This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Cybersecurity Roles and Responsibilities Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire .document To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization's full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
Once a year	Click here to add date	Click here to add date

Table of Contents

Introduction

This document has been developed to define, support and enhance the roles and responsibilities for meeting cybersecurity requirements in <organization name>. All parties involved in the implementation of cybersecurity programs and requirements must understand and perform their cybersecurity roles and responsibilities in<organization name>.

Purpose

This document aims to define the cybersecurity roles and responsibilities in <organization name>in order to achieve the document 's main purpose, which is to ensure that all parties involved in the implementation of cybersecurity controls in the organization are aware of their responsibilities in applying cybersecurity programs and requirements in <organization name> and its affiliates. These roles and responsibilities have been aligned with the Saudi Cybersecurity Workforce Framework issued by NCA (SCyWF – 1:2020).

Document Scope

This document applies to all personnel (employees and contractors) in <organization name>.

ECC sub-domains segregation of responsibilities table (ECC-1:2018)

<cybersecurity function> shall be responsible for **governance, risk, and compliance** aspects of all sub-domains. As for the implementation, it differs from one sub-domain to another, whereas the relevant responsibility is explained in the table below :

ECC Sub-domain number	Cybersecurity sub-domain	Department responsible for the implementation
5-1	Cybersecurity Risk Management	<Cybersecurity function> (Governance, Risk and Compliance Section)
6-1	Cybersecurity in Information	<Cybersecurity function> (Governance, Risk and Compliance Section)

	Technology Projects	
8-1	Cybersecurity Periodical Assessment and Audit	<Cybersecurity function> (Governance, Risk and Compliance Section)
9-1	Cybersecurity in Human Resources	<HR function>
10-1	Cybersecurity Awareness and Training Program	<Cybersecurity function> and<HR function>
1-2	Asset Management	<Information technology function> and <security, safety and facilities management function>
2-2	Identity and Access Management	<Information technology function> and <security, safety and facilities management function>
3-2	Information System and Processing Facilities Protection	<Information technology function>
4-2	Mail Protection	<Information technology function>
5-2	Networks Security Management	<Information technology function>
6-2	Mobile Devices Security	<Information technology function>
7-2	Data and Information Protection	<Information technology function> and <DMO>
8-2	Cryptography	<Information technology function>
9-2	Backup and Recovery Management	<Information technology function>
10-2	Vulnerabilities Management	<Cybersecurity function> Cybersecurity) Operations Section) and<Information technology function>
11-2	Penetration Testing	<Cybersecurity function> Cybersecurity) (Operations Section
12-2	Cybersecurity Event Logs and	<Cybersecurity function> Cybersecurity) (Operations Section

	Monitoring Management	
13-2	Cybersecurity Incident and Threat Management	<Cybersecurity function> Cybersecurity) (Operations Section
14-2	Physical Security	<Security, safety and facilities management function>
15-2	Web Application Security	<Information technology function> and <cybersecurity function>
1-3	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	<Cybersecurity function> and<business continuity function>
1-4	Third-party Cybersecurity	<Cybersecurity function> and <procurement and third party function>
2-4	Cloud Computing and Hosting Cybersecurity	<Information technology function> , <cybersecurity function> and <procurement and third party function>
1-5	Industrial Control Systems (ICS) Protection	<Cybersecurity function> and<ICS function>

Cybersecurity Roles and Responsibilities

<Authorizing official>

#	Responsibilities
1	Establish the <cybersecurity function> and ensure its independence to avoid conflict of interests, and appoint a Saudi national to be<head of cybersecurity function>.
2	Establish the Cybersecurity Steering Committee (CSC).
3	Approve CSC Charter.

4	Allocate sufficient budget for cybersecurity requirements ,including human resources budget.
5	Approve the cybersecurity strategy after being submitted to CSC.
6	Approve cybersecurity policies and procedures by the Authorizing Official after being submitted to CSC.
7	Approve the cybersecurity governance document, organizational structure, and roles and responsibilities after being submitted to CSC in <organization name> by the Authorizing Official.
8	Approve the cyber risk management document after being submitted to CSC.
9	Review cybersecurity status reports periodically and provide required support.

CSC members

#	Responsibilities
1	Follow security requirements as per CSC charter in organization> <name.
2	Establish accountability, responsibility, and authority by setting the roles and responsibilities for the protection of the <organization name>'s information and technology assets.
3	Ensure the presence of an approved document for cybersecurity risks management and assessment and the risk appetite in organization> <name, and reviewing it periodically or upon the occurrence of any material change in risk appetite.
4	Approve, support and monitor cybersecurity risk management procedures.
5	Approve, support and monitor cybersecurity document.

#	Responsibilities
6	Review Cybersecurity Strategy before approval by the Authorizing Official to ensure it is aligned with <organization name> strategic objectives.
7	Approve, support and monitor Cybersecurity Strategy implementation action plan.
8	Support and monitor cybersecurity policies' implementation.
9	Approve, support and monitor cybersecurity programs and initiatives (such as: cybersecurity awareness program, data and information protection, etc.)
10	Approve the key performance indicators (KPIs), monitor their impact on <cybersecurity function>'sbusiness and improve performance level.
11	Follow up and support Cybersecurity Incident Management.
12	Review the periodic reports of<cybersecurity function> that include cybersecurity projects, the overall cybersecurity status, the internal cybersecurity risks that may affect <organization name>'s business as well as the external cybersecurity risks that may directly or indirectly affect <organization name>'s business and provide the necessary support to address those risks.
13	Review and follow up on cybersecurity risks reports, and provide support to address or mitigate the risks.
14	Review security reports of Cybersecurity Incidents and provide relevant recommendations.
15	Review Cybersecurity exception requests and provide relevant recommendations.
16	Review security patches reports, assess and fix security vulnerabilities of all information and technology assets.

#	Responsibilities
17	Review the results of cybersecurity internal and external audit, and ensure setting a plan to fix, follow up and support remediation.
18	Submit periodic reports on cybersecurity status and provide the Authorizing Official with the required support.
19	Review compliance with internal requirements of the organization and the legislative requirements issued by NCA.

<Head of cybersecurity function>

#	Responsibilities
1	Effectively communicate cybersecurity aspects to senior management, and ensure that requirements are aligned with the IT cybersecurity organization's cybersecurity strategy.
2	Collaborate with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements.
3	Effectively manage vulnerability remediation.
4	Supervise and effectively assign work to staff working on cybersecurity relatedtasks.
5	Allocate required resources to cybersecurity roles.
6	Promote awareness of cyber policy and strategy as appropriate among the organization's management.
7	Work with stakeholders to develop cybersecurity policies and associated documentation in alignment with the organization's strategy cybersecurity.
8	Develop / establish the cybersecurity strategy.

#	Responsibilities
9	Align the organization's with its business cybersecurity strategy strategy.
10	Carry out a cybersecurity risk assessment.
11	Support the implementation of policies, processes and procedures relating to cybersecurity and privacy.
12	Ensure that appropriate controls are in place to effectively mitigate cybersecurity risks and address privacy concerns during the risk assessment process.
13	Provide support to implement and maintain the cybersecurity risk management program.
14	Ensure sound principles ,the organization's mission are reflected in vision and goals.
15	Obtain resources to develop and implement effective processes to meet strategic security and information goals.
16	Understand and communicate an organization's cybersecurity status during legal and regulatory scrutiny.
17	Promote and demonstrate to stakeholders the value of cybersecurity within an organization.
18	Communicate effectively with third parties in the event of a cybersecurity incident.
19	Review the effectiveness of the organization's cybersecurity controls against.its strategic goals
20	Manage the regular review and maintenance of the organization's cybersecurity policy and associated documentation.
21	Ensure that appropriate actions are taken to mitigate the risk in the event of a.cybersecurity incident

#	Responsibilities
22	Advocate cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity.
23	Ensure that organizational cybersecurity strategy is effectively addressed by cybersecurity policies and related document.
24	Ensure cybersecurity requirements of all information technology systems are determined.
25	Develop and maintain cybersecurity policies and related appropriate documentation to ensure the organization's critical infrastructure is .appropriately protected
26	Collaborate with stakeholders in the organization and with third parties when identifying future cybersecurity strategy requirements.
27	Identify and recruit appropriately skilled resources to address cybersecurity activities within the organization.
28	Attend and present at international cybersecurity events.
29	Possess appropriate resources to implement and maintain cybersecurity aspects of an effective business continuity plan.
30	Develop and maintain that aligns to the a cybersecurity strategy .organization's business strategy
31	Ensure that cybersecurity requirements for IT are aligned with the .cybersecurity strategy organization's
32	Manage financial aspects of cybersecurity, including budgeting and resourcing.
33	Ensure the effective communication of cybersecurity threats and mitigations to interested third parties.

Roles and Responsibilities of <Cybersecurity Function>

Cybersecurity Architect

#	Responsibilities
1	Perform cybersecurity reviews and identify gaps in security architecture, to develop cybersecurity risk management plans.
2	Provide input to the risk management framework and related documentation.
3	Employ secure configuration management processes.
4	Identify and prioritize critical business functions in collaboration with organizational stakeholders.
5	Provide advice on project costs, design concepts, or design changes.
6	Advise on security requirements to be included in procurement documents.
7	Analyze candidate architectures, allocate security services and select security mechanisms.
8	Define systems security context, concept of operations and baseline requirements in line with applicable.cybersecurity policies
9	Write detailed functional specifications that document the architecture development process.
10	Analyze user needs and requirements to plan architecture.
11	Develop enterprise architecture or system components required to meet user needs.
12	Document and update as necessary all definition and architecture activities.

#	Responsibilities
13	Determine security controls for information systems and networks and document appropriately.
14	Assess and design cybersecurity management functions.
15	Define appropriate availability levels for critical system functions and disaster recovery and continuity of operations requirements to deliver them.
16	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
17	Develop and integrate for systems and networks cybersecurity designs .with multi-level security requirements
18	Document and address organization's security architecture, and systems security engineering requirements throughout the acquisition life cycle.
19	Ensure that acquired or developed systems and architectures are consistent with organization's cybersecurity architecture guidelines.
20	Translate proposed capabilities into technical requirements.
21	Work with agile team members to conduct fast prototyping, feasibility studies and evaluation of new technologies.
22	Design systems and solutions to support successful proofs-of-concept and pilot projects in emerging technology areas.
23	Read and interpret technical diagrams, specifications, drawings, blueprints and schematics relating to systems and networks.
24	Determine and document security controls for systems and networks.

#	Responsibilities
25	Define and document the effect of implementation of a new system or new interfaces between systems on the security posture of the existing environment.
26	Recommend cost-effective security controls to mitigate risks identified through testing and review.

