الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

Regulatory Framework for Licensing Cybersecurity Services, Products and Solutions

(RFCS – 1: 2026)

TLP: Clear

Document Classification: Public

In the Name of Allah, The Most Gracious, The Most Merciful

Traffic Light Protocol (TLP):

This protocol is widely used around the world and comprises four colors (light signals):

Red (Personal and Confidential- for the Intended Recipient Only)

The recipient is not authorized to share the red-classified material with any individual, whether inside or outside the entity; sharing is strictly prohibited beyond the defined scope of receipt.

Amber+ Strict (Internal Sharing within the Same Entity)

The recipient may share the information only with the intended recipients inside the entity.

Amber (Restricted Sharing)

The recipient may share the information only with the intended recipients inside the entity or with recipients who are required to take action related to the shared information.

Green (Sharing within the Same Community)

The recipient may share the information with others within the same entity or with entities that have a relevant relationship or operate within the same sector; however, it is not permitted to disseminate or publish the information via public channels.

Clear (No Restrictions)

Table of Contents

Page

1. Introduction **4**

2. Definitions **5**

3. Framework Objectives **6**

4. Framework Scope **7**

5. License Domain **7**

6. Licensing Categories & Tiers **8**

7. Governance of Providing Licensed Cybersecurity Services, Products, or Solutions **11**

7.1 NCA Mandates & Operations as the National Authority in Charge of Cybersecurity in the Kingdom 11
7.2 Mechanism for Providing Services, Products and Solutions under Specialized License Category, excluding Cybersecurity Incident Response & Investigation Services ... 11
7.3 Mechanism for Providing Cybersecurity Incident Response & Investigation Services 12

8. Provisions of Licenses under Specialized License Category **13**

8.1 Requirements for Obtaining a License under Specialized License Category 13
8.2 Licensee Obligations under Specialized License Category 15
8.2.1 General Obligations 15
8.2.2 Special Obligations 18

9. Provisions of Licenses under General License Category **21**

9.1 Requirements for Obtaining a License under General License Category 21
9.2 Licensee Obligations under General License Category 21

10. License Request, Maintenance & Renewal **24**

11. License Transfer **25**

12. License Cancellation & Suspension **25**

13. Subcontracting **26**

14. General Provisions **27**

15. Appendices **28**

Appendix (A): Cybersecurity Services, Products, and Solutions 28
Appendix (B): Table of Financial Fees for Requesting the Licensing of Cybersecurity Services, Products, or Solutions 52

1. Introduction

The National Cybersecurity Authority (NCA) is the national entity in charge of cybersecurity in the Kingdom of Saudi Arabia and serves as the national authority and reference on its affairs, as per its Statute approved by virtue of Royal Order No. 6801, dated 31/10/2017. NCA aims to improve the cybersecurity posture of the kingdom in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities. NCA mandate includes, but not limited to setting cybersecurity policies, governance rules, frameworks, rules, standards, and directives; communicating the same to relevant agencies; monitoring compliance therewith; and updating them.. In addition, NCA mandate includes licensing individuals and non-government agencies to engage in cybersecurity activities and operations specified by the NCA., as well as stimulating the growth of the cybersecurity sector in the Kingdom and encouraging innovation and investment therein..

In its endeavor to ensure the provision of cybersecurity services, products, and solutions with the highest efficiency, effectiveness, and reliability in the Kingdom, in order to contribute to enhancing national cybersecurity and improving the services provided to national entities, and due to the importance of regulating the cybersecurity market in the Kingdom to create a stimulating environment that enhances the growth of the cybersecurity sector, NCA has issued this Framework to regulate the licensing process for providing cybersecurity services, products, and solutions in the Kingdom, outlining responsibilities and obligations of the licensee when providing any type of service, in addition to limiting the provision of such services only to qualified entities.

2. Definitions

The terms used in this Framework shall have the same meanings as stated in the table below, unless the context requires otherwise:

Term	Definition
NCA	National Cybersecurity Authority
Cybersecurity	The protection of networks, information technology systems, and operational technologies systems, including hardware and software, services provided thereby, and the data included therein, against hacking, disruption, modification, unauthorized access, and unlawful exploitation or use. Cybersecurity includes information security, electronic security, digital security, and the like.
HASEEN	A comprehensive national cybersecurity ecosystem through which NCA provides centralized and decentralized cybersecurity services and products at the national level to beneficiaries (government entities, critical national infrastructure entities, and private entities) in accordance with NCA's mandates and national cybersecurity regulatory requirements.
Framework	Regulatory Framework for Licensing Cybersecurity Services, Products and Solutions issued by NCA.
License	A document issued by NCA that permits practicing the provision of cybersecurity services, products, and solutions in the Kingdom, as determined by NCA.
Qualification Certificate	A document issued by NCA for a natural person establishing their eligibility to provide cybersecurity services, products, and solutions in the Kingdom, as determined by NCA.
Cyberspace	Networks and IT systems, operational technology systems, involving the Internet, communication networks, computer systems, Internet-connected devices, including hardware and software, the services provided thereby, and the data included therein.
Cybersecurity Threat	Any circumstance or event that can adversely impact networks, information technology systems, operational technologies systems, including hardware and software, services provided thereby, or the data included therein, whether such impact is through hacking, disruption, modification, unauthorized access, unlawful exploitation or use.

Cybersecurity Vulnerabilities	Weaknesses in networks, information technology systems, operational technologies systems, including hardware and software, services provided thereby, or the data included therein, which can lead to hacking, disruption, modification, unauthorized access, unlawful exploitation or use.
Cybersecurity Incident	Any event that occurs on networks, information technology systems, operational technologies systems, including hardware and software, services provided thereby, or the data included therein, be it hacking, disruption, modification, unauthorized access, unlawful exploitation or use.
Entity	Any natural or legal person providing or intends to provide cybersecurity-related services, products, or solutions to national entities in the Kingdom, be it public, private, or other entity, including any government entity in the Kingdom, its affiliates, private sector entities that own, operate, or host critical national infrastructure, and other private sector entities, associations, and non-profit organizations.
Beneficiary	The entity that contracts with an entity to obtain cybersecurity services, products, and solutions in the Kingdom.

3. Framework Objectives

This Framework aims to regulate the provision of cybersecurity services and products in the Kingdom through a regulatory framework that defines the responsibilities and obligations of the licensee, contributing to promoting the efficiency and quality of such services, products, and solutions during their delivery to various entities. The objectives that this Framework is seeking to realize are:

1. Contributing to enhancing cybersecurity in the Kingdom by providing high-quality cybersecurity services, products, and solutions, according to specific requirements.
2. Enabling national entities in the Kingdom to fulfil cybersecurity responsibilities and benefit from services, solutions, and products licensed by NCA.
3. Stimulating the growth of the cybersecurity sector in the Kingdom and enhancing its competitiveness.

4. Encouraging innovation and investment in cybersecurity sector by supporting the provision of innovative services and products that meet the growing demand for cybersecurity services and products.
5. Protecting the rights of all stakeholders under this Framework.
6. Enhancing the development of national human capabilities specialized in providing cybersecurity services, products, and solutions.

4. Framework Scope

This Framework applies to any entity that provides or intends to provide cybersecurity-related services, products, or solutions to entities across the Kingdom. This includes direct contracting with such entities, as well as indirect engagement through collaboration with a licensed entity. This excludes the licensing for Managed Security Operations Center (MSOC) services, as licensing such service is regulated by the Regulatory Framework for Licensing Managed Security Operations Center (MSOC) Services.

5. License Domains

Based on the classification of cybersecurity services and products in the Kingdom, license domains have been divided into (5) main domains, comprising (25) subdomains, covering various services, products, and solutions. Figure (1) illustrates main domains and subdomains for classifying cybersecurity services, products, and solutions in the Kingdom. Appendix (1) includes a list of all cybersecurity services, products, and solutions according to NCA classification.

