دائـــــرة الـــصـــحـــة
DEPARTMENT OF HEALTH

ABU DHABI HEALTHCARE INFORMATION AND CYBER SECURITY WORKFORCE GUIDELINE

SEPTEMBER 2022

PUBLIC عـــام

Document Title	Abu Dhabi Healthcare Information and Cyber Security Workforce Guideline		
Document Reference No.	DOH/Guideline/ADHICSWG/1.0	**Version**	1.0
Publication Date	September 2022		
Applies To	This guideline covers all DOH regulated healthcare entities and services within the Emirate of Abu Dhabi, and shall be applicable to all healthcare/medical facility(s), healthcare professional(s) and support staff who have access to patients' health/diagnostic/personal information, diagnostic lab(s), pharmacy(s) and insurance provider(s)		
Effective Date	The effective date of this guideline will be the date of its publication		
Document Classification	Public		
Document Owner/Control	Undersecretary Office - Information & Cyber Security Office		

1. About the guideline

The healthcare sector is one of the most critical sectors dealing with personal information and/or protected information and also one of the most targeted industries across the globe. The advancement of interconnected healthcare equipment and technologies has led to numerous advantages along with alarming threats. This situation has surfaced with a need for healthcare sector information and cyber security professionals to ensure that the necessary skill set is periodically renewed based on new security trends and to be available to defend against new threats as they arise.

Like any other critical sector, the healthcare sector has the immense need to protect its infrastructure and to implement necessary industry security best practices, standards, guidelines, regulations, etc. However, the knowledge required to implement the controls are limited in the healthcare sector and mostly managed within the existing human resources/staff. In this case, either the staff is not from a security background or is partially skilled. It is very rare to see healthcare facilities with the necessary skill set and have dedicated resources to ensure the security of the facility/entity.

This guideline has been developed by the Department of Health with the purpose to detail the knowledge, skills, abilities and competency requirements for the healthcare sector information and cyber security roles considering the healthcare sector demands, regulatory demands and cybersecurity workforce best practices.

This guideline also addresses the common information and cyber security challenges faced in most of the entities globally such as but not limited to the following:

- Job roles and corresponding job descriptions are not identified and documented.
- Competency requirements for each job role is not identified.
- Human resources in the healthcare entities do not have the competence to interview competent information and cyber security resources.
- Redundancy of job responsibilities.
- Lack of information security governance, continuous monitoring and maintenance.
- Absence of independent information security resource or team.

- Information security function either reports to IT/under reports/does not have the authority to take unbiased actions.
- Lack of reporting of information security to top management.
- Lack of information and cyber security competence to respond proactively or reactively to any cyber-attack.
- Lack of identification of information security section or department as part of the organization structure.
- Lack of segregation of duties leading to conflict of interest.
- Lack of budget for information and cyber security.

The guideline outlines the workforce competency capabilities based on basic, transitional and advanced healthcare facilities and draws the path for organizational maturity towards meeting the necessary information and cyber security requirements.

The guideline can be considered based on cybersecurity requirements of the facility such as the strategic mission, vision, objectives, compliance requirements, current/future internal and external risks.

2. Applicability

The guideline aims to serve as a reference model and a guideline for all DoH regulated healthcare entities within the Emirate of Abu Dhabi regardless of the size of the facility. The healthcare entities include hospitals, clinics, centers, labs, pharmacies, and insurance providers. The guideline is applicable for individuals or healthcare entities having the below mentioned requirements,

- Any student or cybersecurity professional aspiring for an information and cyber security career in the healthcare sector;
- Healthcare human resources for healthcare information and cyber security recruitments, talent management and appraisal management/career development;
- Top management of healthcare entities for information and cyber security organization structure improvement; and
- Universities or training institutions for information and cybersecurity curriculum, trainings, courses, seminars and conferences.
- Research and forecast of future capability demand.

3. Suggested reporting structure of information security function in healthcare entities

The information and cyber security function should have the authority to report directly to the management of the entity. In most of the entities, the information security function is currently a part of IT. However, IT and IS are different. In such scenarios, the information security decisions are superseded by the decisions of IT or the IS control implementation gets challenging as per IT's convenience leading to critical security gaps.

The below organization chart is an example of an ideal healthcare entity with emphasis on the reporting structure of the information security function.

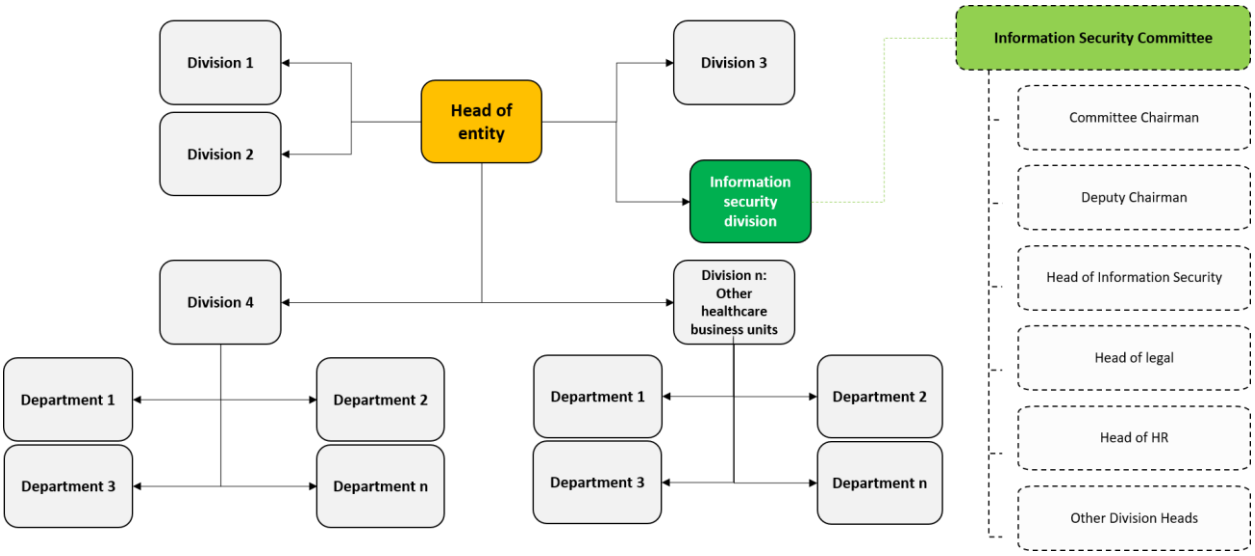

Figure 1- Suggested reporting structure of information security function in healthcare entity

For further information security governance structure details refer ADHICS - Abu Dhabi Healthcare Information Security – Governance Structure

4. Structure of the guideline

4.1. Workforce guideline structure

The guideline is structured into multiple functions based on the information security requirements and best practices for each job role.

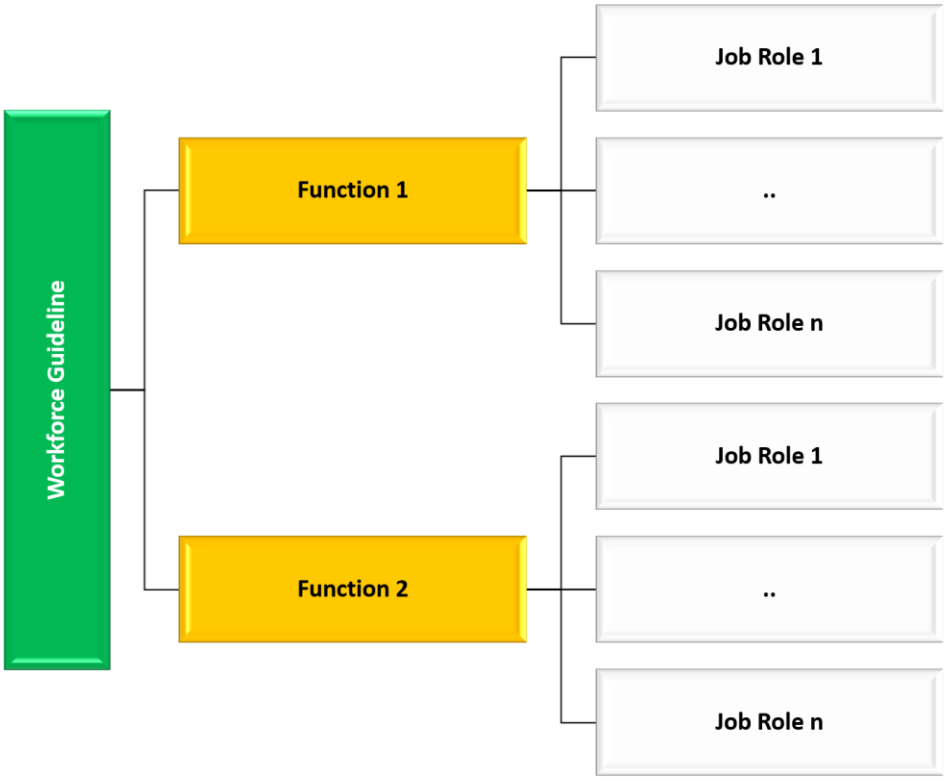

Figure 2 - Workforce guideline structure

4.2. Workforce Functions

The information and cyber security function for healthcare entities can be broadly categorized into the following functions.

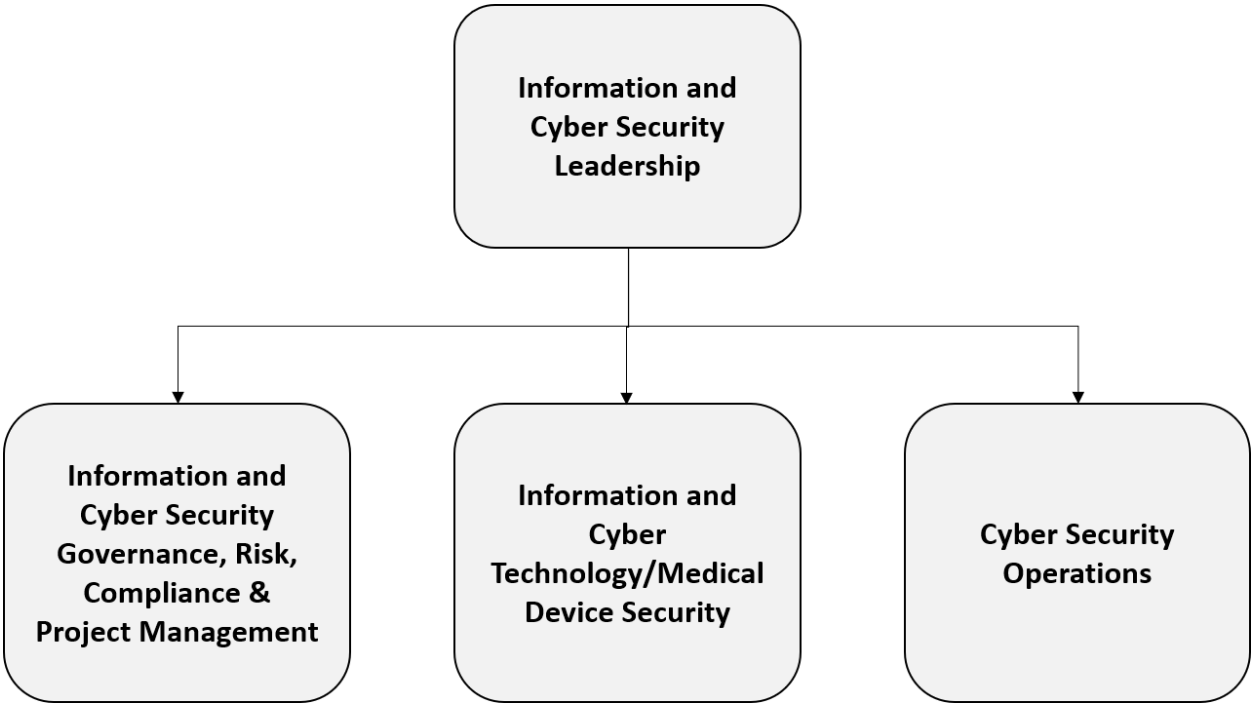

Figure 3 - Workforce functions

4.3. Workforce guideline job roles

Figure 4 - Workforce guideline job roles

4.4. Structure breakdown

Each role is sectioned into the following structure.

