الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Regulatory Framework for Licensing Managed Security Operations Center (MSOC) Services

(RFMSOC-1:2024)

TLP: White
Document Classification: Public

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

DISCLAIMER: The following framework will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential, and for the Intended Recipient Only
The recipient has no right to share information classified in red with any person outside the defined range of recipients, either inside or outside the organization, beyond the scope specified for receipt.

Amber - Restricted Sharing
The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within the Same Community
The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organizations. However, it is not allowed to exchange or publish this information on public channels.

White – No Restrictions

Table of Contents

1. Introduction

The National Cybersecurity Authority (NCA), according to its mandate that was approved by Royal Order number 6801, dated 11/2/1439 AH, 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. The 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. The NCA mandate includes, but not limited to: development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls, and guidelines; as well as circulating them with relevant stakeholders, following up on their compliance, and updating them. In addition, the NCA mandate includes licensing individuals and non-governmental organizations to practice cybersecurity activities and operations as determined by NCA, as well as stimulating cybersecurity sector growth in the Kingdom and encouraging innovation and investment in it.

Due to the importance of Managed Security Operations Center (MSOC) services in enhancing the cybersecurity posture of national organizations, and given the need for establishing clear frameworks and standards to define the scope of such services and the obligations of the service provider, the NCA has issued this framework to license MSOC service providers. This will also contribute to the implementation of the second phase of the NCA strategy (2.0), highlight the responsibilities and obligations of licensees to provide these types of services, and limit the provision of such services only to qualified organizations. The framework includes the qualification requirements for individuals to work as MSOC analysts.

2. Definitions

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

Term	Definition
NCA	National Cybersecurity Authority.
Organization	A public/government, private for-profit, private non-profit, or any other form of organization.
Framework	The Regulatory Framework for Licensing MSOC Services, issued by NCA.
Critical National Infrastructure (CNI)	Basic elements of the infrastructure, such as (assets, facilitates, systems, networks, processes, key employees responsible for the operation and processing of such elements) that the loss of which or being subject to security breaches would lead to: 1- Significant negative impact on the availability, integration or delivery of basic services, including services that if subjected to risk would lead to significant losses in property and/or lives and/or injuries, considering the economic and/or social implications. 2- Significant impact on the National Security and/or National Defense and/or State economy or national capabilities
Security Operations Center (SOC)	It is a center that provides cybersecurity monitoring operations services for the organization's technology ecosystem, which can detect cyber threats, find out how they occur, and provide recommendations, as well as solutions and necessary measures to contain such threats.
Managed Security Operations Center (MSOC) Services	These are the services that the beneficiary organization receives from the service provider in order to monitor cybersecurity in its technology ecosystem to detect cyber threats, know how they occur, and provide recommendations on how to address them by the beneficiary. These services include processes, staffing, related systems, etc.
License	A document issued by the NCA that allows the service provider to perform MSOC services in the Kingdom of Saudi Arabia, as determined by NCA.
Service Provider	A licensed organization by the NCA to provide MSOC services in the Kingdom of Saudi Arabia, according to the framework.
Beneficiary	Any organization that contracts with the service provider, for the purpose of obtaining MSOC services.
Cloud computing service provider	Any natural or legal person (such as companies) licensed by relevant authority in KSA to provide cloud computing services to the public, whether directly or indirectly through Data Centers (whether inside or outside the Kingdom) that are fully or partially manage by them.

Term	Definition
Policy	National Policy for the Managed Security Operations Centers, issued by the NCA.
Qualification Certificate	A document issued by the NCA for a natural person that determines his/her eligibility to work as an MSOC analyst for the service provider.
MSOC Analyst	Any natural person who holds a qualification certificate to work as an analyst at MSOC.

