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



Insert organization logo by clicking on the outlined image.

Cybersecurity Organizational Structure Template

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

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

|  |  |  |
| --- | --- | --- |
| Choose Classification | |  |
| DATE | Click here to add text |  |
| VERSION | Click here to add text |  |
| REF | Click here to add text |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Signature | Date | Name | Job Title | Role |
| <Insert signature> | Click here to add text | <Insert individual’s full personnel name> | <Insert job title> | Choose Role |
|  |  |  |  |  |

Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Updated By | Version Details |
| <Insert version number> | Click here to add text | <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 text | Click here to add text |
|  |  |  |

Table of Contents

[Purpose 4](#_Toc137071354)

[Guidelines 4](#_Toc137071355)

[Cybersecurity Governance 5](#_Toc137071356)

[Individuals of the organizational structure of <organization name> 5](#_Toc137071357)

[Cybersecurity Structure 7](#_Toc137071358)

[Organizational structure of the <cybersecurity function> 7](#_Toc137071359)

[Roles and Responsibilities 27](#_Toc137071363)

[Update and Review 27](#_Toc137071364)

[Compliance 28](#_Toc137071365)

[Reference Table 28](#_Toc137071366)

# [Purpose](C:\\Users\\101191402\\AppData\\Local\\Temp\\Temp1_RE__نماذج_أدوات_الأمن_السيبراني.zip\\نموذج الهيكل التنظيمي للأمن السيبراني [NOT Final]-KM.docx" \o "يهدف هذا القسم إلى توضيح الغرض من بناء الهيكل التنظيمي لإدارة الأمن السيبراني على مستوى الجهة)

This document aims to establish the <cybersecurity function> in <organization name> that is independent from the <information technology function>, as per the Royal Decree No. 37140 dated 14/08/1438H and other relevant legislative and regulatory requirements. This goal is a regulatory requirement as per the controls issued by the National Cybersecurity Authority (NCA) and other relevant legislative and regulatory requirements.

The cybersecurity organizational structure was developed based on best practices and standards to provide the <cybersecurity function> with the needed support to carry out its delegated tasks as required. The <cybersecurity function> is one of the key pillars of <organization name>, and it is responsible for the protection of information and technology assets against cyber risks.

This document aims to define and document the organizational structure of cybersecurity governance, roles and responsibilities within <organization name> .

# Guidelines

1. Ensure that the <cybersecurity function> is independent from the <information technology function>.
2. Ensure that the <cybersecurity function> reports to the head of the organization or his/her delegate in <organization name>, having the power to influence key cybersecurity decisions within <organization name>.
3. Ensure that such reporting relationship of the <cybersecurity function> differs from that of the <information technology function> or <digital transformation function>, as per the Royal Decree No. 37140 dated 14/08/1438H, which is a regulatory requirement under Control No. 1-2-1 in the Essential Cybersecurity Controls (ECC–1:2018).
4. Avoid conflicts of interests, among which:
   1. Managing technology and information system access (or operational systems) validity and their operations at the same time.
   2. Implementing cybersecurity requirements and ensuring compliance with them at the same time.
   3. Conflicts of interests between the cybersecurity monitoring team and the cybersecurity operations team.
   4. Conflicts of interests between the security testing team and the application development team.
5. Ensure that the cybersecurity organizational structure includes the following roles as a minimum:
   1. Cybersecurity governance.
   2. Cybersecurity compliance management.
   3. Cybersecurity risk management.
   4. Cybersecurity strategy management.
   5. Cybersecurity resilience.
   6. Cybersecurity training and awareness.
   7. Cybersecurity operations (Cybersecurity monitoring and incident response).
   8. Data and information protection.
   9. Cybersecurity related to operational systems and industrial control systems (OT/ICS) (if applicable)
6. The following roles might be added to the cybersecurity organizational structure:
   1. Cybersecurity architecture.
   2. Identity and access management.
   3. Cybersecurity infrastructure management.
   4. Physical security.