SECTIONS	DEFINITIONS
Role	Set of named duties or job functions within an organization.
Function	Information security function
Description	Brief description about the role.
Job responsibilities	The ability of an individual that is required to perform a task relevant to the area of work.
Knowledge	Understanding of a particular subject obtained by learning concepts, its use and application.
Skills	The capability needed to apply the necessary people, process and technological knowledge to perform a task.
Abilities	The ability of an individual that is required to perform a task relevant to the area of work.
Experience	Time spent in a workplace learning about the job role and the sector.
Qualification	Official accomplishments that makes an individual suitable for a job role.
Applicability based on entity size	The applicability of the job role based on the organization and resource size i.e., Basic, Transitional and Advanced, as defined in ADHICS Standard. *(Refer: ADHICS Standard for further details).*

Table 1: Structure breakdown

5. Workforce roles and responsibilities

5.1. Chief Information Security Officer

ROLE
• Chief Information Security Officer
FUNCTION
• Information and Cyber Security Leadership
DESCRIPTION
• Manages and owns the cybersecurity assurance activities within the entity, and responsible for establishing, implementing and maintaining a corporate-wide cybersecurity management program covering information, systems and networks of the entity. In addition to other area of responsibility including strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
JOB RESPONSIBILITIES
• Manage the implementation and achievement of cybersecurity objectives and goals. • Support the development, allocation and utilization of cybersecurity budget and exercise expenditure controls where applicable. • Advise the management on the entity's risk levels, security posture, cost/benefit analysis of information security programs, policies, processes and systems. • Lead and oversee information security budget, staffing, and contracting. • Collect and maintain data needed to meet cybersecurity reporting requirements. • Communicate the value of cybersecurity throughout all levels of the organization stakeholders. • Collaborate with stakeholders to establish the business continuity plan and ensure that

cybersecurity requirements are integrated into it.

- Ensure that security improvement actions are evaluated, validated, and implemented as required.
- Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.
- Establish overall enterprise information security architecture with the organization's overall security strategy.
- Interpret and/or approve security requirements relative to the capabilities of new information technologies.
- Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the entity's cybersecurity program.
- Manage the monitoring of information security data sources to maintain organizational situational awareness.
- Manage threat or target analysis of cyber defense information and production of threat information within the entity.
- Monitor and evaluate the effectiveness of the entity's cybersecurity safeguards to ensure that they provide the intended level of protection.
- Oversee the cyber security training and awareness program.
- Develop and apply appropriate Risk Management Strategy.
- Participate in the periodic risk assessments during the Security Assessment and Authorization process.
- Recognize a possible security violation and take appropriate action to report the incident, as required.

- Recommend policy and coordinate review and approval.
- Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
- Review investigations after breaches or incidents, including impact analysis and recommendations for avoiding similar vulnerabilities.
- Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
- Oversee policy and standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
- Establish an appropriate security governance structure, models and program, and oversee Risk Governance process.
- Continuously validate the entity's compliance against policies/guidelines/procedures/ regulations/laws.

KNOWLEDGE

- Common information security management frameworks, programs, principles and techniques.
- Risk management frameworks, approaches and processes, and the current and emerging threats/threat vectors.
- Cyber security laws, regulations, policies, ethics and privacy principles.
- Cyber related threats and vulnerabilities types, information dissemination sources (e.g., alerts and advisories).
- Penetration testing and vulnerability assessment principles, tools, and techniques.
- Encryption algorithms.

- Business continuity and disaster recovery.
- Personal Health Information (PHI) data security standards.
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms, traffic analysis methods, architecture concepts including topology, protocols, components, and principles.
- Incident response and handling concepts, programs, processes, methodologies, roles and responsibilities.
- Intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Current industry methods for evaluating, implementing, and disseminating security assessment, monitoring, detection, and remediation tools.
- Data classification program and procedures for information compromise, and data backup, recovery and controls related to the use, processing, storage, and transmission of data.

SKILLS

- Creating policies that reflect cybersecurity objectives.
- Implementing risk management programs, including executing risk assessments, identifying and implementing controls, and managing the security posture.
- Determining how a security system should work (including its resilience and dependability capabilities) and how changes will affect these outcomes.
- Providing timely, constructive, and actionable feedback that increases individual and team effectiveness.
- Applying strong analytical, creative, and organizational skills.
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the

ability to communicate information security and risk-related concepts to technical and nontechnical audiences at various hierarchical levels, ranging from board members to technical specialists.

ABILITY

- Manage daily security operations.
- Empower and lead a cybersecurity team.
- Provide verbal and written communication that is outstanding to senior management.
- Look at alternatives and consider new ways of thinking to problem solve.
- Change direction where required and showing flexibility to meet new demands.
- Manage several concurrent projects and prioritize demands.

EXPERIENCE

- 6+ years of experience in cyber security and leading multiple security/networks/systems operations, significant involvement with operations management, business continuity and policy compliance development.

QUALIFICATION

- Bachelor's degree in an information technology, cyber security or equivalent work experience.
- CISM: Certified Information Security Manager
- CISA: Certified Information Security Auditor
- CISSP: Certified Information Systems Security Professional
- C-CISO: Certified Chief Information Security Officer
- CompTIA Security+
- LPT: Licensed Penetration Tester/CEH: Certified Ethical Hacker

- GSLC: GIAC Security Leadership
- ISO27001 Lead Auditor/Implementer

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.2. Information Security Officer

ROLE

- Information Security Officer

FUNCTION

- Information and Cyber Security Governance, Risk, Compliance & Project Management

DESCRIPTION

- Responsible for the planning, development and implementation of cybersecurity policies, procedures, standards, and controls. Leads day to day compliance audits/assessments, governance, and risk management functions to ensure the protection of corporate information systems, networks, and data.

JOB RESPONSIBILITIES

- Develop an annual compliance plan to ensure adequate auditing of compliance to cyber security policies and guidelines.
- Develop and maintain detailed compliance monitoring mechanisms and frameworks.
- Execute periodic and ad-hoc compliance checks and cyber risk assessments to ensure that cyber security controls and measures are adherent to the mandated cyber security policies and guidelines.
- Develop policy compliance reports including required corrective actions and recommendations.
- Conduct cyber security risk assessments based on current state of adherence to policies and rate of adoption of security controls and mechanisms.
- Provide remedial actions against non-compliance and collaborate to develop plans to reach a state of compliance.
- Follow up on the implementation status of defined corrective actions to adhere to policies.

- Organize policies, standards training and awareness based the on periodic release of updated regulations or compliance mechanisms as required،
- Assess the effectiveness of security controls.
- Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
- Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
- Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centres).
- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
- Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
- Assure successful implementation and functionality of security requirements and appropriate policies and procedures that are consistent with the organization's mission and goals.
- Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
- Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
- Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
- Ensure the security of bio-medical equipment's.

KNOWLEDGE

- Risk management requirements, frameworks, assessments, approaches, methodologies and processes (e.g., methods for assessing and mitigating risk).
- Organizational security policies.
- Cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication).
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms, traffic analysis methods, security architecture concepts including topology, protocols, components, and principles.
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Information classification program and procedures for information compromise.
- Security scans, vulnerability assessments and penetration testing principles, procedures, methodologies, tools, and techniques.
- Network, system and application security threats and vulnerabilities types.
- Personal Health Information (PHI) data security standards.
- Specific operational impacts of cybersecurity lapses.
- Authentication, authorization, and access control methods.
- Business continuity and disaster recovery continuity of operations plans.
- Enterprise information security architecture.
- Evaluation and validation requirements.
- Security Assessment and Authorization process.
- Current industry methods for evaluating, implementing, and disseminating security assessment,

monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.

- New and emerging information technology (IT) and cybersecurity technologies.

SKILLS

- Creating policies that reflect security objectives.
- Developing security standards and guidelines based on best practices and industry standards.
- Applying confidentiality, integrity, and availability principles.
- Integrating and applying policies that meet security objectives.
- Assessing security controls based on cybersecurity principles and tenets.
- Performing impact/risk assessments.
- Preparing Test & Evaluation reports.
- Assessing security systems designs.
- Information prioritization methodologies as it relates to operations.
- Documenting risk and compliance activities
- Preparing and presenting briefings.
- Preparing plans and related correspondence.
- Reviewing and editing assessment products.

ABILITY

- Assess policy needs and develop policies in compliance with laws, regulations, policies, and standards to support cyber activities.
- Provide policy guidance to cyber management, staff, and users.

- Ensure security practices are followed.
- Meet with business stakeholders to identify top security risks.
- Work with the CISO to determine the acceptable level of risk.
- Monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Produce technical documentation.
- Design valid and reliable assessments.
- Translate data and test results into evaluative conclusions.
- Exercise judgment when policies are not well-defined.
- Function effectively in a dynamic, fast-paced environment.
- Work in a collaborative environment, seeking continuous consultation with other analysts and experts.
- Work across departments and business units to implement the security policy.
- Communicate clearly and concisely in both oral and written forms.

EXPERIENCE

- Entry: 0-3 years of experience in cyber security, security governance/auditing or any other related field.
- Senior: +5 years of experience in cyber security, security auditing, risk assessments or any other related field.

QUALIFICATION

- Bachelor's degree in an information technology, computer science or cyber/ information security.

- CGEIT: Certified Governance of Enterprise IT
- CRISC: Certified Risk and Information Systems Control
- CISA: Certified Information Systems Auditor
- RMP: Risk Management Professional
- CRMA: Certification in Risk Management Assurance
- GRCP: GRC Professional

APPLICABILITY BASED ON ENTITY SIZE

☑ Basic

☑ Transitional

☑ Advanced

5.3. Information and Cyber Security Project Manager

ROLE
• Information and Cyber Security Project Manager
FUNCTION
• Information and Cyber Security Governance, Risk, Compliance & Project Management
DESCRIPTION
• Ensures that cybersecurity projects are following project management best practices and information security requirements in project management.
JOB RESPONSIBILITIES
• Define project scope and priorities centered on end-user demands. • Develop an understanding of the needs and demands of information end-users. • Provide guidance on project costs, principles of design, or adjustments in the design. • Develop and document project risks for critical system elements, as appropriate. • Develop requirements to ensure system, network, and operational security are met. • Coordinate and manage the overall security project end-to-end. • Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). • Review service performance reports that recognize any major problems and variances, undertake corrective steps, if appropriate, and ensure that all unresolved problems are followed up. • Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.

- Conduct import/export reviews for acquiring systems and software.
- Develop cost estimates for new or changed system(s).
- Lead and oversee the budget, staffing, and contracting in coordination with contracts team.
- Review, conduct or participate in audits of cyber and information security programs and projects.
- Draft and post-security and risk control documents.
- Ensure including information security requirements in project management and ensure the protection of data during the project management lifecycle.
- Direct projects based on specified project objectives.

KNOWLEDGE

- Development of project charter, plan.
- General knowledge on the use of Microsoft project planner and project management software's.
- Track the progress, monitor, analyze and report project.
- Project scope, schedule, quality, human resource, communication, risk, procurement, stakeholder management.
- Personal Health Information (PHI) data security standards.

SKILLS

- Problem solving.
- Team building skills.
- Ability to delegate tasks.
- Time management
- Excellent verbal and written communication skills, specifically the ability to explain security

processes and concepts to varied, often non-technical, audiences.

- Excellent critical thinking and business analysis skills with problem solving abilities.

ABILITY

- Ability to demonstrate as a project manager in managing large and complex cyber security projects.

EXPERIENCE

- Minimum 3 years' experience in IT or information security project management.

QUALIFICATION

- Bachelor's degree in computer science, cyber security or related.
- PMP: Project Management Professional/GCPM: GIAC Certified Project Manager

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.4. Information and Cyber Security Awareness Officer

ROLE

- Information and Cyber Security Awareness Officer

FUNCTION

- Information and Cyber Security Governance, Risk, Compliance & Project Management

DESCRIPTION

- Responsible for planning, developing, implementing, measuring and maintaining of the security awareness and training program to ensure secure behaviors are implemented and followed by all employees, and to create a mature security culture within the organization to reduce cyber risks.