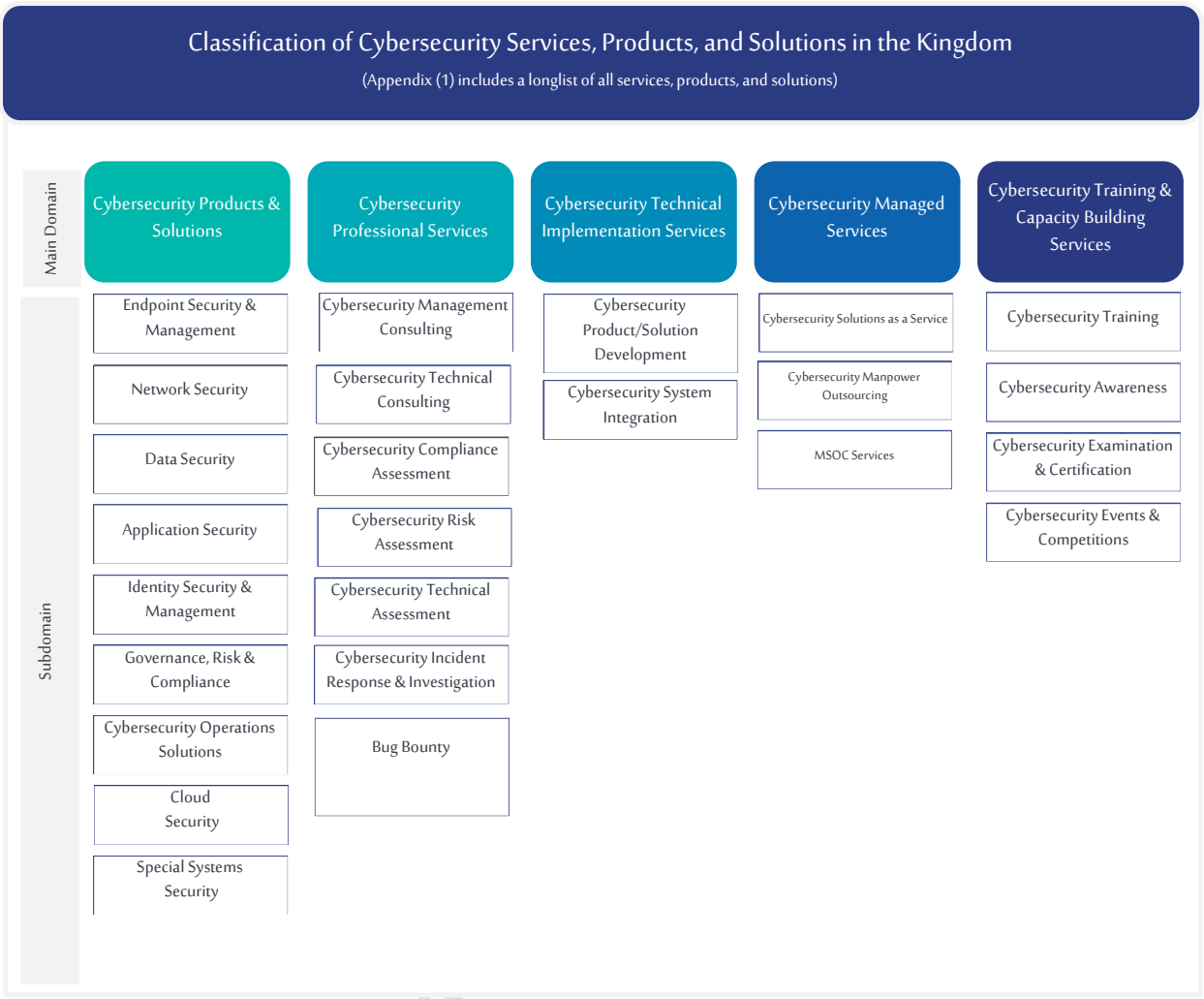

FIGURE (1)

6. Licensing Categories & Tiers

Based on licensing domains under Section (5), specifically the 25 subdomains, NCA will issue 4 license types, which are based on 2 categories and 2 tiers, as specified below:

- **Specialized License Category:** The entity must obtain this license before commencing the provision of a number of **critical** specialized cybersecurity services. Figure (2) illustrates subdomains under this category. Two tiers will be issued within this category (Specialized-1 or Specialized-2), where the licensee at each tier can work with a specific segment of entities.
- **General License Category:** The entity must obtain this license before commencing the provision of a number of cybersecurity services, products or solutions. Figure (2) illustrates

subdomains under this category. Two tiers will be issued within this category (General-1 or General-2), where the licensee at each tier can work with a specific segment of entities.

The following figure outlines the required licensing categories according to each subdomains based on the Classification of Cybersecurity Services, Products, and Solutions in the Kingdom, under Section (5):

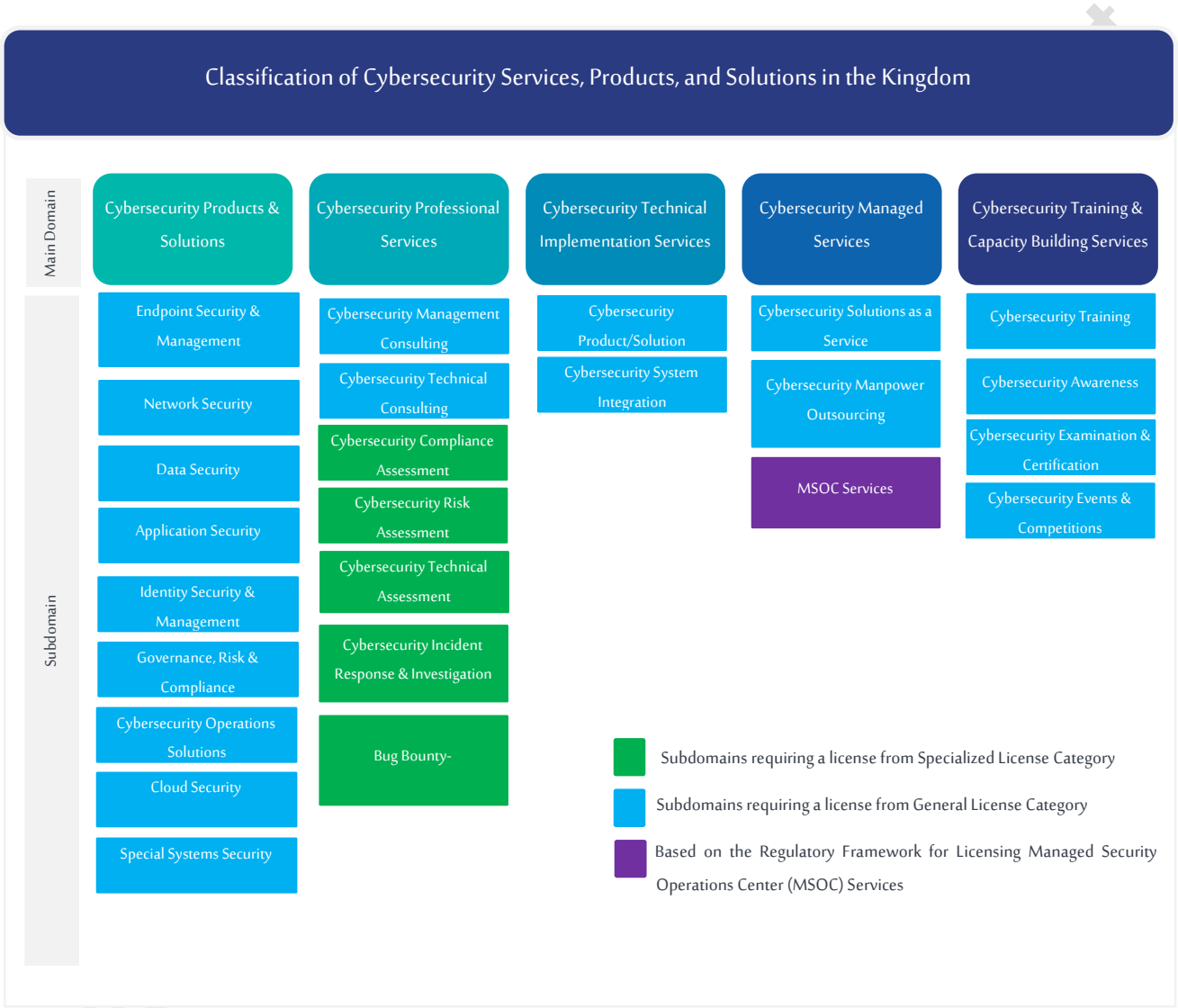

FIGURE (2)

Figure (3) below details license categories, including category definition and tiers:

Specialized License Category	
The entity must obtain this license before commencing the provision of a number of critical specialized cybersecurity services.	
Tier I of Specialized License Category (Specialized - 1)	
License Details	(Specialized - 1) license is granted to entities that meet the provisions outlined in Section (8).
License Scope	(Specialized - 1) license allows the licensee to work with all national entities in the Kingdom, including government entities, and entities that own, operate or host critical infrastructure, for the provision of services specified under Specialized License Category (Figure 2).
Tier II of Specialized License Category (Specialized - 2)	
License Details	(Specialized - 2) license is granted to entities that meet the provisions outlined in Section (8); License under this Tier does not cover Cybersecurity Incident Response and Investigation services, as these services will only be licensed at Tier I.
License Scope	(Specialized - 2) license allows the licensee to work with non-governmental entities, and entities that do not own, operate or host critical infrastructure, for the provision of services specified under Specialized License Category (Figure 2).