# Cybersecurity [Governance](#_أنماط_الحوكمة)

## Individuals of the organizational structure of <organization name>

| # | Individual | Description |
| --- | --- | --- |
|  | Authorizing Official | Head of the organization or his/her delegate. |
|  | Cybersecurity Steering Committee (CSC) | The CSC is a high-level governance board that ensures, monitors, and supports the implementation of cybersecurity programs and regulations within <organization name>. |
|  | Cybersecurity Department | The <cybersecurity function> protects networks, IT/OT systems and their components such as hardware and software, including the services they provide and the data they contain from any illegal breach, disruption, modification, access, use or exploitation. Cybersecurity concept covers information security, electronic security, digital security, etc. |
|  | IT | The <IT function> operates IT and network infrastructure and develops software and technical services among other activities. |
|  | Human Resources (HR) | The <HR function> is responsible for all personnel affairs within <organization name>. |
|  | Legal Affairs | The <legal function> drafts contracts and agreements and protects the legal rights of <organization name>. |
|  | Procurement | The <procurement function> is responsible for contracting with suppliers, as well as all procurement processes and third-party contracts within <organization name>. |
|  | Finance | The <finance function> prepares the general budget of <organization name>. |
|  | Data Management Office (DMO) | The <data management function> manages data and privacy within <organization name>. |
|  | Internal Review and Audit | The <internal review function> audits and reviews the implementation of policies, procedures, and relevant legislative and regulatory requirements by <organization name>. |
|  | Business Continuity Department | The <business continuity function> is responsible for all business continuity related matters within <organization name>, including crisis management and disaster recovery. |
|  | Operational Technology (OT) | The <OT function> is responsible for all OT related matters in <organization name>. |
|  | Project Management Office (PMO) | The <PMO> is responsible for all project management-related matters within <organization name>, including the 2030 Vision Realization Offices (VROs) (if any). |
|  | Business Units | This encompasses all other business units and functions in <organization name>. |

# [Cybersecurity Structure](#_هيكلية_إدارة_الأمن)

In order to <cybersecurity function> perform its responsibilities properly and efficiently, the roles and tasks of the <cybersecurity function> were distributed based on the operational functions of each role, taking into consideration the principles of Segregation of Duties and Conflict of Interest. They are distributed as follows <you can select one of the options below>:

## Organizational structure of the <cybersecurity function>

The following proposed organizational structures are optional. A structure can be selected based on the organization’s business nature, tasks and size.

1. **Option 1** 
   1. This cybersecurity organizational structure aligns with local regulations, including but not limited to: (ECC-1:2018), and focuses on the cybersecurity main domains.
   2. This cybersecurity organizational structure is simple and easier to understand and implement.