JOB RESPONSIBILITIES

- Develop the strategy, goals, and objectives for the cyber security training, and awareness program.
- Develop new or identify existing awareness and training materials that are appropriate for intended audiences.
- Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
- Plan training and awareness strategies such as sessions, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment.
- Conduct interactive training exercises to create an effective learning environment.
- Evaluate the effectiveness and comprehensiveness of existing training and awareness programs.
- Provide direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate

with their responsibilities.

- Develop computer-based training and awareness modules, learning objectives and goals, and awareness assessments for measuring and assessing employees' proficiency.
- Review training and awareness documentation (e.g., Content Documents).
- Create and deliver training and awareness courses tailored to the audience and physical environment.
- Conduct training and awareness needs assessments and identify requirements.
- Design training and awareness curriculum and course content based on requirements.
- Develop training policies and protocols for cyber training.
- Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.
- Plan and coordinate the delivery of training and awareness techniques and formats (e.g., video courses, mentoring, web-based courses, lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment.
- Ensure that training meets the goals and objectives for cybersecurity training and awareness.
- Conduct periodic reviews/revisions of training and awareness content for accuracy, completeness alignment, and currency.
- Develop or assist with the development of privacy training and awareness materials and other communications to increase employee understanding of organization privacy policies, data handling practices and procedures and legal obligations.
- Ensure that the cyber security awareness program communicates the security policies and requirements.
- Ensure security awareness information is updated on regular basis and reflects the latest

security trends and threats.

- Collect and maintain data needed to meet system cybersecurity reporting.
- Identify top human risks in the organization.
- Establish and maintain communication channels with stakeholders.

KNOWLEDGE

- Risk management processes (e.g., methods for assessing and mitigating risk).
- Cybersecurity and privacy principles.
- Technology that can be exploited.
- Multiple cognitive domains, tools and methods applicable for learning in each domain.
- Learning assessment techniques (evaluation plans, tests, quizzes).
- Computer based training and e-learning services.
- Personal Health Information (PHI) data security standards.
- Instructional design and evaluation models.
- Organizational training policies, processes, and procedures.
- Training and awareness levels, modes, styles, principles and methods.
- Learning Management Systems and their use in managing learning.
- Media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.
- Principles and processes for conducting training and awareness needs assessment.
- Cyber competitions as a way of developing skills by providing hands-on experience in simulated, real world situations.

SKILLS

- Communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
- Using social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
- Talking to others to convey information effectively.
- Utilizing or developing training and awareness technologies and activities (e.g., scenarios, instructional games, interactive sessions).
- Utilizing feedback to improve processes, products, and services.
- Writing facts and ideas in a clear, convincing, and organized manner.

ABILITY

- Develop, procure and tailor trainings and awareness materials that speaks to the topic at the appropriate level for the target audience.
- Prepare and deliver training and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.
- Identify top human risks and the behaviors needed to change and manage those risks.
- Answer questions in a clear and concise manner.
- Ask clarifying questions.
- Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Facilitate small group discussions.
- Gauge learner understanding and knowledge level.

- Prepare and present briefings.
- Provide effective feedback.
- Apply critical reading/thinking skills.
- Evaluate information for reliability, validity, and relevance.
- Function in a collaborative environment, seeking continuous consultation with other analysts and experts.
- Tailor technical and planning information to employees' level of understanding.
- Think critically.
- Understand the basic concepts and issues related to cyber and its organizational impact.
- Conduct training and awareness needs assessment.

EXPERIENCE

- 2-3 years of experience in cyber security with an experience in awareness and training programs.

QUALIFICATION

- Bachelor's degree in computer science, cybersecurity, information technology or relevant to the field.
- CompTIA Security+
- CompTIA Network+
- CySA+: Cyber Security Analyst Certification
- CSAP: Certified Security Awareness Practitioner

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.5. Information and Cyber Security Auditor

ROLE

- Information and Cyber Security Auditor

FUNCTION

- Information and Cyber Security Governance, Risk, Compliance & Project Management

DESCRIPTION

- Responsible for conducting cyber and information security audits against a clear audit criteria based on international audit best practices and addresses nonconformance with organization's policies and local or international standards.

JOB RESPONSIBILITIES

- Develop strategies for risk, enforcement, and assurance efforts to track and evaluate compliance.
- Prepare audit reports that describe technical and procedural findings and include strategies/solutions recommended for remediation.
- Review or conduct audits of information technology (IT) programs and projects.
- Track audit findings and recommendations to ensure that appropriate corrective actions are taken.
- Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
- Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.
- Review, conduct, or participate in audits of cyber and information security programs and

projects.

KNOWLEDGE

- Network concepts and protocols, and network security controls.
- Knowledge and understanding of methods for risk identification, analysis, evaluation, mitigation and management
- Legislation and regulatory aspects and requirements in relation to cybersecurity, privacy, and ethics.
- Personal Health Information (PHI) data security standards.
- Cybersecurity and privacy principles.
- Cybersecurity threats and vulnerabilities.
- Various cybersecurity breach impact areas on an organization, including but not limited to the impact on the reputation/image, operations, or financial loss of the company, or any legal and regulatory consequences.
- Best practices, standards and organizationally accepted analysis principles.
- Information technology (IT) architectural concepts and frameworks.
- Organization's risk management framework requirements and the followed processes and procedures.
- Resource management principles and techniques.
- System life cycle management principles, including software security and usability.
- Best practices for risk management of the supply chain.
- Import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.

- Organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).
- Service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).
- Knowledge of how to leverage research and development centers, think tanks, academic research, and industry systems.
- Organizational information security policies.
- Data security standards relevant to the sector in which the organization operations.
- Laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Confidentiality, integrity, and availability principles.

SKILLS

- Determining system performance metrics or indicators and the steps necessary to enhance or correct performance relative to the system's objectives.
- Conducting audits or reviews of technical systems.
- Auditing detection systems for firewalls, perimeters, routers, and intrusion.
- Anticipate new cyber or information security threats.
- Remain aware of evolving technical infrastructures.
- Translate, monitor and prioritize information needs and criteria for intelligence gathering in the extended enterprise.

ABILITY

- Ensure cybersecurity practices and requirements are addressed and followed throughout the

acquisition process.

- Identify and describe target vulnerability.
- Understand the value of auditing the implementation of cybersecurity policies and to clarify them.

EXPERIENCE

- Entry: 0-3 years of experience in cyber security, security governance/auditing.
- Senior: +5 years of experience in cyber security, security auditing, risk assessments.

QUALIFICATION

- Bachelor's degree in computer science, cybersecurity, information technology or relevant to the field.
- CISA: Certified Information Security Auditor
- ISO27001 Lead Auditor/Implementer

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.6. Data Privacy Protection Officer

ROLE

- Data Privacy Protection Officer

FUNCTION

- Information and Cyber Security Governance, Risk, Compliance & Project Management

DESCRIPTION

- Develops and oversees privacy compliance program and privacy program, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.

JOB RESPONSIBILITIES

- Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
- Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
- Conduct functional and connectivity testing to ensure continuing operability.
- Establish a risk management strategy for the organization that includes a determination of risk tolerance.
- Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).
- Develop and maintain strategic plans.
- Evaluate contracts to ensure compliance with funding, legal, and program requirements.
- Evaluate cost/benefit, economic, and risk analysis in decision-making process.

- Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.
- Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.
- Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
- Present technical information to technical and nontechnical audiences.
- Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.
- Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
- Work with the general counsel, public relations and businesses to ensure both existing and new services comply with privacy and data security obligations.
- Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
- Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
- Liaise with regulatory and accrediting bodies.
- Work with public relations to develop relationships with regulators and other government officials responsible for privacy and data security issues.
- Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure

organizational adaptation and compliance.

- Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.
- Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.
- Work with organization senior management to establish an organization-wide Privacy Oversight Committee
- Serve in a leadership role for Privacy Oversight Committee activities
- Collaborate on cyber privacy and security policies and procedures
- Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation
- Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations
- Provide strategic guidance to corporate officers regarding information resources and technology
- Assist the Security Officer with the development and implementation of an information infrastructure
- Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations.
- Work cooperatively with applicable organization units in overseeing consumer information access rights
- Serve as the information privacy liaison for users of technology systems

- Act as a liaison to the information systems department
- Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations
- Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties
- Conduct on-going privacy training and awareness activities
- Work with public relations to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security
- Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.
- Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee
- Work with public relations to respond to press and other inquiries regarding concern over consumer and employee data
- Provide leadership for the organization's privacy program
- Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization
- Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information

security officer, administration and legal counsel as applicable

- Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures
- Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices
- Develop and coordinate a risk management and compliance framework for privacy
- Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.
- Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations
- Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization's privacy policies and procedures
- Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity
- Provide leadership in the planning, design and evaluation of privacy and security related projects
- Establish an internal privacy audit program
- Periodically revise the privacy program considering changes in laws, regulatory or company policy
- Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel
- Assure that the use of technologies maintains, and does not erode, privacy protections on use,

collection and disclosure of personal information

- Monitor systems development and operations for security and privacy compliance
- Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected
- Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions
- Review all system-related information security plans to ensure alignment between security and privacy practices
- Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements
- Account for and administer individual requests for release or disclosure of personal and/or protected information
- Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements
- Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed
- Act as, or work with, counsel relating to business partner contracts
- Mitigate effects of a use or disclosure of personal information by employees or business partners
- Develop and apply corrective action procedures

- Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel
- Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations
- Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations
- Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units
- Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices
- Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations
- Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials

KNOWLEDGE

- Computer networking concepts and protocols, and network security methodologies.
- Risk management processes (e.g., methods for assessing and mitigating risk).
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cybersecurity and privacy principles.
- Cyber threats and vulnerabilities.
- Specific operational impacts of cybersecurity lapses.

- Applicable business processes and operations of customer organizations.
- Privacy Impact Assessments.
- Applicable laws, Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
- Knowledge on what constitutes a “threat” to a network.
- Knowledge on who the organization’s operational planners are, how and where they can be contacted, and what are their expectations.
- Personal Health Information (PHI) data security standards.
- Wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.
- Privacy disclosure statements based on current laws.

SKILLS

- Creating policies that reflect the business’s core privacy objectives.
- Negotiating vendor agreements and evaluating vendor privacy practices.
- Communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).

ABILITY

- Develop clear directions and instructional materials.
- Develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.
- Develop, update, and/or maintain standard operating procedures (SOPs).

- Select the appropriate implant to achieve operational goals.
- Tailor technical and planning information to a customer's level of understanding.
- Monitor advancements in information privacy laws to ensure organizational adaptation and compliance.
- Work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
- Monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
- Develop or procure curriculum that speaks to the topic at the appropriate level for the target.
- Work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
- Author a privacy disclosure statement based on current laws.

EXPERIENCE

- 5 years of experience in cyber security, security risk assessments.

QUALIFICATION

- Bachelor's degree in computer science, cybersecurity, information technology or relevant to the field.
- CIPP: Certified Information Privacy Professional
- CIPM: Certified Information Privacy Manager
- HCISSP: HealthCare Information Security and Privacy Practitioner

- CDPSE: Certified Data Privacy Solutions Engineer

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.7. Information and Cyber Security Legal Advisor

ROLE

- Information and Cyber Security Legal Advisor

FUNCTION

- Information and Cyber Security Governance, Risk, Compliance & Project Management

DESCRIPTION

- Responsible for providing legal advice on cyber or information security laws and regulations.

JOB RESPONSIBILITIES

- Advocate organization's official position in legal and legislative proceedings.
- Evaluate contracts to ensure compliance with funding, legal, and program requirements.
- Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.
- Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.
- Resolve conflicts in laws, regulations, policies, standards, or procedures.
- Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.
- Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.
- Develop guidelines for implementation.
- Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.
- Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.

- Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
- Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.
- Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).

