and testimony to support actual or potential proceedings
- 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
- Develop and maintain security policies, procedures, and practices that comply with relevant laws regarding investigations, personnel security, information security and other areas

3. Personnel Security & Business Continuity - Develop, implement and manage systems and security practices that protect people and practices to ensure enterprise continuity and risk resilience.

- Develop, implement and manage background investigations to validate individual for hiring, promotion or retention
- Develop, implement, manage, and evaluate policies, procedures, and programs, and methods to protect individuals in the workplace against harassment, threats and

violence

- 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
- Clearly define resource requirements for the Business Continuity Plan and solicit management support and commitment for required resources
- Present and obtain management/leadership support, approval, and sponsors of Business Continuity Plan
- 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
- 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
- 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.
- Identify and establish relationships with the internal departments and personnel and external agencies, contractors, and others with responsibility for emergency preparedness and response
- Develop an incident response strategy and plan to limit incident effect and to repair incident damage
- Identify trigger points for key service and support areas to identify, escalate and execute strategies selected to take advantage of key risks
- Develop formal reports and presentations focused on increasing the awareness and potential impact of risks to the organization from a business continuity perspective
- 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.)
- 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
- 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
- Conduct a debrief meeting immediately following training, drills and exercises and document actions to be taken to improve emergency preparedness and response capabilities
- Design framework and define document structure for the plan documentation
- 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. <u>Physical Security</u> - 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.
▪ Survey facilities in order to manage and or evaluate the current status of physical security, emergency and or restoration capabilities ▪ Select, implement and manage security processes to reduce the risk of loss ▪ Assess the effectiveness of security measures by testing and monitoring ▪ Identify assets to determine their value loss impact and criticality ▪ Assess the nature of threats so that scope of the problem can be determined ▪ Conduct a physical security survey in order to identify the vulnerability of the organization ▪ Perform risk analysis so that appropriate countermeasures can be developed ▪ Establish security system requirements and performance specifications ▪ Apply physical security measures and select appropriate system components ▪ Develop and conduct system design and pre-implementation plans ▪ Outline criteria for pre-bid meeting to ensure comprehensiveness of implementation ▪ Procure physical security measures, implement recommended quality assurance plan(s) ▪ Conduct commissioning acceptance testing, and delivery of the physical security measure
5. <u>Cyber/Information Security</u> - The practice of protecting physical and electronic information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
▪ 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. ▪ 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. ▪ 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. ▪ 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.

▪ 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. ▪ 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
6. <u>Crisis Management</u> - 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.
▪ Assess and prioritize risks to mitigate potential consequences of incidents. ▪ Prepare and plan how the organization will respond to incidents. ▪ Respond to and manage an incident. ▪ Recover from incidents by managing the recovery and resumption of operations.
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.
▪ Develop and manage investigation programs. ▪ 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). ▪ Manage or conduct surveillance processes. ▪ Manage or conduct specialized investigations. ▪ Manage or conduct investigative interviews.
8. <u>Case Management</u> - A system to manage, analyze, report and present findings from investigations for internal enterprise stakeholders and external systems.
▪ Analyze case for applicable ethical conflicts ▪ Analysis and assess case elements and strategies ▪ Determine need and develop strategy by reviewing procedural options ▪ Prepare reports to substantiate investigative findings ▪ Prepare and present business case, testimony or other case presentation by reviewing case files, meeting with stakeholders and presenting relevant facts.
9. <u>Globalization & Cultural Awareness</u> - Integrating cultures and global dynamics into

security systems, metrics and responses.
▪ Understand how security supports and is affected by globalization ▪ Understand the impact of globalization on the business model ▪ Interpret and adhere to global standards and standardization ▪ Integrates cultural aspects into security applications and functions
10. <u>Governance</u> - Specialty areas providing leadership, management, direction, and or development and advocacy so that individual and organization may effetely conduct security work.
▪ Leading security policy and decision-making for the enterprise. ▪ Accountability with budgets, finance and security decisions. ▪ Managing employment decisions, qualifications and related policies. ▪ Leading communication with executive decision makers and external representations.

Tier 5 – Industry-Sector Functional Areas

UNDER DEVELOPMENT :: ASIS INTERNATIONAL

NOTE: The 'Industry-Sector Functional Areas' tier correspond to workforce roles in a large number industries, and are 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. <u>Manufacturing</u> - 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. <u>Services Sales, Equipment</u> - Is a specialized area of security-related products and services have resulting from emerging threats and evolving high technology.
9. <u>Transportation</u> - 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. <u>Utilities</u> - 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.

References:

- 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)
- Scope and Emerging Trends, ASIS Foundation Security Report. ASIS Foundation, Justice & Safety Center, Eastern Kentucky University and the National Institute of Justice (2005)
- Trends in Proprietary Information Loss, Survey Report, ASIS Foundation, National Counterintelligence Executive, ASIS Information Asset Protection Council (2007)
- ASIS Foundation CRISP Report (Connecting Research in Security to Practice): Lost Laptops = Loss Data Measuring Costs, Managing Threats, by Glen Kitteringham, CPP, (2008)
- ASIS Foundation CRISP Report (Connecting Research in Security to Practice): Situational Crime Prevention and Supply Chain Security, Theory For Best Practice, Harland Haelterman, PhD, (2013)
- ASIS Foundation CRISP Report (Connecting Research in Security to Practice): Tackling the Insider Threat, Nick Catrantzos, CPP (2010)
- Business Continuity Guidelines, A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, ASIS International (2005)
- 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, ASIS International (2006)
- Chief Security Office (CS0) Organizational Standard, ASIS CSO1.-2008, American National Standard. ASIS International.