3. Framework Objectives

This framework aims to regulate the provision of MSOC services, through clearly outlining defined licensee responsibilities and obligations to enhance the efficiency of services provided to national organizations (beneficiaries). The objectives that this framework is seeking to realize are:

1. Contribution to enhancing cybersecurity in the Kingdom by providing high-quality MSOC services at competitive prices according to specific requirements.
2. Allowing national organizations in the Kingdom to fulfil cybersecurity responsibilities through licensed and qualified service providers.
3. Stimulating the growth of the cybersecurity sector in the Kingdom and enhancing its competitiveness, and organizations working in it.
4. Promoting innovation and investment in the cybersecurity sector by supporting the provision of innovative solutions and products that meet the increasing demand for MSOC services.
5. Protecting the rights of national organizations benefiting from cybersecurity services provided under this framework.
6. Enhancing the development of national capabilities specialized in providing MSOC services.

4. Framework Scope

This framework applies to:

1. Any organization that desires to provide MSOC services in the Kingdom of Saudi Arabia.
2. Individuals who work or desire to work for service providers as MSOC analysts in the Kingdom of Saudi Arabia.

5. Provisions for Licensing MSOC Services

5.1 Obtain, maintain and renew license

5.1.1 To obtain a license for providing MSOC services, a request shall be submitted to the NCA and that request shall meet the requirements outlined in appendices (b), (c), (d), (e) and (f) in this framework according to the license tier.

5.1.2 The license for providing MSOC services will be valid for (5) years starting from the date of license issuance.

5.1.3 The service provider shall continue to fulfil the requirements outlined in appendices (b), (c), (d), (e) and (f) of this framework in order to maintain the license according to its tier.

5.1.4 The service provider 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 the NCA.

5.1.5 If the service provider does not desire to renew the license, or if the NCA rejects the submitted license renewal request, or if the service provider has submitted a license cancellation request, in any of these cases, the service provider 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 the NCA.

5.2 License Transfer

5.2.1 The service provider shall not transfer their license without obtaining a prior written approval from the NCA.

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

5.2.3 The NCA will issue its decision on the transfer request and the service provider shall adhere to it.

5.3 Cancellation and suspension of the license

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

5.3.2 The NCA, at its discretion, reserves the right to cancel or suspend a service provider's license in cases it deems necessary, such as but not limited to the case where the service provider:

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 the NCA, including but not limited to decisions, regulations, frameworks, instructions, directions, circulars, controls.

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

5.3.3 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.

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

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

6. Service Provider Obligations

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

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

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

6.3 Connecting with the NCA's National Security Operations Center in accordance with the instructions and requirements specified by the NCA. The service provider is responsible for the cost of connection and any necessary operational expenses throughout the license period.

6.4 Adhering to localization requirements and keeping all their facilities and data within the Kingdom of Saudi Arabia.

6.5 Implementing and operating MSOC services and providing services to beneficiaries from within the Kingdom.

6.6 Adhering to technical requirements issued by the NCA for the construction and operation of the MSOC and any updates to the technical requirements.

6.7 Ensuring that data processing and storage related to the MSOC services is within the Kingdom.

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

6.9 Providing the 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 threats, indicators of compromise, vulnerabilities, cybersecurity alerts and actions to handle them. This is in addition to the cyber threats that have been contained and the measures taken.

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

6.11 Refraining from publishing and/or sharing any data related to beneficiaries within the scope of the license, or any data that is related to Saudi cyberspace with any party for any justification or purpose, including government or private organizations, inside and outside the Kingdom before obtaining written approval from the NCA.

6.12 Stating in its contracts related to this framework with beneficiaries, provisions that address cases of license expiration, non-renewal, or cancellation.

6.13 Implementing the necessary procedures in the event of the expiration or termination of the contractual relationship with the beneficiary in accordance with the NCA decisions, which include as a minimum the following:

6.13.1 Notify the beneficiary of the desire to terminate the contract no less than (270) days before the date of ceasing the provision of MSOC services.

6.13.2 If the beneficiary is in scope of the Policy, the Tier 1 service provider shall also notify the NCA no less than (270) days before the date of ceasing the provision of MSOC services.

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

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

6.16 Maintaining accurate and complete records of cybersecurity events for the past (18) months, for each beneficiary from its services.

