A picture containing boat, building, outdoor, water

Description automatically generated



**Cybersecurity Training for Professionals**

2023

### **Table of Contents**

[**Introduction 3**](#_Toc141266524)

[**Function 1 Governance Certifications 4**](#_Toc141266525)

[**Function 2 Defense Certifications 5**](#_Toc141266526)

[**Function 3 Response Certifications 6**](#_Toc141266527)

[**Function 4 Other Categories Certifications 7**](#_Toc141266528)

# Introduction

Cyber security is crucial in the digital world as most individuals' and enterprises' data are processed and stored online and within systems and devices. Protecting systems, networks, and data from unauthorized access and cyberattacks is vital by taking the proper actions and best practices obtained from international standards and certified institutes. Cybersecurity training and certifications qualify individuals with the necessary knowledge and skills, which leads to safeguarding information systems and data from cyber threats and ensuring adequate experience is obtained to protect the enterprises' assets and reduce cyber risks.

National Cyber Security Center (NCSC) encourages cybersecurity training by providing a list of NCSC approved internationally accredited certifications offered by global cybersecurity Institutes. This document lists the required cybersecurity certifications classified into three levels: foundation, intermediate, and expert. The foundation level requires implementing the basic cybersecurity measures, while the intermediate requires performing an advanced level of cybersecurity requirements, and the expert level requires the ability to establish robust defense with a deep understanding and proficiency in the field. This document was built in accordance with the National Cybersecurity Framework of Bahrain (NCFB).

NCFB was developed by the NCSC in alignment with Bahrain National Cyber Security Strategy (2020 – 2024) with the aim of minimizing the technological risks, maximizing the technological benefit, and heightening the cyber security environment throughout the kingdom. NCFB has addressed four main functions Governance, Defense, Response, and Other Categories. .ch function involves certain areas known as categories. The Governance function covers the processes, policies, and structures an organization uses to manage its cybersecurity risks, in addition to business continuity and compliance. The Defense function is technical protection measures that involve preventing attackers from gaining access to sensitive information or disrupting critical operations. The Response function is the process of taking action to mitigate the damage caused by a cyber attack. It is a critical component as it helps to ensure that the organization can recover quickly from an attack. The last function is other categories that require all the previously mentioned functions to operate, such as Cloud Computing and Industrial Control Systems, etc., as illustrated in Figure 1. The certifications in this document are categorized according to the NCFB's four functions.

