4.7 7 Knowledge Area: Organizational Security

The Organizational Security knowledge area focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission. Organizations have responsibility to meet the needs of many constituencies and those needs must inform each of these knowledge units.

4.7.1 Knowledge Units and Topics

Students should be able to identify the types of security laws, regulations, and standards within which an organization operates. A government organization has a set of security profiles while a corporate entity has other focuses. A security policy needs to fit the current organization and be able to grow with the organization. A security professional should understand current governances and how they convey compliances to their respective business verticals such as healthcare and Ecommerce.

The following table lists the essentials, knowledge units, and topics of the Organizational Security knowledge area. Due to the overlap in topics, reference the knowledge units in the Societal Security knowledge area.

ORGANIZATIONAL SECURITY		
Essentials - Risk management, - Governance and policy, - Laws, ethics, and compliance, and - Strategy and planning.		
Knowledge Units	**Topic**	**Description/Curricular Guidance**
Risk Management		Risk management is finding and controlling risks to organizational information assets.
	Risk identification	Asset identification is the cataloging of information assets in an organization, such as databases or hardware, to aid in the determination of risk should the assets be compromised or lost. Threats include any event leveraging a vulnerability that has the potential to cause loss or damage for the organization. Threat intelligence (threat modeling) is increasingly used by organizations to maintain awareness and reactive capacity for existing and emerging threats.
	Risk assessment and analysis	Risk analysis is the organizational process to determine and deal with possible accidental or intentional losses, and designing and implementing procedures to minimize the impact of these losses. This can also encompass Threat Analysis and Threat Intelligence.

	Insider threats	This topic covers malicious human behavioral factors that might cause harm as a result of a conscious violation of trust, or best-use, or inadvertent error. An *insider* is defined as any person with authorized access to an organization's resources including personnel, facilities, information, equipment, networks, and systems. An *insider threat* is defined as the risk that an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems, or equipment; actual or threatened harm to employees; or, other actions that would prevent the company from carrying out its normal business practices This topic covers motive-means-opportunity behaviors: motivation and discipline factors, accountability, awareness and quality control. The FBI has developed materials including indicators useful in identifying potential insider threat risks.
	Risk measurement and evaluation models and methodologies	Risk models are used to explain how assets encounter risk. In addition, there a number of industry-accepted methodologies to measure, evaluate, and communicate risk to stakeholders. This topic includes both quantitative and qualitative approaches to risk assessment, application of models and methods for various business contexts (e.g., HIPAA for healthcare facilities). Tools of interest might include the Cyber Resilience Review self-assessment, Cybersecurity Evaluation Tool (CSET) as well as Security Risk Assessment tool from HSS.
	Risk control	*Risk control* is defined as the act of lessening the consequences of a cyber event, and as a result lessening the amount of risk. Each approach should include the means to communicate risk to decision makers including the *residual risk*. Topics covered should include assessment and ranking of risk and the Avoid, Reduce, Transfer, Accept categories. Curricular content should include widely-used risk control methodologies that are available for exposure and practice.

Security Governance & Policy [*See also Societal Security KA for related content*]		Each organization addresses its operating environment, internal and external, through policy and governance. Governance is the responsibility of the senior management of an organization to assure the effective implementation of strategic planning, risk management, and regulatory compliance usually by means of comprehensive managerial policy, plans, programs, and budgetary controls so as to secure the information of the organization. The implementation of security governance and policy should be framed within global, national, and local laws, regulations and standards. This knowledge unit focuses on an understanding of the security policy development cycle, from initial research to implementation and maintenance as well as giving exposure to real-world examples of security policies and practices.
	Organizational context	Many factors influence how security is operationalized in organizations. These contexts are critical when designing a curriculum and should inform the entire process. This topic covers how internal versus external contextual differences have a major impact on the coverage of policy, regulation, and statute (or jurisdiction). Also, location- or country-specific issues and concerns should be evaluated. Applicable standards and guidelines for compliance to industry/sector should also be evaluated. The variance between governments versus private organizations is a factor as is the need to include international aspects including but not limited to import/export restrictions. Further, there is significant difference between organizations in various business vertical industry segments such as energy versus agriculture.
[*See also Data Security KA, Human Security KA, and Societal Security KA, related content.*]	Privacy	Privacy is a concept with cultural and national variations in its definition. At its core, privacy is based on the right to be forgotten, and various levels of choice and consent for the collection, use, and distribution of an individual's information. This topic addresses social and localized variances in privacy. Jurisdictional variance in privacy definitions should be explored. The relationships between individuals, organizations, or governmental privacy requirements should also be addressed. The impact of privacy settings in new tools/software, identifying a need for tools and techniques to be covered in most areas. Additional consideration should be given to privacy in the context of consumer protection and health care regulations. Organizations with international engagement must consider variances in privacy laws, regulations, and standards across the jurisdictions in which they operate.

[*See also Societal Security KA for related content*]	Laws, ethics, and compliance	Laws, regulations, standards as well as ethical values are derived from the social context and how organizations meet requirements to comply with them. This topic includes how laws and technology intersect in the context of the judicial structures that are present – international, national and local – as organizations safeguard information systems from cyberattacks. Ethical instruction should also be an element. Professional codes of conduct and ethical standards should be addressed. Compliance efforts should include those efforts to conform to laws, regulations, and standards, and to include breach notification requirements by state, national, and international governing authorities. Examples of international laws and standards include GDPR and ISO/IEC 27000 et al. National laws of importance for U.S. organizations include HIPAA, Sarbanes-Oxley, GLBA, etc.
	Security governance	The principles of corporate governance are applicable to the information security function. Governance is the responsibility of the senior management of an organization to assure the effective implementation of strategic planning, risk management, and regulatory compliance usually by means of comprehensive managerial policy, plans, programs, and budgetary controls to secure the information of the organization. This topic should frame the implementation of security governance and policy within global, national, and local laws, regulations and standards, and programs of instruction should seek to convey the concepts with clarity and sound examples.
	Executive and board level communication	Delivering information to executives and external decision makers is a critical skill for information security leaders. This topic includes communication skills that are taught and practiced with rehearsals that include critical analysis and meaningful feedback.
	Managerial policy	Organizational guidelines that dictate certain behavior within an organization. This topic content should seeks to convey the concepts with clarity and sound examples including security program policy, issue-specific policy and system- specific policy as per NIST SP 800-12 Rev 1. This should also cover an understanding of the security policy development cycle, from initial research to implementation and maintenance, as well as giving exposure to real-world examples of security policies and practices.
Analytical Tools		This knowledge unit is a set of techniques using data analytics to recognize, block, divert, and respond to cyberattacks. Monitoring real-time network activities enables agile decision making, detection of suspected malicious activities, utilization of real-time visualization dashboard and employment of a set of hardware and software to manage such detected suspicious activities.

	Performance measurements (metrics)	A process of designing, implementing, and managing the use of specific measurements to determine the effectiveness of the overall security program. Built on metrics, a term used to describe any detailed statistical analysis technique on performance, but now commonly synonymous with performance measurement. Curricular content should include approaches and techniques to define and evaluate the utility of performance measurements should be explained to students.
	Data analytics	Data analytics is a set of techniques used to manipulate (often) large volumes of data to recognize, block, divert, and respond to cyberattacks. Monitoring real-time network activities enables agile decision making, detection of suspected malicious activities, utilization of a real-time visualization dashboard, and employment of a set of hardware and software to manage such detected suspicious activities. This topic includes definitions; the differences between security control and security analytic software and tools; the type and classifications of analytic tools and techniques (with examples such as OpenSOC); collect, filter, integrate and link diverse types of security event information; how security analytics tools work; the relationship between analytic software and tools and forensics; differences between forensic tools and analytic tool; network forensics (to include packet analysis, tools, Windows, Linux, UNIX, Mobile); differences between cyber forensics (social media for example) and network forensics.
Security intelligence		Collection, analysis, and dissemination of security information including but not limited to threats and adversary capabilities. In this topic, tools and techniques should be explored to include data collection and aggregation, data mining, data analytics, statistical analysis. Examples of sources for security intelligence include SIEM for internal data, and public and private intelligence services for external data. Dissemination includes an understanding of the Information Sharing and Analysis Center approach as well as organizations like InfraGard.
Systems Administration		System administration works behind the scenes to configure, operate, maintain, and troubleshoot the technical system infrastructure that supports much of modern life. Prerequisite knowledge: Basic understanding of computer systems (Windows/Linux), networks (OSI Model), software, and database (Oracle/SQL).

	Operating system administration	This topic covers the upkeep, reliable operation, configuration, and troubleshooting of technical systems, especially multi-user systems and servers. This topic includes but not be limited to account management, disk administrations, system process administration, system task automation, performance monitoring, optimization, administration of tools for security and backup of disks and process.
	Database system administration	This topic covers managing and maintaining databases by utilizing available and applicable management system software. This topic includes but not be limited to installation and configuration of database servers, creation and manipulation of schemas, tables, indexes, views, constraints, stored procedures, functions, user account creation and administration, and tools for database backup and recovery. Coverage should include the data storage technologies in wide use as well as emerging data management technologies.
	Network administration	Network administration relates to installation, and supporting various network system architectures (LANs, WANs, MANs, intranets, extranets, perimeter networks [DMZs], etc.), and other data communication systems. This topic includes but is not limited to the OSI Model, securing of network traffic, and tools for configuration of services.
[*See also Data Security KA, Human Security KA, and Societal Security KA, p. 62, for related content.*]	Cloud administration	Cloud administration refers to the upkeep and reliable access to a dynamic pool of configurable remote resources (e.g., networks, servers, storage, applications and services) that can be rapidly configured, provisioned and released with minimal oversight. This topic includes but is not limited to configuring and deploying applications and users in cloud infrastructures, analyzing performance, resource scaling, availability of cloud platforms, identifying security and privacy issues and mitigating risks.
	Cyber-physical system administration	Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. CPS administration refers to installation and upkeep by ensuring safety, capability, adaptability, scalability, resiliency, security, and usability. This topic includes but is not limited to the architecture of cyber-physical systems, underlying communication standards (Zigbee), middleware, service-oriented architecture, tools supporting real-time control and application of real-world examples (power grid, nuclear facility, IoT, SCADA).

	System hardening	This topic covers securing a system by finding and remediating risks. This may include hardening or securing configuration, system software, firmware, and application. This topic includes but is not limited to identifying risks, threats, and vulnerabilities in commonly used systems (operating systems, database systems, networks); defining and administering procedures and practices to safeguard against threats; hardening through suitable tools (firewall, anti-virus, IDS, honeypot).
Cybersecurity Planning		
Availability		Sound system operation requires all systems sustain targeted levels of availability by having their current state recoverable from failure through redundancy and backup and recovery. This topic includes but is not limited to identifying key assets and administering tools to have validated system backup and recovery.
	Strategic planning	The process of defining an organization's cybersecurity strategy – or direction – and determining the actions needed and resources to be allocated in order to implement such a strategy. This topic covers concepts such as determining the current organization's position; performing Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis; developing a strategy that fulfills the mission, values, and vision of the organization; determining long-term objectives; selecting key performance indicators(KPIs) to track progress; allocating the necessary budget; rolling out the strategy to the organization; and updating and adapting yearly.
[*See also Data Security KA, p. 16, Human Security KA, p. 44, and Societal Security KA, p. 62, for related content.*]	Operational and tactical management	The organization ability to securely operate organizational technical infrastructure. This topic includes a discussion of data protection and privacy by default and design, and cover basic concepts, issues, and techniques for efficient and effective operations. Special emphasis is placed on process improvement and supply chain management. Topics include operations strategy; tactical strategy; product and service design; process design and analysis; capacity planning; lean production systems; materials and inventory management; quality management and six sigma; project management; and supply chain management.

[*See also Data Security KA, p. 16, Human Security KA, p. 44, and Societal Security KA, p. 62, for related content.*]	Operational and tactical management	The organization ability to securely operate organizational technical infrastructure. This topic includes a discussion of data protection and privacy by default and design, and cover basic concepts, issues, and techniques for efficient and effective operations. Special emphasis is placed on process improvement and supply chain management. Topics include operations strategy; tactical strategy; product and service design; process design and analysis; capacity planning; lean production systems; materials and inventory management; quality management and six sigma; project management; and supply chain management.
Business Continuity, Disaster Recovery, and Incident Management		Description of the role disaster recovery (DR) plays within business continuity (BC). BC planning includes contingency planning, incident response, emergency response, and backup and recovery efforts of an organization to ensure the availability of critical resources during an emergency situation while the disaster recovery refers to the recovery of the systems in the event of a disaster. Continuity of organizations in the wake of major events is also a component. This topic includes creation and use of the IR/DR/BP BC plans, organization of the plans, occasions to review/rewrite plans, examination of sanitized plans, opportunities should be given for students to write case-based or actual plans to gain some experience.
	Incident response	Incident response (IR) refers to the actions taken by senior management to specify the organization's processes and procedures to anticipate, detect, and mitigate the effects of an incident. This topic includes the creation and use of the IR plans, organization of the plans, occasions to review/rewrite plans, and examination of sanitized plans. Opportunities should be given for students to write case-based or actual plans to gain some experience.
	Disaster recovery	Disaster recovery (DR) refers to the actions taken by senior management to specify the organization's efforts in preparation for and recovery from a disaster. Specifically, DR refers to the recovery of the systems in the event of a disaster. This topic includes the creation and use of the DR plans, organization of the plans, occasions to review/rewrite plans, and examination of sanitized plans. Opportunities should be given for students to write case-based or actual plans to gain some experience.

	Business continuity	Business continuity refers to the actions taken by senior management to specify the organization's efforts if a disaster renders the organization's primary operating location unusable. Business continuity (BC) planning includes contingency planning, incident response, emergency response, and backup and recovery efforts of an organization to ensure the availability of critical resources during an emergency situation. Continuity of organizations in the wake of major events is also a component. Curricular content should include the creation and use of the BC plans, organization of the plans, occasions to review/rewrite plans, and examination of sanitized plans. Opportunities should be given for students to write case-based or actual plans to gain some experience.
Security Program Management		
	Project management	Project management is the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements. This topic includes project integration; project scope management; project time and cost management; quality management; human resource considerations; communications; risk management; and procurement management.
	Resource management	Resource management is the efficient and effective deployment and allocation of an organization's resources when and where they are needed. Such resources may include financial resources, inventory, human skills, production resources, or information technology. This topic explains and develops current practices in resource management, specifically in the context of projects typical of cybersecurity.
	Security metrics	Metrics, often described as measures, are effective tools to discern the effectiveness of the components of their security programs and drive actions taken to improve a security program. This topic includes the elements of security metrics, and how to design, develop, validate and organize them. The use of metrics in various contexts should be included such as: ● Use of security metrics in decision making, ● Use of security metrics in strategic, tactical and operational planning, and ● Use of security metrics in security program evaluation, audition, and performance.

	Quality assurance and quality control	Quality assurance (QA) and quality control (QC) are methods used to prevent mistakes which might impact the character of a deliverable such as a software system; control specifically refers to methods used to increase the quality of these systems. This topic explains and develop current practices in QA/QC, specifically in the context of projects typical of cybersecurity.
Personnel Security		
[*See also Human Security KA, p. 44, for related content.*]	Security awareness, training and education	This topic covers the avoidance and/or proper use of Fear Uncertainty, and Doubt (FUD) as a tool for awareness. This topic includes physical security; desktop security; password security; wireless networks; security phishing; file sharing and copyright; browsing; encryption; insider threat; international travel; social networking and social engineering.
	Security hiring practices	The practices, governed by policies, used by organizations to recruit, hire and train employees across the organization. This topic includes the principles of this topic, and students should gain experience with a review of fictional resumes, fictional background checks, fictional acted-out interview techniques, fingerprint analysis results, and financial review.
	Security termination practices	The practices, governed by policies, used by organizations to terminate employees across the organization including assigned asset recovery, removal of credentials and proactive prevention of data exfiltration. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.
	Third-party security	Those practices of firms to manage the risks from contractors, consultants and the staff of key business partners. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.
	Security in review processes	Those practices of firms to manage the periodic review of staff members. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.
See also Data Security KA, Human Security KA,and Societal Security KA, for related content.]	Special issue in privacy of employee personal information	Those practices of firms to secure the personal information of employees and other stakeholders. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.

Security Operations		This knowledge unit covers efforts to enhance the security of the origin and traceability of sourced system components, such as externally produced hardware or software.
	Security convergence	The merging of management accountability in the areas of corporate (physical) security, corporate risk management, computer security, network security, and InfoSec has been an observed phenomenon in practice in many moderate and large organizations. This topic includes emerging examples of convergence in practice, which can be a useful outlet for classroom discussion of emerging topics.
	Global security operations centers (GSOCs)	Optimized processes can add value to broad organizational operations centers that intersect physical security and cybersecurity. This topic covers how correlating global attacks with local compliance measures is a necessity at times. How does an attack in Malaysia affect business functions in Colorado? GSOC functions need to have clear communications of the identified attack as well as the identified region of attack and the region of origin. A GSOC will need to be able to completely determine the type of attack, the profile and where it originated to be able to disseminate that information to the other security operation centers.

4.7.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Risk Management	
	Describe risk management and its role in the organization.
	Describe risk management techniques to identify and prioritize risk factors for information assets and how risk is
	Discuss the strategy options used to treat risk and be prepared to select from them when given background information.
	Describe popular methodologies used in the industry to manage risk.
Governance and policy	
	Discuss the importance, benefits, and desired outcomes of cybersecurity governance and how such a program would be implemented.
	Describe information security policy and its role in a successful information security program.
	Describe the major types of information security policy and the major components of each.
	Explain what is necessary to develop, implement, and maintain effective policy and what consequences the organization may face if it does not do so.

Laws, ethics, and compliance	
	Differentiate between law and ethics.
	Describe why ethical codes of conduct are important to cybersecurity professionals and their
	Identify significant national and international laws that relate to cybersecurity.
	Explain how organizations achieve compliance with national and international laws and regulations, and specific industry
Strategy and planning	
	Explain strategic organizational planning for cybersecurity and its relationship to organization-wide and IT strategic planning.
	Identify the key organizational stakeholders and their roles.
	Describe the principal components of cybersecurity system implementation planning.