General License Category	
The entity must obtain this license before commencing the provision of a number of cybersecurity services, products or solutions.	
Tier I of General License Category (General - 1)	
License Details	(General - 1) license is granted to entities that meet the provisions outlined in Section (9).
License Scope	(General - 1) license allows the licensee to work with all national entities in the Kingdom, including government entities, and entities that own, operate or host critical infrastructure, for the provision of services, products, or solutions specified under General License Category (Figure 2).
Tier II of General License Category (General - 2)	
License Details	(General - 2) license is granted to entities that meet the provisions outlined in Section (9).
License Scope	(General - 2) license allows the licensee to work with non-governmental entities, and entities that do not own, operate or host critical infrastructure, for the provision of services, products, or solutions specified under General License Category (Figure 2).

FIGURE (3)

7. Governance of Providing Licensed Cybersecurity Services, Products, or Solutions

7.1 NCA Mandates & Operations as the National Authority in Charge of Cybersecurity in the Kingdom

To fulfill its mandates as per its Statue issued under Royal Order No. 6801, dated 31/10/2017, aimed at fostering the cybersecurity posture of the Kingdom in order to safeguard its vital interests and national security, NCA provides a number of critical cybersecurity services centrally and directly to national entities (especially government and private sector entities that own, operate, or host national critical infrastructure). Such services include conducting assessments of compliance with controls, standards, and frameworks and other regulatory requirements issued by NCA, cybersecurity risk assessments, cybersecurity technical assessments, as well as responding to cybersecurity incidents among others. Figure (4) illustrates how such services provided through HASEEN, where NCA executes its mandates through service request and assignment to (HASEEN) operator, who in turn carries out such mandates in coordination with national entities (public, private, and others).

7.2 Mechanism for Providing Services, Products and Solutions under Specialized License Category, excluding Cybersecurity Incident Response & Investigation Services

To fulfill their cybersecurity responsibilities, national entities have to take measures to enhance cybersecurity readiness at both the entity and internal operational process levels, ensuring full and continuous compliance with NCA cybersecurity policies, governance mechanisms, frameworks, standards, controls, and guidelines. This includes, for example, conducting preparatory

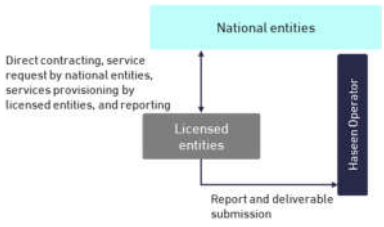

FIGURE (5)

and indicative assessments prior to NCA official assessment via HASEEN, or assessments conducted before launch of e-services, including compliance assessments, technical assessments, or cybersecurity risk assessments, among others. If needed, national entities (public, private, and others) can contract with a licensee under Specialized License Category as per the associated Tier to deliver such services. The licensee shall provide NCA with all documents, information, and data related to services provided, as well as deliverables and results of executing the services through HASEEN according to the approved forms. All licensees must inform HASEEN of all activities carried out before, during, and after provision of the service. Figure (5) illustrates how these services are rendered.

7.3 Mechanism for Providing Cybersecurity Incident Response & Investigation Services

In case any national entity (public, private, or other) suspects or detects a cybersecurity incident, it must report such incident immediately via HASEEN or NCA official channels such the number (936). The cybersecurity incident will be classified and prioritized (Triage Process) through HASEEN, followed by directions to complete necessary procedures as follows:

A. If the cybersecurity incident classified under Level I, II, or III, HASEEN will promptly respond to the entity's cybersecurity incident.
B. If the cybersecurity incident classified under Level IV or V, the MSOC licensee will provide necessary support to handle the incident according to license requirements, and the national entity may seek any licensee to provide incident response services when needed, who in turn shall deliver the services. In such case, the licensee shall enter into an agreement with HASEEN operator and proceed as per HASEEN methodology. The licensee shall also provide NCA with all related documents, information, and data, as well as the outputs of HASEEN services as per the applicable forms. All licensees must inform HASEEN of all activities carried out before, during, and after provision of the service. NCA reserves at its discretion the right to respned directly to a Level IV or V cybersecurity incident as appropriate.

8. Provisions of Licenses under Specialized License Category[1]

8.1 Requirements for Obtaining a License under Specialized License Category

Any entity seeking a Tier I or Tier II license to provide any cybersecurity service under Specialized License Category outlined in Section (6) shall meet the requirements for obtaining, renewing, and maintaining the license, as detailed in the table below:

General Requirements		
Requirements	Tier I Requirements under Specialized License Category (Specialized - 1)	Tier II Requirements under Specialized License Category (Specialized - 2)
Regulatory Requirements	• The license applicant shall be a legally established entity in the Kingdom. • The license application form shall be filled and submitted. • The license applicant shall provide the entity's ownership data (direct and indirect), relevant information (the articles of association, incorporation contract, commercial registration, along with a list of all controlling persons, indicating their number and the percentage of ownership owned by each of them), the entity's organizational structure, and the percentage of Saudization for leadership positions. • The license applicant shall provide NCA with the entity's data (national address document, authorized representative appointment form signed and stamped by the Chamber of Commerce, and Foreign Investment Registration Certificate from Ministry of Investment in case of foreign ownership). • Cybersecurity must be one of the entity's core activities.	
Entity Requirements	• The ownership of the Saudi citizen(s) to the stakes or shares (whether direct or indirect ownership through companies that	• The ownership of the Saudi citizen(s) to the stakes or shares (whether direct or indirect ownership through companies that are fully or partially owned by one

[1] Excluding licensing for Managed Security Operations Center (MSOC) services, as licensing such service is regulated by the Regulatory Framework for Licensing Managed Security Operations Center (MSOC) Services.

	are fully or partially owned by one or more citizens) in the entity requesting a license shall not be less than 75%. • The entity shall have high technical capabilities and operational efficiency, the ability to comply with service provision conditions, and must demonstrate high maturity in both operations conducted and tier of cybersecurity, along with its ability to ensure quality and operational continuity.	or more citizens) in the entity requesting a license shall not be less than 25%. • The entity shall have appropriate technical capabilities and operational efficiency, the ability to comply with service provision conditions, and must demonstrate appropriate maturity in both operations conducted and tier of cybersecurity, along with its ability to ensure quality and operational continuity.
Capital	• The entity applying for Tier I license under Specialized License Category shall have a capital of no less than (10) million SAR.	• The entity applying for Tier II license under Specialized License Category shall have a capital of no less than (500) thousand SAR.
Technical Requirements	• The entity shall submit initial/estimated service delivery plan, indicating the number of employees for each service and service delivery mechanism. • The entity must meet HASEEN qualification requirements, including passing technical assessment and cybersecurity compliance assessment issued by NCA, which apply to the licensee, as per NCA instructions and requirements.	
Functional Separation & Segregation of Duties	The entity must ensure that teams are separated to avoid conflicts of interest.	
Qualified Personnel	Services must be provided by qualified and experienced personnel holding a qualification certificate, as specified by NCA.	

8.2 Licensee Obligations under Specialized License Category

8.2.1 General Obligations

The licensee shall always adhere to the provisions in this Framework and the decisions, regulations, frameworks, controls, instructions, directions, circulars and the like issued by NCA. The licensee is obliged to:

8.2.1.1 Adhering to the enforced laws, regulations, and instructions in the Kingdom of Saudi Arabia.

8.2.1.2 Starting to provide licensed services within (3) months as a maximum from the date of license issuance, unless NCA decides otherwise.

8.2.1.3 Adhering to localization requirements, keeping all relevant information and data created before, during, or after service provision within the Kingdom, and not storing or copying them outside the Kingdom.

8.2.1.4 Implementing the licensed services and providing services to national entities (public, private, or others) from within the Kingdom.

8.2.1.5 Ensuring that service-related data is processed and stored within the Kingdom, with no access permitted from outside the Kingdom.

8.2.1.6 Adhering to HASEEN service provision methods, and providing NCA with all relevant documents, information, and data, as well as service outputs through HASEEN within the specified timeframe.

8.2.1.7 Complying with all responsibilities and obligations when providing services to national entities, according to NCA instructions.

8.2.1.8 Implementing the security and cybersecurity recommendations or requirements shared by NCA, including cyber alerts, threat detection rules, and indicators of compromise. Furthermore, providing NCA with the results according to the requirements and the specified period.

8.2.1.9 Providing NCA with periodic reports - as decided by NCA - and any other information NCA requests, and to adhere to the deadlines, methods, and templates prescribed for this. Reports may include, but are not limited to, cybersecurity assessments conducted, cybersecurity incidents addressed, beneficiaries, etc.