Organization head

Department

Team

Head of the organization or his/her delegate

Internal Audit Department

Data Management Office

Cybersecurity Department

Information Technology Department

Cybersecurity Operations

Governance, Risk, and Compliance

IT Security

OT Cybersecurity

| Governance, Risk, and Compliance | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity architect | Designs and oversees the development,  implementation and configuration of  cybersecurity systems and networks. |
|  | Secure Cloud Specialist | Designs, implements and operates secure cloud computing systems and develops secure cloud policies. |
|  | Secure Software Assessor | Assesses the security of computer applications, software, code, or programs, and provides actionable results. |
|  | Cybersecurity Researcher | Conducts scientific research in the cybersecurity field. |
|  | Cybersecurity Risk Officer | Identifies, assesses and manages an  organization’s cybersecurity risks to protect its information and technology assets in line with organizational policies and procedures and related laws and regulations. |
|  | Cybersecurity Compliance Officer | Ensures an organization’s cybersecurity  program complies with applicable requirements, policies and standards. |
|  | Cybersecurity Policy Officer | Develops, updates and maintains cybersecurity policies to support and align with an organization’s cybersecurity requirements. |
|  | Security Controls Assessor | Analyzes cybersecurity controls and assesses their effectiveness |
|  | Cybersecurity Specialist | Provides general cybersecurity support. Assists in cybersecurity tasks. |
|  | ICS/OT Cybersecurity Architect | Designs and oversees the development,  implementation and configuration of  cybersecurity systems and networks in ICS/  OT environments. |
|  | ICS/OT Cybersecurity Risk Officer | Identifies, assesses and manages cybersecurity risks within ICS/OT environments. Evaluates and analyzes the effectiveness of existing cybersecurity controls and provides feedback  and recommendations based on assessments. |
|  | Cybersecurity Legal Specialist | Provides legal services on topics related to cyber laws and regulations. |
| |  |  |  | | --- | --- | --- | | Cybersecurity Department | | | | # | Role | Description | |  | Cybersecurity Advisor | Provides expert consultancy and advice on  cybersecurity topics to an organization’s  leadership and to its cybersecurity leadership  and teams. | | | |
| Cybersecurity Operations | | |
| # | Role | Description |
|  | Cybersecurity Defense Analyst | Uses data collected from cyber defense tools  to analyze events that occur within their  organization to detect and mitigate cyber  threats. |
|  | Vulnerability Assessment Specialist | Performs vulnerability assessments of  systems and networks. Identifies where they  deviate from acceptable configurations or  applicable policies. Measures effectiveness of  defense-in-depth architecture against known  vulnerabilities. |
|  | Penetration Tester/Red Team Specialist | Conducts authorized attempts to penetrate  computer systems or networks and physical  premises, using realistic threat techniques, to  evaluate their security and detect potential  vulnerabilities. |
|  | Cybersecurity Incident Responder | Investigates, analyzes and responds to  cybersecurity incidents. |
|  | Digital Forensics Specialist | Collects and analyzes digital evidence,  investigates cybersecurity incidents to derive  useful information to mitigate system and  network vulnerabilities. |
|  | Cyber Crime Investigator | Identifies, collects, examines and preserves  evidence using controlled and documented  analytical and investigative techniques. |
|  | Malware Reverse Engineering Specialist | Analyzes (by disassembling and/or  decompiling) malicious software, understands  how it works, its impact and intent and  recommends mitigation techniques and  incident response actions. |
|  | Threat Intelligence Analyst | Collects and analyzes multi-source information about cybersecurity threats to develop deep understanding and awareness of cyber threats and actors’ Tactics, Techniques and Procedures (TTPs), to derive and report indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats. |
|  | Threat Hunter | Proactively searches for undetected threats in  networks and systems, identifies their Indicators of Compromise (IOCs) and recommends mitigation plans |
|  | ICS/OT Cybersecurity Defense Analyst | Uses data collected from a variety of  cybersecurity tools to analyze events that  occur within ICS/OT environments to detect  and mitigate cybersecurity threats. |

| IT Security | | |
| --- | --- | --- |
| # | Role | Description |
|  | Systems Security Development Specialist | Designs, develops, tests and evaluates security of information systems throughout the  development life-cycle. |
|  | Cybersecurity Developer | Develops cybersecurity software, applications,  systems and products. |
|  | Cybersecurity Infrastructure Specialist | Tests, implements, deploys, maintains and  administers hardware and software that protect  and defend systems and networks against  cybersecurity threats. |
|  | Cryptography Specialist | Develops cryptography systems and algorithms. |
|  | Identity and Access Management Specialist | Manages individuals and entities identities  and access to resources through applying  identification, authentication and authorization  systems and processes. |
|  | Systems Security Analyst | Develops, tests and maintains systems’ security. Analyzes security of operations and integrated systems. |

| Data Management Office (DMO) | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity Data Science Specialist | Uses mathematical models and scientific  methods and processes to design and  implement algorithms and systems that extract  cybersecurity insights and knowledge from  multiple large-scale data sets. |
|  | Cybersecurity Artificial Intelligence Specialist | Uses artificial intelligence models and  techniques (including machine learning ones) to design and implement algorithms and systems that automate and improve the efficiency and effectiveness of cybersecurity tasks. |
|  | Privacy/Data Protection Officer | Studies personal data schemes and the  applicable privacy laws and regulations.  Analyzes privacy risks. Develops and oversees  the implementation of an organization’s privacy  and data protection compliance program and  internal policies. Supports organizational  response to a privacy or data protection  incident. |

| Internal Audit Office | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity Auditor | Designs, performs and manages cybersecurity  audits to assess an organization’s compliance  with applicable requirements, policies,  standards and controls. Prepares audit reports  and communicates them to authorized parties. |

1. **Option 2**
   1. This cybersecurity organizational structure addresses in particular privacy and legal matters.
   2. This organizational structure helps protect the confidentiality, integrity, and availability of the <organization name>’s OT/ICS assets against cyber attacks.