- Facilities Physical Security Measures, ASIS GLD FPSM-2009 Guideline. ASIS International.
- Organizational Resilience: Security, Preparedness, and Continuity Management Systems
- Requirements with Guidance for Use, ASIS SPC 1-2009, American National Standard. ASIS International
- Information Asset Protection, Guideline, ASIS International (2007)
- Pre-employment Background Screening, ASIS GDL PBS 2009, Guideline, ASIS International.
- Workplace Violence Prevention and Intervention, ASIS/SHRM WVPI.1-2011, American National Standard, ASIS International.
- Workplace Violence Prevention and Response, Guideline, ASIS International (2005).
- 2013 O*NET Summary Reports for category: Security Managers 11-9199.07, http://www.onetonline.org/link/summary/11-9199.07;
- 2013 O*NET Summary Reports for category: Security Management Specialists 13-1199.02, http://www.onetonline.org/link/summary/13-1199.02;
- 2013 O*NET Summary Reports for category: Security Officers 33-9032.00, http://www.onetonline.org/link/summary/33-9032.00;
- 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;
- 2013 O*NET Summary Reports for category: Loss Prevention Managers 11-9199.08, http://www.onetonline.org/link/summary/11-9199.08;
- Retail Loss Prevention Specialists 33-9099.02, http://www.onetonline.org/link/summary/33-9099.02;
- 2013 O*NET Summary Reports for category: Security Guards 33-9032.00, http://www.onetonline.org/link/summary/33-9032.00
- 2013 O*NET Summary Reports for category: Private Detectives and Investigators 33-9021.00, http://www.onetonline.org/link/summary/33-9021.00;
- 2013 O*NET Summary Reports for category: Occupational Health and Safety Specialists 29-9011.00, http://www.onetonline.org/link/summary/29-9011.00
- 2013 O*NET Summary Reports for category: Occupational Health and Safety Technicians 29-9012.00, http://www.onetonline.org/link/summary/29-9012.00;

- 2013 O*NET Summary Reports for category: Information Security Analysts 15-1122.00, http://www.onetonline.org/link/summary/15-1122.00;
- 2013 O*NET Summary Reports for category: Intelligence Analysts 33-3021.06, http://www.onetonline.org/link/summary/33-3021.06;
- 2013 O*NET Summary Reports for category: Business Continuity Planners 13-1199.04, http://www.onetonline.org/link/summary/13-1199.04;
- 2013 O*NET Summary Reports for category: Risk Management Specialists 13-2099.02, http://www.onetonline.org/link/summary/13-2099.02;
- 2013 O*NET Summary Reports for category: Emergency Management Directors 11-9161.00, http://www.onetonline.org/link/summary/11-9161.00;
- 2013 O*NET Summary Reports for category: Industrial Safety and Health Engineers 17-2111.01, http://www.onetonline.org/link/summary/17-2111.01;
- 2013 O*NET Summary Reports for category: Supply Chain Managers 11-9199.04, http://www.onetonline.org/link/summary/11-9199.04;
- 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 Qualified Certification (LPQ) Loss Prevention Foundation
- Loss Prevention Certified Certification (LPC) Loss prevention Foundation
- Certified Lodging Security Director (CLSD) American Hotel & Lodging Educational Institute Certified Financial Services Security Professional (CFSSP), American Bankers Association (ABA)
- Certified Information Systems Security Professional (CISSP) (ISC)2
- System Operator Certification (SOC) NERC
- Certified Ethical Hacker (CEH) EC-Council
- Certified information Security Auditor (CISA) ISACA
- Certified Information Security Manager (CISM) ISACA
- Certified in Risk and Information Systems Control (CRISC) ISACA
- Certified Incident Handler (GCIH) GIAC
- Certified Intrusion Analyst (GCIA) GIAC
- Penetration Tester (GPEN) GIAC

- Web Application Penetration Tester (GWAPT) GIAC
- Basic Certification for the Healthcare Security Officer – IAHSS (International Association for Healthcare Security and Safety.
- 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 – IAHSS
- Certified Fraud Examiner (CFE) offered by the Association of Certified Fraud Examiners.
- Certified Healthcare Protection Administrator (CHPA) offered by the International Association of Healthcare Security and Safety Professionals (IAHSSP).
- Certified Information Systems Security Professional (CISSP) offered by the International Information Systems Security Certification Consortium (ISC)2.
- Certified Lodging Security Supervisor (CLSS) and Certified Lodging Security Director (CLSD) offered by the Educational Institute of the American Hotel and Lodging Association (AH&LA)
- Global Information Assurance Certificate (GIAC) offered by SANS Institute.
- Industrial Security Professional (ISP) offered by the National Classification Management Society (NCMS).