8.2.1.10 Refraining from publishing any data related to cybersecurity and any related information gathered by the licensee while providing services to national entities (public, private or others) in the Kingdom before obtaining written approval from NCA.

8.2.1.11 Refraining from publishing and/or sharing any data related to national entities (public, private or others) served by the licensee, whether individually or after aggregating that data or information, with any party for any justification or purpose, including government or private entities, inside and outside the Kingdom before obtaining written approval from NCA.

8.2.1.12 Stating in its contracts related to this Framework the provisions that address cases of license expiration, non-renewal, or cancellation.

8.2.1.13 Implementing the necessary procedures in the event of the expiration or termination of the contractual relationship with national entities (public, private or others) in accordance with NCA decisions.

8.2.1.14 When the services of cloud service provider (CSP) are needed, a licensed CSP by relevant authority in KSA shall be contracted before utilizing the services.

8.2.1.15 Informing NCA immediately of any change in information or data related to the license application and/or upon discovery of any information that is inaccurate or contrary to the reality of what was reported to NCA indicating the reasons of inaccurate or incorrect submission and the reason for the change in it.

8.2.1.16 Informing NCA immediately of any actual or potential risk, threat, or breach detected by the licensee at the national entity (public, private or others).

8.2.1.17 Informing NCA immediately of any legal or regulatory action against the licensee that may impact providing services, regardless of the regulatory body or jurisdiction, and whether it is from inside or outside the Kingdom.

8.2.1.18 Submitting financial statements audited by an independent licensed auditor in accordance with the laws of the Kingdom, showing revenues from providing cybersecurity services, products, or solutions for each fiscal year throughout the license period.

8.2.1.19 Fully cooperating with NCA when exercising its regulatory and supervisory authority on the licensee and making available all its possible resources to implement any oversight and inspection requirements from NCA, including audits, verifications,

cybersecurity assessments and any other requirements on their business and systems, whatever they may be.

8.2.1.20 Providing NCA with all documents, data, information and reports that prove their compliance with NCA's requirements and regulations, including, but not limited to, the following:

8.2.1.19.1 Financial performance information for cybersecurity activities, including revenues and its sources, capital, technology investments, infrastructure investments, and training and development expenses.

8.2.1.19.2 Information about the cybersecurity services provided, the beneficiaries of the services, their numbers and names, the type of services provided to them and meetings and interactions with them, etc.

8.2.1.19.3 Information about the licensee's employees involved in providing services within Specialized License Category, and other services as deemed necessary by NCA, including the number of employees, their CVs and qualifications, etc.

8.2.1.19.4 Information about the technical requirements imposed on the licensee, technology tools and subscriptions, any IT infrastructure related to implementing cybersecurity services by the licensed entity, etc.

8.2.1.19.5 Any evidence, document, or proof required by NCA, for the purpose of verifying the compliance of the licensee with the provisions outlined in this Framework, and other documents issued by NCA, and other relevant entities.

8.2.1.21 Adhering to local content and localization percentages for jobs, as determined by NCA and relevant authorities.

8.2.1.22 Complying with the decisions issued by NCA in any disputes that may arise with beneficiaries regarding the services provided under the license.

8.2.1.23 Fully and continually applying all cybersecurity controls issued by NCA that apply to the licensee; including but not limited to, Essential Cybersecurity Controls (ECC), Critical Systems Cybersecurity Controls (CSCC), and Data Cybersecurity Controls (DCC); and submitting annual documentation of compliance with the controls approved by NCA.

8.2.1.24 Adhering to notify NCA immediately if any change occurs in the ownership of the licensed entity in any way.

8.2.1.25 Adhering to obtain NCA's prior written approval before taking any action that would result in a change in the ownership of the licensed entity in any way.

8.2.2 Special Obligations

8.2.2.1 Obligations on Providing Cybersecurity Compliance Assessment, Cybersecurity Risk Assessment, and Cybersecurity Technical Assessment Services

8.2.2.1.1 The licensee shall conduct assessments according to a specific and systematic mechanism that includes developing a comprehensive final report for the assessments of various types in accordance with HASEEN methodologies and frameworks, and submit the same through HASEEN in the format specified by NCA within the specified timeframe.

8.2.2.1.2 The licensee must follow clear methodologies for conducting compliance assessments, which should include criteria for acceptable evidence and standards that determine the entity's performance being assessed in such category; NCA reserves the right to specify the evaluation mechanism, its methodology, and its contents, as well as to make any amendments or remove any of its elements.

8.2.2.1.3 The licensee shall conduct assessments through qualified and experienced Saudi personnel holding academic qualifications and certifications in cybersecurity or related fields, and must be seasoned in assessments, as specified by NCA.

8.2.2.1.4 The licensee shall maintain accurate and complete records of the assessments provided to beneficiaries for a period of five (5) years from the date those services were rendered; such records should include, but are not limited to, the service provision date, name of the beneficiary, details of personnel involved in delivering the service, detailed assessment results, and any third parties involved in providing any part of the assessment services.

8.2.2.2 Obligations on Providing Bug Bounty Programs

8.2.2.2.1 Limiting participation in bug bounty programs to citizens and residents of the Kingdom who meet the necessary requirements.

8.2.2.2.2 The scope of the programs must be limited to assets that are not likely to affect national security, and to public-facing assets, excluding operational systems and social engineering.

8.2.2.2.3 Bug bounty program platforms must have the following features: (1) Statistics and real-time tracking of activities on the platform, e.g. average resolution time, number of rewards paid, and number of vulnerabilities detected. (2) Participating entities ability to select the participating researchers. (3) The ability to generate reports and data for entities.

8.2.2.2.4 Verify the identities of platform users and maintain platform records for at least five (5) years.

8.2.2.2.5 Grant NCA the right to directly access information and data of the bug bounty program platforms.

8.2.2.2.6 Obtain approval and sign NDA between researchers and platform participant entities before providing the service.

8.2.2.2.7 Privacy policies on bug bounty program platforms must adhere to National Data Governance Policies issued by the relevant authority, the Personal Data Protection Law and relevant regulations applicable in the Kingdom.

8.2.2.3 Obligations on Providing Cybersecurity Incident Response & Investigation Services (Only licensed within Tier I under Specialized License Category "Specialized - 1")

8.2.2.3.1 The licensee shall establish a clear Service Level Agreement (SLA) with national entities (public, private, or others).

8.2.2.3.2 The licensee shall employ (full-time) cybersecurity incident response specialists who are Saudi citizens, as specified by NCA.

8.2.2.3.3 The licensee shall provide cybersecurity incident response and investigation services through qualified and experienced Saudi personnel holding academic qualifications

and certifications in cybersecurity or related fields, and must be seasoned in incident response and investigation, as specified by NCA.

8.2.2.3.4 The licensee shall maintain accurate and complete records of cybersecurity incidents responded to and investigated for a period of twenty five (25) years from the date those services were rendered; such records should include, but are not limited to, the service provision date, name of the beneficiary, details of incident responders involved in delivering the service, and any third parties involved in providing any part of incident response services.

8.2.2.3.5 The licensee shall retain accurate and complete copies of digital evidence related to cybersecurity incidents they responded to and investigated for a minimum of ten (10) years from the date of providing those services. This includes, but is not limited to, system logs, digital copies of hard drives, RAM, and other data. The licensee shall ensure that these copies remain undamaged, unaltered, and untampered with during collection and storage. This information shall not be destroyed before being handed over to the National Cybersecurity Authority.

8.2.2.3.6 The licensee shall conduct an analysis and provide actionable measures to the entity affected by the cybersecurity incident. The licensee is also responsible for reviewing the incident and providing lessons learned to the affected entity after completion.

8.2.2.3.7 The licensee shall follow a systematic mechanism for providing incident response services that includes preparing a comprehensive final report detailing the incident, according to NCA methodologies and models, and submit such report in the format specified by NCA; NCA reserves the right to specify the incident response mechanism, its methodology, and its contents, as well as to make any amendments or remove any of its elements.

8.2.2.3.8 The licensee must operate according to the Mechanism for Providing Cybersecurity Incident Response & Investigation Services outlined in Section (7.3).

9. Provisions of Licenses under General License Category

9.1 Requirements for Obtaining a License under General License Category

Any entity seeking a Tier I or Tier II license to provide any cybersecurity services, products, or solutions under General License Category outlined in Section (6) shall meet the requirements for obtaining, renewing, and maintaining the license, as detailed in the table below:

General Requirements		
Requirements	Tier I Requirements under General License Category (General - 1)	Tier II Requirements under General License Category (General - 2)
Regulatory Requirements	• The license applicant shall be a legally established entity in the Kingdom. • The license application form shall be filled and submitted. • The license applicant shall provide NCA with the entity's data (commercial registration, articles of association, national address document, authorized representative appointment form signed and stamped by the Chamber of Commerce, and Foreign Investment Registration Certificate from Ministry of Investment in case of foreign ownership). • The license applicant must pass the necessary qualification requirements from HASEEN. • The entity shall have a website indicating the entity's branches and cybersecurity services, products or solutions offered, along with proof of the entity's website ownership.	
Requirements on Entity's Business Activity	• Cybersecurity must be one of the entity's core activities. • The entity applying for a license under General License Category shall have a capital of no less than (500) thousand SAR.	