6.17 Maintaining records of the MSOC services provided to beneficiaries, for a period of (5) years from the date of providing such services. The records shall include, but not limited to, the date the service was provided, the name of the beneficiary of the service, and details of the MSOC analysts working for the service provider who participated in providing the service. This is in addition to any third party involved in providing any part of the center's services in any way for its benefit, according to the forms approved by the NCA for that purpose.

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

6.19 Fully cooperating with the 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 the NCA, including audits, verifications, cybersecurity assessments and any other requirements on their business and systems, whatever they may be.

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

A. Financial performance information for the MSOC business, including revenues and its sources, capital, technology investments, infrastructure investments, and training and development expenses.

B. Information about the operations of the MSOC, the beneficiaries of the services, their numbers and names, the type of services provided to them and meetings and interactions with them; in addition to records of activities related to the MSOC, etc.

C. Information about the service provider's employees involved in provisioning of MSOC services, including the number of employees, their CVs and qualifications, etc.

D. Information about the technical requirements imposed on service provider, technology tools and subscriptions, any IT infrastructure related to implementing MSOC services, etc.

E. Any evidence, document, or proof required by the NCA, for the purpose of verifying the compliance of the MSOC service provider with the provisions outlined in this framework, and other documents issued by the NCA, and other relevant organizations.

6.21 Adhering to employee Saudization percentages as approved by the NCA and the other competent authorities.

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

6.23 Permanently and continually applying all cybersecurity controls issued by the NCA that apply to the service provider; 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 the NCA.

6.24 Providing 24/7/365 (24 hours a day, 7 days a week, 365 days a year) MSOC services.

6.25 Adhering to provide all MSOC services as listed in appendix (a) of this framework for Tier 1; and adhering to provide at least one service as listed in appendix (a) of this framework for Tier 2.

6.26 Adhering to notify the NCA immediately if any change occurs in the ownership of the service provider in any way.

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

6.28 Ensuring that the employees of the service provider as MSOC analysts obtain qualification certificates to work at MSOCs and renew it in accordance with this framework and what the NCA decides.

7. Subcontracting MSOC Services

7.1 The service provider may subcontract MSOC services according to the following conditions:

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

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

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

7.1.4 Subcontracting arrangements shall be documented in the internal logs of the service provider in addition to compliance with the related instructions by the NCA.

7.2 The service provider shall only subcontract with another service provider to provide MSOC services. In case the MSOC services are provided to the organizations in scope of the Policy, the subcontracted service provider shall be at the same license tier.

7.3 The NCA may, at its discretion, set a cap for subcontracts for the Tier 1 service provider.

7.4 Under all circumstances, the subcontractor shall fulfil all obligations of the service provider under this framework.

8. Requirements for Obtaining a Qualification Certificate to Work at MSOC

8.1 To work as MSOC analysts, individuals shall fulfil the requirements for obtaining the qualification certificate from the NCA, and fulfil all regulatory requirements outlined in appendix (c) of this framework.

8.2 Applying to obtain or renew a qualification certificate shall be in accordance with what the NCA decides in this regard.

8.3 The qualification certificate to work at MSOCs will be valid for (3) years starting from the date of the certificate issuance.

8.4 Renewal of the qualification certificate to work at MSOCs may be requested not earlier than (90) calendar days before the certificate expiry date and not later than (30) calendar days before the certificate expiry date. The qualification certificate renewal request shall meet all requirements stipulated in appendix (c) and any related requirements.

8.5 The NCA, at its discretion, reserves the right to cancel or suspend the qualification certificate in cases it deems necessary, such as but not limited to the case where the MSOC Analyst:

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 the NCA, including but not limited to decisions, regulations, frameworks, instructions, directions, circulars, controls and the like.
C. Repeatedly fails to fulfill the obligations on individuals outlined in this framework and any relevant NCA regulations.
D. Fails to fulfill any requirements for maintaining the qualification certificate as determined by NCA.

8.6 The qualification certificate suspension period shall have no effect on the certificate's expiry date, as the suspension period will be counted as part of the certificate duration.

8.7 Changing from one service provider to another shall not impact the validity and duration of the qualification certificate. In all cases, it is necessary to comply with the decision of the NCA in this matter.

