The Future of Security

The Enterprise Security Competency Model
Making security more secure

In the United States, security is a $410 billion industry,¹ and globally it is one of the fastest growing fields.² Today, careers in the enterprise security industry³ play critical roles in the protection of national and global economies.

However, despite its size and importance, the security industry did not have a clear set of competencies and skills to help the workforce develop with expanding roles and responsibilities — until now.

The College of Security and Criminal Justice at University of Phoenix®, in collaboration with ASIS Foundation, has written and published a competency model for the enterprise security industry. This model is now the first comprehensive security model for enterprise security organizations and their workforce. As the field continues to grow, professionals can develop and adapt with it.

¹ See ASIS International and the Institute of Finance & Management (IOFM), The United States Security Industry: Size and Scope, Insights, Trends, and Data.
² Security Industry is led by two industry subsectors: 1) cybersecurity and 2) operational security, also known as enterprise security. This brief and model address the competencies required of operational security workers, and the U.S. Department of Labor Cybersecurity Industry Competency Model governs cybersecurity workforce competencies.
³ The security industry is segmented into two district domains: operational security and IT security. This competency model and supporting brief addresses the operational security domain. For more information on IT security, please see the U.S. DOL CyberSecurity Industry Draft Model. Draft available upon request.
The Enterprise Security Industry Competency Model

This pyramid represents the core competencies required by industry practitioners, as recognized by the U.S. Department of Labor. There are five tiers in the security model, and competencies become more specialized. The base of the model includes introductory foundational competencies, the middle embodies industry-related competencies and the top portrays the occupation-related competencies.
Tier 1

Personal Effectiveness Competencies

This tier includes personal attributes essential for all life roles, which can be used to define an individual’s character.

Interpersonal Skills and Teamwork
Displaying skills to work with others from diverse backgrounds.
- Demonstrating concern for others
- Demonstrating insight into behavior
- Maintaining open communication
- Respecting diversity

Integrity
Displaying accepted social and work behaviors.
- Behaving ethically
- Acting fairly
- Taking responsibility

Professionalism
Maintaining a professional demeanor at work.
- Demonstrating self-control
- Maintaining a professional appearance
- Maintaining a positive attitude

Initiative
Demonstrating a willingness to work.
- Persisting
- Taking initiative
- Setting challenging goals
- Working independently

Adaptability and Flexibility
Displaying the capability to adapt to new, different, or changing requirements.
- Employing unique analyses
- Entertaining new ideas
- Dealing with ambiguity

Dependability and Reliability
Displaying responsible behaviors at work.
- Fulfilling obligations
- Attending to details
- Complying with policies and procedures

Lifelong Learning
Displaying a willingness to learn and apply new knowledge and skills.
- Demonstrating an interest in learning
- Participating in training
- Anticipating changes in work
- Identifying career interests

We’ve aligned with the ASIS Foundation so that, as our students receive their academic credentialing through the University of Phoenix, they also receive a professional credentialing that’s recognized out there in the industry.
Between 2013 and 2014, the security industry has gone from a $350 billion industry to a $410 billion industry.
Primarily learned in an educational setting and likely apply to all industries.

**Security Fundamentals**
Understanding and applying basic security principles to the security of the enterprise or a specific structure, system or process.
– Planning, organizing, directing and managing a security program
– Developing, managing or conducting threat analyses
– Evaluating current security methods

**Business Foundations**
Understanding basic business principles, trends and economics.

**Critical and Analytical Thinking**
Using logic, reasoning, and analysis to address problems.
– Reasoning
– Mental agility

**STEM Literacy** (Science, Technology, Engineering, Mathematics)
Understanding and applying 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.
– **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
  – Define: Frame a problem that needs information in order to be solved
  – Access: Search and retrieve appropriate information relative to the task
  – Manage: Apply an organizational or classification system to organize retrieved information
– **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.
  – Project planning
  – Prioritize tasks
  – Create milestones
– **Mathematics:** Using mathematics to express ideas, implement metrics, create fiscal projections and solve problems.

**Reading and Writing**
Understanding written sentences and paragraphs in work-related documents. Using standard English to compile information and prepare written reports.
– Comprehension
– Attention to detail
– Application
– Organization and development
– Mechanics
– Tone

**Communication**
Giving full attention to what others are saying, and communicating in English well enough to be understood by others.
– Listening
– Communication
– Two-way communication
– Persuasion/influence

41,000

In 2014, there were 41,000 jobs in the security field; however, only 6,000 degrees were issued. There’s a big opportunity to provide academic background to the security industry.
To respond to workforce development challenges, the ASIS Foundation, collaborated with the University of Phoenix, and engaged in multiple research initiatives to identify the specific professional competencies and skills that are required to respond to the security risks that enterprises are most likely to face over the next five years. The goal of these research efforts was to establish consensus on which security competencies are needed across industries to close the skills gap by defining clearer career pathways for tomorrow’s professionals.

This tier contains motives and traits, as well as interpersonal and self-management styles.