9.2 Licensee Obligations under General License Category

The licensee shall always adhere to the provisions in this Framework and the decisions, regulations, frameworks, controls, instructions, directions, circulars and the like issued by NCA. The licensee is obliged to:

9.2.1 Adhering to the enforced laws, regulations, and instructions in the Kingdom of Saudi Arabia.

9.2.2 Starting to provide licensed services within (3) months as a maximum from the date of license issuance, unless NCA decides otherwise.

9.2.3 Adhering to localization requirements, keeping all relevant information and data created before, during, or after delivering the services or products within the Kingdom, and not storing or copying them outside the Kingdom.

9.2.4 Implementing the security and cybersecurity recommendations or requirements shared by NCA, including cyber alerts, threat detection rules, and indicators of compromise. Furthermore, providing NCA with the results according to the requirements and the specified period.

9.2.5 Refraining from publishing any data related to cybersecurity and any related information before obtaining written approval from NCA.

9.2.6 Refraining from publishing and/or sharing any data related to national entities (public, private or others) served by the licensee, whether individually or after aggregating that data or information, with any party for any justification or purpose, including government or private entities, inside and outside the Kingdom before obtaining written approval from NCA.

9.2.7 Stating in its contracts related to this Framework the provisions that address cases of license expiration, non-renewal, or cancellation.

9.2.8 Informing NCA immediately of any change in information or data related to the license application and/or the licensee and/or upon discovery of any information that is inaccurate or contrary to the reality of what was reported to NCA indicating the reasons of inaccurate or incorrect submission and the reason for the change in it.

9.2.9 Informing NCA immediately of any legal or regulatory action against the licensee that may impact providing services, regardless of the regulatory body or jurisdiction, and whether it is from inside or outside the Kingdom.

9.2.10 Fully cooperating with NCA when exercising its regulatory and supervisory authority on the licensee and making available all its possible resources to implement any oversight and inspection requirements from NCA, including audits, verifications, cybersecurity assessments and any other requirements on their business and systems, whatever they may be.

9.2.11 Complying with the decisions issued by NCA in any disputes that may arise with beneficiaries.

9.2.12 Adhering to local content and localization percentages for jobs, as determined by NCA and relevant authorities.

9.2.13 Complying with all responsibilities and obligations when providing cybersecurity services, products, or solutions to national entities, according to NCA instructions.

9.2.14 Fully and continually applying all cybersecurity controls issued by NCA that apply to the licensee; including but not limited to, Essential Cybersecurity Controls (ECC), Critical Systems Cybersecurity Controls (CSCC), and Data Cybersecurity Controls (DCC); and submitting annual documentation of compliance with the controls approved by NCA.

9.2.15 Adhering to notify NCA immediately if any change occurs in the ownership of the licensed entity in any way.

9.2.16 Adhering to obtain NCA's prior written approval before taking any action that would result in a change in the ownership of the licensed entity in any way.

9.2.17 Complying with the decisions issued by NCA in any disputes that may arise with beneficiaries regarding the services, products, or solutions provided under the license.

9.2.18 Providing NCA with periodic reports - as decided by NCA - and any other information NCA requests, and to adhere to the deadlines, methods, and templates prescribed for this. Reports may include, but are not limited to, services, products, or solutions provided to beneficiaries, etc.

9.2.19 The licensee providing cybersecurity services, products, and solutions shall maintain accurate and complete records of the cybersecurity services, products, and solutions provided to beneficiaries for a period of five (5) years from the date of service provision; such records should include, but are not limited to, the date of service provision, name of the beneficiary, and any third party involved in delivering any part of the cybersecurity services, products, and solutions.

9.2.20 The licensee operating within subdomains related to delivering cybersecurity products and solutions shall adhere to the following:

9.2.20.1 Provide NCA with details of the product or solution and users in the Kingdom on a regular basis.

9.2.20.2 Inform NCA immediately of any critical vulnerabilities, cybersecurity risks, or data breach incidents discovered or alerted regarding the products or solutions provided, and submit an initial remediation plan to NCA within a short period through HASEEN.

9.2.20.3 Provide a team available 24/7 to communicate with NCA regarding any issues related to risks and threats that may arise regarding the product or solution.

9.2.20.4 Conduct necessary cybersecurity assessments to ensure the security of cybersecurity products or solutions provided by the licensee, as per NCA instructions.

9.2.20.5 Use encryption and data protection mechanisms when transmitting data over networks using internationally recognized algorithms or encryption algorithms, as per NCA instructions.

9.2.20.6 Follow an approved methodology for secure software development.

9.2.20.7 Comply with all standards or controls for the clearance and licensing of importing, exporting, and using highly senstive cybersecurity hardware and software defined by NCA.

10. License Request, Maintenance & Renewal

10.1 To obtain a license for providing services under Specialized License Category, a request shall be submitted to NCA and that request shall meet the requirements outlined in Section (8.1) and in the Appendix (B) in this Framework, according the license tier.

10.2 To obtain a license for providing services under General License Category, a request shall be submitted to NCA and that request shall meet the requirements outlined in Section (9.1), and in the Appendix (B) in this Framework, according the license tier.

10.3 The license for providing cybersecurity services, products or solutions will be valid for five (5) years starting from the date of license issuance.

10.4 The licensee shall continue to fulfil the requirements outlined in Sections (8.1) and (8.2) and Appendix (B) of this Framework to maintain the license according to its Tier and type of service under the Specialized License Category.

10.5 The licensee shall continue to fulfil the requirements outlined in Sections (9.1) and (9.2) and Appendix (B) of this Framework to maintain the license under the General License Category.

10.6 The licensee may submit a license renewal request not earlier than (90) calendar days prior to the license expiry date and not later than (30) calendar days prior to the license expiry date. The license renewal request shall meet all related regulatory requirements outlined in this Framework and any other related requirements imposed by NCA.

10.7 If the licensee does not desire to renew the license, or if NCA rejects the submitted license renewal request, or if the licensee has submitted a license cancellation request, in any of these cases, the licensee shall not enter any new contracts under the scope of the license and shall inform the service beneficiaries of that according to the decision of NCA.

11. License Transfer

11.1 The licensee shall not transfer their license without obtaining a prior written approval from NCA.

11.2 The licensee, who desires to transfer their license, shall submit a written request to NCA, including the reasons and rationales for the transfer request; and submit any information or additional documents requested by NCA while processing the request.

11.3 NCA will issue its decision on the transfer request and the licensee shall adhere to it.

12. License Cancellation & Suspension

12.1 The licensee who desires to cancel the issued license shall submit a written request to NCA, including the reasons and rationales for the cancellation request; and submit any information or additional documents requested by NCA while processing the request. After receiving the completed cancellation request from the licensee, NCA issues its decision on the request and the licensee shall adhere to it.

12.2 NCA, at its discretion, reserves the right to cancel or suspend the license in cases it deems necessary, such as but not limited to the case where the licensee:

A. Fails to comply with the provisions outlined in this Framework and any modifications to it.

B. Fails to comply with any regulatory documents or requirements issued by NCA, including but not limited to decisions, regulations, frameworks, instructions, directions, circulars, controls and the like.

C. Repeatedly fails to fulfill their obligations outlined in this Framework and any relevant NCA regulations.

12.3 The license suspension period shall have no effect on the license expiry date, as the suspension period will be counted as part of the license duration.

12.4 NCA, at its sole discretion, will lift the license suspension after the licensee has taken the necessary corrective measures communicated by NCA, and NCA acceptance of these corrective measures implementation/application.

12.5 The licensee may not, in any way or form, provide services within the scope of the license upon license expiration, cancellation, or suspension.

13. Subcontracting

13.1 The licensee may not subcontract except through other licensees within the same category and tier they hold a license for. Therefore, Tier I licensees under Specialized License Category (Specialized - 1) may only subcontract through Tier I licensees under Specialized License Category (Specialized - 1). The same hold true for all license types. The licensee may not subcontract to provide cybersecurity services, products, or solutions except through another licensee for the same service, product, or solution.

13.2 The licensee may subcontract cybersecurity services, products, or solutions according to the following conditions:

13.2.1 Submit a written request to NCA in accordance with the requirements determined by NCA.

13.2.2 Prohibit the subcontracted entity from commencing any work prior to obtaining the approval from NCA on the submitted subcontracting request.

13.2.3 All licensee obligations emerging from licensing in this Framework toward NCA shall be the responsibility of the main licensee. Any requirements or conditions that violate these obligations toward NCA in the contracts between the licensee and sub-contractors shall be regarded as invalid with no legal implications by NCA.

13.2.4 Subcontracting arrangements under this Section shall be documented in the internal logs of the licensee in addition to compliance with related NCA instructions.

13.3 NCA may, at its discretion, set a cap for subcontracts for the Tier I licensee.

13.4 Under all circumstances, the subcontractor shall fulfil all obligations of the licensee under this Framework.

14. General Provisions

14.1 Any entity that provides or desires to provide cybersecurity services, products, or solutions in the Kingdom shall obtain a license to do so from NCA, in accordance with the provisions outlined in this Framework and NCA's decisions.

14.2 NCA will determine a grace period for entities providing cybersecurity services and activities that fall under the scope of this Framework. Such entities shall rectify their status in-line with this Framework and what NCA issues.

14.3 NCA will issue the relevant instructions and controls that shall be applied to all current and future contracts with the entities that fall under the scope of this Framework.

14.4 The entities that fall under the scope of this Framework shall submit all the documents, information, and contracts relevant to these services as well as any information requested by NCA at its discretion within a period not exceeding thirty (30) days from the effective date of this Framework.

14.5 NCA, pursuant to sector regulation requirements, may impose additional conditions or requirements, or cancel existing ones, on licensees or holders of qualification certificates.

14.6 NCA reserves the right to reject any license issuance, renewal or cancelation requests, pursuant to this Framework.

14.7 Licensees shall submit periodic reports to NCA as well as any other information NCA may request at its discretion.

14.8 Taking into consideration the provisions in this Framework regarding the cancellation or suspension of the license, NCA, based on its regulatory mandate, will take the necessary decisions to address any incurred violations pursuant to this Framework.

14.9 NCA reserves the right to impose other fees on the licensees.

14.10 Appendices contained in this Framework, shall be considered an integral part of this Framework and shall be read and enforced as a single unit.

14.11 The Arabic version of this Framework shall be the official and approved version. In case of any discrepancies between the Arabic text and any other foreign translation, the Arabic text shall prevail.

14.12 NCA reserves the right to revise and update this Framework in accordance with the requirements of regulating the cybersecurity sector, and any updates thereto shall be adhered to in accordance with NCA's decisions.

14.13 NCA reserves the right to withhold, cancel, or suspend the license in order to protect national security, provided that its decision is based on objective grounds and in coordination with relevant authorities.

15. Appendices

Appendix (A): Cybersecurity Services, Products, and Solutions

1	Cybersecurity Products & Solutions		
1-1	Endpoint Security & Management		
Cybersecurity solutions to protect endpoints, covering servers, workstations and mobile devices.			License Category to Provide Service/Product/Solution
1-1-1	Browser Security Solutions	Endpoint security solutions to secure web browsers, hardened local browsers, and browser add-ons.	General License Category

1-1-2	Endpoint Protection Solutions	Endpoint security solutions to secure PCs, servers, etc., by detecting and preventing malware, viruses, trojans, ransomware, etc.	General License Category
1-1-3	Endpoint Threat Detection and Response (EDR) Solutions	Endpoint security solutions to do live analysis of threats, containment, investigation, and response.	General License Category
1-1-4	Mobile Device Protection Solutions	Endpoint security solutions and apps that protect mobile devices and their applications/data.	General License Category
1-1-5	Mobile Device Management (MDM) Solutions	Endpoint security solutions that manage and enforce policy on corporate and employee-owned (BYOD) mobile devices.	General License Category
1-1-6	Host Based Firewall Solutions	Endpoint security solutions that create software firewalls to protect endpoints against malicious connections.	General License Category
1-1-7	Security Configuration Management Solutions	Endpoint security solutions to manage and control configurations across enterprise endpoints.	General License Category
1-1-8	Asset Management Solutions	Endpoint security solutions used to manage all assets across an entity, including asset discovery	General License Category

		and maintaining an asset configuration management database.	
1-1-9	Patch Configuration and Management Solutions	Endpoint security solutions to identify, prioritize, test and, install patches across an entity.	General License Category
1-2	Network Security		
Cybersecurity solutions to protect the IT environment starting from the network perimeter to endpoints.			License Category to Provide Service/Product/Solution
1-2-1	Intrusion Detection/Prevention Systems (IDPS)	Network security solutions that inspect network traffic, detects malicious content, sends alert (detection-only) or takes action like blocking (detection and prevention).	General License Category
1-2-2	Network Access Control Solutions	Network security solutions that allow entities to control access to corporate networks through authentication, configuration, role-based, and other policies.	General License Category
1-2-3	Network Firewall Solutions	Network security solutions that use rules to monitor and block malicious incoming and outgoing network traffic, including next generation firewalls (NGFW), which have more advanced	General License Category

		features like deep packet inspection.	
1-2-4	Secure Web Gateway (SWG) Solutions	Network security solutions that filter users web traffic and blocks malicious or unwanted (e.g., against corporate policy) content.	General License Category
1-2-5	Network APT Protection and Sandboxing Solutions	Network security solutions, either automated or manual, that allows suspicious content to be analyzed in a segregated environment.	General License Category
1-2-6	Proxy Solutions	Network security solutions that act as an intermediary between a user and the Internet, offering efficiency, security, and/or privacy advantages.	General License Category
1-2-7	Honeynets/Honeypots Solutions	Network security solutions that is set-up as a decoy to lure attackers away from valuable assets and give security teams opportunity to investigate and remediate attacks.	General License Category
1-2-8	Unified Threat Management (UTM) Solutions	Network security solutions for small and medium sized entities that serves multiple functions, e.g., firewall, content filtering, antivirus, etc.	General License Category

1-2-9	DDoS Protection Solutions	Network security solutions to detect and protect against dedicated denial of service (DDoS) attacks that attempt to flood a corporate network and limits its availability to legitimate requests.	General License Category
1-3	Data Security		
Cybersecurity solutions to provide protection for data covering data at rest and in transit.			License Category to Provide Service/Product/Solution
1-3-1	Data Discovery and Classification Solutions	Data security solutions that identify sensitive data and apply appropriate classification tags.	General License Category
1-3-2	Data Loss Prevention (DLP) Solutions	Data security solutions installed on endpoints and networks that prevent the loss or leakage of sensitive data.	General License Category
1-3-3	Data Masking & Tokenization Solutions	Data security solutions that facilitate protecting sensitive information inside data, either by replacing it with a token (tokenization) or obscuring/ removing (masking) sensitive data.	General License Category
1-3-4	Endpoint Encryption Solutions and Key	Data security solutions that protect data-at-rest, (e.g., files, folders, etc.), by using	General License Category

	Management Systems (KMS)	cryptography to prevent unauthorized access; also includes systems that manage (e.g. generate, distribute, destroy, etc.) cryptographic keys.	
1-3-5	Network Encryption	Data security solutions that protect data-in-transit, and secure protocols like SSL/TLS.	General License Category
1-3-6	Database/Storage Security Solutions	Data security solutions that protect databases and other storage containers, including monitoring, access control, encryption, auditing, etc.	General License Category
1-3-7	Secure File Transfer Solutions	Data security solutions for sharing data in a secure manner.	General License Category
1-3-8	Secure Email Gateway (SEG)	Data security solutions that scans for and blocks spam and malicious inbound email (email APT protection and sandboxing).	General License Category
1-3-9	Privacy Enhancing Technology (PET) Solutions	Data security solutions for managing and protecting personal data throughout its lifecycle, including compliance, consent, control, audit, etc.	General License Category

1-3-10	Digital Rights Management (DRM) Solutions	Data security solutions used to restrict and manage access to protected content.	General License Category
1-3-11	Ransomware Protection Solutions	Data security solutions specifically designed and packaged for preventing, detecting, and responding to ransomware threats.	General License Category
1-4	Application Security		
Cybersecurity solutions to provide protection at the application level.			License Category to Provide Service/Product/Solution
1-4-1	Application Security Testing (AST) Solutions	Application security solutions for analyzing and testing applications for security vulnerabilities, includes static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and runtime application security protection (RASP).	General License Category
1-4-2	Web Application Firewall (WAF) Solutions	Application security solutions that protect web applications by filtering and monitoring HTTP/S requests for malicious activity.	General License Category

1-4-3	Application Control Solutions	Application security solutions to define the list of authorized applications for use in an entity and restrict the execution of unauthorized applications (covers application whitelisting and blacklisting).	General License Category
1-4-4	Web API Security Solutions	Application security solutions to protect web application programming interfaces (APIs), in order to security data transfer through APIs and prevent malicious attacks on, or misuse of, web APIs.	General License Category
1-5	Identity Security & Management		
Cybersecurity solutions to provide identity governance and management of digital identities for applications and solutions within the IT environment.			License Category to Provide Service/Product/Solution
1-5-1	Password Manager Solutions	Identity security & management solutions used to securely store and manage users' credentials;	General License Category
1-5-2	Identity Governance Solutions	Identity security & management solutions to manage user identities across an entity or ecosystem, including identity federation.	General License Category

1-5-3	Access Management Solutions	Identity security & management solutions that provide access control through centralized authentication, single sign on (SSO), remote access, session management, etc.	General License Category
1-5-4	Privileged Access Management (PAM) Solutions	Identity security & management solutions for securing and managing elevated access to critical assets.	General License Category
1-5-5	Authentication Solutions	Identity security & management solutions that verify an individual's digital identity and provide access to solutions.	General License Category
1-5-6	Digital Certificate Management Solutions	Identity security & management solutions that stores, signs, and issues digital certificates that certify the identities of trusted parties.	General License Category
1-5-7	High Trust Computing Solutions	Identity security & management solutions enabling higher levels of trust, e.g. trusted computing (TC), cross-domain security (CDS) and multilevel security solutions.	General License Category

1-5-8	Multi-factor Authentication Solutions	Identity security & management solutions that provide additional authentication factors, e.g. tokens, biometrics, etc.	General License Category
1-6	Governance, Risk & Compliance		
Cybersecurity solutions to provide governance planning, risk management, and compliance management for the IT environment.			License Category to Provide Service/Product/Solution
1-6-1	Governance, Risk, and Compliance (GRC) Solutions	Governance, risk & compliance solutions to track and manage enterprise cyber risk and compliance programs and responsibilities.	General License Category
1-6-2	Third Party Risk Management (TPRM) Solutions	Governance, risk & compliance solutions that protect against supply chain risks, including vendor risk rating and vendor management security solutions.	General License Category
1-7	Cybersecurity Operations Solutions		
Cybersecurity solutions that are used in order to execute day-to-day cybersecurity activities and tasks.			License Category to Provide Service/Product/Solution
1-7-1	Extended Detection and Response (XDR) Solutions	Integrated security solutions to expand threat detection and response operations across	General License Category

		multiple environments (e.g. networks, endpoints, servers, applications, cloud, email, identity), by integrating and analyzing security data from diverse sources in a unified platform.It aims to achieve comprehensive visibility, analyze complex threats, and proactively automate responses.	
1-7-2	Network Detection and Response (NDR) Solutions	Cybersecurity operations solutions to use of security analytics to detect and mitigate known and unknown network threats.	General License Category
1-7-3	Cyber Threat Hunting Solutions	Cybersecurity operations solutions that supports proactively uncovering previously unknown active threats and threat actors.	General License Category
1-7-4	Digital Forensic Investigation Solutions	Cybersecurity operations solutions for identifying, acquiring, and analyzing electronic evidence and completing computer investigations.	General License Category

1-7-5	Behavior Analysis and Anomaly Detection Solutions	Cybersecurity operations solutions used to detect suspicious actions based on standard behaviors, including fraud detection and prevention.	General License Category
1-7-6	Vulnerability Assessment/Scanning Solutions	Cybersecurity operations solutions that identify, categorize, and manage vulnerabilities.	General License Category
1-7-7	Penetration Testing Solutions	Cybersecurity operations solutions to detect, test, and flag exploitable security posture weaknesses, e.g. privilege escalation.	General License Category
1-7-8	Incident Management and Security Orchestration, Automation and Response (SOAR) Solutions	Cybersecurity operations solutions that coordinate, automate, and manage security incident response.	General License Category
1-7-9	Security Information and Event Management (SIEM) Solutions	Cybersecurity operations solutions for event collection/aggregation, log management and log correlation.	General License Category
1-7-10	Threat Intelligence Solutions	Cybersecurity operations solutions to ingest, analyze, and examine the intentions, objectives, and attack techniques	General License Category

		of threat actors, including both machine-readable and human-readable intelligence such as indicators of compromise (IoC).	
1-7-11	Cybersecurity Training & Awareness Tools	Cybersecurity operations solutions to upskill users and cyber professionals, e.g., anti-phishing campaigns, cyber-ranges, etc.	General License Category
1-8	Cloud Security		
Cybersecurity solutions to provide protection for cloud-based applications.			License Category to Provide Service/Product/Solution
1-8-1	Cloud Access Security Broker (CASB) Solutions	Cloud security solutions to add security controls to cloud services and ensure users are complying with cloud use policies.	General License Category
1-8-10	Cloud Workload Security	Cloud security solutions that protect workloads as they move through different cloud environments.	General License Category
1-9	Special Systems Security		
Cybersecurity solutions to provide protection for systems of special nature, such as operational technology (OT).			License Category to Provide Service/Product/Solution

1-9-1	Industrial Security Solutions	Critical systems security solutions to protect industrial control systems (ICS) and operational technology (OT), including HMI, SCADA, and DCS cybersecurity.	General License Category
1-9-2	Embedded & IoT Security Solutions	Critical systems security solutions that protect non-traditional and single- purpose Internet-connected devices from threats.	General License Category
2	Cybersecurity Professional Services		
2-1	Cybersecurity Management Consulting		
Cybersecurity professional services that are conducted in order to identify strategic areas of improvement and provide recommendations.			License Category to Provide Service/Product/Solution
2-1-1	Cybersecurity Strategy & Roadmap Development	Cybersecurity consulting services to create a cybersecurity strategy (e.g., vision, mission, etc.) and an implementation roadmap.	General License Category
2-1-2	Cybersecurity Policy, Process, Procedure and Framework Development	Cybersecurity consulting services to develop cybersecurity policies, processes, procedures and frameworks inline with an entity's cybersecurity strategy and internal/external standards.	General License Category

2-1-3	Cybersecurity Capability Model Development	Cybersecurity consulting services to develop an entity's cybersecurity capabilities including entity structure, roles & responsibilities, governance, etc.	General License Category
2-1-4	Cybersecurity Certification & Accreditation of Entities	Cybersecurity consulting services accredit/certify an entity against an externally recognized accreditation/certification standard and based on a cybersecurity assessment.	General License Category
2-1-5	Cybersecurity Change and Project Management	Cybersecurity consulting services to provide CS change management and CS project management as part of product/solution implementation and upgrade/update and as part of cybersecurity transformation.	General License Category
2-2	Cybersecurity Compliance Assessment		
Cybersecurity professional services to conduct cybersecurity assessments at the governance level of an entity.			License Category to Provide Service/Product/Solution
2-2-1	Cybersecurity Policy, Process, Procedure and Framework Assessment	Cybersecurity entity assessment services to analyze an entities cybersecurity policies, processes, procedures and frameworks and identify gaps and improvements.	Specialized License Category

2-2-2	Cybersecurity Capability Model Assessment	Cybersecurity entity assessment services to evaluate an entity's cybersecurity capabilities including entity structure, roles & responsibilities, governance, etc.	Specialized License Category
2-2-3	Cybersecurity Maturity Assessment	Cybersecurity entity assessment services to evaluate a entity's cybersecurity maturity against a defined standard and using a maturity assessment model, e.g. NCA ECC maturity assessment.	Specialized License Category
2-2-4	Cybersecurity Audit/Compliance Assessment	Cybersecurity entity assessment services to audit compliance with regulations or other national/international standards.	Specialized License Category
2-3	Cybersecurity Risk Assessment		
Professional services in risk assessment conducted to identify cybersecurity risks and determine actions to address threats and security threat factors.			License Category to Provide Service/Product/Solution
2-3-1	Cybersecurity Risk Assessment Exercise	Risk assessment services to identify, assess, and prioritize cybersecurity risks in the entity.	Specialized License Category
2-3-2	Development of a Cybersecurity Risk Register	Risk assessment services to document cybersecurity risks and risk management actions in a risk management repository.	Specialized License Category