Secure Cloud Specialist

#	Responsibilities
1	Develop security architecture elements to mitigate threats as they emerge.
2	Deliver secure cloud solutions to development teams, ensure security of cloud migrations and cloud application development.
3	Work within and across multi-disciplinary teams as a domain expert in cloud security architecture standards and methodologies.
4	Evaluate and determine the adequacy of security architectures and designs.
5	Develop and implement secure cloud strategy in conjunction with enterprise architecture.
6	Develop and enforce secure designs for technology teams to consume cloud services.
7	Build solutions to identify existing organizational data within cloud environments.
8	Provide subject matter expertise to develop and architect the next generation of organizational cybersecurity.

#	Responsibilities
9	Build the security controls in place to properly monitor and protect information held in cloud environments.
10	Serves as a subject matter expert for security cloud architecture, including networking, storage, databases, provisioning and management.

Secure Software Assessor

#	Responsibilities
1	Perform risk analysis whenever an application or system undergoes a major change.
2	Analyze exercise results and system environment to plan and recommend modifications and adjustments.
3	Supervise and effectively assign work to staff working on cybersecurity .related tasks
4	Apply coding and testing security standards.
5	Apply secure code documentation.
6	Integrate cybersecurity into the requirements process by defining and capturing security controls.
7	Develop threat model based on customer interviews and requirements.
8	Evaluate interface between hardware and software, in consultation with engineering staff.
9	Inform hardware configuration through evaluation of cost constraints and security restrictions.

#	Responsibilities
10	Apply methodologies to correct common coding errors with security implications to ensure development of secure software.
11	Ensure that cybersecurity is built into software development, maintenance and decommissioning processes.
12	Perform integrated quality assurance testing of security systems' functionality and resilience.
13	Address security implications in the software acceptance phase.
14	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
15	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling and defining any specific security criteria.
16	Ensure penetration testing is carried out when required for new or updated applications.
17	Consult with customers about cybersecurity systems design and maintenance.
18	Direct cybersecurity software programming and development of documentation.
19	Analyze and provide information to stakeholders to support the development or modification of security applications.
20	Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.
21	Conduct trial runs of programs and software applications to ensure that the desired information is produced, and instructions and security levels are correct.

#	Responsibilities
22	Develop secure software testing and validation procedures.
23	Develop system testing and validation procedures, programming and documentation.
24	Perform secure program testing, review and assessment to identify potential flaws in codes and mitigate vulnerabilities.
25	Determine and document software patches or the extent of releases that would leave software vulnerable.
26	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.

Cybersecurity Researcher

#	Responsibilities
1	Research current technology to understand cyber defense capability required by systems or networks.
2	Identify and develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
3	Develop secure data management capabilities to support a mobile workforce.
4	Review and validate data mining and data warehousing programs, processes and requirements.
5	Identify cybersecurity capability strategies for custom hardware and software development based on organization's requirements.

#	Responsibilities
6	Collaborate with stakeholders to identify appropriate cybersecurity solutions technology.
7	Design and develop new cybersecurity tools and technologies.
8	Evaluate network infrastructure vulnerabilities.
9	Follow software and systems engineering life cycle standards and processes when developing cybersecurity systems and solutions.
10	Troubleshoot prototype design and process issues throughout the product design, development and pre-launch phases.
11	Find opportunities to develop new capability to address vulnerabilities.
12	Research and evaluate available technologies and standards to meet customer requirements.
13	Review, approve, prioritize and submit operational requirements for research, development and acquisition of cyber capabilities.

Cybersecurity Data Science Specialist

#	Responsibilities
1	Collect metrics and trending data.
2	Present technical information to technical and non-technical audiences.
3	Present data in creative formats.
4	Analyze and define data requirements and specifications.

#	Responsibilities
5	Analyze and plan for anticipated changes in data capacity requirements.
6	Develop data standards, policies and procedures.
7	Manage the compilation, cataloging, caching, distribution and retrieval of data.
8	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.
9	Provide recommendations on new database technologies and architectures.
10	Analyze data sources to provide actionable recommendations.
11	Assess the validity of source data and subsequent findings.
12	Conduct hypothesis testing using statistical processes.
13	Confer with systems analysts, engineers, programmers and others to design cybersecurity applications.
14	Develop and facilitate data-gathering methods.
15	Develop strategic insights from large data sets.
16	Program custom algorithms.
17	Provide stakeholders with actionable recommendations derived from data analysis and findings.
18	Utilize technical documentation or resources to implement new mathematical, data science, or computer science methodologies.
19	Effectively allocate storage capacity in the design of data management systems.

#	Responsibilities
20	Read, interpret, write, modify and execute simple scripts to perform tasks.
21	Utilize different programming languages to write code, open files, read files and write output to different files.
22	Utilize open source languages.
23	Develop and implement data mining and data warehousing programs.
24	Use quantitative techniques.

Cybersecurity Manager

#	Responsibilities
1	Effectively communicate cybersecurity risks and posture to senior management.
2	Effectively communicate financial aspects of cybersecurity related activities to senior management.
3	Collaborate with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements.
4	Ensure that protection and detection capabilities are aligned with the organization's cybersecurity strategy, policies and other related documentation.
5	Ensure that decisions relating to cybersecurity are based on sound risk management principles.
6	Recognize patterns of non-compliance with cybersecurity policies and related documentation to identify ways to improve the documentation.

#	Responsibilities
7	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
8	Effectively manage vulnerability remediation.
9	Ensure the organization's cybersecurity requirements are considered in mergers, acquisitions, outsourcing and other operations involving third parties.
10	Periodically review cybersecurity strategy, policies and related documents to maintain compliance with applicable legislation and regulation.
11	Maintain knowledge of cybersecurity threats to the organization.
12	Ensure sound principles ,the organization's mission are reflected in vision and goals.
13	Obtain resources to develop and implement effective processes to meet strategic security and information goals.
14	Ensure appropriate data is collected and maintained to meet defined cybersecurity reporting requirements.
15	Promote and demonstrate the value of cybersecurity to stakeholders within an organization.
16	Ensure that cybersecurity improvement actions are evaluated, implemented and reviewed as required.
17	Ensure that cybersecurity inspections, tests and reviews are coordinated for the network environment.
18	Ensure that cybersecurity requirements are included in all business continuity and disaster recovery planning operations.
19	Ensure that cybersecurity architecture design is aligned with the organization's cybersecurity strategy.

#	Responsibilities
20	Evaluate development of new systems and processes to ensure that appropriate security controls are implemented.
21	Identify alternative cybersecurity strategies to address organizational security objective.
22	Identify the implications of new technologies and upgrades on cybersecurity across the organization.
23	Communicate effectively with third parties in the event of a cybersecurity incident.
24	Review and, if appropriate, approve cybersecurity capabilities of proposed new technologies prior to organizational adoption.
25	Ensure that information relating to the organization's cybersecurity is appropriately managed, evaluated and shared.
26	Review the effectiveness of the organization's cybersecurity controls against its strategic goals.
27	Ensure that cybersecurity training and awareness programs are carried out on a regular basis.
28	Participate in cybersecurity risk assessment as required.
29	Participate in the development or modification of cybersecurity program plans and requirements.
30	Ensure that all documentation relating to network security is developed, issued and maintained.
31	Ensure that cybersecurity awareness training is provided to all members of staff.
32	Ensure that cybersecurity requirements are included as appropriate in any procurement action.

#	Responsibilities
33	Ensure that appropriate reporting is provided to senior management as necessary.
34	Identify potential security incidents and report as necessary.
35	Ensure that appropriate resources are allocated to meet the organization's cybersecurity requirements.
36	Manage the regular review and maintenance of the organization's cybersecurity policy and associated documentation.
37	Ensure that appropriate actions are taken to mitigate the risk in the event of a cybersecurity incident .
38	Use internationally available documentation relating to cybersecurity implementation to inform and enhance organizational documentation.
39	Advocate cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity.
40	Ensure that organizational cybersecurity strategy is effectively addressed by cybersecurity policies and related documents.
41	Review the effectiveness and efficiency of the procurement function in ensuring that cybersecurity requirements and supply chain risks are addressed as necessary and make improvements where necessary.
42	Ensure cybersecurity requirements of all information technology .systems are determined
43	Participate in the acquisition process as necessary and ensure that appropriate supply chain risk management practices are adopted.
44	Ensure that appropriate cybersecurity resources are always available.
45	Develop and maintain cybersecurity policies and related appropriate documentation to ensure the organization's critical infrastructure is .appropriately protected

#	Responsibilities
46	Ensure that cybersecurity assumptions are reviewed on a regular basis.
47	Possess appropriate resources to implement and maintain cybersecurity aspects of an effective business continuity plan.
48	Communicate relevant changes in the organization's cybersecurity posture to senior management.
49	Ensure that cybersecurity requirements for IT are aligned with the organization’s cybersecurity strategy.
50	Manage financial aspects of cybersecurity, including budgeting and resourcing.
51	Ensure the effective communication of cybersecurity threats and mitigations to interested third parties.
52	Regularly review and ensure that cybersecurity policies and related documentation are aligned with the organization's stated business objectives and strategy.
53	Provide support to compliance activities as necessary.

Cybersecurity Advisor

#	Responsibilities
1	Effectively communicate cybersecurity risks and posture to senior management.
2	Effectively communicate financial aspects of cybersecurity related activities to senior management.

#	Responsibilities
3	Work with stakeholders to develop cybersecurity policies and the organization's associated documentation in alignment with .strategy cybersecurity
4	Understand and communicate an organization's cybersecurity status during legal and regulatory scrutiny.
5	Promote and demonstrate the value of cybersecurity to stakeholders within an organization.
6	Communicate effectively with third parties in the event of a cybersecurity incident.
7	Review the effectiveness of the organization's cybersecurity controls against its strategic goals.
8	Manage the regular review and maintenance of the organization's cybersecurity policy and associated documentation.
9	Advocate cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity.
10	Ensure that organizational cybersecurity strategy is effectively .and related documents cybersecurity policies by addressed
11	Brief senior management on developments and trends in cybersecurity.
12	Brief senior management on cybersecurity controls required to protect the organization.
13	Evaluate cybersecurity aspects of supplier selection and proposition.
14	Report findings from international cybersecurity events to senior management.
15	Communicate relevant changes in the organization's cybersecurity posture to senior management.

#	Responsibilities
16	Develop and maintain that aligns to the a cybersecurity strategy .organization's business strategy
17	Serve as an internal consultant and advisor in own area of expertise.