**Teamwork**
Working cooperatively with others to complete work assignments.
- Acknowledging team membership and role
- Establishing productive relationships
- Identifying with the team and its goals
- Resolving conflicts

**Planning and Organizing**
Planning and prioritizing work to manage time effectively and accomplish assigned tasks.
- Planning
- Prioritizing
- Allocating resources
- Project management

**Innovative and Strategic Thinking**
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

**Problem-Solving and Decision-Making**
- Identifying the problem
- Locating, gathering, and organizing relevant information
- Generating alternatives
- Choosing a solution
- Implementing the solution

**Working with Tools and Technology**
- Selection and application
- Keeping current

**Business Acumen**
- Situational awareness
- Business practices
- Business ethics
Tier 4

Industry-Wide Technical Competencies

Covers the broad knowledge, skills and abilities from which workers across the industry can benefit.

**Risk Management**
Demonstrating the 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.
- Classifying risks
- Identifying the organization's risk exposures from both internal and external sources
- Assessing an organization's risk exposure over multiple assets

**Compliance and Legal Aspects**
Developing and maintaining security policies, procedures and practices that comply with relevant elements of criminal, civil, administrative and regulatory law to minimize adverse legal consequences.

**Personnel Security and Business Continuity**
Developing, implementing and managing systems and security practices that protect people and practices to ensure enterprise continuity and risk resilience.

**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.

**Cyber and Information Security**
The practice of protecting physical and electronic information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

**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.

**Investigations**
The methodology the enterprise undertakes to collect and preserve information and evidence and document in reports to enable the enterprise to make reliable decisions in response to situations, events and effectively interface with stakeholders including but not limited to legal representatives and systems and human resource representatives.

**Case Management**
A system to manage, analyze, report and present findings from investigations for internal enterprise stakeholders and external systems.

**Globalization and Cultural Awareness**
Integrating cultures and global dynamics into security systems, metrics and responses.

**Governance**
Specialty areas providing leadership, management, direction and/ or development, and advocacy so that individual and organization may effectively conduct security work.
Tier 5

Industry-Sector Technical Areas

Workforce roles frequently aligned to a specialty area.

Loss Prevention
Practices to reduce preventable losses and secure corporate systems, policies and procedures to mitigate losses caused by deliberate or inadvertent human actions.

Banking and Finance
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.

Engineering and Design
Focusing 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.

Government Services
Special services ranging from the protection of classified information, to the protection of buildings, people and assets from employees to contractors, grantees and licensees of the U.S. government.

Hospitality and Entertainment
Security professionals operate in hospitality, hotel, lodging, entertainment, event and gaming applying risk and personnel management, budgeting and finance, and a host of other areas within this specialization.

Health Care
Security in the health care industry involves hospitals, long-term care facilities, clinics, pharmaceuticals and nursing homes with 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.

Manufacturing
The manufacturing and industrial sectors, as well as food and beverage production and processing, warehouse and distribution, facilities and operations can be susceptible to industry security risks including workplace threats and violence, theft and pilferage, counterfeiting, sabotage, terrorist attack, trespassing, activist disruption, vandalism, contamination.

Services Sales and Equipment
A specialized area of security-related products and services resulting from emerging threats and evolving high technology.

Transportation
This niche area of security includes shipping, carrying, railroads, highways, freight, trucking, tourism, air cargo, ports and other transportation domains with unit standards for security within the industry.

Utilities
This field deals with 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.

Tier 6 & 7

Management-Related Competencies

Occupation-Specific Management Competencies
These upper tiers help to define performance in a workplace, design competency-based curriculum, and articulate the requirements for an occupational credential such as a license or certification.
Competency-Related Courses at University of Phoenix

Tier 1
**Personal Effectiveness Competencies**
SEC 321 Survey of Security Specializations
This course identifies and contrasts the benefits of proprietary and contract security operations and introduces the student to a variety of security specializations. It also examines the purposes, objectives, procedures, risks and types of organizations associated with the respective specializations.

Tier 2
**Academic Competencies**
SEC 371 Finance and Budgeting Practices
This course provides the student with an understanding of the various elements of a program budget; the process of budget development, justification and presentation; and principles of contract preparation. Special emphasis is given to these processes, procedures and practices in relation to security-oriented environments.

Tier 3
**Workplace Competencies**
SEC 351 Legal and Regulatory Issues in Security Management
This course examines legal, regulatory, ethical and policy issues that influence the work performance of security personnel. It also discusses the potential consequences of noncompliance for individuals and institutions.

Tier 4
**Industry-Wide Technical Competencies**
SEC 411 Physical Security
This course provides the student with an understanding of the various levels of security that can be employed for the protection of people, property and data housed in physical facilities.

Tier 5
**Industry-Sector Technical Competencies**
SEC 240 Loss Prevention and Asset Protection
This course is an introduction and general overview of loss prevention and asset protection strategies and programs. Students will learn the basic principles and methodologies involved with the prevention of shrinkage or loss and the protection of an organization's physical assets. Students will be introduced to basic theories and concepts, key terms and definitions, and current critical issues. Additionally, this course provides an overview of integrated security systems, workplace violence threats, emergency plans and procedures, and how to conduct interviews and investigations.
The security industry is projected to grow 13 percent between 2012 and 2020. Excluding security guards, industry growth will be closer to 23 percent. Through the College of Security and Criminal Justice, University of Phoenix prepares its students to reach for their goals and rewarding careers.