2-4	Cybersecurity Technical Assessment		
Cybersecurity professional services that assess the technical aspects for an environment.			License Category to Provide Service/Product/Solution
2-4-1	Vulnerability Assessment	Cybersecurity technical services to broadly identify, classify, and prioritize vulnerabilities in specific solution or an entity.	Specialized License Category
2-4-2	Penetration Testing	Cybersecurity technical services to deliberately find and demonstrate exploitable vulnerabilities in specific solutions or entities.	Specialized License Category
2-4-3	Cybersecurity Architecture Review	Cybersecurity technical services to assess the completeness and suitability of solutions' or entities' cybersecurity architecture.	Specialized License Category
2-4-4	Compromise Assessment/ Threat Hunting Services	Cybersecurity technical services to identify undetected threats either proactively (threat hunting) or reactively (compromise assessment) in response to finding indicators of compromise (IoCs).	Specialized License Category
2-4-5	Red Teaming Exercise	Cybersecurity technical services where ethical hackers (red team) attack an entity's systems, while	Specialized License Category

		the entity defenders (blue team) try to defend the network. This also includes tests involving collaboration between the red and blue teams (purple team).	
2-4-6	Application Security Assessment	Cybersecurity technical services to identify flaws and vulnerability in an application, e.g. source code review, application security testing, etc.	Specialized License Category
2-4-7	Cybersecurity Configuration Review	Cybersecurity technical services to review the security configuration of devices and identify misconfiguration and opportunities to harden.	Specialized License Category
2-4-8	Cybersecurity Assessment & Certification of a Solution	Cybersecurity technical services to assess and certify solutions and products (hardware and software) according to national accreditation standards issued by NCA or in accordance with internationally recognized standards and certifications.	Specialized License Category
2-5	Bug Bounty		
Cybersecurity services provided for bug bounty programs.			License Category to Provide Service/Product/Solution

2-5-1	Bug Bounty Program Services	Cybersecurity technical services to run a program that incentivizes crowd sourced ethical hackers to conduct independent assessments and responsible disclosures.	Specialized License Category
2-6	Cybersecurity Technical Consulting		
Cybersecurity professional services that are conducted to provide technical recommendations and technical consulting activities.			License Category to Provide Service/Product/Solution
2-6-1	Cybersecurity Architecture Design	Cybersecurity technical services to design the security architecture of the entity using best practices and secure design principles.	General License Category
2-6-2	Cybersecurity Technical Standards Development	Cybersecurity technical services to develop and make actionable industry-standard and custom cybersecurity standards, including development of minimum baseline security standards (MBSS).	General License Category
2-6-3	Cybersecurity Technical Plan Development	Cybersecurity technical services to develop plans and detailed processes, e.g. disaster recovery and business continuity plan, vulnerability/risk mitigation plan, incident response plan, etc.	General License Category

2-7	Cybersecurity Incident Response & Investigation		
Cybersecurity professional services to analyze and/or handle cybersecurity incidents and breaches.			License Category to Provide Service/Product/Solution
2-7-1	Cybersecurity Incident Response	Cybersecurity incident response services to help entities manage, analyze, contain, remediate, and learn from cybersecurity incidents.	Specialized License Category (Only licensed within Tier I under Specialized License Category "Specialized - 1")
2-7-2	Cybersecurity Forensics Investigation	Cybersecurity incident investigation services to preserve evidence and analyze threat actor and threat vector techniques (e.g. malware analysis).	Specialized License Category (Only licensed within Tier I under Specialized License Category "Specialized - 1")
3-7-2	Cybersecurity Threat Intelligence Services	Cybersecurity technical services to provide information and reports to ingest, analyze, and examine the intentions, objectives, and attack techniques of threat actors and threat vectors (including dark web, brand, and cyber threat monitoring).	Specialized License Category (Only licensed within Tier I under Specialized License Category "Specialized - 1")
3	Cybersecurity Technical Implementation Services		
3-1	Cybersecurity Product/Solution Development		

Cybersecurity services to develop cybersecurity products and solutions.			License Category to Provide Service/Product/Solution
3-1-1	Cybersecurity Product/Solution Development	Cybersecurity technical services to develop custom cybersecurity products/solutions for technology vendors (e.g. white labeled products), governments, and other advanced users.	General License Category
3-2	Cybersecurity System Integration		
Cybersecurity services that are offered by cybersecurity vendors, IT vendors and system integrators in order to implement and/or configure a cybersecurity solution.			License Category to Provide Service/Product/Solution
3-2-1	Cybersecurity Implementation Requirements	Cybersecurity technical services to define cybersecurity requirements for new CS products and for CS product/solution implementation.	General License Category
3-2-2	Cybersecurity Solution Design and Architecture	Cybersecurity technical services to design the cybersecurity architecture of a solution before the solution implementation using best practices and secure design principles (covering high-level and low-level design).	General License Category
3-2-3	Cybersecurity Implementation,	Cybersecurity technical services to implement, configure, and	General License Category

	Solutions Configuration and Integration	integrate cybersecurity solutions into an entity' environment. In addition, this service includes maintenance and support contracts for a product/solution.	
4	Cybersecurity Managed Services		
4-1	Managed SOC		
Based on the Regulatory Framework for Licensing Managed Security Operations Center (MSOC) Services			
4-2	Cybersecurity Solutions as a Service		
Cybersecurity services related to outsourcing of cybersecurity solutions to an entity, including solution management and operations.			License Category to Provide Service/Product/Solution
4-2-1	Cybersecurity Solutions as a Service	Cybersecurity outsourcing services that provide day-to-day operational control and execution of cybersecurity solutions covering solution administration and operations, excluding managed SOC, and incident response.	General License Category
4-3	Cybersecurity Manpower Outsourcing		
Cybersecurity services related to outsourcing of cybersecurity manpower to an entity.			License Category to Provide Service/Product/Solution

4-3-1	Cybersecurity Manpower Outsourcing	Cybersecurity outsourcing services that provide contractors (i.e., body leasing) to fill staffing gaps in a cybersecurity entity, excluding incident response activities.	General License Category
5	Cybersecurity Training & Capacity Building Services		
5-1	Cybersecurity Training		
Delivery of cybersecurity training courses and workshops for cybersecurity and non-cybersecurity employees.			License Category to Provide Service/Product/Solution
5-1-1	Cybersecurity Academic Training	Cybersecurity training services focused on cybersecurity concepts, theory, and management.	General License Category
5-1-2	Cybersecurity Technical Training	Cybersecurity training services focused on cybersecurity hand-on experience with tools and applied techniques.	General License Category
5-1-3	Cybersecurity Simulations and Drills	Cybersecurity training services focused on practicing approaches to detecting, responding, and recovering from cyber incidents.	General License Category
5-2	Cybersecurity Awareness		

Delivery of cybersecurity training courses and workshops for cybersecurity and non-cybersecurity employees.			License Category to Provide Service/Product/Solution
5-2-1	Cybersecurity Awareness Content Development	Cybersecurity awareness services focused on creating customized content to improve employee/customer/etc. cybersecurity consciousness and understanding.	General License Category
5-2-2	Cybersecurity Awareness Sessions/Workshops	Cybersecurity awareness services focused on delivering live/remote cybersecurity awareness sessions for employees/customers/etc.	General License Category
5-3	Cybersecurity Examination & Certification		
Delivery of cybersecurity exams and certificates to individuals.			License Category to Provide Service/Product/Solution
5-3-1	Cybersecurity Examination for Individuals	Cybersecurity examination services to test the knowledge, skills, and competency of cybersecurity students and professionals.	General License Category

5-3-2	Cybersecurity Certification for Individuals	Cybersecurity certification services to verify raining/experience and accredit/certify individual with recognized cybersecurity certifications (includes certification by equivalency).	General License Category
5-4	Cybersecurity Events & Competitions		
Delivery of cybersecurity exams and certificates to individuals.			License Category to Provide Service/Product/Solution
5-4-1	Cybersecurity Events	Cybersecurity services to plan, organize and conduct cybersecurity events, conferences and forums.	General License Category
5-4-2	Cybersecurity Competitions	Cybersecurity services to plan, organize and conduct cybersecurity competitions such as hackathons and capture the flag (CTF).	General License Category

Appendix (B): Table of Financial Fees for Requesting the Licensing of Cybersecurity Services, Products, or Solutions

- Under this Framework, the applicant shall pay the fee as specified in this Appendix to apply for obtaining or renewing a license. NCA reserves the right to make any modifications it deems appropriate to this fee and/or impose other fees on the licensee.

- All fees paid under this Appendix are non-refundable.
- The table below shows the fees to apply for obtaining or renewing a license to provide cybersecurity services, products, or solutions under this Framework:

License Category	Fee based on the entitie size of the applicant The entitie size shall be determined according to the definition of Small and Medium Enterprises General Authority (Monsha'at)				
	Description	Micro	Small	Medium	Large
Specialized – Tier I (Specialized - 1)	Fee upon application and annually during the license term (for each subdomain)	N/A	SAR 300,000	SAR 500,000	SAR 1,000,000
Specialized – Tier II (Specialized - 2)		SAR 150,000	SAR 200,000	SAR 300,000	SAR 500,000
General – All Tiers	Fee for license request or renewal under General License Category	SAR 50,000			