Cybersecurity Risk Officer

#	Responsibilities
1	Effectively communicate cybersecurity risks and posture to senior management.
2	Develop security risk profiles of computer systems by assessing threats to, and vulnerabilities of, those systems.
3	Develop risk mitigation strategies to effectively manage risk in accordance with organizational risk appetite.
4	Develop specific cybersecurity countermeasures and risk mitigation strategies.
5	Develop statements of preliminary or residual cybersecurity risks for system operation.
6	Ensure that decisions relating to cybersecurity are based on sound risk management principles.
7	Perform risk analysis whenever an application or system undergoes a major change.
8	Provide input to the risk management framework and related documentation.
9	Ensure cybersecurity risks are identified and managed appropriately through the organization's risk governance process.

#	Responsibilities
10	Carry out a cybersecurity risk assessment.
11	Work with others to implement and maintain a cybersecurity risk management program.
12	Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.
13	Establish a risk management strategy for the organization that includes a determination of risk tolerance.
14	Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.
15	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.
16	Use continuous monitoring tools to assess risk on an ongoing basis.
17	Develop methods to effectively monitor and measure risk, compliance and assurance efforts.
18	Determine and document supply chain risks for critical system elements, where they exist.

Cybersecurity Compliance Officer

#	Responsibilities
1	Analyze organization's cybersecurity defense policies and configurations to evaluate compliance with regulations and organizational directives.
2	Evaluate cybersecurity aspects of contracts to ensure compliance with financial, contractual, legal and regulatory requirements.

#	Responsibilities
3	Ensure that any products implemented to manage cybersecurity risks have been effectively evaluated and authorized for use.
4	Recognize patterns of non-compliance with cybersecurity policies and related documentation to identify ways to improve the documentation.
5	Periodically review cybersecurity strategy, policies and related documents to maintain compliance with applicable legislation and regulation.
6	Work with stakeholders to resolve cybersecurity incidents and vulnerability compliance issues.
7	Develop methods to effectively monitor and measure risk, compliance and assurance efforts.
8	Develop specifications to ensure that risk, compliance and assurance efforts conform with cybersecurity requirements.
9	Maintain knowledge of applicable cybersecurity defense policies, regulations and compliance documents as they pertain to cybersecurity defense auditing.
10	Monitor and evaluate a system's compliance with cybersecurity, resilience and dependability requirements.
11	Provide an accurate technical evaluation of software applications, systems, or networks and document their compliance with agreed cybersecurity requirements.
12	Develop cybersecurity compliance processes and audits for services provided by third parties.
13	Provide support to compliance activities as necessary.
14	Maintain knowledge of applicable legislation, regulation and accreditation standards and regularly review these to ensure continued organizational compliance.

#	Responsibilities
15	Cooperate with relevant regulatory agencies and other legal entities in any compliance reviews or investigations.
16	Maintain awareness of applicable privacy laws, regulations and accreditation standards.

Cybersecurity Policy Officer

#	Responsibilities
1	Develop cybersecurity policies and related documentation.
2	Establish and maintain appropriate communication channels with stakeholders.
3	Review existing and proposed policies and related documentation with stakeholders.
4	Provide cybersecurity expertise on organizational and sectoral policy boards.
5	Ensure that appropriate funding for cybersecurity training resources is made available.
6	Ensure that cybersecurity workforce management policies and processes comply with legal and organizational requirements.
7	Promote awareness of cyber policy and strategy as appropriate among the organization's management.
8	Review and assess cybersecurity staff effectiveness to identify skills gaps and training requirements.
9	Interpret and apply applicable laws, statutes and regulatory documents to ensure they are reflected in the cybersecurity policies.

#	Responsibilities
10	Analyze an organization's cybersecurity policy.
11	Work with stakeholders to develop cybersecurity policies and the organization's associated documentation in alignment with .strategy cybersecurity
12	Align the organization's cybersecurity strategy with its business strategy.
13	Create and publish the organization's cybersecurity policy.
14	Monitor how effectively cybersecurity policies, principles and practices are implemented in the delivery of planning and management services.
15	Seek consensus on proposed cybersecurity policy changes from stakeholders.
16	Provide policy guidance to cybersecurity management, staff and users.
17	Review, conduct, or participate in audits of cyber programs and projects.
18	Support the Chief Information Officer (CIO) in the formulation of cybersecurity policies.

Security Controls Assessor

#	Responsibilities
1	Perform cybersecurity reviews and identify gaps in security architecture, to develop cybersecurity risk management plans.
2	Perform cybersecurity reviews and identify security gaps in security architecture to inform risk mitigation strategies.
3	Perform risk analysis whenever an application or system undergoes a major change.

#	Responsibilities
4	Provide input to the risk management framework and related documentation.
5	Review, update and maintain cybersecurity related documentation reflecting system design.
6	Ensure cybersecurity risks are identified and managed appropriately through the organization's risk governance process.
7	Effectively manage vulnerability remediation.
8	Ensure the organization's cybersecurity requirements are considered in mergers, acquisitions, outsourcing and other operations involving third parties.
9	Assess the effectiveness of cybersecurity controls.
10	Assess the configuration management process.
11	Manage and approve agreed accreditation packages.
12	Plan and conduct cybersecurity authorization reviews and assurance case development for initial installation of systems and networks.
13	Review risk registers or other similar documents to confirm that the level of risk is within acceptable limits for each software application, system and network.
14	Carry out an audit of application software/network/system security against documented cybersecurity policies and provide recommendations for remediation where gaps appear.
15	Develop cybersecurity compliance processes and audits for services provided by third parties.
16	Regularly review and ensure that cybersecurity policies and related documentation are aligned with the organization's stated business objectives and strategy.

#	Responsibilities
17	Define and document the effect of implementation of a new system or new interfaces between systems on the security posture of the existing environment.
18	Ensure that security design and cybersecurity development activities are appropriately documented.
19	Provide support to compliance activities as necessary.
20	Ensure that software application, network, or system configurations comply with the organization's cybersecurity policies.

Cybersecurity Legal Specialist

#	Responsibilities
1	Evaluate cybersecurity aspects of contracts to ensure compliance with financial, contractual, legal and regulatory requirements.
2	Perform system administration on specialized cybersecurity applications and systems.
3	Understand and communicate an organization's cybersecurity status during legal and regulatory scrutiny.
4	Evaluate the effectiveness of policies, standards, or procedures against the organization's strategy.
5	Interpret and apply laws, regulations, policies, standards, or procedures as necessary.
6	Resolve conflicts in policies, standards, or procedures where they contradict applicable laws or regulations.

#	Responsibilities
7	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures etc.
8	Provide cybersecurity expertise to the framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.
9	Develop guidelines for implementation of relevant cybersecurity controls.
10	Provide cybersecurity guidance to oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.
11	Evaluate the impact of changes in laws and regulations on an organization's cybersecurity policies and related documentation.
12	Provide cybersecurity related guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
13	Assist with the implementation of new or revised laws, regulations, executive orders etc. as they relate to cybersecurity policies and other documentation.
14	Provide cybersecurity related guidance in the preparation of legal and other relevant documents.
15	Maintain awareness of applicable privacy laws, regulations and accreditation standards.

Cybersecurity Defense Analyst

#	Responsibilities
1	Correlate incident data to identify vulnerabilities.
2	Use cybersecurity products and security control technologies to reduce identified risk to an acceptable level.
3	Document and escalate incidents that may cause immediate or ongoing impact.
4	Analyze and report cyber defense trends.
5	Correlate information from multiple sources to understand situation and determine the effectiveness of an observed attack.
6	Perform cybersecurity reviews and identify security gaps in security architecture to inform risk mitigation strategies.
7	Analyze exercise results and system environment to plan and recommend modifications and adjustments.
8	Analyze network alerts from multiple sources to determine possible causes.
9	Provide timely detection, identification and alerting of possible attacks, anomalous activities and misuse activities and distinguish them from benign activities.
10	Use cyber defense tools to monitor and analyze system activity continuously to identify malicious activity.
11	Analyze malicious activity to determine vulnerabilities exploited, exploitation methods and effects on system and information.
12	Determine Tactics, Techniques, and Procedures (TTP) for intrusion sets.

#	Responsibilities
13	Examine network topologies to understand data flows through the network.
14	Recommend vulnerability corrections for the environment.
15	Use metadata to identify and analyze anomalies in network traffic.
16	Identify indications and warnings through research, analysis and correlation across multiple data sets.
17	Use packet analysis tools to validate intrusion detection system alerts.
18	Isolate and remove malware.
19	Use network traffic to identify a network device's applications and operating systems.
20	Use network traffic to reconstruct malicious activity.
21	Identify network mapping and operating system fingerprinting activities.
22	Assist in the construction of signatures for implementation on cybersecurity network tools to respond to new or observed threats within the environment.
23	Report suspected cyber incidents in line with the organization's cyber incident response plan.
24	Analyze and report on trends in the organization's security posture.
25	Assess the adequacy of access controls against organizational policies.
26	Monitor external data sources to keep understanding of currency of cybersecurity threats up to date and determine which security issues may have an impact on the organization.
27	Assess and monitor the cybersecurity of the organization's system implementation and testing practices.

#	Responsibilities
28	Make cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
29	Work with stakeholders to resolve cybersecurity incidents and vulnerability compliance issues.
30	Develop cyber defense tools.
31	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
32	Coordinate with other cyber defense staff to validate network alerts.
33	Provide summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.

Cybersecurity Infrastructure Specialist

#	Responsibilities
1	Apply security policies to meet system security objectives.
2	Perform system administration on specialized cybersecurity applications and systems.
3	Identify, prioritize and coordinate the protection of critical cyber defense infrastructure and resources.
4	Apply cybersecurity functions (e.g., encryption, access control and identity management) to reduce exploitation opportunities.
5	Manage and administer the updating of rules and signatures for cyber defense applications.

#	Responsibilities
6	Build, install, configure, patch and test dedicated cyber defense hardware and software.
7	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.
8	Administer test beds and test and evaluate applications, hardware infrastructure, rules, signatures, access controls and configurations of platforms managed by service providers.
9	Create, edit and manage network access control lists on specialized cyber defense systems.
10	Identify and report potential conflicts with implementation of any cyber defense tools.
11	Implement risk management framework and security assessment and authorization requirements for dedicated cyber defense systems within the organization and document and maintain records for them.
12	Select the security controls for a system and document the functional description of the planned control implementations in a security plan.
13	Implement the security controls specified in a security plan or other system documentation.
14	Develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.

Cybersecurity Specialist

#	Responsibilities
1	Apply security policies to meet system security objectives.
2	Correlate incident data to identify vulnerabilities.
3	Analyze log files from multiple sources to identify possible threats to network security.
4	Analyze and report cyber defense trends.
5	Assess and monitor the cybersecurity of the organization's system implementation and testing practices.
6	Perform technical and nontechnical risk and vulnerability assessments of organizational technology environments.
7	Make recommendations to enable effective remediation of vulnerabilities.
8	Develop cyber defense tools.
9	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
10	Coordinate with other cyber defense staff to validate network alerts.
11	Provide summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.