KNOWLEDGE

- Computer networking concepts and protocols, and network security methodologies.
- Risk management processes (e.g., methods for assessing and mitigating risk).
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cybersecurity and privacy principles.
- Cyber threats and vulnerabilities.
- Specific operational impacts of cybersecurity lapses.
- Concepts and practices of processing digital forensic data.
- New and emerging information technology (IT) and cybersecurity technologies.
- Insider Threat investigations, reporting, investigative tools and laws/regulations.
- Cyber defense and information security policies, procedures, and regulations.
- Payment Card Industry (PCI) data security standards.
- Personal Health Information (PHI) data security standards.
- Laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Intelligence gathering principles, policies, and procedures including legal authorities and

restrictions.

- Business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.
- Foreign disclosure policies and import/export control regulations as related to cybersecurity.
- Privacy disclosure statements based on current laws.

SKILLS

- Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).

ABILITY

- Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies.

EXPERIENCE

- 3 years of experience.

QUALIFICATION

- Bachelor's degree in computer science, cybersecurity, information technology or relevant to the field with specialization in Cyber Laws.
- Diploma in Cyber Law.

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.8. Information and Cyber Technology/Medical Device Security Manager

ROLE

- Information and Cyber Technology/Medical Device Security Manager

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Manages and ensures the daily security operations of IT systems, applications, network devices, bio-medical equipment's, IT Assets in the organization.

JOB RESPONSIBILITIES

- Review and approve current security measures and recommend and implement enhancements.
- Ensure that acquired or developed systems and architectures are consistent with the organization's cybersecurity architecture guidelines.
- Manage the monitoring of information security data sources to maintain organizational situational awareness.
- Manage the publishing of Computer Network Defense guidance for the enterprise constituency.
- Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.
- Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.
- Oversee the information security training and awareness program.
- Participate in an information security risk assessment during the Security Assessment and Authorization process.
- Participate in the development or modification of the computer environment cybersecurity

program plans and requirements.

- Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
- Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
- Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.
- Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.
- Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.
- Recognize a possible security violation and take appropriate action to report the incident, as required.
- Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
- Recommend policy and coordinate review and approval.
- Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
- Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
- Use federal and organization-specific published documents to manage operations of their computing environment system(s).

- Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
- Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
- Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
- Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
- Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
- Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
- Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.
- Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
- Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.
- Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
- Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.

- Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.
- Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.

KNOWLEDGE

- Communication methods, principles, and concepts that support.
- Capabilities and applications of network equipment including (routers, switches, bridges, servers, transmission media, and related hardware).
- Enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)
- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Risk management processes (e.g., methods for assessing and mitigating risk).
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cybersecurity and privacy principles.
- Cyber threats and vulnerabilities.
- Knowledge of specific operational impacts of cybersecurity lapses.
- Applicable business processes and operations of customer organizations.
- Encryption algorithms
- Data backup and recovery.
- Business continuity and disaster recovery continuity of operations plans.
- Host/network access control mechanisms (e.g., access control list, capabilities list).

- Cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- Vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
- Incident response and handling methodologies.
- Industry-standard and organizationally accepted analysis principles and methods.
- Intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Risk Management Framework (RMF) requirements.
- Measures or indicators of system performance and availability.
- Current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.
- Network traffic analysis methods.
- New and emerging information technology (IT) and cybersecurity technologies.
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
- System and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- Resource management principles and techniques.
- Server administration and systems engineering theories, concepts, and methods.

- Server and client operating systems.
- System software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.
- System life cycle management principles, including software security and usability.
- Technology integration processes.
- Knowledge of the organization's enterprise information technology (IT) goals and objectives.
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
- Information security program management and project management principles and techniques.
- Supply Chain Risk Management Practices (NIST SP 800-161)
- Knowledge of organization's risk tolerance and/or risk management approach.
- Enterprise incident response program, roles, and responsibilities.
- Current and emerging threats/threat vectors.
- Critical information technology (IT) procurement requirements.
- System administration, network, and operating system hardening techniques.
- Applicable laws, regulations, and/or administrative/criminal legal guidelines and procedures.
- Information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
- Critical infrastructure systems with information communication technology that were designed without system security considerations.
- Network security architecture concepts including topology, protocols, components, and

principles (e.g., application of defense-in-depth).

- Network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).
- Personally Identifiable Information (PII) data security standards.
- Knowledge of Payment Card Industry (PCI) data security standards.
- Personal Health Information (PHI) data security standards.
- Laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Knowledge of an organization's information classification program and procedures for information compromise.
- Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Penetration testing principles, tools, and techniques.
- Controls related to the use, processing, storage, and transmission of data.
- Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

SKILLS

- Creating policies that reflect system security objectives.
- Determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- Evaluating the trustworthiness of the supplier and/or product.

ABILITY

- Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
- Integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).
- Identify critical infrastructure systems with information communication technology that were designed without system security considerations.

EXPERIENCE

- 5 years of experience in information security, security engineering, or system and software programming.

QUALIFICATION

- Bachelor's degree in computer science/engineering, information security, software engineering, systems engineering or information systems.
- CompTIA Security+
- ECSA: EC-Council Certified Security Analyst
- CISSP: Certified Information Systems Security Professional
- CCNP: Certified Network Professional Security

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.9.System Security Engineer

ROLE

- System Security Engineer

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Responsible for the planning, implementing, evaluating and maintaining systems security within the entity by ensuring all security measures are integrated into systems throughout the systems life cycle to protect systems boundaries and harden systems from a cybersecurity perspective.

JOB RESPONSIBILITIES

- Analyze business needs and requirements to plan and conduct system security development.
- Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, and processing Sensitive Compartmented Information).
- Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
- Implement and integrate security system development life cycle methodologies.
- Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.
- Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability and authentication.
- Develop mitigation strategies to address cost, schedule, performance, and security risks.
- Provide input to implementation plans and standard operating procedures as they relate to

information systems security.

- Trace system requirements to design components and perform gap analysis.
- Verify stability, interoperability, portability, and/or scalability of system architecture.
- Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.
- Implement specific cybersecurity countermeasures for systems.
- Perform cybersecurity testing of developed systems.
- Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
- Properly document all systems security implementation, operations, and maintenance activities and update as necessary.
- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
- Verify and update security documentation reflecting the system security design features.
- Assess the effectiveness of security controls.
- Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.
- Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance.
- Assess and monitor cybersecurity related to system implementation and testing practices.

KNOWLEDGE

- Cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability and authentication).
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms, and traffic analysis methods.
- Knowledge of risk management policies, requirements, procedures and processes (e.g., methods for assessing and mitigating risk).
- Installation, integration, and optimization of system components.
- Human-computer interaction principles.
- Information technology (IT) security principles and methods (e.g., firewalls and encryption).
- System design tools, methods, and techniques, including automated systems analysis and design tools.
- System life cycle management principles, including software security and usability.
- Systems testing and evaluation methods.
- Systems engineering processes, approaches, methodologies and principles.
- Configuration management techniques.
- Information classification program and procedures for information compromise.
- Countermeasure design for identified security risks.

SKILLS

- Determining how a system should work securely (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect the security posture.

- Conducting vulnerability scans and recognizing vulnerabilities in systems.
- Assessing and designing security controls based on cybersecurity principles and tenets
- Designing countermeasures to identified security risks.
- Writing code in a currently supported programming language (e.g., Java, C++).
- Developing and applying system security access controls.
- Discerning the protection needs (i.e., security controls) of information systems and networks.
- Evaluating the adequacy of security designs.
- Conducting security audits or reviews of technical systems.
- Integrating and applying policies that meet system security objectives.

ABILITY

- Identify systemic security issues based on the analysis of vulnerability and configuration data.
- Apply secure system design tools, methods and techniques.
- Ensure security practices are followed throughout the acquisition process.
- Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Produce technical documentation.
- Translate data and test results into evaluative conclusions.
- Function in a collaborative environment, seeking continuous consultation with other analysts and experts.
- Regularly perform security checks and troubleshooting.
- Identify problems in a timely manner.

- Suggest and implement solutions for improvement.
- Implement new processes with the goal to optimize system security.
- Stay up to date with latest security system technology and trends.

EXPERIENCE

- +5 years of experience in information security, security engineering, or system and software programming.

QUALIFICATION

- Bachelor's degree in computer science/engineering, information security, software engineering, systems engineering or information systems.
- CompTIA Security+
- ECSA: EC-Council Certified Security Analyst
- CISSP: Certified Information Systems Security Professional
- ISSEP: Information Systems Security Engineering Professional
- ISSAP: Information Systems Security Architecture Professional

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.10. Network Security Engineer

ROLE

- Network Security Engineer

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Responsible for the planning, provision, deployment, installation, configuration and optimization of the network's security including hardware and software components in the aim of safeguarding networks infrastructure against cyber interruptions.

JOB RESPONSIBILITIES

- Design, configure, implement and maintain network security and associated software and hardware such as routers, switches, firewalls, intrusion detection/intrusion prevention, anti-virus, cryptography systems, SIEM, Anti-SPAM, and MDM.
- Ensure network security best practices are implemented through auditing.
- Maintain network architecture security as per the security policy.
- Analyze and recommend architectural networking systems.
- Conduct periodic network monitoring and intrusion detection analysis.
- Plan, engineer, and monitor the security arrangements for the protection of the network.
- Identify, monitor, and define the requirements of the overall security of the network and create different ways to solve the existing threats and security networking issues.
- Configure and implement intrusion detection systems and firewalls.
- Supervise the configuration and installation of new networking software and hardware.

- Test and check the network for weaknesses in software and hardware.
- Maintain firewalls, virtual private networks, web protocols, and email security.
- Maintain virus and threat detection systems.
- Determine latest technologies and processes that improve the overall security of the network.
- Use industry-standard analysis criteria to test the security level of the network.
- Develop tracking documents to note network vulnerabilities.
- Modify the technical, legal, and regulatory aspects of the network security.
- Define and maintain network security policies and protocols for greater efficiency against any threat or malfunctions.
- Occasionally replace the security network protocol and architecture.
- Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
- Develop and implement network backup and recovery procedures.
- Implement new network design procedures, test procedures, and quality standards.
- Integrate new systems into existing network architecture.
- Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
- Provide feedback on network requirements, including network architecture and infrastructure.
- Test and maintain network infrastructure including software and hardware devices.

KNOWLEDGE

- Computer networking concepts and protocols, and network security methodologies.
- Network related cyber threats and vulnerabilities.

- Communication methods, principles, and concepts that support the network infrastructure.
- Applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
- Different types of network communication (e.g., LAN, WAN, WLAN), connections, networking principles and concepts including bandwidth management.
- How traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
- Server administration and systems engineering theories, concepts, and methods.
- Virtual Private Network (VPN) security.
- Network tools (e.g., ping, traceroute, nslookup)
- Common attack vectors on the network layer.
- Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wi-Fi.
- Information classification program and procedures for information compromise.

SKILLS

- Analyzing network traffic capacity and performance characteristics.
- Establishing a routing schema.
- Implementing, maintaining, and improving established network security practices.
- Installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.
- Using network management tools to analyze network traffic patterns (e.g., simple network management protocol).
- Securing network communications.
- Protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
- Configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
- Implementing and testing network infrastructure contingency and recovery plans.

ABILITY

- Operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
- Operate common network tools (e.g., ping, traceroute, nslookup) and interpret collected information.
- Execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
- Monitor measures or indicators of system performance and availability.
- Monitor traffic flows across the network.

- Deal with high-stress situations and thrive in a fast-paced environment.
- Communicate and report network security issues to the upper management.

EXPERIENCE

- +5 years of experience in information security with +2 years of experience in network security.

QUALIFICATION

- Bachelor's degree in information technology, information security or network security.
- CompTIA Network+
- FCNSP: Fortinet Certified Network Security Professional
- CCNP: Certified Network Professional Security
- CCNA Routing and Switching certification

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.11. Software/Application Security Engineer

ROLE

- Software/Application Security Engineer

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Responsible for maintaining the security of new or existing software or applications by carrying out regular security tests, appropriate security reviews, defenses and countermeasures throughout software/application development lifecycle, and provide actionable results to ensure a robust and reliable software/application.

JOB RESPONSIBILITIES

- Implement, test and operate advanced software/application security techniques in compliance with technical reference architecture.
- Provide engineering designs for new software/application to help mitigate security vulnerabilities.
- Perform integrated quality assurance testing for security functionality and resiliency.
- Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or software undergoes a major change.
- Address security implications in the software/application acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
- Translate security requirements into software/application design elements including documenting the elements of attack surfaces, conducting threat modeling, and defining any specific security criteria.