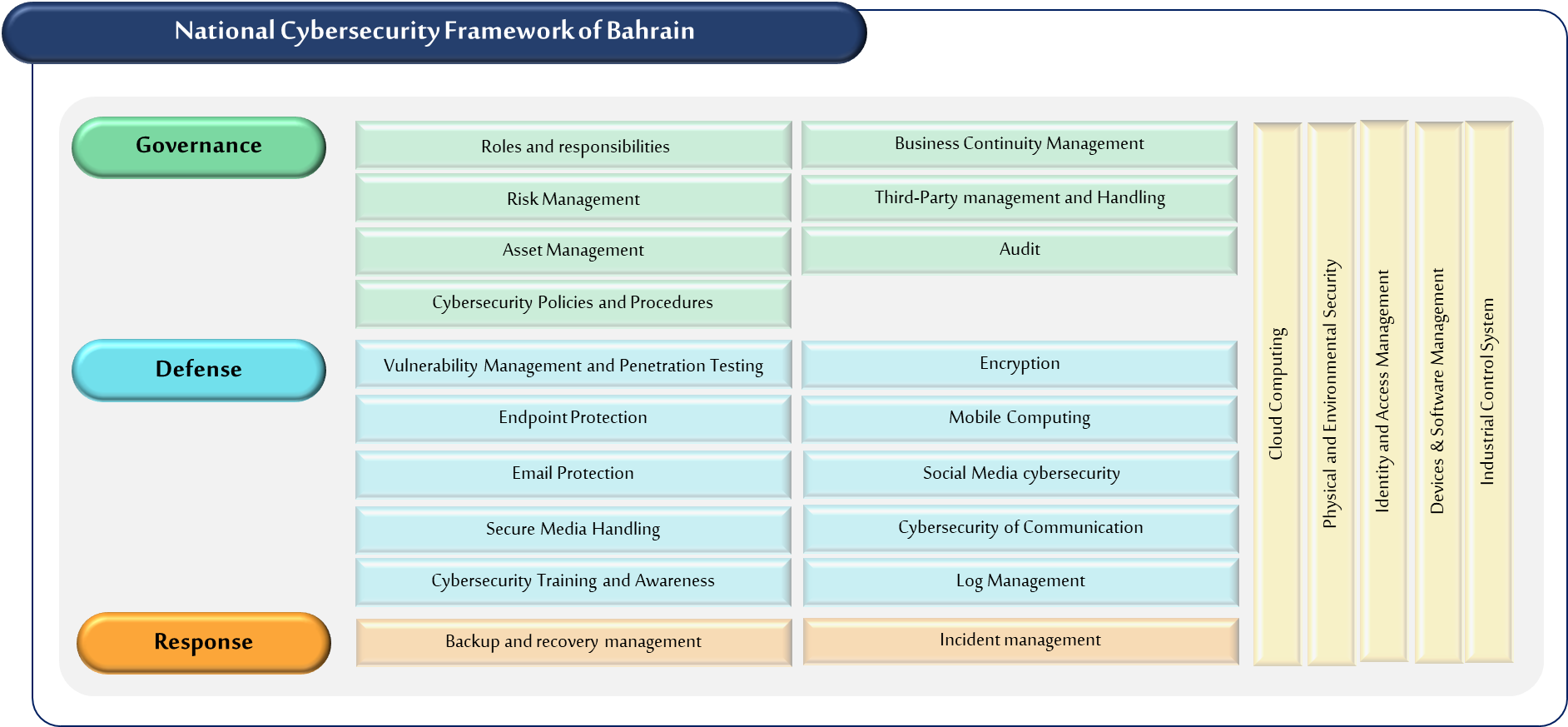


Figure 1: Bahrain National Cyber Security Framework

# Governance Certifications

This function aims to ensure that a set of processes, structures, and policies exists to direct the entity's approach to cybersecurity protection. It ensures the alignment of the cybersecurity program with the business objective by providing a strategic view of how cybersecurity will be controlled and handled. Therefore, seeking cybersecurity governance certifications which are approved by NCSC defined in Figure 2 is crucial for ensuring that an organization's cybersecurity policies and procedures are aligned with industry standards and best practices. The certifications addressed for this function cover the following categories: Roles and Responsibilities, Risk Management, Asset Management, Cybersecurity Policies and Procedures, Business Continuity Management, Third-Party Management, and Handling and Audit.

A table of information

Description automatically generated Several main skills should be considered when implementing cybersecurity governance it requires a combination of technical expertise, communication skills, and knowledge of cybersecurity frameworks, policies, and procedures. It is also important to determine roles and responsibilities in maintaining cybersecurity as well as having communication and collaboration skills to deliver policies and procedures effectively. Knowledge of cybersecurity frameworks is essential for understanding and implementing best practices and regulatory requirements including risk management framework. In addition, cybersecurity specialists are required to have expertise in asset management tools and maintain asset inventory. It is critical to successfully develop business continuity and incident response plans, besides understanding critical business processes and conducting business impact analyses. Furthermore, Knowledge of third-party risk management methodologies is necessary to manage third-party associated risks effectively. In addition, Technical expertise in cybersecurity concepts, strong analytical skills, and meticulous attention to detail are essential skills for assessing and auditing an organization's cybersecurity posture.

Figure 2: Cybersecurity governance certifications for all CNI sectors

# Defense Certifications

Defence function aims to provide defensible security measures to protect the entity’s environment from cyber-attacks. By having a strong cyber defense, organizations can reduce the risk of cyber-attacks and data breaches and safeguard their reputation, financial stability, and competitive advantage. The certifications addressed for this function which are defined in Figure 3, cover the following categories: Vulnerability Management and Penetration Testing, Endpoint Protection, Email Protection, Secure Media Handling, Cyber Training and Awareness, Encryption, Mobile Computing, Social Media Cyber Security, Cyber Security of Communications, and Log Management.

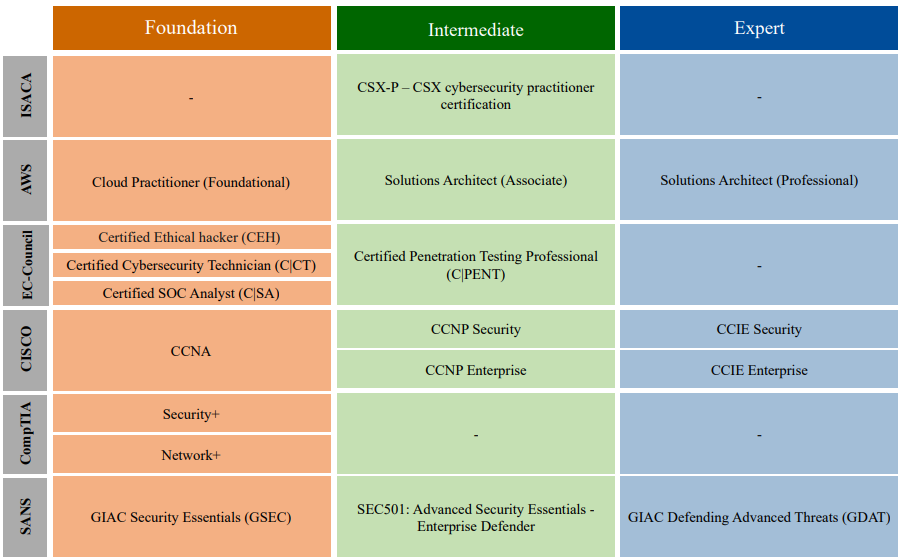
 Effective defense skills are essential for cybersecurity specialists to identify and mitigate potential cyber threats, prevent vulnerabilities, and conduct penetration testing which requires having the ability to detect, prioritize, and patch vulnerabilities. Moreover, obtaining technical deep knowledge in vulnerability scanning, penetration testing tools, operating systems, network infrastructure, endpoint protection, system installation & configurations is significant. Providing defense to the entity demand having hands-on in email security tools, secure handling of Media, encryption algorithms, encryption techniques, log management tools & systems, and social media cybersecurity protection. Also, delivering effective cybersecurity training and awareness programs is necessary to ensure employees are aware of common cybersecurity risks and adhere to established policies and procedures. Without these skills, an organization's security posture may be compromised, leading to an increased risk of successful cyberattacks.

Figure :Cybersecurity defense certifications for all CNI sectors

# Response Certifications

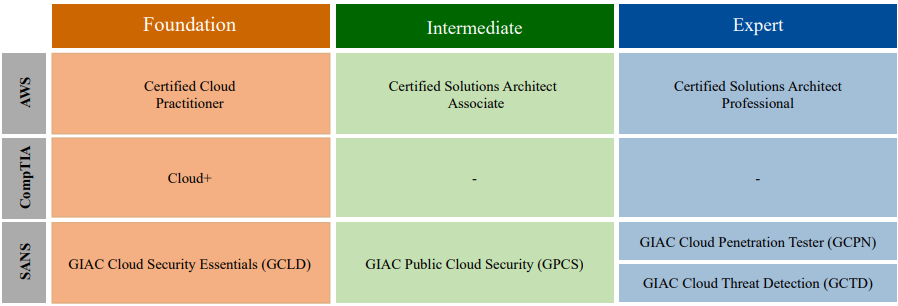
A table of information

Description automatically generatedThis function has a national power to contain and eradicate threats and incidents. Having excellent skills in cybersecurity response and obtaining relevant certifications are critical to ensure that an organization's cybersecurity policies and procedures are in line with industry standards and best practices. The response function skills and certifications, NCSC approved addressed in Figure 4, cover the following categories: Backup, recovery management, and Incident management.

cybersecurity specialist responsible for backup should possess a range of skills, including knowledge of backup and recovery tools and techniques, understanding of data storage and retrieval methods, and familiarity with disaster recovery planning and implementation. It is important to have the ability to assess the impact of data loss and system downtime, knowledge of backup scheduling and monitoring, expertise in recovery tools and techniques, comprehension of system and data architecture, and familiarity with disaster recovery planning and implementation. Responding to an incident required encompass proficiency in incident response frameworks and methodologies, knowledge of security tools and techniques, and the ability to assess the severity of security incidents. Moreover, understand forensic investigation techniques, and have excellent communication and collaboration skills.

Figure 4: Cybersecurity response certifications for all CNI sectors

# Other Categories Certifications

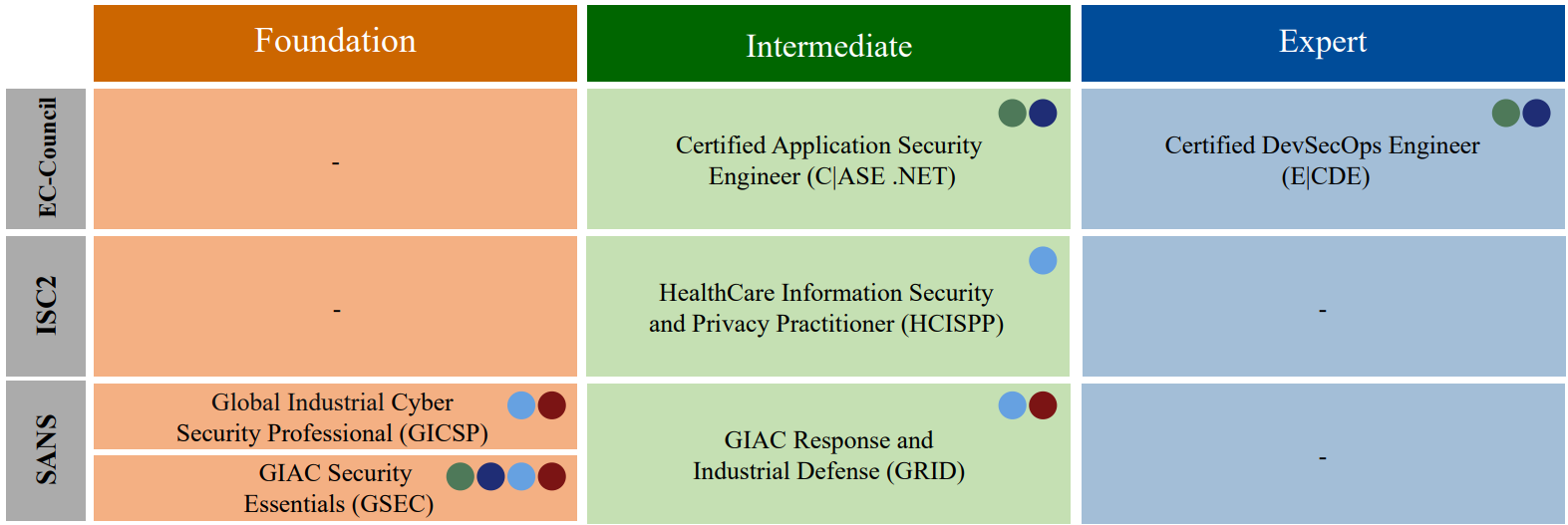
This function covers the categories that require operating all the previous functions, governance, defense, and response. The certifications addressed for this function cover the following categories: Cloud Computing, Identity and Access Management, Devices & Software Management, and Industrial Control Systems. Some certifications are applicable to all CNI sectors.

The skills required to manage and secure cloud-based systems and applications effectively are expertise in cloud computing & network architectures and technologies, familiarity with cloud security and compliance standards, and the capability to conduct cloud risk assessments. Managing and securing user identities, authentication, and authorization effectively required knowledge of Identity and Access Management (IAM) frameworks and technologies, an understanding of user behavior and risk management, ability to perform identity and access risk assessments. Securing Industrial Control Systems (ICS) networks, devices, and systems encompass expertise in ICS architectures and technologies, knowledge of government regulation, and cybersecurity national and international standards. The certifications that are crucial for cloud computing are mentioned in Figure 5. It contains the list of certifications approved by the NCSC and targets all CNI sectors. It is important to mention that this document does not recommend specific certifications for physical and environmental security.

Figure 5: Cloud Computing Certifications for all CNI

 NCSC approved certifications that could enhance identity and access management required skills as mentioned in Figure 6 bellow.

Figure 6:Identity and Access Management Certifications for all CNI sectors

Figure 7 includes a sector-specific approved which are government, financial, oil, electricity & gas, and critical industry

A red green and blue circles

Description automatically generated

Figure 7: Sector-specific Certifications

- End of the document –