Vulnerability Assessment Specialist

#	Responsibilities
1	Analyze organization's cybersecurity defense policies and configurations to evaluate compliance with regulations and organizational directives.
2	Correlate incident data to identify vulnerabilities.
3	Maintain a deployable cyber defense audit toolkit based on industry best practice to support cyber defense audits.
4	Prepare cybersecurity assessment and audit reports that identify technical and procedural findings, and include recommended remediation strategies and solutions.
5	Perform technical and nontechnical risk and vulnerability assessments of organizational technology environments.
6	Use continuous monitoring tools to assess risk on an ongoing basis.
7	Maintain knowledge of applicable cybersecurity defense policies, regulations and compliance documents as they pertain to cybersecurity defense auditing.
8	Conduct or support authorized penetration testing of infrastructure and assets.
9	Conduct required reviews, including reviews of defensive measures, according to the organization’s policies.
10	Recommend cost-effective security controls to mitigate risks identified through testing and review.
11	Carry out vulnerability scanning on systems and assets.
12	Use security testing and code scanning tools to conduct code reviews.

Penetration Tester/Red Team Specialist

#	Responsibilities
1	Conduct or support authorized penetration testing of infrastructure and assets.
2	Gather information about network topography and usage through technical analysis and open source research and document findings.
3	Mimic malicious social engineering techniques that an attacker would use to attempt a system breach to uncover security gaps and vulnerabilities.
4	Identify methods that attackers could use to exploit system and network vulnerabilities.
5	Include business considerations in security strategies and recommendations.
6	Carry out vulnerability scanning on systems and assets.
7	Report penetration testing and vulnerability assessment findings including risk level, proposed mitigation and details necessary to reproduce the test results.
8	Discuss security findings with management, leadership and IT teams.
9	Design and develop penetration testing team processes.
10	Conduct remote testing of a network to expose weaknesses in security.
11	Plan and create penetration methods, scripts and tests.
12	Design simulated attacks to reflect impact in the organization's business and its users.
13	Present test findings, risks and conclusions to technical and non-technical audiences.
14	Explain business impact of vulnerabilities identified through testing to make case for addressing them.

#	Responsibilities
15	Conduct physical security assessments of servers, systems and network devices.
16	Test for vulnerabilities in web applications, client applications and standard applications.
17	Identify foreign language terminology within computer programs (e.g., comments, variable names).

Cybersecurity Incident Responder

#	Responsibilities
1	Correlate incident data to identify vulnerabilities.
2	Analyze log files from multiple sources to identify possible threats to network security.
3	Triage incidents to identify specific vulnerability, determine scope, urgency and potential impact, make recommendations that enable expeditious remediation.
4	Analyze and report cyber defense trends.
5	Perform initial collection of images to relevant forensic standards; inspect to evaluate possible mitigation and remediation measures.
6	Perform incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis and system remediation.
7	Analyze network alerts from multiple sources to determine possible causes.

#	Responsibilities
8	Track and document cyber incidents from initial detection to final resolution.
9	Write and publish cyber defense techniques, guidance and post incident reports to appropriate constituencies.
10	Employ defense-in-depth principles and practices in line with organizational policies.
11	Collect intrusion artefacts and use discovered data to mitigate potential cybersecurity incidents within the organization.
12	Write and publish reviews to learn and promulgate lessons from cybersecurity events.
13	Monitor external data sources to keep understanding of currency of cybersecurity threats up to date and determine which security issues may have an impact on the organization.
14	Coordinate incident response functions.
15	Provide expert technical support to resolve cyber defense incidents.
16	Work as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required.
17	Coordinate with threat intelligence analysts to correlate threat assessment data.
18	Report cyber incidents to inform cyber defense.
19	Identify and select most effective sources of information to assist with incident investigation.

Digital Forensics Specialist

#	Responsibilities
1	Perform technical decryption of seized data.
2	Perform file signature analysis.
3	Perform real-time forensic analysis.
4	Perform timeline analysis.
5	Perform incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis and system remediation.
6	Capture and analyze network traffic associated with malicious activities using network monitoring tools.
7	Analyze log files, evidence and other information to determine best methods for identifying perpetrators of a network intrusion.
8	Confirm what is known about an intrusion and seek to discover new information.
9	Create a forensically sound duplicate of the evidence to use for data recovery and analysis processes, in line with national or organizational policies as applicable.
10	Provide technical summary of findings in accordance with established reporting procedures.
11	Ensure that chain of custody is followed for all acquired digital media in accordance with national law or organizational policies as applicable.
12	Identify digital evidence for examination and analysis.
13	Perform dynamic analysis to boot an “image” of a drive - with or without the original - to see the intrusion as the user may have seen it, in a native environment.

#	Responsibilities
14	Perform hash comparison against databases required by organizational policies.
15	Perform static media analysis.
16	Perform tier 1, 2 and 3 malware analysis.
17	Ensuring data integrity when preparing digital media for imaging.
18	Provide technical assistance in acquiring, securing, handling or analyzing digital evidence.
19	Recognize and report forensic artifacts in line with reporting policies.
20	Extract data from devices.
21	Use specialized equipment and techniques to perform forensic tasks in line with policy.
22	Conduct cursory binary analysis.
23	Work as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required.
24	Perform virus scanning on digital media.
25	Perform forensic analysis of file systems.
26	Perform static analysis to mount an "image" of a drive - with or without the original.
27	Perform static malware analysis.
28	Utilize deployable forensics toolkits to support operations.
29	Coordinate with threat intelligence analysts to correlate threat assessment data.
30	Process image with tools appropriate to the investigation's objectives.

#	Responsibilities
31	Perform Windows registry analysis.
32	Perform file and registry monitoring on the running system after identifying intrusion.
33	Enter information for acquired digital media into tracking database.
34	Report cyber incidents to inform cyber defense.
35	Build and maintain a deployable cybersecurity incident response toolkit.
36	Use results from analysis of intrusion artefacts to inform advice on the mitigation of potential cyber defense incidents.
37	Review forensic images, volatile data and other data sources to recover potentially relevant information.
38	Write and publish recommendations and reports on incident findings to appropriate constituencies.
39	Examine recovered data for information of relevance to the issue at hand.
40	Identify intrusion via dynamic analysis.
41	Perform tier 1 and 2 malware analysis.

Cyber Crime Investigator

#	Responsibilities
1	Build relationships between the incident response team and internal and external partners.
2	Identify data which will add value to investigations.
3	Interview victims of a possible cybercrime and witnesses.
4	Develop a plan to investigate alleged cybercrime, violation, or suspicious activity.
5	Fuse results from analysis of networks, infrastructure and digital evidence with results from other criminal investigations and operations.
6	Determine whether a cybersecurity incident may be a violation of law requiring specific legal action.
7	Identify digital evidence for examination and analysis.
8	Identify evidence that can prove that a cybercrime took place.
9	Identify, collect and seize documentary or physical evidence associated with cyber intrusion incidents, investigations and operations.
10	Process crime scenes.
11	Secure electronic devices and information sources required for analysis.
12	Use specialized equipment and techniques to perform forensic tasks in line with policy.
13	Assess and report on actions and behaviors relevant to the investigation of victims, witnesses, or suspects.
14	Determine the extent of threats and risks arising from them and recommend courses of action or countermeasures to mitigate them.
15	Provide criminal investigative support to legal authorities during the judicial process.

#	Responsibilities
16	Report cyber incidents to inform cyber defense.
17	Analyze material from cybersecurity incidents for evidence of hostile foreign actor or criminal activity.
18	Gather and preserve evidence that could be used to prosecute perpetrators of the cybercrime.
19	Identify and develop leads and sources of information to assist identification or prosecution of those responsible for a cybercrime.
20	Document original condition of digital and associated evidence in line with national or organizational policies.
21	Analyze IT systems and digital media to solve, investigate and prosecute cybercrimes.
22	Document the investigation in line with legal standards and requirements.
23	Identify and select most effective sources of information to assist with incident investigation.
24	Examine recovered data for information of relevance to the issue at hand.
25	Interview those suspected of having committed a cybercrime.

Malware Reverse Engineering Specialist

#	Responsibilities
1	Identify and develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
2	Review and analyze cybersecurity threats to provide stakeholders with information needed to respond to threats.
3	Perform tier 1, 2 and 3 malware analysis.
4	Review gathered information for validity and relevance to the investigation in line with organizational policies.
5	Sanitize reports to protect proprietary, commercial, personal or otherwise sensitive or confidential data or methods.
6	Document lessons learned from the outcome of events or exercises.
7	Identify potential malicious activity from memory dumps, logs and packet captures.
8	Conduct nodal analysis.
9	Identify threat tactics and methodologies.
10	Monitor and report on validated threat activities.
11	Perform tier 1 and 2 malware analysis.
12	Maintain a common intelligence picture.
13	Conduct in-depth research and analysis.
14	Develop information requirements necessary for answering priority information requests.
15	Generate requests for information.
16	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).

#	Responsibilities
17	Provide current intelligence support to critical internal/external stakeholders as appropriate.
18	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements and operations.
19	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
20	Identify cyber threat tactics and methodologies.
21	Identify foreign language terminology within computer programs (e.g., comments, variable names).

Threat Intelligence Analyst

#	Responsibilities
1	Track status of requests for information in line with the organization's policies.
2	Answer requests for information in line with the organization's policies.
3	Use knowledge of threat actors and activities to build common understanding of organization's current risk profile.
4	Use knowledge of threat actors and activities to inform organization's response to a cyber incident.
5	Coordinate, validate and manage the organization's cyber threat intelligence sources and feeds.

#	Responsibilities
6	Identify information gaps in threat intelligence and assess their implications for the organization.
7	Prepare and deliver briefs on specific threats to the organization.
8	Work collaboratively and share information with threat intelligence analysts working in related fields.
9	Conduct nodal analysis.
10	Evaluate threat decision-making processes.
11	Identify the principal threats to the organization's known vulnerabilities.
12	Identify threat tactics and methodologies.
13	Monitor and report changes in threat dispositions, activities, tactics, capabilities and objectives.
14	Monitor and report on validated threat activities.
15	Monitor open source websites for hostile content directed towards organizational or partner interests.
16	Monitor and report on threat actor activities to fulfil organization's threat intelligence and reporting requirements.
17	Use expertise on threat actors and activities to support activities to plan and develop the organization's cybersecurity strategy and resources.
18	Provide information and assessments of threat actors to assist stakeholders in planning and executing cybersecurity activities.
19	Provide real-time cyber threat intelligence analysis and support during cybersecurity incidents and exercises.
20	Monitor cyber threat intelligence feeds and report significant network events and intrusions.

#	Responsibilities
21	Maintain a common intelligence picture.
22	Conduct in-depth research and analysis.
23	Develop information requirements necessary for answering priority information requests.
24	Generate requests for information.
25	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
26	Provide current intelligence support to critical internal/external stakeholders as appropriate.
27	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements and operations.
28	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
29	Work closely with planners, intelligence analysts and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.
30	Identify cyber threat tactics and methodologies.

Threat Hunter

#	Responsibilities
1	Correlate incident data to identify vulnerabilities.
2	Establish and maintain appropriate communication channels with stakeholders.
3	Build relationships between the incident response team and internal and external partners.
4	Identify data which will add value to investigations.
5	Analyze log files from multiple sources to identify possible threats to network security.
6	Triage incidents to identify specific vulnerability, determine scope, urgency and potential impact, make recommendations that enable expeditious remediation.
7	Analyze and report cyber defense trends.
8	Perform file signature analysis.
9	Perform real-time forensic analysis.
10	Perform timeline analysis.
11	Perform incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis and system remediation.
12	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
13	Capture and analyze network traffic associated with malicious activities using network monitoring tools.
14	Provide timely detection, identification and alerting of possible attacks, anomalous activities and misuse activities and distinguish them from benign activities.

#	Responsibilities
15	Use cyber defense tools to monitor and analyze system activity continuously to identify malicious activity.
16	Analyze malicious activity to determine vulnerabilities exploited, exploitation methods and effects on system and information.
17	Identify, prioritize and coordinate the protection of critical cyber defense infrastructure and resources.
18	Ensure an audit log of evidence of security measures is maintained.
19	Use packet analysis tools to validate intrusion detection system alerts.
20	Collect metrics and trending data.
21	Identify and develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
22	Review, conduct, or participate in audits of cyber programs and projects.
23	Review and analyze cybersecurity threats to provide stakeholders with information needed to respond to threats.
24	Make recommendations to enable effective remediation of vulnerabilities.
25	Advocate cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity.
26	Identify digital evidence for examination and analysis.
27	Perform tier 1, 2 and 3 malware analysis.
28	Use specialized equipment and techniques to perform forensic tasks in line with policy.
29	Use reviews to recommend new or revised security, resilience and reliability measures.

#	Responsibilities
30	Analyze the results of software, hardware, or interoperability testing to identify cost-effective improvements that can reduce identified risks.
31	Prepare and deliver briefs on specific threats to the organization.
32	Conduct network scouting and analyze vulnerabilities of systems within a network.
33	Conduct nodal analysis.
34	Detect exploits against networks and hosts of interest to inform understanding of threat actor activity.
35	Determine what technologies are used by threat actors of interest.
36	Develop information sources to deepen understanding of threat actors of interest.
37	Apply analytic techniques to gain information about threats actors of interest.
38	Evaluate threat decision-making processes.
39	Identify the principal threats to the organization's known vulnerabilities.
40	Evaluate available capabilities to combat likely threat activities to recommend efficient solutions.
41	Identify threat tactics and methodologies.
42	Identify and evaluate threat critical capabilities, requirements and vulnerabilities.
43	Identify the threat actor's structure and components.
44	Provide input to or develop courses of action based on understanding of threat.

#	Responsibilities
45	Monitor and report changes in threat dispositions, activities, tactics, capabilities and objectives.
46	Monitor and report on validated threat activities.
47	Perform incident handling, event triage, network analysis, threat detection, trend analysis, metric development and vulnerability information dissemination.
48	Support threat and vulnerability analysis and cybersecurity advisory services and recommendations.
49	Perform tier 1 and 2 malware analysis.
50	Conduct in-depth research and analysis.
51	Identify cyber threat tactics and methodologies.

ICS/OT Cybersecurity Architect

#	Responsibilities
1	Perform cybersecurity reviews and identify gaps in security architecture, to develop cybersecurity risk management plans.
2	Provide input to the risk management framework and related documentation.
3	Employ secure configuration management processes.
4	Identify and prioritize critical business functions in collaboration with organizational stakeholders.
5	Provide advice on project costs, design concepts, or design changes.

#	Responsibilities
6	Advise on security requirements to be included in procurement documents.
7	Analyze candidate architectures, allocate security services and select security mechanisms.
8	Define systems security context, concept of operations and baseline requirements in line with applicable cybersecurity policies.
9	Write detailed functional specifications that document the architecture development process.
10	Analyze user needs and requirements to plan architecture.
11	Develop enterprise architecture or system components required to meet user needs.
12	Document and update as necessary all definition and architecture activities.
13	Determine security controls for information systems and networks and document appropriately.
14	Assess and design cybersecurity management functions.
15	Define appropriate availability levels for critical system functions and disaster recovery and continuity of operations requirements to deliver them.
16	Define and document the effect of implementation of a new system or new interfaces between systems on the security posture of the existing environment.
17	Recommend cost-effective security controls to mitigate risks identified through testing and review.

#	Responsibilities
18	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event in IT and ICS/OT environments.
19	Develop and integrate cybersecurity designs for systems and networks with multilevel security requirements in IT and ICS/OT environments.
20	Document and address organization's security, architecture and systems security engineering requirements throughout the acquisition life cycle in IT and ICS/OT environments.
21	Ensure that acquired or developed systems and architectures are consistent with organization's cybersecurity architecture guidelines in IT and ICS/OT environments.
22	Translate proposed capabilities into technical requirements in IT and ICS/OT environments.
23	Work with agile team members to conduct fast prototyping, feasibility studies and evaluation of new technologies in IT and ICS/OT environments.
24	Design systems and solutions to support successful proofs-of-concept and pilot projects in emerging technology areas in IT and ICS/OT environments.
25	Read and interpret technical diagrams, specifications, drawings, blueprints and schematics relating to systems and networks in IT and ICS/OT environments.
26	Understand and troubleshoot fault areas in industrial automation and communication systems.
27	Determine and document security controls for systems and networks in IT and ICS/OT environments.

ICS/OT Cybersecurity Defense Analyst

#	Responsibilities
1	Correlate incident data to identify vulnerabilities.
2	Use cybersecurity products and security control technologies to reduce identified risk to an acceptable level.
3	Document and escalate incidents that may cause immediate or ongoing impact.
4	Analyze and report cyber defense trends.
5	Correlate information from multiple sources to understand situation and determine the effectiveness of an observed attack.
6	Perform cybersecurity reviews and identify security gaps in security architecture to inform risk mitigation strategies.
7	Analyze exercise results and system environment to plan and recommend modifications and adjustments.
8	Analyze network alerts from multiple sources to determine possible causes.
9	Provide timely detection, identification and alerting of possible attacks, anomalous activities and misuse activities and distinguish them from benign activities.
10	Use cyber defense tools to monitor and analyze system activity continuously to identify malicious activity.
11	Analyze malicious activity to determine vulnerabilities exploited, exploitation methods and effects on system and information.
12	Employ defense-in-depth principles and practices in line with organizational policies.

#	Responsibilities
13	Determine Tactics, Techniques, and Procedures (TTP) for intrusion sets.
14	Examine network topologies to understand data flows through the network.
15	Recommend vulnerability corrections for the environment.
16	Use metadata to identify and analyze anomalies in network traffic.
17	Identify indications and warnings through research, analysis and correlation across multiple data sets.
18	Use packet analysis tools to validate intrusion detection system alerts.
19	Isolate and remove malware.
20	Use network traffic to identify a network device's applications and operating systems.
21	Use network traffic to reconstruct malicious activity.
22	Identify network mapping and operating system fingerprinting activities.
23	Assist in the construction of signatures for implementation on cybersecurity network tools to respond to new or observed threats within the environment.
24	Report suspected cyber incidents in line with the organization's cyber incident response plan.
25	Analyze and report on trends in the organization's security posture.
26	Analyze and report on trends in the system’s security posture.
27	Assess the adequacy of access controls against organizational policies.

#	Responsibilities
28	Monitor external data sources to keep understanding of currency of cybersecurity threats up to date and determine which security issues may have an impact on the organization.
29	Assess and monitor the cybersecurity of the organization's system implementation and testing practices.
30	Make cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
31	Work with stakeholders to resolve cybersecurity incidents and vulnerability compliance issues.
32	Develop cyber defense tools.
33	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
34	Coordinate with other cyber defense staff to validate network alerts.
35	Provide summary reports of network events and other cybersecurity-relevant activities in line with organizational policies and requirements.

ICS/OT Cybersecurity Risk Officer

#	Responsibilities
1	Effectively communicate cybersecurity risks and posture to senior management.
2	Develop security risk profiles of computer systems by assessing its threats and vulnerabilities.
3	Develop risk mitigation strategies to effectively manage risk in accordance with organizational risk appetite.

#	Responsibilities
4	Develop specific cybersecurity countermeasures and risk mitigation strategies.
5	Develop statements of preliminary or residual cybersecurity risks for system operation.
6	Ensure that decisions relating to cybersecurity are based on sound risk management principles.
7	Perform incident response tasks to support deployable incident response teams including forensic collection, intrusion correlation, tracking, threat analysis and system remediation.
8	Perform risk analysis whenever an application or system undergoes a major change.
9	Provide input to the risk management framework and related documentation.
10	Ensure cybersecurity risks are identified and managed appropriately through the organization's risk governance process.
11	Carry out a cybersecurity risk assessment.
12	Review, conduct, or participate in audits of cyber programs and projects.
13	Work with others to implement and maintain a cybersecurity risk management program.
14	Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.
15	Establish a risk management strategy for the organization that includes a determination of risk tolerance.
16	Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.

#	Responsibilities
17	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.
18	Use continuous monitoring tools to assess risk on an ongoing basis.
19	Make recommendations to enable effective remediation of vulnerabilities.
20	Develop methods to effectively monitor and measure risk, compliance and assurance efforts.
21	Coordinate and provide expert technical support to the organization's cybersecurity team to resolve ICS/OT cybersecurity incidents.
22	Perform risk analysis for ICS/OT environments whenever an application or a system undergoes a change.

ICS/OT Cybersecurity Incident Responder

#	Responsibilities
1	Correlate incident data to identify vulnerabilities.
2	Analyze log files from multiple sources to identify possible threats to network security.
3	Triage incidents to identify specific vulnerability, determine scope, urgency and potential impact, make recommendations that enable expeditious remediation.
4	Analyze and report cyber defense trends.
5	Perform initial collection of images to relevant forensic standards; inspect to evaluate possible mitigation and remediation measures.

#	Responsibilities
6	Analyze network alerts from multiple sources to determine possible causes.
7	Track and document cyber incidents from initial detection to final resolution.
8	Write and publish cyber defense techniques, guidance and post incident reports to appropriate constituencies.
9	Employ defense-in-depth principles and practices in line with organizational policies.
10	Collect intrusion artefacts and use discovered data to mitigate potential cybersecurity incidents within the organization.
11	Write and publish reviews to learn and promulgate lessons from cybersecurity events.
12	Monitor external data sources to keep understanding of currency of cybersecurity threats up to date and determine which security issues may have an impact on the organization.
13	Coordinate incident response functions.
14	Work as a technical expert in support of law enforcement, explaining incident details and forensic analysis as required.
15	Coordinate with threat intelligence analysts to correlate threat assessment data.
16	Coordinate and provide expert technical support to the organization's cybersecurity team to resolve ICS/OT cybersecurity incidents.
17	Perform real-time cybersecurity incident handling tasks in ICS/OT environment to support deployed incident response team.

<DMO head>

#	Responsibilities
1	Ensure compliance of <DMO> with all cybersecurity requirements.
2	Lead and direct<DMO> personnel by overseeing cybersecurity awareness and training in line with their responsibilities.
3	Ensure the <DMO> is engaged in all data security issues.
4	Work with <DMO> to develop security controls to protect data.
5	Oversee the prompt implementation of recommendations to mitigate cybersecurity risks.

Personnel of <DMO>

Cybersecurity Artificial Intelligence Specialist

#	Responsibilities
1	Develop security architecture elements to mitigate threats as they emerge.
2	Utilize different programming languages to write code, open files, read files and write output to different files.
3	Utilize open source languages.
4	Develop world class automated processes and artificial intelligence solutions.
5	Define and develop automated computational solutions, including analytic and algorithmic solutions.
6	Leverage statistical and machine learning techniques for trend identification and predictive analysis.

#	Responsibilities
7	Apply knowledge of machine learning, computer vision, remote sensing and big data processing to important problems by developing software to measure the feasibility of algorithms and approaches.
8	Analyze data and conduct quantitative data analysis using a variety of datasets to identify, monitor and explore operations.
9	Keep current with computer vision and machine learning research to replicate and baseline new techniques.
10	Use visualization tools to visualize data and create dashboards to communicate results.
11	Perform data profiling, statistical and machine learning analysis.
12	Use quantitative techniques.

Cybersecurity Auditor

#	Responsibilities
1	Maintain a deployable cyber defense audit toolkit based on industry best practice to support cyber defense audits.
2	Perform system administration on specialized cybersecurity applications and systems.
3	Perform risk analysis whenever an application or system undergoes a major change.
4	Prepare cybersecurity assessment and audit reports that identify technical and procedural findings, and include recommended remediation strategies and solutions.

#	Responsibilities
5	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
6	Effectively manage vulnerability remediation.
7	Ensure an audit log of evidence of security measures is maintained.
8	Review, conduct, or participate in audits of cyber programs and projects.
9	Maintain knowledge of applicable cybersecurity defense policies, regulations and compliance documents as they pertain to cybersecurity defense auditing.
10	Carry out an audit of application software/network/system security against documented cybersecurity policies and provide recommendations for remediation where gaps appear.
11	Develop cybersecurity compliance processes and audits for services provided by third parties.
12	Regularly review and ensure that cybersecurity policies and related documentation are aligned with the organization's stated business objectives and strategy.
13	Ensure that security design and cybersecurity development activities are appropriately documented.
14	Ensure that cybersecurity audits test all relevant aspects of the organization's infrastructure and policy compliance.
15	Develop processes with any external auditors on information sharing in a secure manner.

Privacy/Data Protection Officer

#	Responsibilities
1	Conduct Privacy Impact Assessments (PIAs) to ensure that Personally Identifiable Information (PII) is appropriately protected.
2	Work with others on policies, processes and procedures relating to cybersecurity and privacy.
3	Ensure that appropriate controls are in place to effectively mitigate cybersecurity risks and address privacy concerns during the risk .assessment process
4	Work with the organization's legal advisers and relevant third parties to ensure that all services comply with privacy and data security requirements.
5	Work with the organization's legal advisers, management and other stakeholders to ensure the organization has and maintains appropriate privacy and confidentiality documentation.
6	Work with stakeholders to develop relationships with regulators and government departments responsible for privacy and data security issues.
7	Ensure all processing and data source are registered with the relevant privacy and data protection authorities where required.
8	Work with business teams and senior management to ensure awareness of best practices relating to information privacy and data security.
9	Work with senior management to establish a committee responsible for the oversight of data privacy.
10	Provide leadership on the committee responsible for the oversight of data privacy.
11	Develop and document procedures for reporting self disclosures of any evidence of privacy violations.

#	Responsibilities
12	Serve as the information privacy liaison for users of technology systems, reporting breaches to senior management.
13	Develop training materials and other communications to increase employees understanding of company privacy policies, data handling practices and legal obligations.
14	Oversee, direct and ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties.
15	Ensure that privacy training and awareness activities are delivered on a regular basis.
16	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues.
17	Work with organization administration, legal advisers and other related parties to represent the organization's information privacy interests with external parties.
18	Report on a periodic basis regarding the status of the privacy program to senior management and other responsible individuals or committees.
19	Provide leadership for the organization's privacy program.
20	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior management to ensure consistency across the organization.
21	Ensure compliance with privacy practices across the organization.
22	Work with legal and HR teams to develop appropriate sanctions for failure to comply with the organization's privacy policies and procedures.

#	Responsibilities
23	Resolve allegations of noncompliance with organizational privacy policies or notice of information practices in a timely manner.
24	Establish and maintain a risk management and compliance framework for privacy.
25	Review the organization's data and privacy projects to ensure that they are compliant with the organization's privacy and data security policies.
26	Establish a process for managing all aspects of complaints concerning the organization’s privacy policies and procedures.
27	Provide leadership in the planning, design and evaluation of privacy and cybersecurity related projects.
28	Establish and maintain an internal privacy audit program.
29	Periodically review and update the privacy program to incorporate changes in laws, regulations or organizational policy.
30	Provide development guidance and assistance relating to the organization's information privacy policies and procedures.
31	Ensure that the use of technologies maintains and does not erode, privacy protections on use, collection and disclosure of personal information.
32	Monitor systems development and operations to ensure compliance with cybersecurity and privacy policies.
33	Conduct privacy impact assessments of proposed rules on the privacy of personal information.
34	Review all cybersecurity plans to ensure alignment between cybersecurity and privacy practices.

#	Responsibilities
35	Develop and manage procedures for vetting and auditing vendors for compliance with appropriate privacy, data security, legislative and regulatory requirements.
36	Ensure all complaints concerning the organization's privacy policies and related documentation are addressed in a timely manner by appropriate resource.
37	Identify and remediate areas where the organization is not fully compliant with privacy requirements.
38	Coordinate with the Chief Information Security Officer (or equivalent) to ensure alignment between cybersecurity and privacy practices.
39	Develop and maintain appropriate communications and training to promote and educate all employees including senior management regarding privacy compliance and the consequences of noncompliance.
40	Ensure that privacy compliance monitoring activities are carried out on an ongoing basis.
41	Ensure that appropriate technologies are used to maintain compliance with privacy requirements.
42	Develop strategic plans with senior management to ensure that personal information is processed in accordance with applicable privacy requirements.
43	Develop and maintain enterprise-wide procedures to ensure that new products and services are developed in accordance with organizational privacy policies and legal obligations.
44	Work with the Chief Information Security Officer, legal counsel and senior management to manage privacy incidents and breaches in accordance with legal and regulatory requirements.

#	Responsibilities
45	Maintain awareness of applicable privacy laws, regulations and accreditation standards.

<Head of information technology function>

#	Responsibilities
1	Ensure compliance of <information technology function> with all cybersecurity requirements.
2	Lead and direct <information technology function> personnel by overseeing cybersecurity awareness and training in line with their responsibilities.
3	Participate in and contribute to developing and applying risk management framework, procedures and processes.
4	Use manual patching whenever automated methods are not supported in <organization name>.
5	Oversee and monitor the implementation of automated solution(s) for patch management on a regular basis.
6	Review patch management effectiveness and efficiency for critical systems of information technology.
7	Ensure<cybersecurity function> is engaged in all information and technology assets, project management and procurement security matters.
8	Ensure<cybersecurity function> is engaged to ensure that all information and technology assets of <organization name> are appropriately protected.

#	Responsibilities
9	Review current maintenance contracts with information technology and / or critical systems vendors to ensure that <organization name> is supplied with latest patches.
10	Oversee the prompt implementation of recommendations to mitigate cybersecurity risks.
11	Oversee the management of cybersecurity technology assets operations.

Personnel of <information technology function>

#	Responsibilities
1	Implement cybersecurity requirements applicable to <information technology function>, including cybersecurity policies, procedures, processes, standards, and guidelines.
2	Remediate vulnerabilities and follow up the implementation of security patches and configuration.
3	Implement cybersecurity requirements related to the concerned personnel business nature.
4	Escalate and report cybersecurity suspicious activities or concerns to <cybersecurity function>.
5	Assist in providing input to the risk management framework process activities and related documentation.
6	Coordinate with the <cybersecurity function> in all information and technology assets and project management issues.
7	Coordinate with the <cybersecurity function> to ensure that all information and technology assets of <organization name> are appropriately protected and secured.

8	Review current maintenance contracts with information technology and / or critical systems vendors to ensure that <organization name> is supplied with latest patches.

<Information technology security> roles and responsibilities

Systems Security Development Specialist

#	Responsibilities
1	Apply security policies to applications that interface with one another.
2	Develop security risk profiles of computer systems by assessing threats to, and vulnerabilities of, those systems.
3	Conduct Privacy Impact Assessments (PIAs) to ensure that Personally Identifiable Information (PII) is appropriately protected.
4	Develop risk mitigation strategies to effectively manage risk in accordance with organizational risk appetite.
5	Develop specific cybersecurity countermeasures and risk mitigation strategies.
6	Ensure that any products implemented to manage cybersecurity risks have been effectively evaluated and authorized for use.
7	Perform cyber risk analysis whenever an application or system undergoes a major change.
8	Provide input to the risk management framework and related documentation.
9	Design, develop, integrate and update system security measures that provide confidentiality, integrity, availability, authentication and non-repudiation.

#	Responsibilities
10	Carry out a cybersecurity risk assessment.
11	Provide subject matter expertise to develop and architect the next generation of organizational cybersecurity.
12	Identify and prioritize critical business functions in collaboration with organizational stakeholders.
13	Analyze design constraints and trade-offs in detailed system cybersecurity design and consider life cycle support.
14	Assess the effectiveness of systems' cybersecurity measures.
15	Build, test and modify product prototypes to demonstrate compliance with cybersecurity requirements using working or theoretical models.
16	Design and develop cybersecurity or cybersecurity-enabled products.
17	Design hardware, operating systems and software applications to address cybersecurity requirements.
18	Design or integrate appropriate secure system backup and protected storage of back up data capabilities into designs.
19	Develop and direct procedures and documentation for system testing and validation.
20	Develop detailed security design documentation for component and interface specifications to support system design and development.
21	Develop and test disaster recovery and continuity of operations plans for systems under development prior to systems entering a production environment.
22	Identify and allocate security functions to components and describe the relationships between them.

#	Responsibilities
23	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems.
24	Ensure that cybersecurity is built into software development, maintenance and decommissioning processes.
25	Ensure that alerting on vulnerabilities is built into system designs.
26	Manage the compilation, cataloging, caching, distribution and retrieval of data.
27	Provide guidelines for implementing developed systems to customers or installation teams.
28	Support security certification test and evaluation activities.
29	Utilize models and simulations to analyze or predict system performance under different operating conditions.
30	Design and develop key cybersecurity management functions.
31	Analyze user needs and requirements to plan and conduct system security development.
32	Develop cybersecurity designs to meet operational needs and environmental factors.
33	Implement and integrate system development life cycle methodologies into cybersecurity systems development environment.
34	Employ configuration management processes when implementing cybersecurity systems.
35	Design, implement, test and evaluate secure interfaces between information systems, physical systems and embedded technologies.
36	Design to security requirements to ensure requirements are met for all systems and applications.

#	Responsibilities
37	Develop mitigation strategies to address cost, schedule, performance and security risks.
38	Perform security reviews and identify security gaps in architecture.
39	Provide input to information systems security implementation plans and standard operating procedures.
40	Trace system requirements to design components and perform gap analysis.
41	Verify stability, interoperability, portability and scalability of system architecture.
42	Ensure that security design and cybersecurity development activities are appropriately documented.

ICS/OT Cybersecurity Infrastructure Specialist

#	Responsibilities
1	Apply security policies to meet system security objectives.
2	Perform system administration on specialized cybersecurity applications and systems.
3	Identify, prioritize and coordinate the protection of critical cyber defense infrastructure and resources.
4	Apply cybersecurity functions (e.g., encryption, access control and identity management) to reduce exploitation opportunities.
5	Manage and administer the updating of rules and signatures for cyber defense applications.
6	Build, install, configure, patch and test dedicated cyber defense hardware and software.

#	Responsibilities
7	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.
8	Administer test beds and test and evaluate applications, hardware infrastructure, rules, signatures, access controls and configurations of platforms managed by service providers.
9	Create, edit and manage network access control lists on specialized cyber defense systems.
10	Identify and report potential conflicts with implementation of any cyber defense tools.
11	Implement risk management framework and security assessment and authorization requirements for dedicated cyber defense systems within the organization and document and maintain records for them.
12	Select the security controls for a system and document the functional description of the planned control implementations in a security plan.
13	Implement the security controls specified in a security plan or other system documentation.
14	Develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.
15	Select the security controls for a system and document the functional description of the planned control implementations in a security plan in IT and ICS/OT environments.
16	Implement the security controls specified in a security plan or other system documentation in IT and ICS/OT environments.
17	Understand and troubleshoot fault areas in industrial automation and communication systems.

Systems Security Analyst

#	Responsibilities
1	Apply security policies to applications that interface with one another.
2	Apply security policies to meet system security objectives.
3	Use cybersecurity products and security control technologies to reduce identified risk to an acceptable level.
4	Perform cybersecurity reviews and identify gaps in security architecture, to develop cybersecurity risk management plans.
5	Analyze exercise results and system environment to plan and recommend modifications and adjustments.
6	Provide input to the risk management framework and related documentation.
7	Review, update and maintain cybersecurity related documentation reflecting system design.
8	Assess the effectiveness of cybersecurity controls.
9	Assess the configuration management process.
10	Analyze and report on trends in the organization's security posture.
11	Analyze and report on trends in the system's security posture.
12	Assess the adequacy of access controls against organizational policies.
13	Assess and monitor the cybersecurity of the organization's system implementation and testing practices.
14	Make cybersecurity recommendations to leadership based on significant threats and vulnerabilities.

#	Responsibilities
15	Work with stakeholders to resolve cybersecurity incidents and vulnb erability compliance issues.
16	Identify and allocate security functions to components and describe the relationships between them.
17	Apply service-oriented security architecture principles to meet the organization's confidentiality, integrity and availability requirements.
18	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.
19	Apply security patches to commercial products in accordance with the timelines dictated by the management authority for the intended operational environment.
20	Implement specific cybersecurity countermeasures for systems and applications.
21	Integrate automated capabilities for updating or patching system software where practical.
22	Ensure cybersecurity testing of developed applications and systems.
23	Document and update systems security implementation, operations and maintenance activities.
24	Provide cybersecurity guidance to leadership.
25	Develop and test procedures to transfer system operations to an alternate site.
26	Execute business continuity and disaster recovery procedures.
27	Implement security measures to system or system components to resolve vulnerabilities, mitigate risks and recommend security changes.

#	Responsibilities
28	Implement system security measures in accordance with established procedures.
29	Ensure the integration and implementation of cross-domain solutions in a secure environment.
30	Make recommendations to management to make mitigation and correction measures or accept risks when security deficiencies are identified during testing.
31	Verify minimum security requirements are in place for all applications.
32	Develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.

Identity and Access Management Specialist

#	Responsibilities
1	Assess the adequacy of access controls against organizational policies.
2	Apply cybersecurity functions (e.g., encryption, access control and identity management) to reduce exploitation opportunities.
3	Develop cybersecurity designs to meet operational needs and environmental factors.
4	Create, edit and manage network access control lists on specialized cyber defense systems.
5	Work with other teams to design, develop and provide identity access management solutions.

#	Responsibilities
6	Work with cybersecurity architect to develop the identity access management strategy.
7	Ensure identity access management implementations follow organization's standards and policies.
8	Work with stakeholders to identify and address gaps in the identity access management implementation.
9	Mentor and advise team members on identity access management systems and processes.
10	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
11	Manage accounts, network rights, and access to systems and equipment.
12	Design and develop systems administration and management functionality for privileged access users.
13	Administer accounts, network rights and access to systems and equipment.
14	Establish continuous monitoring tools and technologies access control process and procedures.
15	Ensure that continuous monitoring tools and technologies access control is managed adequately.

Cryptography Specialist

#	Responsibilities
1	Perform technical decryption of seized data.

#	Responsibilities
2	Ensure that protection and detection capabilities are aligned with the organization's cybersecurity strategy, policies and other related documentation.
3	Develop secure data management capabilities to support a mobile workforce.
4	Enable applications with public keying, using existing public key infrastructure libraries and incorporating certificate management and encryption when appropriate.
5	Design, develop, integrate and update system security measures that provide confidentiality, integrity, availability, authentication and non-repudiation.
6	Apply cybersecurity functions (e.g., encryption, access control and identity management) to reduce exploitation opportunities.
7	Apply service-oriented security architecture principles to meet the organization's confidentiality, integrity and availability requirements.
8	Detect and analyze encrypted and concealed data.
9	Implement system security measures in accordance with established procedures.
10	Develop, design and implement cryptographic algorithms to meet organization's requirements.
11	Analyze cryptographic algorithms to find weaknesses and break ciphers.

Cybersecurity Developer

#	Responsibilities
1	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
2	Perform risk analysis whenever an application or system undergoes a major change.
3	Analyze exercise results and system environment to plan and recommend modifications and adjustments.
4	Enable applications with public keying, using existing public key infrastructure libraries and incorporating certificate management and encryption when appropriate.
5	Apply cybersecurity functions (e.g., encryption, access control and identity management) to reduce exploitation opportunities.
6	Analyze information to determine, recommend and plan the development of a new application or modification of an existing application.
7	Assess how user needs and software requirements can be met in line with cybersecurity policies and determine feasibility of design within time and cost constraints.
8	Apply coding and testing security standards.
9	Apply secure code documentation.
10	Integrate cybersecurity into the requirements process by defining and capturing security controls.
11	Ensure program development and revisions are fully documented and can be understood by others by using comments in the coded instructions.
12	Determine project limitations and capabilities, performance requirements and interfaces.

#	Responsibilities
13	Evaluate interface between hardware and software, in consultation with engineering staff.
14	Ensure that desired results are produced by rechecking the program and correct errors by making appropriate changes.
15	Develop secure code and error handling processes and documentation.
16	Apply methodologies to correct common coding errors with security implications to ensure development of secure software.
17	Ensure that cybersecurity is built into software development, maintenance and decommissioning processes.
18	Perform integrated quality assurance testing of security systems' functionality and resilience.
19	Prepare detailed workflow charts and diagrams that describe input, output and logical operation of security systems.
20	Address security implications in the software acceptance phase.
21	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling and defining any specific security criteria.
22	Consult with customers about cybersecurity systems design and maintenance.
23	Direct cybersecurity software programming and development of documentation.
24	Utilize different programming languages to write code, open files, read files and write output to different files.
25	Identify and leverage enterprise-wide security processes and services while designing and developing secure applications.

#	Responsibilities
26	Conduct trial runs of programs and software applications to ensure that the desired information is produced, and instructions and security levels are correct.
27	Develop software testing and validation procedures, programming and documentation.
28	Modify and maintain existing software to correct errors, adapt to new hardware, or upgrade interfaces and improve performance.
29	Determine and document software patches or the extent of releases that would leave software vulnerable.
30	Devise creative and custom exploits, solutions and techniques to discover vulnerabilities and exploitability of the targets.

<Application Development Officer>

#	Responsibilities
1	Oversee the implementation of the cybersecurity requirements related to application development in <organization name>.
2	Coordinate with the cybersecurity team on cybersecurity issues affecting the <application development function>.
3	Ensure the implementation of application cybersecurity standards (e.g. Open Web Application Security Project “OWASP”).
4	Oversee the application of security Testing Standards, security Coding Standards, including “fuzzing” static-analysis and Code Reviews.
5	Define and document patches and ensure their proper installation.

#	Responsibilities
6	Ensure that the source code of application internal and external development processes (through third party) in <organization name> is documented to enable the monitoring and reviewing of vulnerabilities management.
7	Ensure secure programming by error handling, and identification of potential flaws in codes to mitigate vulnerabilities.
8	Ensure remediation of vulnerabilities in the software acceptance phase, including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing, and inform <cybersecurity function> of all application development projects.
9	Ensure that cybersecurity functions and services (e.g., cryptography, access control, and identity management) are identified and leveraged to reduce exploitation opportunities.

Application Development Employees

#	Responsibilities
In addition to all responsibilities of <information technology function>'s personnel, application development employees shall assume the following responsibilities:	
1	Implement application development cybersecurity requirements in <organization name> and follow application development standards and procedures (e.g. secure application development standards).
2	Follow the <organization name>'s projects and change management processes for all changes applied to the <organization name>'s applications.
3	Identify and document patches.

#	Responsibilities
4	Perform secure programming, error handling, and identify potential flaws in codes to mitigate vulnerabilities.
5	Apply security Testing Standards, security Coding Standards, including “fuzzing” static-analysis and Code Reviews.
6	Determine and document software patches and the extent of releases that would leave software vulnerable.

<Information Technology Operation Officer>

#	Responsibilities
1	Prioritize, plan, and schedule maintenance windows for patch deployment according to <organization name>’s projects and change management policy without affecting assets cybersecurity.
2	Oversee the automated patch management solution(s), and ensures manual patching is conducted whenever automated patching is not supported
3	Oversee regular backups and backup tests.
4	Oversee the implementation of the cybersecurity requirements related to information technology processes in <organization name>.
5	Ensure information and technology asset patch testing prior to deployment.
6	Verify the success of the systems patching.
7	Ensure <organization name>’s information and technology asset related cybersecurity policies are enforced (e.g. workstation security policy, server security policy template, etc.).

#	Responsibilities
8	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after the occurrence of a catastrophic cybersecurity failure event affecting systems and business continuity.
9	Define appropriate levels of system information availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and business continuity requirements to include any appropriate fail-over site requirements, backup requirements, and material supportability requirements for system recovery/restoration.
10	Oversee Disaster Recovery Plan (DRP) efficiency test and participate in Business Continuity Plan (BCP) test.

Information Technology Employees

#	Responsibilities
In addition to all responsibilities of <information technology function>'s personnel, information technology employees shall assume the following responsibilities:	
1	Assist in coordinating with<cybersecurity function> on cybersecurity related matters affecting the information technology function.
2	Implement the cybersecurity requirements related to information technology processes in <organization name>.
3	Implement automated solution(s) for patch management.
4	Take and test backups regularly.

#	Responsibilities
5	Implement the automated patch management solution(s), and ensure manual patching is conducted whenever automated patching is not supported.
6	Enable and secure appropriate logs and integrate them with a centralized log management system.
7	Configure all management software, protection software, operating systems on the information and technology assets.
8	Oversee privileges and user accounts seeking to access information and technology assets as per the respective policy.
9	Isolate information and technology assets and apply logical and secure segmentation of network.
10	Engage in threats and incidents management of information technology systems in relevant phases (e.g. Containment, Eradication, Recovery.)
11	Assist in defining and prioritizing essential system capabilities or business functions required for partial or full system restoration after a catastrophic cybersecurity failure event.
12	Assist in defining appropriate levels of system information availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and business continuity requirements to include any appropriate fail-over site requirements, backup requirements, and material supportability requirements for system recovery/restoration.

<Head of Human Resources function>

#	Responsibilities

1	Oversee the implementation of the cybersecurity requirements related to human resources in <organization name>.
2	Ensure screening or vetting of the personnel of cybersecurity functions and privileged technology functions in coordination with stakeholders.
3	Support the implementation of acceptable asset use policy and apply disciplinary actions to violations as per the <organization name>'s procedures.
4	Update and review human resources cybersecurity policy.
5	Attend and participate in the CSC meetings as necessary.
6	Advocate for adequate funding for cybersecurity training resources, to include both internal and industry-related courses, instructors, and related materials.
7	Conduct cybersecurity learning needs assessments and identify requirements.
8	Ensure standardized roles and responsibilities based on established cybersecurity work roles are developed and implemented.
9	Establish cybersecurity career paths to allow career progression, deliberate development, and growth within and between cybersecurity career fields.
10	Assist in coordinating and liaising with the<cybersecurity function> on cybersecurity related matters affecting the <human resources function>.
11	Review and provide input to the cybersecurity strategy and policies.
12	Deal with non-compliance with cybersecurity policies violations in coordination with the < legal function>.

Personnel of <human resources function>

#	Responsibilities
1	Implement the cybersecurity requirements related to human resources in <organization name>.
2	Screen or vet personnel of cybersecurity functions and privileged technology functions in coordination with stakeholders.
3	Evaluate cybersecurity awareness of all personnel, and define and address cybersecurity weaknesses.
4	Implement the cybersecurity awareness and training program in coordination with the cybersecurity awareness and training function.
5	Develop and implement standardized position descriptions based on established cybersecurity work roles.
6	Assist in the establishment of cybersecurity career paths to allow career progression, deliberate development, and growth within and between cybersecurity career fields.
7	Support in advocating for adequate funding for cybersecurity training resources, to include both internal and industry-related courses, instructors, and related materials.

<Head of internal audit function>

#	Responsibilities
1	Oversee the periodic review and audit of cybersecurity programs and requirements as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.

#	Responsibilities
2	Oversee cybersecurity audits according to the stipulations of the cybersecurity review and audit policy.
3	Ensure that all cybersecurity-related documentation is reviewed and updated periodically.
4	Coordinate with cybersecurity function to attend and participate in the CSC meetings as necessary.
5	Ensure that all cybersecurity risks are updated and re-assessed as per the cybersecurity risk management policy.
6	Ensure risk acceptance is aligned with the cybersecurity risk management policy.
7	Propose a remediation plan for the audit results and observations.
8	Document, report, and discuss the results and / or observations with the relevant function.
9	Present the audit results and / or observations to the CSC.
10	Discuss and document corrective actions with the audit results owners.
11	Report on ineffective cybersecurity controls.
12	Report on non-compliances with the cybersecurity requirements.
13	Coordinate and liaison with the cybersecurity team on cybersecurity related matters affecting the internal audit function.
14	Review and provide input to the cybersecurity strategy and policies.

Personnel of <internal audit function>

#	Responsibilities
1	Assist in reviewing and auditing the implementation of cybersecurity controls as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.
2	Implement cybersecurity requirements related to internal audit in <organization name>.
3	Ensure that all cybersecurity-related documentation is reviewed and updated periodically.
4	Conduct reviews to ensure that all cybersecurity risks are updated and re-assessed as per the cybersecurity risk management policy.
5	Conduct reviews to ensure risk acceptance is aligned with the cybersecurity risk management policy.
6	Conduct reviews and notify the internal audit head on non-compliances with the cybersecurity requirements.
7	Conduct cybersecurity audits according to the stipulations of the cybersecurity review and audit policy.
8	Analyze and provide recommendations to the internal audit head on ineffective cybersecurity controls.
9	Suggest corrective actions to the internal audit head based on the audit results and observations.
10	Assist in developing a remediation plan for the audit results and observations.
11	Assist in coordinating and liaising with the cybersecurity team on cybersecurity related matters affecting the internal audit function.

<The legal function>

#	Responsibilities
1	Define national cybersecurity legislative and regulatory requirements, and locally-approved international agreements and commitments that include cybersecurity requirements applicable to <organization name>.
2	Translate cybersecurity controls, regulations, policies, standards, and procedures into legally binding clauses.
3	Ensure that terms and conditions and non-disclosure clauses are legally binding for employees and third parties in order to protect the <organization name>'s information and technology assets.
4	Oversee the implementation of the cybersecurity requirements related to legal matters in <organization name>.
5	Attend and participate in the CSC meetings as necessary.
6	Evaluate the effectiveness of cybersecurity laws, and regulations.
7	Review <organization name>'s third-party security policy according to the relevant legal requirements.
8	Liaison with the <cybersecurity function> on cybersecurity related matters affecting the legal function.
9	Support cybersecurity incidents when required.

Personnel of <legal function>

#	Responsibilities
1	Assist in interpreting and applying cybersecurity laws, regulations, standards, and procedures to specific issues.

2	Implement cybersecurity requirements related to legal matters in <organization name>.
3	Assist in evaluating the effectiveness of cybersecurity laws and regulations.

All personnel in the <organization name>.

#	Responsibilities
1	Deal with data and information according to their classification.
2	Avoid infringing the copyrights, patents, and intellectual property rights (or any other similar laws or regulations) of any person or company.
3	Comply with cybersecurity policies and procedures.
4	Adhere to the cybersecurity requirements related to the workstations protection.
5	Adhere to the cybersecurity requirements related to the internet and software use.
6	Adhere to the cybersecurity requirements related to the e-mail.
7	Adhere to the relevant requirements related to cybersecurity protection systems and technologies.
8	Use all information and technology assets of <organization name> for business purposes only and according to <organization name>'s acceptable use policy.
9	Obtain the required authorization from <the organization's function> or <organization name>'s authorizing official before hosting visitors in critical sites in <organization name>.
10	Cybersecurity incidents reporting.
11	Comply with acceptable use policy.

Table of segregating management and operation duties of cybersecurity systems and tools.

The **governance, risk, and compliance** aspects of all cybersecurity systems and tools are the responsibility of <cybersecurity function>. As for the management and operation of systems and tools, the responsibility varies according to the system or tool used, as clarified in the table below:

Cybersecurity systems and tools	**Management and operation of systems and tools responsibility**	
	<Cybersecurity function>	<Information technology function>
Identity and Access Management Tools and Systems		✓
Privileged Access Management Tools and Systems		✓
Security Information and Event Management (SIEM) Tools and Systems	✓	
Networks Security Tools and Systems (e.g. firewalls)		✓
Penetration Testing Tools	✓	
Technical Vulnerabilities Detection & Assessment Tools	✓	
Intelligence Feeds Tools	✓	
Governance, Risk and Compliance Management Systems and Tools	✓	
Digital Forensics Tools	✓	
Cybersecurity Incident Response Tools	✓	
Protection against Viruses, Suspicious Activities and Malware Tools and Systems		✓
Backup and Recovery Systems and Tools		✓
Data Classification Systems and Tools		✓

Data Loss Prevention Systems and Tools		✓
Cryptography Systems and Tools		✓
Mobile Devices Management Systems and Tools		✓
Asset Management Systems and Tools		✓

Roles and Responsibilities

1- **Document Owner:** <head of cybersecurity function>.
2- **Document Review and Update:** <cybersecurity function>.
3- **Document Implementation and Execution:** <cybersecurity function> and <HR function>.
4- **Document Compliance Measurement**: <cybersecurity function>.

Update and Review

<cybersecurity function> must review the document at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant legislative and regulatory requirements.

Compliance

1- The <Head of cybersecurity function> will ensure the compliance of <organization name> with this document on a regular basis.
2- All personnel at <organization name> must comply with this document.
3- Any violation of this document may be subject to disciplinary action according to <organization name>'s procedures.

Reference Table

Relevant Regulation	Reference in regulation controls	Control No.
Essential Cybersecurity Controls (ECC)	1-4-1	1-4
	1-4-2	1-4