- Perform penetration testing as required for new or updated software or applications.
- Provide consultation about software/application design and maintenance.
- Direct software programming and development of documentation.
- Analyze security needs and software/application requirements to determine feasibility of design within time and cost constraints and security mandates.
- Conduct trial runs of software/application to ensure that the desired information is produced with instructions and the security levels are correct.
- Develop software/application testing and validation procedures, programming, and documentation.
- Perform secure software/application testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.
- Determine and document software/application patches or the extent of releases that would leave it vulnerable.

KNOWLEDGE

- Software/ application development life cycle.
- Software/application engineering processes, approaches and methodologies.
- Structured analysis principles and methods.
- System and application security threats and vulnerabilities.
- Secure configuration management techniques.
- Software/application debugging principles.
- Software/application designing tools, methods, and techniques including automated analysis and design tools.

- Software/application related security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).
- Software/application quality assurance process.
- Risk management policies, requirements, and procedures.
- Computer programming principles.
- Cybersecurity and privacy principles and methods that apply to software/application development.
- Secure coding techniques.
- Secure software/application deployment methodologies, tools, and practices.
- Vulnerability scans and penetration testing principles, tools, and techniques.
- Root cause analysis techniques.
- Application Security Risks (e.g. Open Web Application Security Project Top 10 list).

SKILLS

- Discerning the protection needs (i.e., security controls) of software and applications.
- Integrating testing tools into quality assurance process of software and application releases.
- Secure test plan design (e. g. unit, integration, system, acceptance).
- Conducting vulnerability scans and recognizing vulnerabilities.
- Designing countermeasures to identified security risks within software and applications.
- Developing controls and using tools that improve the defense of software and applications.

ABILITY

- Make sure teams are using the right security measures when required.

- Develop secure software/application according to secure deployment methodologies, tools, and practices.
- Apply cybersecurity and privacy principles to software/application development requirements (relevant to confidentiality, integrity, availability, authentication).
- Articulate, plan, implement and manage software security best practices.

EXPERIENCE

- +5 years of experience in information security, security engineering, and applications and software programming.

QUALIFICATION

- Bachelor's degree in computer science, information technology, software engineering or computer engineering.
- ECSP: EC-Council Certified Secure Programmer
- CSSLP: Certified Secure Software Lifecycle Professional
- GSSP-JAVA: GIAC Secure Software Programmer-Java
- GSSP-NET: GIAC Secure Software Programmer- .NET
- CASE: Certified Application Security Engineer

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.12. Information Security Architect

ROLE

- Information Security Architect

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Manage the security architecture program of the organization and ensure all necessary security requirements are adequately addressed by designing, building, deploying and maintaining secure solutions to protect systems and information assets from external and internal threats.

JOB RESPONSIBILITIES

- Develop/integrate security designs for systems and networks with multilevel security requirements.
- Review current security measures and recommend and implement enhancements.
- Conduct regular system tests and ensure continuous monitoring of network security.
- Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
- Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements.
- Ensure that acquired or developed systems and architectures are consistent with the organization's cybersecurity architecture guidelines.
- Identify and prioritize critical business functions in collaboration with organizational

stakeholders.

- Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
- Provide advice on project costs, design concepts, or design changes.
- Provide input on security requirements to be included in statements of work and other appropriate procurement documents.
- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
- Define and document how the implementation of a new system impacts the security posture of the current environment.
- Analyze candidate architectures, allocate security services, and select security mechanisms.
- Develop a security system context and define baseline security requirements in accordance with applicable cybersecurity requirements.
- Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.
- Write detailed functional specifications that document the architecture development process.
- Analyze user needs and requirements to plan architecture.
- Develop enterprise architecture or system components required to meet user needs.
- Document and update as necessary all definition and architecture activities.
- Determine the protection needs (i.e., security controls) for the information system(s) and

network(s) and document appropriately.

- Translate proposed capabilities into technical requirements.
- Assess and design security management functions as related to cyberspace.

KNOWLEDGE

- Communication methods, principles, and concepts that support the network infrastructure.
- Capabilities and applications of network equipment including (routers, switches, bridges, servers, transmission media, and related hardware).
- Enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)
- Electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).
- System components installation, integration, and optimization processes.
- Software and system engineering, testing and evaluation methods.
- Technology integration processes.
- Critical infrastructure systems with information communication technology that were designed without system security considerations.
- Network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Various types of computer architectures.
- Multi-level security systems and cross domain solutions.
- Risk management frameworks, approaches and processes (e.g., methods for assessing and mitigating risk).

- Specific operational impacts of cybersecurity lapses.
- Cyber defense and vulnerability assessment tools and their capabilities.
- Business continuity and disaster recovery, continuity of operations plans.
- Human-computer interaction principles.
- Cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication).
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms, traffic analysis methods, architecture concepts including protocols, components, and principles.
- New and emerging information technology (IT) and cybersecurity technologies.
- Key concepts in security management (e.g., Release Management, Patch Management).
- Application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).

SKILLS

- Applying and incorporating information technologies into proposed solutions.
- Designing countermeasures to identified security risks.
- Designing the integration of security hardware and software solutions.
- Determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.

- Using Virtual Private Network (VPN) devices and encryption.
- Configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
- Designing multi-level security/cross domain solutions.
- Using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).
- Applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
- Translating operational requirements into protection needs (i.e., security controls).
- Setting up sub-networks that separate an internal local area network (LAN) from other untrusted networks.
- Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) and identify issues that stem from connections with internal and external customers and partner organizations.

ABILITY

- Integrate the organization’s goals and objectives into the architecture.
- Design architectures and frameworks.
- Apply the methods, standards, and approaches for describing, analyzing, and documenting an organization’s information technology (IT) architecture.
- Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Conduct vulnerability scans and recognize vulnerabilities in security systems.

- Optimize security systems to meet performance requirements.
- Apply secure system design tools, methods and techniques.
- Work closely and coordinate with system security analysts, advise authorizing officials, chief information security officers, and the senior accountable official for risk management on a range of security-related issues (e.g. establishing system boundaries; assessing the severity of weaknesses and deficiencies in the system; plans of action and milestones; risk mitigation approaches; security alerts; and potential adverse effects of identified vulnerabilities).
- Identify critical infrastructure systems with information communication technology that were designed without system security considerations.

EXPERIENCE

- +4 years of experience in information security and/or IT risk management with a focus on security, performance and reliability.

QUALIFICATION

- Bachelor's degree in computer science, cybersecurity, information technology, software/network engineering, or computer engineering.
- CompTIA Security+
- ECSA: EC-Council Certified Security Analyst
- CNDA: Certified Network Defense Architect
- GDSA: GIAC Defensible Security Architecture
- CSSA: IACRB Certified SCADA Security Architect
- CISSIP-ISSAP: Information Systems Security Architecture Professional

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.13. Cloud Security Specialist

ROLE

- Cloud Security Specialist

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Leads the cloud security program within the entity, which includes implementing, evaluating and governing of secure cloud deployments, applications and services by ensuring full compliance with security standards and regulations. Responsible for strategizing and coordinating internal cybersecurity efforts with those of cloud providers.

JOB RESPONSIBILITIES

- Plan, implement, upgrade and monitor security controls for the protection of cloud-based networks and information systems.
- Ensure appropriate cloud security policies and controls are in place that will safeguard digital files and vital electronic systems.
- Develop cloud security compliance processes and/or audits.
- Develop cloud-based data management capabilities.
- Provide technical assistance in the selection, configuration, and maintenance of cloud security devices/systems including, but not limited to, firewalls, IPS/IDS, SIEM, WAF, Network-based Malware detection and related platforms as well as software-defined systems.
- Advise developers, architects, security engineers and other stakeholders to ensure confidentiality, integrity, resiliency, and privacy into cloud platforms designs.
- Designing processes and procedures for public cloud integration.

- Analyze security requirements for public cloud implementation and integration.
- Implementation of technological solutions dedicated to the data protection in cloud.
- Integration and configuration of Security as a Service.
- Build and/or evaluate cloud-based solutions while actively driving risk down using industry best practice.
- Create security specifications, develop processes and evaluate tools for the secure adoption of cloud services.
- Oversee cloud related projects to ensure appropriate usage of security tools and security methodologies used.
- Assist in implementation of security related product features like authentication, cryptography, etc.
- Evaluate 3-rd party Cloud services, systems, tools and solutions from a cybersecurity perspective.
- Responsible for contributing to, implementing and measuring strategic cloud security programs.
- Work with Application Developers, Systems Engineers, and Executives to ensure mitigation of risks identified in cloud-based solutions.
- Assist in the evaluation, research and development of IT cloud security risk assessments, security tools and implementation plans.
- Engage with cross-functional teams in the design and implementation of cloud and cloud-security projects and initiatives.

KNOWLEDGE

- Cloud ecosystems.
- Cloud service models and how those models can limit incident response.
- Cloud Security frameworks.
- Industry cloud computing standards - ISO 17788/17789, CSA CCM/STAR.
- Cloud security standards including NIST, CIS, NCSC and ISO.
- Private, hybrid and public cloud-based solutions.
- Common cloud security threats and security controls.
- Associated technologies and practices related to securing cloud platforms.
- Cloud services and associated IT resources based on typical cloud technologies.
- Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.
- Use cases related to collaboration and content synchronization across cloud platforms.
- IT security solutions (Cloud Access Security Broker, Data Leakage Prevention, Multi Factor Authentication, Data Rights Management, etc.).
- Networking configurations and practices in cloud environments.
- Trends and emerging changes to the cloud security landscape.
- Security Assessment and Authorization process.
- Networking concepts and protocols, and network security methodologies.

SKILLS

- Using and understanding of advanced cloud security protocols, standards, principles and practices as well as latest scalable technologies (hard and soft).
- Cloud Platform configuration and administration of security features and services (including and not limited to identity and access management, service-related security features, networking, firewalls, encryption, and related best practices).
- Designing incident response for cloud service models.
- Using cloud-based virtual machines.
- Establishing security requirements needed for cloud services security.
- IaaS and PaaS deployments, connectivity, network security, virtualization and compute.
- Articulating and documenting design and implementation approaches for secure cloud architectures.

ABILITY

- Drive cloud cyber security compliance programs.
- Embed best practice security through evaluation of cloud environments.
- Interact with internal and external teams on cloud security-related projects and operational tasks.
- Prepare/conduct brief outs to senior staff members and executives on a regular basis.
- Manage multiple priorities and work effectively in a fast-paced, high volume, results driven environment.
- Rapidly assess a situation and identify, isolate and communicate problems and issues.
- Clearly communicate risks and risk management issues to technologists and non-technologists.

- Effectively present complex technical information in a clear and concise manner to a variety of audiences.
- Demonstrate innovative security approaches in non-traditional IT environments.

EXPERIENCE

- +5 years of experience in public cloud environment and infrastructure, secure application development or cloud computing, with +2 years of practical/technical cloud security experience.

QUALIFICATION

- Bachelor's degree in computer science, information security, information technology or computer engineering.
- CCSP: Certified Cloud Security Professional
- CompTIA Cloud+
- PCS: Professional Cloud Security Manager
- SANS Cloud Security and Risk Fundamentals

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.14. IoMT Security Specialist

ROLE

- IoMT Security Specialist

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Identifies and mitigates security threats and risks on IoMT and implements security controls and best practices.

JOB RESPONSIBILITIES

- Perform IoMT system security reviews and evaluations, including application design, embedded applications, web apps, web services, and mobile apps.
- Contribute actively to the growth of the organization security software with an emphasis on IoMT devices.
- Engage with stakeholders, understand their goods and criteria for evaluation, and identify test programs.
- Monitor the growth of the cybersecurity industry in terms of IoMT environments.

KNOWLEDGE

- Knowledge to identify, mitigate, and manage security threats and risks on IoMT.

SKILLS

- Identify security threats and risks on IoMT.
- Implements security controls and best practices.
- Mitigate security threats and risks on IoMT.

ABILITY

- Ability to define relationships between two or more data sources linked to cybersecurity that may initially appear unrelated.

EXPERIENCE

- 3 years of experience in information security.

QUALIFICATION

- Bachelor's degree in computer science/engineering, information security.
- CISSP: Certified Information Systems Security Professional.
- CompTIA Security+
- Certified Internet of Things Security Practitioner

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.15. Artificial Intelligence Security Specialist

ROLE

- AI Security Specialist

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Designs, develops, tests and maintains artificial intelligence in cybersecurity solutions and tools.

JOB RESPONSIBILITIES

- Suggest implementation of artificial intelligence in threat detection and response for cybersecurity.
- Evaluate and test cybersecurity solutions with machine learning functionality to ensure that it meets the organization's needs.

KNOWLEDGE

- Knowledge of approved intelligence dissemination processes.
- Knowledge of cyber intelligence/information collection capabilities and repositories.

SKILLS

- Design and develop artificial intelligence in cybersecurity solutions and tools.
- Test and maintain artificial intelligence in cybersecurity solutions and tools.

ABILITY

- Ability to develop statistical and machine learning models.

EXPERIENCE

- 3 years of experience in information security.

QUALIFICATION

- Bachelor's degree in computer science/engineering, information security.
- CISSP: Certified Information Systems Security Professional.
- CompTIA Security+
- AI/ML in Cybersecurity
- Python

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.16. Information Security Analyst

ROLE

- Information Security Analyst

FUNCTION

- Information and Cyber Technology/Medical Device Security

DESCRIPTION

- Actively monitor the networks, systems, applications, IT assets and bio-medical equipment's for suspicious activity and threats. Using offensive and defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or may occur within the network and make the initial decision on the event/ threat severity.

JOB RESPONSIBILITIES

- Manage network, intrusion detection and prevention systems.
- Conduct periodic compromise assessments across selected networks and propose recommendations based on assessment results.
- Conduct physical security assessment of the organization's systems, including servers and networks, ensuring that any unauthorized external physical interference is not actually possible.
- Conduct ongoing network hunt activities.
- Conduct proactive vulnerability assessment across the network, subnetworks and service traffic to identify potential points of intrusion.
- Research and develop methods of tracking and detecting malicious activity within a network.
- Develop tools, signatures, and methods of detection for use in incident response activities.
- Develop SIEM integrations, dashboards, and analytics to illuminate and visualize threat activity.
- Analyze network traffic to provide timely detection, identification, and alerting of possible

attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.

- Uses data collected from a variety of cyber defense tools (e.g., anti-virus, IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments, perform cyber defense trend analysis and reporting, and perform event correlation to mitigate threats and gain situational awareness and determine the effectiveness of an observed attack.
- Carries out triage to ensure that a genuine security incident is occurring.
- Coordinate with entity-wide cyber defense staff to validate network alerts.
- Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.
- Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.
- Provide daily summary reports of network events and activity relevant to cyber defense practices.
- Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
- Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
- Isolate and remove malware.
- Develop content for cyber defense tools use them for continual monitoring and analysis of network activity to identify malicious activity.
- Assist in the construction of signatures which can be implemented on cyber defense tools in

response to new or observed threats within the network environment.

- Analyze and report organizational security posture trends.
- Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus, Threat Intelligence Providers) to maintain updated of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
- Provides cybersecurity recommendations based on significant threats and vulnerabilities.
- Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operational Plans.
- Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber incidents within the enterprise.
- Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
- Utilize deployable forensics toolkit to support operations as necessary.

KNOWLEDGE

- Security concepts such as cyber-attacks and techniques, threat vectors, risk and threat management, incident management etc.
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms, traffic analysis methods.
- Cyber threats and vulnerabilities and information dissemination sources (e.g., alerts and advisories).
- Cyber defense and vulnerability assessment tools and their capabilities.
- System and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections,

race conditions, covert channel, replay, return-oriented attacks, malicious code).

- Scripting languages (e.g., Python, Perl, Bash) used in an incident response environment
- Incident response and handling methodologies.
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools, applications, methodologies and techniques for detecting host and network-based intrusions.
- Threat investigations, reporting and investigative tools.
- Cyber defense and information security policies, procedures, and regulations.
- Common attack vectors, the different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks) and attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored), and attackers' methodologies.
- Signature implementation impact for viruses, malware, and attacks.
- Windows/Unix ports and services.
- Relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
- Packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- Use of sub-netting tools.
- Penetration testing principles, tools, and techniques.
- Investigation, auditing and forensics methods, processes, procedures and standards.
- Different types of hardware, storage, imaging and file system analysis.

- Data backup and recovery.

SKILLS

- Using SIEM/SOAR and Vulnerability Management tools and services.
- Sysadmin skills (Linux/Mac/Windows).
- Programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more).
- Identifying, analyzing and interpreting trends or patterns in complex data sets.
- Developing and deploying signatures.
- Detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort).
- Using incident handling methodologies.
- Collecting data from a variety of cyber defense resources.
- Recognizing and categorizing types of vulnerabilities and associated attacks.
- Performing packet-level analysis.
- Conducting trend analysis.
- Using cyber defense reporting structure and processes.
- Utilizing a combination of automated and manual testing methods.
- Developing automated vulnerability testing scripts and using off the shelf vulnerability testing tools.
- Conducting vulnerability scans and recognizing vulnerabilities in networks, systems and applications.
- Using of penetration testing tools and techniques.
- Applying analytical and problem-solving skills.

ABILITY

- Collaborate with other sections across the department to enhance detection capabilities.
- Perform Malware analysis.
- Work closely with management to respond appropriately to the results of assessments and mitigation oversight of found vulnerabilities.
- Perform data analysis, correlation, and analytics leveraging Security Information and Event Management (SIEM) tools.
- Conduct vulnerability scans and recognize vulnerabilities in security systems & devices.
- Accurately and completely source all data used in intelligence, assessment and/or planning products.
- Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
- Interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
- Prepare and create regular reports to document any security breaches/ incidents.
- Provide forensic support to Cyber Security Operations during the investigation of any detected threat or contained incident / event to determine root cause and propose response recommendations as required.

EXPERIENCE

- 3 years of experience.

QUALIFICATION

- Bachelor's degree in an information technology, computer science, cyber security or equivalent work experience.
- CompTIA Security+

- GCFA: GIAC Certified Forensic Analyst
- GCIH: GIAC Certified Incident Handler
- GCIA: GIAC Certified Intrusion Analyst
- OSCP: Offensive Security Certified Professional
- CEH: Certified Ethical Hacker
- CPT: Certified Penetration Tester
- CISSP: Certified Information Systems Security Professional

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.17.Security Operations Manager

ROLE

- Security Operations Manager

FUNCTION

- Cyber Security Operations

DESCRIPTION

- Direct, oversee and serve as a senior subject matter expert of the day-to-day operations of the 24x7x365 Security Operation Center that provides threat detection, event monitoring, incident triage, incident handling, incident responses, recovery services, cyber hunting, and forensic and malware analysis functionality across all served network environments.

JOB RESPONSIBILITIES

- Lead and manage 24x7x365 Security Operations Center using the latest in monitoring and analytic technologies to identify and respond to threats effectively.
- Direct SOC team, functions, processes, and operations.
- Lead the expansion and growth of the SOC; drive integration of new products and services.
- Oversee and ensure security incident optimal identification, assessment, reporting, communication, mitigation, monitoring, escalation, and resolution.
- Develop and maintain an incident response management program that includes incident detection, analysis, containment, recovery and chain of evidence/ forensic artifacts required for additional investigations.
- Manage outsourced and in-house SOC relationships and services for quality performance, compliance and fulfillment of Service Level Agreements (SLA).
- Revise and develop processes to strengthen the current Security Operations Framework, and

review policies and highlight the challenges in managing SLAs.

- Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for Security Operations Center.
- Management and administration of security tools and devices which consists of state-of-the art technologies.
- Perform threat management, threat modeling, identify threat vectors and develop use cases for security monitoring.
- Creation of reports, dashboards and metrics for SOC operations and presentation to senior leadership.
- Develop and maintain processes and procedures associated with security monitoring and response use cases to address and respond to potential security incidents and promote timely escalation and incident coordination.
- Assist with the configuration of SIEM tools and evaluate existing rules, filters, events and use cases to analyze security event data, detect suspicious activity, and alert on potential security incidents.
- Develop and ensure crisis communication plans implementation.
- Direct the Cyber/ Threat Intelligence capability to identify potential threats, and deliver strategies to minimize the impact of the threat.
- Ensure the SOC to consume the latest threat intelligence data obtained internally or externally and develop appropriate response strategies based on intelligence received.
- Oversee the provision of forensics and malware reverse engineering capabilities within the center to support remaining functions in determining effective security counter measures to common and unique threats.

- Communicate threats to Senior Management that may impact the entity's risk profile.
- Drive collaboration efforts between the SOC and counterparts to maximize effectiveness of detection efforts and knowledge of the local cyber security landscape.
- Identify and communicate key performance indicators to help stakeholders understand the SOC roles and responsibilities and the effectiveness of the SOC program and establish performance goals and priorities.

KNOWLEDGE

- Security concepts such as cyber-attacks and techniques, threat vectors, risk and threat management, incident management etc.
- Cyber related threats and vulnerability types, information dissemination sources (e.g., alerts and advisories).
- Insider Threat investigations, reporting and investigative tools.
- Relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
- Security policies based on industry standards and best practices.
- Networking concepts and protocols, and network security attacks, vulnerabilities.
- Penetration testing and vulnerability assessment principles, tools, and techniques.
- Incident response and handling concepts, programs, processes, methodologies, roles and responsibilities.
- Intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Various operating systems including but not limited to Windows, Linux, Unix.

- Applications, databases, middleware to address security threats against the same.
- Thorough knowledge of SIEM and SOAR technologies.
- End Point Security, Internet Policy Enforcement, Firewalls, Web Content Filtering, Database Activity Monitoring (DAM), Data Loss Prevention (DLP) and Identity and Access Management (IAM).

SKILLS

- Use incident handling methodologies
- Assist staff on using security devices and SIEM.
- Recognizing and categorizing types of vulnerabilities and associated attacks.
- Troubleshooting in a technical environment.
- Providing timely, constructive, and actionable feedback that increases individual and team effectiveness.
- Applying strong analytical, creative, and organizational skills.
- Excellent written and verbal communication skills, interpersonal and collaborative skills.
- Coaching and mentoring SOC staff to ensure employees are working as efficiently as possible while fostering a team-oriented environment.
- Preparation of reports, dashboards and documentation.
- Establish performance goals and priorities.
- Highly self-motivated and directed, with a keen attention to detail.

ABILITY

- Recommend specific tools and processes to maximize security monitoring and response capability.

- Handle high pressure situations.
- Promote knowledge sharing amongst staff and unify different groups as appropriate.
- Create and deliver concise, clear, and compelling oral and written briefing materials within tight timelines and for multiple audiences.
- Provide recommendations and develop proposals, presentations, and other critical documentation for senior leaders.
- Perform supervisory/managerial responsibilities.
- Be resilience to stressful situation.
- Drive efficient and timely operations.
- Actualize continual improvement and innovation.
- Build and maintain employee morale and motivation.
- Establish and maintain cooperative working relationships with other employees, vendors, and other organizations.

EXPERIENCE

- 7-10 years of experience in cyber security with +5 years of experience in leading security operations, significant involvement with operations management, business continuity and policy compliance development.

QUALIFICATION

- Bachelor's degree in an information technology, cyber security or equivalent work experience.
- CISM: Certified Information Security Manager
- GCFE: GIAC Certified Forensic Examiner
- GCIH: GIAC Certified Incident Handler

- GCIA: GIAC Certified Intrusion Analyst
- CEH: Certified Ethical Hacker
- GSLC: GIAC Security Leadership

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☑ Transitional

☑ Advanced

5.18.Security Operation Center (SOC) analyst – Tier 1

ROLE

- Security Operation Center (SOC) analyst – Tier 1

FUNCTION

- Cyber Security Operations

DESCRIPTION

- Serve as the front-line in the SOC by actively monitoring the networks/ systems for suspicious activity and threats, carry out proactive threat detection exercises using information collected from a variety of sources and make the initial decision on the event/ threat severity.

JOB RESPONSIBILITIES

- Examine network topologies to understand data flows through the network.
- Analyze network traffic to provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
- Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events, perform cyber defense trend analysis and reporting, and perform event correlation to mitigate threats.
- Carry out triage to ensure that a genuine security incident is occurring.
- Notify Tier 2 SOC Analyst on suspected events for further analysis.
- Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.
- Document and escalate incidents (including event's history, status, and potential impact for

further action) that may cause ongoing and immediate impact.

- Provide daily summary reports of network events and activity relevant to cyber defense practices.
- Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
- Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
- Isolate and remove malware.
- Identify network mapping and operating system (OS) fingerprinting activities.
- Develop content for cyber defense tools used for continual monitoring and analysis of network activity to identify malicious activity.
- Assist in the construction of signatures which can be implemented on cyber defense tools in response to new or observed threats within the network environment or enclave.
- Analyze and report organizational security posture trends.
- Monitor external data sources (e.g., cyber defense vendor sites and Computer Emergency Response Teams) to maintain updated cyber defense threat condition and determine which security issues may have an impact
- on the enterprise.
- Assess and monitor cybersecurity related to system implementation and testing practices.
- Provides cybersecurity recommendations based on significant threats and vulnerabilities.
- Work with stakeholders to resolve security incidents and vulnerability compliance.
- Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.

KNOWLEDGE

- Security concepts such as cyber-attacks and techniques, threat vectors, risk and threat management, incident management etc.
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms, traffic analysis methods.
- Cyber threats and vulnerabilities and information dissemination sources (e.g., alerts and advisories)
- Cyber defense and vulnerability assessment tools and their capabilities.
- System and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- Incident response and handling methodologies.
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools, applications, methodologies and techniques for detecting host and network-based intrusions.
- Threat investigations, reporting and investigative tools.
- Cyber defense and information security policies, procedures, and regulations.
- Common attack vectors, the different classes of attacks (e.g., passive, active and insider attacks) and attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
- Windows/Unix ports and services.
- Packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).

- Penetration testing principles, tools, and techniques.

SKILLS

- Using SIEM and SOAR technologies.
- Sysadmin skills (Linux/Mac/Windows).
- Programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more).
- Developing and deploying signatures.
- Detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort).
- Using incident handling methodologies.
- Collecting data from a variety of cyber defense resources.
- Recognizing and categorizing types of vulnerabilities and associated attacks.
- Performing packet-level analysis.
- Using cyber defense Service Provider reporting structure and processes within one's own organization.
- Applying analytical and problem-solving skills.

ABILITY

- Perform Malware analysis.
- Conduct vulnerability scans and recognize vulnerabilities in security systems.
- Accurately and completely source all data used in intelligence, assessment and/or planning products.
- Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

- Interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
- Work in a flexible schedule within a 24x7x365 Security Operations Center (SOC) environment, as well as possibly be expected to work holidays.
- Prepare regular reports to document any security breaches/ incidents.

EXPERIENCE

- 0-3 years of experience in cyber security and security operations including incident response.

QUALIFICATION

- Bachelor's degree in an information technology, computer science, cyber security or equivalent work experience.
- CompTIA Security+
- CEH: Certified Ethical Hacker
- GCIH: GIAC Certified Incident Handler
- GCIA: GIAC Certified Intrusion Analyst

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.19.Security Operation Center (SOC) analyst – Tier 2

ROLE

- Security Operation Center (SOC) analyst – Tier 2

FUNCTION

- Cyber Security Operations

DESCRIPTION

- Monitors the security of the entity's network and evaluates incidents identified by Tier 1 analysts. Responsible for responding to incidents or urgent situations to mitigate immediate and potential threats by using mitigation, preparedness, and response and recovery approaches, as needed.

JOB RESPONSIBILITIES

- Mentor and lead Tier 1 analysts on the techniques of detection and analysis.
- Handle and validate incident escalations by Tier 1 analysts.
- Conduct recommended proactive response actions and predictive analysis of potential cybersecurity threats.
- Receive and analyze network alerts from various sources and determine possible causes of such alerts.
- Interact with internal and external parties to resolve the queries related to raised incidents.
- Use SOC tools for continual monitoring and analysis of system/ network activity to identify potential malicious activities.
- Monitor external data sources (threat intelligence sources, GovCERT, Healthcare CERT, etc.) to maintain updated threat condition and determine which security issues may have an impact on the entity's services and information.

- Coordinate and provide expert technical support to Tier 1 analysts to resolve cyber incidents.
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
- Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
- Perform cyber incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability.
- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on entity systems.
- Perform real-time cyber incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
- Conduct test of security controls in accordance with established Incident Response plans and procedures.
- Track and document cyber incidents from initial detection through final resolution.
- Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies, and update the knowledge base with Lessons Learned after every incident.
- Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
- Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber incidents within the entity.
- Serve as technical expert and liaison to law enforcement personnel and explain incident details

as required.

- Coordinate with intelligence analysts to correlate threat assessment data.
- Generate daily, weekly and monthly reports and maintain timely delivery.

KNOWLEDGE

- Security concepts such as cyber-attacks and techniques, threat vectors, risk and threat management, incident management etc.
- Cyber related threats and vulnerabilities types, information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms and traffic analysis methods.
- Risk management frameworks, approaches and processes (e.g., methods for assessing and mitigating risk).
- Business continuity, disaster recovery and continuity of operations plans.
- Incident response and handling concepts, programs, processes, methodologies, roles and responsibilities.
- Incident categories, incident responses, and timelines for responses.
- Intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- System and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- Cyber defense and information security policies, procedures, and regulations.
- Common attack vectors, the different classes of attacks (e.g., passive, active, insider, close-in,

distribution attacks) and attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).

- Cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
- Malware analysis concepts and methodologies.

SKILLS

- Using SIEM and SOAR technologies.
- Identifying, capturing, containing, and reporting malware.
- Preserving evidence integrity according to standard operating procedures or national standards.
- Designing and applying incident response plans, models and methodologies.
- Perform Malware analysis.
- Conduct vulnerability scans and recognize vulnerabilities in security systems.
- Sysadmin skills (Linux/Mac/Windows).
- Programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more).
- Detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort).
- Collecting data from a variety of cyber defense resources.
- Recognizing and categorizing types of vulnerabilities and associated attacks.
- Performing packet-level analysis.
- Using cyber defense Service Provider reporting structure and processes within one's own organization.
- Applying analytical and problem-solving skills.

- Mentoring and training skills.

ABILITY

- Apply risk management frameworks, approaches and processes when needed.
- Implement Incident response and handling programs, processes and methodologies when needed.
- Accurately and completely source all data used in intelligence, assessment and/or planning products.
- Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
- Establish, confirm, and publish channels of communication.
- Work in a flexible schedule within a 24x7x365 Security Operations Center (SOC) environment, as well as may be expected to work holidays.
- Prepare and create regular reports to document any security breaches/ incidents.
- Be resilience to stressful situation.

EXPERIENCE

- +3 years of experience in cyber security and security operations including security monitoring and incident handling and response.

QUALIFICATION

- Bachelor's degree in an information technology, cyber security or equivalent work experience.
- CompTIA Security+
- CEH: Certified Ethical Hacker
- GCIH: GIAC Certified Incident Handler

- GCIA: GIAC Certified Intrusion Analyst
- CPT: Certified Penetration Tester

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

5.20. Security Operation Center (SOC) analyst – Tier 3

ROLE

- Security Operation Center (SOC) analyst – Tier 3

FUNCTION

- Cyber Security Operations

DESCRIPTION

- Monitor the security of the entity's network by carrying out proactive threat identification exercises, reviewing vulnerability assessment data, exploring ways to identify potential threats that may have found their way inside the network, without detection, and recommends how to optimize security monitoring tools based on threat hunting discoveries.

JOB RESPONSIBILITIES

- Provide targeted threat information and analysis and be actively involved in incident response and threat hunting activities.
- Review vulnerability assessment reports.
- Uses advanced threat intelligence techniques to identify cyber threats which may have found their way into the network.
- Conducts periodic compromise assessment/ penetration testing and vulnerability assessments to gauge resilience, find vulnerable entry-points, and propose recommendations based on assessments results.
- Identify potential security intrusions and carry out threat hunting exercises across the network against any known points of entry or network weaknesses.
- Hunt, track, and analyze advanced persistent threats (APTs).
- Provide timely notice of imminent or hostile intentions or activities which may impact

organization objectives, resources, or capabilities.

- Recommends ways to optimize security monitoring tools through threat hunting findings.
- Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment.
- Conduct research, collect & analyze data and evaluate intelligence.
- Expand the usage of security monitoring tools to improve the security of the environment based on business use cases or changes in threat landscape, root causes from security incident response, or output from
- security analytics.
- Qualify potential security incidents for further investigation.
- Manage and executes multi-level responses and addresses reported or detected incidents.
- Coordinates and distributes directives, vulnerability, and threat advisories.
- Collaborate with SOC team members to enhance detection capabilities based on new threat intelligence and to develop new incident handling strategies.
- Disseminate threat intelligence and learnings to enhance security operation center detection capabilities on an ongoing basis
- Provide subject matter expertise to the development of cyber operations specific indicators.
- Identify situational or recurring issues that pose a threat to the network and propose remedies that could decrease threat points.
- Develop focused reporting and briefings for advanced cyber threats to various teams and leaders.
- Provide guidance to leadership on strategies and plans of action to eradicate threats.

- Provide actionable intelligence to detection operations that proactively monitor systems for potential threats.
- Mentor and teach Tier 1 and 2 SOC analysts.

KNOWLEDGE

- Cyber related threats and vulnerabilities types, information dissemination sources (e.g., alert and advisories).
- Networking concepts and protocols, and network security attacks, vulnerabilities, processes, methodologies, access control mechanisms and traffic analysis methods.
- Risk management frameworks, approaches and processes (e.g., methods for assessing and mitigating risk).
- Incident response and handling concepts, programs, processes, methodologies, roles and responsibilities.
- Knowledge of what constitutes a “threat” to a network.
- Common attack vectors, the different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks) and attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
- Cyber intelligence/information collection capabilities and repositories.
- Host-based security products and how those products affect exploitation and reduce vulnerability.
- Tactics to anticipate and/or emulate threat capabilities and actions.
- Unix/Linux and SIEM/ SOAR tools.

SKILLS

- Using SIEM and SOAR technologies.
- Performing advanced event and incident analysis.
- Identifying cyber threats which may threaten organization's networks, systems and services.
- Providing understanding of threats through the identification and link analysis of functional or behavioral relationships.
- Writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
- Evaluating information for reliability, validity, and relevance.
- Identifying alternative analytical interpretations to minimize unanticipated outcomes.
- Using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).
- Preparing and presenting briefings.
- Utilizing feedback to improve processes, products, and services.
- Providing oversight and guidance to junior analysts and fulfill SOC manager responsibilities in the absence of the SOC Manager.
- Communicating complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.

ABILITY

- Remain current on cyber security trends and intelligence (open source and commercial) to guide the security analysis & identification capabilities of the SOC team.
- Provide timely advice and guidance on the response action plans for events and incidents based

on incident type and severity.

- Ensure that all identified events are promptly validated and thoroughly investigated.
- Document and report changes, trends and implications concerning the design and integration of evolving systems and solutions.
- Follow detailed operational processes and procedures to analyze, escalate, and support the remediation of critical information security incidents.
- Evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
- Function effectively in a dynamic, fast-paced environment and in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization to leverage analytical and technical expertise.
- Apply critical thinking.

EXPERIENCE

- +4 years of experience in cyber security and security operations including security monitoring and incident handling and response.

QUALIFICATION

- Bachelor's degree in an information technology, computer science, cyber security or equivalent work experience.
- GCIH: GIAC Certified Incident Handler
- OSCP: Offensive Security Certified Professional
- GCTI: GIAC Cyber Threat Intelligence certification
- GCIA: GIAC Certified Intrusion Analyst

- CPT: Certified Penetration Tester
- CEH: Certified Ethical Hacker
- GCFE: GIAC Certified Forensic Examiner

APPLICABILITY BASED ON ENTITY SIZE

☒ Basic

☒ Transitional

☑ Advanced

6. Capability Maturity Model

The capability maturity model sets the necessary expectations and levels reflective of the size, organization structure, information security capabilities and complexity of healthcare entities and supports to assess the maturity level based on the existing roles and competencies. The model helps to improve the security resources and overall information and cyber security capabilities of the entity.

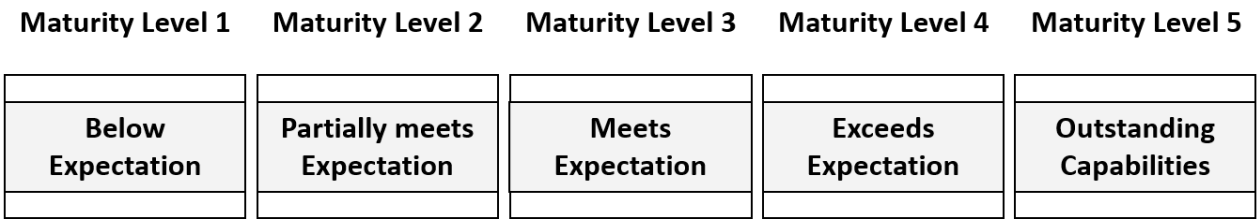

Figure 5: Capability maturity levels

Maturity Level	Description	Role requirements
Maturity Level 1: Below Expectation	Information security capabilities does not exist. The entity has no idea about the attacks and that their actions can have direct impact on the security of the organization. The entity does not have information security policy and is highly probable to fall victim to attacks.	No roles
Maturity Level 2: Partially meets Expectation	Information security capabilities exists only to meet specific compliance or audit requirements. The entity staff are unaware of the policies and/or role in protecting their entities information.	Operational staff with minimal Information Security competence

Maturity Level 3: Meets Expectation	Information security capabilities are comprehensive. The entity staff understand, follow the entity's policies and can actively recognize, prevent and report incidents.	Basic Information Security Roles
Maturity Level 4: Exceeds Expectation	Entity-wide information security capabilities including the processes, resources are deployed, managed regularly and possess leadership support. As a result, Information security is an established part of the entity's culture and is changing staff beliefs, attitudes and perceptions of security.	Transitional Information Security Roles
Maturity Level 5: Outstanding Capability	Information security capabilities are mature, effective and measurable. As a result, information security is continuously improving.	Advanced Information Security Roles

Table 2: Capability maturity levels and description

7. Maturity Level Identification Criteria

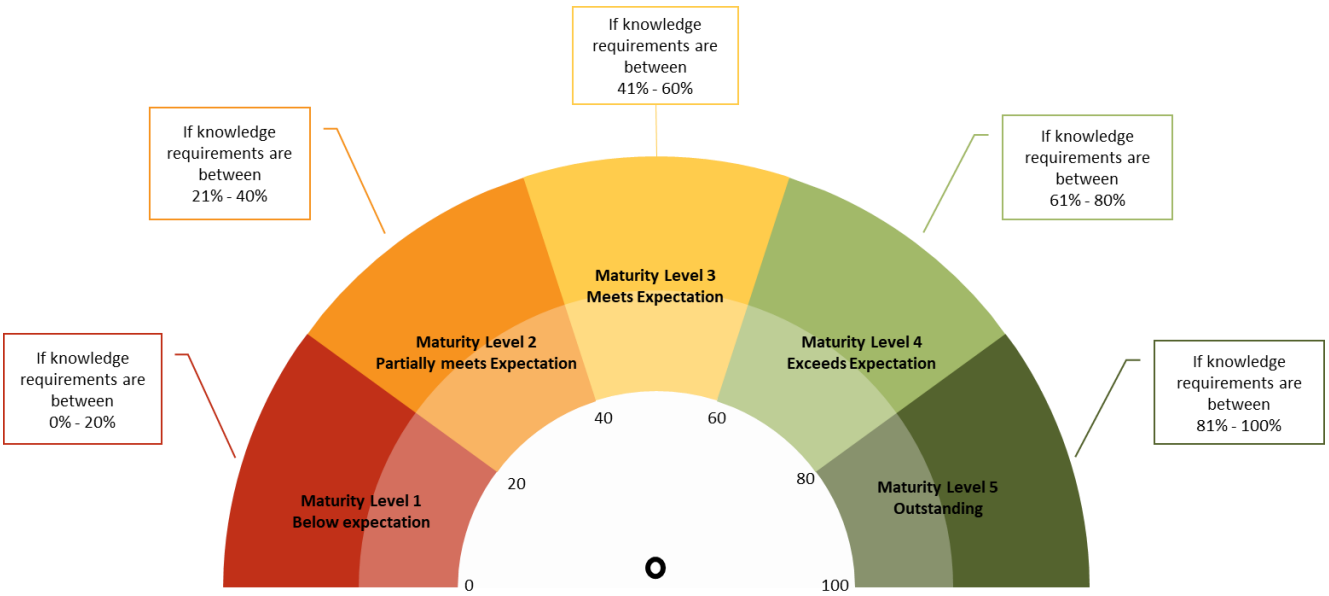

Figure 6: Maturity Level Identification Criteria

To identify the percentage of maturity level per role or for a combined role, the knowledge capabilities shall be assessed for each requirement. The number of requirements that are met against the total number of requirements shall be calculated for percentage to obtain the maturity score.

Example:

Role X has 10 knowledge requirements and Staff Y meets 5 knowledge requirements which calculates to 50% i.e., the maturity score of Staff Y and falls under Maturity level 3: Meets expectation.

8. Maturity Levels and Roles Mapping

This guideline only highlights the necessary capabilities for each role. The roles can be handled by a dedicated staff member or handled as part of shared responsibility model of the entity. However, during shared responsibility necessary knowledge, accountability and segregation of duties must be ensured.

APPLICABILITY	APPLICABLE ROLES
Basic	• Information Security Officer/Information and Cyber Security Governance, Risk and Compliance Officer
Transitional	• Chief Information Security Officer • Information Security Officer/Information and Cyber Security Governance, Risk and Compliance Officer • Information and Cyber Security Awareness Officer • Information and Cyber Security Auditor • Information and Cyber Technology/Medical Device Security Manager • System Security Engineer • Network Security Engineer • Software/Application Security Engineer • Information Security Architect • Information Security Analyst • Security Operations Manager
Advanced	• Chief Information Security Officer Information Security Officer/Information and Cyber Security Governance, Risk and

	Compliance Officer • Information and Cyber Security Project Manager • Information and Cyber Security Awareness Officer • Information and Cyber Security Auditor • Data Privacy Protection Officer • Information and Cyber Security Legal Advisor • Information and Cyber Technology/Medical Device Security Manager • System Security Engineer • Network Security Engineer • Software/Application Security Engineer • Information Security Architect • Cloud Security Specialist • IoMT Security Specialist • AI Security Specialist • Information Security Analyst • Security Operations Manager • Security Operation Center (SOC) analyst – Tier 1 • Security Operation Center (SOC) analyst – Tier 2 • Security Operation Center (SOC) analyst – Tier 3

Table 3 - Maturity levels and roles mapping

9. Recommendations

- Information security job roles and descriptions to be documented.
- Competency requirement for each role to be identified.
- The information security of the organization should be governed and necessary compliance requirements should be adhered.
- Necessary resources or competence should be available to manage and maintain the information security aspects in an organization.
- Information security should report to the top management of the entity.
- Information security should be an independent function and must be given the same level of importance as other independent departments in the organization.
- The CISO should have the authority to decide on the information security aspects of the organization.
- Segregation of duties should be ensured.

10. References

- NICE framework https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf Accessed July 2022
- DoH cybersecurity strategy https://www.doh.gov.ae/en/programs-initiatives/Aamen Accessed July 2022
- Abu Dhabi healthcare information and cyber security (ADHICS) standard https://www.doh.gov.ae/en/programs-initiatives/Aamen Accessed July 2022
- Guidelines for the implementation of the Abu Dhabi Healthcare Information and Cyber Security Standard https://www.doh.gov.ae/en/resources/guidelines Accessed July 2022
- DoH standard on patient healthcare data privacy https://www.doh.gov.ae/en/programs-initiatives/Aamen Accessed July 2022
- IoMT security standard for healthcare https://www.doh.gov.ae/en/programs-initiatives/Aamen Accessed July 2022
- AD cybersecurity work roles guideline https://www.adda.gov.ae/ Accessed July 2022
- ADDA cyber strategy guidelines https://www.adda.gov.ae/ Accessed July 2022
- UAE information assurance regulation https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation Accessed July 2022

11. Abbreviations

ACRONYM	ABBREVIATION
ADDA	Abu Dhabi Digital Authority
ADHICS	Abu Dhabi Healthcare Information and Cyber Security
AI	Artificial Intelligence
APT	Advanced Persistent Threats
BC	Business Continuity
CASE	Certified Application Security Engineer
C-CISO	Certified Chief Information Security Officer
CCNP	Certified Network Professional Security
CCSP	Certified Cloud Security Professional
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CGEIT	Certified Governance of Enterprise IT
CIS	Center for Internet Security
CISA	Certified Information Security Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSIP-ISSAP	Information Systems Security Architecture Professional
CISSP	Certified Information Systems Security Professional
CMMI	Capability Maturity Model Integration
CNDA	Certified Network Defence Architect
CPT	Certified Penetration Tester
CRISC	Certified Risk and Information Systems Control
CRMA	Certification in Risk Management Assurance
CSA	Cloud Security Alliance

CSAP	Certified Security Awareness Practitioner
CSSA	IACRB Certified SCADA Security Architect
CSSLP	Certified Secure Software Lifecycle Professional
CySA	Cyber Security Analyst Certification
DAM	Database Activity Monitoring
DNS	Domain Name System
DoH	Department of Health
DR	Disaster Recovery
ECSA	EC-Council Certified Security Analyst
ECSP	EC-Council Certified Secure Programmer
FEA	Federal Enterprise Architecture
GCFA	GIAC Certified Forensic Analyst
GCFE	GIAC Certified Forensic Examiner
GCIA	GIAC Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler
GCMP	GIAC Certified Project Manager
GCTI	GIAC Cyber Threat Intelligence certification
GDSA	GIAC Defensible Security Architecture
GIAC	Global Information Assurance Certification
GRCP	GRC Professional
GSLC	GIAC Security Leadership
GSLC	GIAC Security Leadership
GSM	Global System for Mobile Communications
GSSP-JAVA	GIAC Secure Software Programmer-Java
GSSP-NET	GIAC Secure Software Programmer- .NET
HR	Human Resource
IAM	Identity and Access Management
IoMT	Internet of Medical Things

IP	Internet Protocol
IR	Infrared
IRT	Incident Response Teams
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSAP	Information Systems Security Architecture Professional
ISSEP	Information Systems Security Engineering Professional
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
LAN	Local Area Network
LPT	Licensed Penetration Tester
MDM	Mobile Data Management
ML	Machine Learning
NCSC	National Computer Security Center
NIDS	Network Intrusion Detection Systems
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
OLA	Operating Level Agreements
OS	Operating System
OSCP	Offensive Security Certified Professional
OSI	Open System Interconnection Model
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
PCS	Professional Cloud Security Manager
PHI	Personal Health Information
PHP	Hypertext Pre-processor

PII	Personally Identifiable Information
PKI	Public-Key Infrastructure
PL	Procedural Language
PMP	Project Management Professional
REST	Representational State Transfer
RFID	Radio Frequency Identification
RMF	Risk Management Framework
RMP	Risk Management Professional
S/MIME	Secure/Multipurpose Internet Mail Extension
SANS	Sysadmin, Audit, Network and Security
SIEM	Security Information and Event Management
SLA	Service Level Agreements
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operation Center
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UAE	United Arab Emirates
VPN	Virtual Private Network
WAN	Wide Area Network
Wi- Fi	Wireless Fidelity
WLAN	Wireless Local Area Networking

Table 4: Acronyms and Abbreviations