8.8 Individuals who obtain the qualification certification shall be prohibited from performing related work at MSOCs upon the expiration, cancellation or suspension of the certificate issued for them by the NCA.

9. General Provisions

9.1 Any organization that provides or desires to provide MSOC services in the Kingdom shall obtain a license to do so from the NCA, in accordance with the provisions outlined in this framework and the NCA's decisions.

9.2 The NCA will determine a grace period for organizations providing cybersecurity services and activities that fall under the scope of this framework in order for such organizations to rectify their status in-line with this framework and what the NCA issue.

9.3 The NCA will issue the relevant instructions and controls that shall be applied to all current and future contracts with the organizations operating in cybersecurity services and activities that fall under the scope of this framework.

9.4 The organizations operating in cybersecurity services and activities 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 the NCA at its discretion within a period not exceeding (30) days from the effective date of this framework.

9.5 The NCA, pursuant to sector regulation requirements, may impose additional conditions or requirements, or cancel existing ones, on service providers or holders of qualification certificates.

9.6 The NCA reserves the right to reject any license issuance, renewal or cancelation requests, pursuant to this framework. This also applies to qualification certificate issuance or renewal requests.

9.7 Service providers and holders of qualification certificates shall submit periodic reports to the NCA as well as any other information the NCA may request at its discretion.

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

9.9 The NCA reserves the right to impose other fees on service providers and holders of qualification certificates.

9.10 The appendices contained in this framework, in addition to the "Technical Requirements for MSOC Service Providers" document shall be considered an integral part of this framework and shall be read and enforced as a single unit.

9.11 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.

9.12 The 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 the NCA's decisions.

10. Appendices

Appendix (a): MSOC Services

MSOC services are services provided to the beneficiary organization from a service provider, to monitor cybersecurity events in the technology ecosystem of the beneficiary organization, to detect cybersecurity threats, understand how they occur, and provide recommendations on how to address them in order to implement these recommendations by the beneficiary. These services, which the beneficiary receives from the service provider, include operations, staffing, systems, etc.
Below is a description of the minimum MSOC services:

1. Threat Monitoring and Detection

This involves providing a continuous monitoring service for the technology ecosystem of the national beneficiary, including the organization's networks and systems, early detection of cybersecurity threats and attacks, and issuing alerts via monitoring and detection tools using different detection methods, such as pre-defined detection use-cases, indicators of compromise, and detection rules, and classifying alerts according to their severity. This is in addition to issuing immediate alerts to the beneficiary about detected threats, and periodic technical and executive reports on the state of cybersecurity, by managing and operating cybersecurity tools specialized in monitoring and detection.

2. Threat Analysis and Investigation

This involves analyzing and investigating the detected alerts, linking the various events and understanding them within the context of the beneficiary's ecosystem. It also includes identifying the true alerts related to actual cybersecurity incidents and identifying false alerts based on a systematic method of analysis of all threats. In addition, this service involves providing the national beneficiary with initial and in-depth analysis including the causes of alerts and incidents. The service also includes conducting a sweeping and threat hunting exercises, as well as conducting analysis and investigation into cases that the national beneficiary has reported to the service provider.

3. Threat Containment Recommendations

This involves providing integrated and effective recommendations to the national beneficiary on how to contain and neutralize cybersecurity threats, to be applied by the beneficiary to control the risks of the detected threats and attacks.

Appendix (b): MSOC services licensing tiers, requirements, renewal and maintenance

As per the provisions of this framework, the NCA will issue two licensing tiers to provide MSOC services according to the scope specified in the following table:

License Tier	Scope
Tier 1	This tier allows the service provider to provide MSOC services to all organizations, including government organizations and organizations that own, operate, or host CNIs.
Tier 2	This tier allows the service provider to provide MSOC services to all organizations, excluding government organizations and organizations that own, operate, or host CNIs.