Organization head

Department

Team

Head of the organization or his/her delegate

Internal Audit Department

Data Management Office

Cybersecurity Department

Information Technology Department

Cybersecurity Operations

Governance, Risk, and Compliance

IT Security

OT Cybersecurity

|  |  |  |
| --- | --- | --- |
| Cybersecurity Department | | |
| # | Role | Description |
|  | Cybersecurity Advisor | Provides expert consultancy and advice on  cybersecurity topics to an organization’s  leadership and to its cybersecurity leadership  and teams. |

| Governance, Risk, and Compliance | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity architect | Designs and oversees the development,  implementation and configuration of  cybersecurity systems and networks. |
|  | Secure Cloud Specialist | Designs, implements and operates secure cloud computing systems and develops secure cloud policies. |
|  | Secure Software Assessor | Assesses the security of computer applications, software, code, or programs, and provides actionable results. |
|  | Cybersecurity Researcher | Conducts scientific research in the cybersecurity field. |
|  | Cybersecurity Risk Officer | Identifies, assesses and manages an  organization’s cybersecurity risks to protect its information and technology assets in line with organizational policies and procedures and related laws and regulations. |
|  | Cybersecurity Compliance Officer | Ensures an organization’s cybersecurity  program complies with applicable requirements, policies and standards. |
|  | Cybersecurity Policy Officer | Develops, updates and maintains cybersecurity policies to support and align with an organization’s cybersecurity requirements. |
|  | Security Controls Assessor | Analyzes cybersecurity controls and assesses their effectiveness |
|  | Cybersecurity Specialist | Provides general cybersecurity support. Assists in cybersecurity tasks |
|  | Cybersecurity Legal Specialist | Provides legal services on topics related to cyber laws and regulations. |

|  |  |  |
| --- | --- | --- |
| Cybersecurity Operations | | |
| Description | Role | # |
| Uses data collected from cyber defense tools to analyze events that occur within their  organization to detect and mitigate cyber  threats. | Cybersecurity Defense Analyst |  |
| Performs vulnerability assessments of  systems and networks. Identifies where they  deviate from acceptable configurations or  applicable policies. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. | Vulnerability Assessment Specialist |  |
| Conducts authorized attempts to penetrate  computer systems or networks and physical  premises, using realistic threat techniques, to evaluate their security and detect potential  vulnerabilities. | Penetration Tester/Red Team Specialist |  |
| Investigates, analyzes and responds to  cybersecurity incidents. | Cybersecurity Incident Responder |  |
| Collects and analyzes digital evidence,  investigates cybersecurity incidents to derive  useful information to mitigate system and  network vulnerabilities. | Digital Forensics Specialist |  |
| Identifies, collects, examines and preserves  evidence using controlled and documented  analytical and investigative techniques. | Cyber Crime Investigator |  |
| Analyzes (by disassembling and/or  decompiling) malicious software, understands how it works, its impact and intent and recommends mitigation techniques and incident response actions. | Malware Reverse Engineering Specialist |  |
| Collects and analyzes multi-source information about cybersecurity threats to develop deep understanding and awareness of cyber threats and actors’ Tactics, Techniques and Procedures (TTPs), to derive and report indicators that help organizations detect and predict cyber  incidents and protect systems and networks  from cyber threats. | Threat Intelligence Analyst |  |
| Proactively searches for undetected threats in networks and systems, identifies their Indicators of Compromise (IOCs) and recommends mitigation plans. | Threat Hunter |  |

| OT Cybersecurity | | |
| --- | --- | --- |
|  | #Role | Description |
|  | ICS/OT Cybersecurity Architect | Designs and oversees the development,  implementation and configuration of  cybersecurity systems and networks in ICS/  OT environments. |
|  | ICS/OT Cybersecurity Risk Officer | Identifies, assesses and manages cybersecurity risks within ICS/OT environments. Evaluates and analyzes the effectiveness of existing cybersecurity controls and provides feedback and recommendations based on assessments. |
|  | ICS/OT Cybersecurity Defense Analyst | Uses data collected from a variety of  cybersecurity tools to analyze events that  occur within ICS/OT environments to detect  and mitigate cybersecurity threats. |
|  | ICS/OT Cybersecurity Infrastructure Specialist | Tests, implements, deploys, maintains and  administers hardware and software that  protect and defend systems and networks  against cybersecurity threat in ICS/OT  environments. |
|  | ICS/OT Cybersecurity Incident Responder | Investigates, analyzes and responds to  cybersecurity incidents within ICS/OT  environments. |

| IT Security | | |
| --- | --- | --- |
| # | Role | Description |
|  | Systems Security Development Specialist | Designs, develops, tests and evaluates security of information systems throughout the  development life-cycle. |
|  | Cybersecurity Developer | Develops cybersecurity software, applications,  systems and products |
|  | Cybersecurity Infrastructure Specialist | Tests, implements, deploys, maintains and  administers hardware and software that protect  and defend systems and networks against  cybersecurity threats. |
|  | Cryptography Specialist | Develops cryptography systems and algorithms. |
|  | Identity and Access Management Specialist | Manages individuals and entities identities  and access to resources through applying  identification, authentication and authorization  systems and processes. |
|  | Systems Security Analyst | Develops, tests and maintains systems’ security. Analyzes security of operations and integrated systems. |

| Data Management Office (DMO) | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity Data Science Specialist | Uses mathematical models and scientific  methods and processes to design and  implement algorithms and systems that extract  cybersecurity insights and knowledge from  multiple large-scale data sets. |
|  | Cybersecurity Artificial Intelligence Specialist | Uses artificial intelligence models and  techniques (including machine learning ones) to design and implement algorithms and systems that automate and improve the efficiency and effectiveness of cybersecurity tasks. |
|  | Privacy/Data Protection Officer | Studies personal data schemes and the  applicable privacy laws and regulations.  Analyzes privacy risks. Develops and oversees  the implementation of an organization’s privacy  and data protection compliance program and  internal policies. Supports organizational  response to a privacy or data protection  incident. |

| Internal Audit Office | | |
| --- | --- | --- |
| # | Role | Description |
| 1 | Cybersecurity Auditor | Designs, performs and manages cybersecurity  audits to assess an organization’s compliance  with applicable requirements, policies,  standards and controls. Prepares audit reports  and communicates them to authorized parties. |

1. **Option 3**
   1. The cybersecurity organizational structure supervises the budget, and is responsible for security technology and the workforce that operates and manages same.
   2. The cybersecurity organizational structure avoids transferring the control of security technologies, which may expose <organization name> to unacceptable risks.
   3. The cybersecurity organizational structure enables the use of cutting-edge technologists that promote rapid innovation and the adoption of new security controls.
   4. This cybersecurity organizational structure provides a cybersecurity operations center (CSOC) whose manager shall have more direct subordinates, authorities, and powers.

Organization head

Department

Team

Head of the organization or his/her delegate

Internal Audit Department

Data Management Office

Information Technology Department

Cybersecurity Department

Cybersecurity Architecture

Cybersecurity Operations

IT Security

Governance

Risk and Compliance

|  |  |  |
| --- | --- | --- |
| Cybersecurity Department | | |
| # | Role | Description |
|  | Cybersecurity Advisor | Provides expert consultancy and advice on  cybersecurity topics to an organization’s  leadership and to its cybersecurity leadership  and teams. |

| Governance | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity Researcher | Conducts scientific research in the cybersecurity field. |
|  | Cybersecurity Policy Officer | Develops, updates and maintains cybersecurity  policies to support and align with an  organization’s cybersecurity requirements. |
|  | Cybersecurity Specialist | Provides general cybersecurity support. Assists in cybersecurity tasks. |

| Risk and Compliance | | |
| --- | --- | --- |
| # | Role | Description |
|  | Secure Software Assessor | Assesses the security of computer applications, software, code, or programs, and provides actionable results. |
|  | Cybersecurity Risk Officer | Identifies, assesses and manages an  organization’s cybersecurity risks to protect its  information and technology assets in line with  organizational policies and procedures and  related laws and regulations. |
|  | Cybersecurity Compliance Officer | Ensures an organization’s cybersecurity  program complies with applicable requirements, policies and standards. |
|  | Security Controls Assessor | Analyzes cybersecurity controls and assesses  their effectiveness |
|  | ICS/OT Cybersecurity Risk Officer | Identifies, assesses and manages cybersecurity risks within ICS/OT environments. Evaluates and analyzes the effectiveness of existing cybersecurity controls and provides feedback and recommendations based on assessments. |
|  | Cybersecurity Legal Specialist | Provides legal services on topics related to cyber laws and regulations. |

| Cybersecurity architecture | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity architect | Designs and oversees the development,  implementation and configuration of  cybersecurity systems and networks. |
|  | Secure Cloud Specialist | Designs, implements and operates secure cloud computing systems and develops secure cloud policies. |
|  | ICS/OT Cybersecurity Architect | Designs and oversees the development,  implementation and configuration of  cybersecurity systems and networks in ICS/  OT environments. |
|  | ICS/OT Cybersecurity Infrastructure Specialist | Tests, implements, deploys, maintains and  administers hardware and software that  protect and defend systems and networks  against cybersecurity threat in ICS/OT  environments. |

| Cybersecurity Operations | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity Defense Analyst | Uses data collected from cyber defense tools  to analyze events that occur within their  organization to detect and mitigate cyber  threats. |
|  | Vulnerability Assessment Specialist | Performs vulnerability assessments of  systems and networks. Identifies where they  deviate from acceptable configurations or  applicable policies. Measures effectiveness of  defense-in-depth architecture against known  vulnerabilities. |
|  | Penetration Tester/Red Team Specialist | Conducts authorized attempts to penetrate  computer systems or networks and physical  premises, using realistic threat techniques, to  evaluate their security and detect potential  vulnerabilities. |
|  | Cybersecurity Incident Responder | Investigates, analyzes and responds to  cybersecurity incidents. |
|  | Digital Forensics Specialist | Collects and analyzes digital evidence,  investigates cybersecurity incidents to derive  useful information to mitigate system and  network vulnerabilities. |
|  | Cyber Crime Investigator | Identifies, collects, examines and preserves  evidence using controlled and documented  analytical and investigative techniques. |
|  | Malware Reverse Engineering Specialist | Analyzes (by disassembling and/or  decompiling) malicious software, understands  how it works, its impact and intent and  recommends mitigation techniques and  incident response actions. |
|  | Threat Intelligence Analyst | Collects and analyzes multi-source information  about cybersecurity threats to develop deep  understanding and awareness of cyber threats  and actors’ Tactics, Techniques and Procedures (TTPs), to derive and report indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats. |
|  | Threat Hunter | Proactively searches for undetected threats in  networks and systems, identifies their Indicators of Compromise (IOCs) and recommends mitigation plans |
|  | ICS/OT Cybersecurity Defense Analyst | Uses data collected from a variety of  cybersecurity tools to analyze events that  occur within ICS/OT environments to detect  and mitigate cybersecurity threats. |
|  | ICS/OT Cybersecurity Incident Responder | Investigates, analyzes and responds to  cybersecurity incidents within ICS/OT  environments. |

| IT Security | | |
| --- | --- | --- |
| # | Role | Description |
|  | Systems Security Development Specialist | Designs, develops, tests and evaluates security of information systems throughout the  development life-cycle. |
|  | Cybersecurity Developer | Develops cybersecurity software, applications,  systems and products |
|  | Cybersecurity Infrastructure Specialist | Tests, implements, deploys, maintains and  administers hardware and software that protect  and defend systems and networks against  cybersecurity threats. |
|  | Cryptography Specialist | Develops cryptography systems and algorithms. |
|  | Identity and Access Management Specialist | Manages individuals and entities identities  and access to resources through applying  identification, authentication and authorization  systems and processes. |
|  | Systems Security Analyst | Develops, tests and maintains systems’ security. Analyzes security of operations and integrated systems. |

| Internal Audit Office | | |
| --- | --- | --- |
| # | Role | Description |
|  | Cybersecurity Auditor | Designs, performs and manages cybersecurity  audits to assess an organization’s compliance  with applicable requirements, policies,  standards and controls. Prepares audit reports  and communicates them to authorized parties. |

# [Roles and Responsibilities](#الأدوار" \o "This section aims to define the roles and responsibilities related to the cybersecurity organizational structure.)

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 regulatory requirements.

# [Compliance](#الالتزام)

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

|  |  |  |
| --- | --- | --- |
| Control number | Reference in regulation controls | Relevant regulation |
| 1-2 | 1-2-1 | Essential Cybersecurity Controls (ECC) |