Any organization seeking to obtain a license to provide MSOC services shall fulfill the requirements for obtaining, renewing and maintaining the license according to the table below:

License Tier	Requirements
Tier 1	1. The license applicant shall be a legally established entity in the Kingdom. 2. The license application form shall be filled and submitted. 3. 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 or more citizens) in the entity requesting a license shall be in accordance with percentage approved by the NCA. 4. 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 organizational structure of the service provider, and the percentage of Saudization for leadership positions. 5. The license applicant shall have a capital of no less than 50 million SAR. 6. Shall provide all of the MSOC services as defined in appendix (a). 7. Shall submit a report of compliance with all technical requirements specified in the "Technical Requirements for MSOC Service Provider" document and pass the assessment conducted by the NCA. 8. Shall employ (full-time) MSOC analysts who are Saudi citizens in accordance with appendix (e) as a minimum. 9. Shall submit a business plan according to which the service will be provided for a period of (5) years including, but not limited to: A. Service provider's vision and business strategy. B. Pro forma financial statements for (5) years of operations. C. A plan for knowledge transfer in MSOC services.

Tier 1	D. Human capital and technical capacity investment roadmap and targets. 10. Shall submit a report to the NCA on the cybersecurity program of the MSOC service provider to be reviewed. The report shall be consistent with the "Technical Requirements for MSOC Service Provider" document issued by the NCA. The report shall include, but not limited to, the following: A. Information about the MSOC service provider's cybersecurity program. B. General procedures for data storage, transfer, use and access monitoring. C. Network and physical security requirements, including encryption procedures. D. Procedures for notification and investigation of cybersecurity breaches. E. Information about incident containment teams and capabilities. F. Information about backup and business continuity. G. Procedures for data recovery or data destruction upon termination, at no charge to the service beneficiary. H. Service agreements with service beneficiaries. 11. 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.
Tier 2	1. The license applicant shall be a legally established entity in the Kingdom. 2. The license application form shall be filled and submitted. 3. 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 or more citizens) in the entity requesting a license shall be in accordance with percentage approved by the NCA. 4. 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 organizational structure of the service provider, and the percentage of Saudization for leadership positions. 5. The license applicant shall have a capital of no less than 500 thousand SAR. 6. Shall provide at least one of the MSOC services as defined in appendix (a).

Tier 2	7. Shall submit a report of compliance with all technical requirements specified in the "Technical Requirements for MSOC Service Provider" document and pass the assessment conducted by the NCA. 8. Shall employ (full-time) MSOC analysts who are Saudi citizens in accordance with appendix (f) as a minimum. 9. Shall submit a report to the NCA on the cybersecurity program of the MSOC service provider to be reviewed. The report shall be consistent with the "Technical Requirements for MSOC Service Provider" document issued by the NCA. The report shall include, but not limited to, the following: A. Information about the MSOC service provider's cybersecurity program. B. General procedures for data storage, transfer, use and access monitoring. C. Network and physical security requirements, including encryption procedures. D. Procedures for notification and investigation of security breaches. E. Information about incident containment teams and capabilities. F. Information about backup and business continuity. G. Procedures for data recovery or data destruction upon termination, at no charge to the service beneficiary. H. Service agreements with service recipients. 10. 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.

Appendix (c): Requirements for obtaining, renewing and maintaining a qualification certificate

In accordance with the provisions of this framework, the NCA will issue a qualification certificate to individuals in three categories, as follows:

Certificate category	Requirements for obtaining, renewing and maintaining a qualification certificate
Category (A)	1. The applicant shall be a Saudi citizen. 2. Shall have the knowledge, skills, and abilities necessary to work as a cybersecurity defense analyst specified in the Saudi Cybersecurity Workforce Framework (SCyWF). 3. Shall fulfil any of the following requirements: A. At least one year of experience working as SOC analyst or administrator in a cybersecurity or network role. B. A recognized university degree in IT, cybersecurity, data science, or any related discipline. 4. Completion of training courses and passing their tests, as determined by the NCA. 5. Completion of the required annual professional development hours (including cybersecurity courses, participation in cybersecurity conferences, and other learning and development activities, in the field of cybersecurity).
Category (B)	1. The applicant shall be a Saudi citizen. 2. Shall have the knowledge, skills, and abilities necessary to work as a cybersecurity defense analyst specified in the Saudi Cybersecurity Workforce Framework (SCyWF). 3. Shall fulfil any of the following requirements: A. At least (3) years of experience as SOC Analyst. B. A valid Category (A) certificate, obtained for at least (3) years. 4. Completion of training courses and passing their tests, as determined by the NCA. 5. Completion of the required annual professional development hours (including cybersecurity courses, participation in cybersecurity conferences, and other learning and development activities, in the field of cybersecurity).
Category (C)	1. The applicant shall be a Saudi citizen 2. Shall have the knowledge, skills, and abilities necessary to work as a cybersecurity defense analyst specified in the Saudi Cybersecurity Workforce Framework (SCyWF). 3. Shall fulfil any of the following requirements: A. At least (5) years of experience as SOC Analyst. B. A valid Category (B) certificate, obtained for at least (3) years. 4. Completion of training courses and passing their tests, as determined by the NCA.

	5. Completion of the required annual professional development hours (including cybersecurity courses, participation in cybersecurity conferences, and other learning and development activities, in the field of cybersecurity).

Appendix (d): Schedule of fees to apply for a license to provide MSOC services

- Under this framework, the applicant shall pay the fee as specified in this appendix to apply for obtaining or renewing a license. The 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 MSOC services under this framework.

The fee to apply for obtaining or renewing a license	
License Tier	The fee to apply for obtaining or renewing a license
Tier 1	50,000 SAR
Tier 2	15,000 SAR

Appendix (e): Table of the minimum number of MSOC Analysts qualified under this framework that a Tier 1 Service Provider shall employ (full-time)

- The table below shows the minimum numbers of Saudi national MSOC analysts for a Tier 1 service provider. The service provider shall evaluate the need to increase the number of MSOC Analysts in order to fulfil its obligations to the beneficiaries of the provided services, taking into account the technical aspects of each beneficiary, such as the size and complexity of the systems and technologies being monitored.
- The NCA may, in accordance with the mechanism it determines, reduce the minimum number of MSOC analysts required from the service provider, if it is proven that the service provider uses appropriate solutions, including automation, in a way that reduces the need for a large number of MSOC analysts.

# of Beneficiaries	# of MSOC Analysts (FTE) in Category (A)	# of MSOC Analysts (FTE) in Category (B)	# of MSOC Analysts (FTE) in Category (C)	Total Number of MSOC Analysts (FTE)
1-30	20	10	2	32
31-40	25	12	3	40
41-50	30	15	4	49
51-60	35	17	4	56
61-70	40	20	5	65
71-80	45	22	5	72
81-90	50	25	6	81
91+	The service provider shall submit a request to the NCA to determine the minimum number of MSOC analysts			

Appendix (f): Table of the minimum number of MSOC Analysts qualified under this framework that a Tier 2 Service Provider shall employ (full-time)

- The table below shows the minimum numbers of Saudi national MSOC analysts for a Tier 2 service provider. The service provider shall evaluate the need to increase the number of MSOC analysts to be able to fulfill its obligations to the beneficiaries of the provided services, taking into account the specific technical aspects of each beneficiary, such as the size and complexity of the systems and technologies being monitored.
- The NCA may, in accordance with the mechanism it determines, reduce the minimum number of MSOC analysts required from the service provider, if it is proven that the latter uses appropriate solutions, including automation, in a way that reduces the need for a large number of MSOC analysts.

# of Beneficiaries	# of MSOC Analysts (FTE) in Category (A)	# of MSOC Analysts (FTE) in Category (B)	# of MSOC Analysts (FTE) in Category (C)	Total Number of MSOC Analysts (FTE)
1-10	2	1	1	4
11-20	3	2	2	7
21-30	4	2	2	8
31-40	5	3	3	11
41-50	6	3	3	12
51-60	7	4	4	15
61-70	8	4	4	16
71-85	9	5	5	19
86+	The service provider shall submit a request to the NCA to determine the minimum number of MSOC analysts			


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority