الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Regulatory Framework for Licensing Managed SOC Services

(Public Consultation)

TLP: White
Document Classification: Public

مقيد - عام

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

Traffic Light Protocol (TLP):

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

Red – Personal, Confidential and for Intended Recipients Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

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 organization. However, it is not allowed to exchange or publish this information on public channels.

White – No Restriction

Public Consultation

Contents

Public Consultation

1. Introduction

The National Cybersecurity Authority (NCA) is the national entity in charge of cybersecurity in Saudi Arabia and serves as the national authority on its affairs. The NCA aims to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, government services and activities in accordance with its regulation under Royal Decree #6801 on 11/2/1439 A.H. The NCA's mandate includes introducing cybersecurity 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 determined by NCA, as well as developing and updating the necessary standards or controls for clearance and licensing the import, export, and use of highly sensitive hardware and software, as determined by NCA. The NCA's mandate also includes promoting the growth of the cybersecurity sector in Saudi Arabia and encouraging innovation and investment in it.

Public Consultation

2. Definitions

The terms used in this regulation shall have the following meanings, unless the context requires otherwise:

Term	Definition
NCA	National Cybersecurity Authority.
Organization	A public, private for-profit, private non-profit, or any other form of organization.
Certification	A qualification process for cybersecurity individuals who intend to provide restricted cybersecurity services in Saudi Arabia, as determined by NCA.
Critical national infrastructure (CNI)	These are the assets (i.e. facilities, systems, networks, processes, and key operators who operate and process them), whose loss or vulnerability to security breaches may result in: 1) Significant negative impact on the availability, integration or delivery of basic services, including services that could result in serious loss of property and/or lives and/or injuries, alongside observance of significant economic and/or social impacts. 2) Significant impact on national security and/or state economy or national capacities.
Cybersecurity Event	Something that happens to the cybersecurity state of network, systems, applications at a specific time.
Cybersecurity Program of Managed SOC Service Providers	Refers to a set of documents that detail a managed SOC service provider's plans and procedures for maintaining cybersecurity within the managed SOC service provider's internal organization. These set of documents address the handling of breaches, backing up data, and returning or destroying data upon contract termination.
License	A document issued by NCA for natural or legal persons in order to provide or develop cybersecurity services, products, and solutions in Saudi Arabia, or for individuals to practice cybersecurity-related activities and operations, as determined by NCA.
License transfer	The transfer of all rights and obligations associated with the license to any other party, in accordance with the provisions and procedures, as determined by NCA.
Security Operations Center (SOC)	A combination of people, processes, and technologies specialized in monitoring networks, IT systems, operational technologies, or its components of hardware or software, services, or data. As well as detecting anomalies, threat analysis and containment.
Managed SOC (MSOC)	A Center that aims to monitor the cybersecurity state in the technical ecosystem of the beneficiary, for the early detection of cyber threats, discovering how they occur, and providing comprehensive recommendations on how to address them and take the necessary

Public Consultation

	measures to contain them. The business model includes a contract between the beneficiary and the managed services provider, to take full responsibility of cybersecurity monitoring activities including operations, staff and systems in accordance to Appendix A.
Managed SOC (MSOC) Service Provider	An organization providing managed SOC services.
National SOC	A national platform used by NCA, that collects and analyses cybersecurity threats to Saudi Arabia's infrastructure, cybersecurity threats across SOCs and any other matters deemed necessary by the NCA.
Service beneficiary	An organization that outsources its SOC related operations, whether fully or partially, to a Managed SOC service provider in Saudi Arabia. This category includes organizations covered by the scope of the National Policy for Managed SOCs, as well as other organization that are not mandated to work with Managed SOC providers.
Policy	National Policy for Managed Security Operations Centers

Public Consultation

3. Objectives of the Managed SOC Licensing Framework

The purpose of introducing licensing for Managed SOC service providers is to regulate the Cybersecurity market in the Kingdom, guarantee a certain quality across all Managed SOCs and improve the overall level of SOC services provided to all organizations in the Kingdom of Saudi Arabia as well as leapfrog national maturity by having Managed SOC service providers in the Kingdom with the capacity to provide services, drive ecosystem development by creating a broader and more regulated market for Managed SOC services, as well as to enhance cybersecurity throughout the Kingdom's cyberspace, enable access by increasing opportunities for Saudi Managed SOC service providers to provide services for the government, and drive talent and retention of SOC analysts in the market through certification and requirements for individuals.

Public Consultation

4. Framework Scope

4.1 Managed SOC Service Providers

The provisions of this framework shall apply to all service providers in Saudi Arabia who intend to provide Managed SOC services for any public or private organizations in Saudi Arabia. Provisions of this framework shall also apply to the employed staff of Managed SOC service providers who, in certain cases, will be required to hold certifications issued by NCA.

4.2 Service Beneficiaries and Organizations under the scope of the National Policy for Managed SOCs

Service beneficiaries are organizations that outsource their SOC related operations, whether fully or partially, to a managed SOC service provider in Saudi Arabia. As part of the provisions of this regulatory framework, organizations covered by the scope of the National Policy for Managed SOCs are required to use a Tier 1 licensed Managed SOC service provider when engaging Managed SOC services. Other organizations are strongly encouraged by the NCA and they are free to choose any Tier 1 or Tier 2 licensed Managed SOC service provider to meet their cybersecurity needs.

Public Consultation

5. Managed SOC Licensing Methodology

NCA is taking a phased approach with the licensing of managed SOC services in Saudi Arabia. NCA will introduce multiple, tiered licenses for managed SOC service providers. NCA will first introduce provisional licenses for service providers that meet the minimum requirements for the different tiered licenses, until the training and certification requirements stipulated by NCA are met.

Any service provider that intends to provide any SOC services to any public or private organization in Saudi Arabia, as defined in this framework, shall be required to obtain the relevant license and ensure the certification requirements of their staff are met. Appendix B provides details on the minimum requirements expected from Managed SOC service providers, by tier, in order to obtain a license from the NCA. Appendix C provides details on the requirements around certification for SOC analysts.

For the provisional licensees, NCA will waive the requirement for Managed SOC service providers to provide proof of compliance with the regulation and standards, and to meet the Certified SOC Analyst thresholds as well as the Saudization threshold. All other minimum requirements, as outlined in Appendix B for Managed SOC service providers and their staff are binding. NCA will require holders of provisional licenses to convert provisional licenses to full licenses within 24 months. NCA reserves the right to increase or decrease the duration period of provisional licenses at its discretion.

Public Consultation

6. Obligations under the License

In order to provide Managed SOC services for all categories, the service provider shall comply with the provisions of this framework, all relevant NCA regulatory provisions, the laws of Saudi Arabia, and the following obligations:

6.1 Comply with the regulations, acts, standards, decisions, and instructions related to cybersecurity in force in Saudi Arabia.

6.2 Meet license maintenance requirements for licensed Managed SOC service providers and their corresponding certified staff, in accordance with the license awarded, including but not limited to the terms stipulated in Appendix B.

6.3 Integrate with the National SOC in accordance with the technical details determined by the NCA regarding the integration mechanism and the information required form the service provider.

6.4 Comply the National Standard for Managed SOC Services issued by the NCA, and all applicable laws and regulations regarding data cybersecurity in Saudi Arabia, including the Essential Cybersecurity Controls (ECC).

6.5 Fully cooperate with any NCA mandated technical assessments. NCA reserves the right to assess the technical capabilities of Managed SOC service providers at any point in time and at any frequency it deems necessary.

6.6 Produce a "Cybersecurity Program of Managed SOC Service Providers" report to be submitted to NCA for review. The report shall include, in alignment with NCA managed SOC standards, but is not limited to:

- 6.6.1 Information about the service provider's cybersecurity program;
- 6.6.2 General procedures for data storage, transfer, and access and use monitoring;
- 6.6.3 Network and physical security requirements, including encryption procedures;
- 6.6.4 Procedures for notification and investigation of security breaches;
- 6.6.5 Information about incident containment teams and capabilities;
- 6.6.6 Information about backup and business continuity; and
- 6.6.7 Procedures for returning or destroying data upon termination, at no charge to the service beneficiary.

Public Consultation

6.7 Shall not release cybersecurity data or information related to service beneficiary organization's data or information on the Saudi cyber space with any entities (public or private) without obtaining formal written approval from the NCA.

6.8 If Managed SOC service provider is compelled or decides, on its own accord, to end the contractual relationship with a service beneficiary due to any reason, service provider shall notify service beneficiary no less than 180 calendar days before the effective date of ceasing managed SOC services for the service beneficiary. If the service beneficiary is an organization covered by the scope of the National Policy for MSOCs, the Tier 1 licensed Managed SOC service provider must also notify NCA no less than 180 calendar days before the effective date of ceasing managed SOC services for the service beneficiary.

6.9 Notify NCA immediately of any changes of information or any discovered inaccuracy in information, of an administrative nature, that is reported to NCA.

6.10 Notify NCA within 30 calendar days of any legal or regulatory action pertaining to managed SOC services against licensed Managed SOC service provider, regardless of the regulatory body or jurisdiction, inside or outside Saudi Arabia.

6.11 Managed SOC licensed service providers are only permitted to sub-contract other licensed Managed SOC service providers. Moreover, upon making sub-contracting arrangement, the NCA shall be notified of the same no later than 5 working days after engaging in a sub-contracting relationship.

6.12 Retain accurate and complete records of cybersecurity events of the previous 18 months for each Managed SOC service beneficiary.

6.13 Maintain accurate and complete records for a period of 5 years of managed SOC applications and renewal applications, all legal, human resource and financial document, certified staff that carried out managed SOC services, any licensed Managed SOC service provider which delivers any part of the managed SOC services on behalf of the licensee, and any correspondence with NCA regarding managed SOC and the maintenance of the service provider's license.

6.14 Fully cooperate with NCA, facilitate its mission, and make available all possible resources of the service provider to carry out the inspection process, including providing NCA with all the required documents and information that would confirm the service provider's compliance with NCA's regulations. NCA will deal, at its discretion, with collected documents and information in strict confidentiality. The information that NCA may request includes, but is not limited to:

Public Consultation

6.14.1 Information related to financial performance (including but not limited to revenue and sources, capital and sources, investments in technology and infrastructure, and training and development expenses).

6.14.2 Information relating to managed SOC operations and the corresponding service beneficiaries (including, but not limited to, number and nature of service beneficiaries, meetings and interactions with service beneficiaries, and maintained records and archives of SOC related activities).

6.14.3 Information relating to incident containment procedures and activities, information sharing procedures and activities, collaboration in national cyber drills.

6.14.4 Information relating to service provider's staff carrying out Managed SOC related services (including but not limited to number of employees and analysts, biographical information of analysts, relevant certification information, and analyst records in compliance with NCA regulations).

6.14.5 Information relating to service provider's technical requirements, technology tools and subscriptions, and other IT infrastructure for the purposes of carrying out managed SOC activities.

6.15 Commitment to the local Saudi talent employment conditions stipulated by NCA and the relevant government authorities.

Public Consultation

7. Financial consideration

Licensed Managed SOC service providers are subject to the relevant financial consideration requirements stipulated in Appendix D in return for services provided by the NCA. Such financial consideration includes, but is not limited to, financial consideration for new license application, license renewal, and annual service. The NCA reserves the right to amend and/or cancel any or all financial considerations stipulated in this document. Financial consideration requirements are due as soon as the payment invoice is issued. Managed SOC service providers and/or their staff are obligated to pay the financial considerations on their due dates and without any delay within 30 calendar days from the date of their issuance.

Public Consultation

8. License Duration and Renewal

8.1 License Duration

Licensed Managed SOC service providers may provide SOC services as stipulated by their awarded license for the duration of 5 years. The license duration period for licensed Managed SOC service providers begins from the date of the service provider's full license issuance by NCA and expires exactly 5 years after.

8.2 License renewal and conditions

Licensed Managed SOC service providers must apply to renew their license. Renewal applications shall be submitted no earlier than 90 calendar days before the expiration date of the license and no later than 30 calendar days before the expiration date of the license. Applications received by NCA outside of this window are under NCA's discretion.

Unless otherwise specified, the approval to renew the license for Managed SOC service providers is subject to similar conditions to that of a new license application. The term of the license and upon renewal shall be the same as the validity period of the license upon its issuance.

8.3 Cancellation of license

Licensed Managed SOC service providers may elect to cancel their license by submitting a request in writing to NCA. NCA shall review the request and inform the licensed Managed SOC service provider of its decision and any requirements or obligations that must be satisfactorily fulfilled towards NCA, service beneficiaries being serviced by the licensed Managed SOC service provider at the present time, or any other parties before implementing the request.

All financial consideration requirements owed and unpaid by the service provider and/or their staff before the date of cancellation shall remain valid and payable to NCA.

NCA, at its discretion, reserves the right to cancel the license of the managed SOC service providers and/or their certified staff, under certain circumstances, including failure to comply with the regulations stipulated in this document, failure to comply with any modifications, amendments, or deletions made by NCA, under its discretion, to the regulations stipulated in this document, failure to comply with any written directive from NCA, or failure to remedy any violations within a specific period, as determined by NCA, from the date of receipt of a notice from NCA.

Public Consultation

8.4 Carrying on providing Managed SOC services upon the expiration, cancellation, or revocation of the license

Managed SOC service providers are not permitted, under any circumstances, to carry on providing Managed SOC services upon the expiration, cancellation or revocation of the Managed SOC service provider's license.

In the event that a service provider does not intend to renew its license or its renewal application has been rejected by NCA or it is subject to license revocation due to not satisfying the requirements set out in Appendix B, or it has elected to cancel its license, the Managed SOC service provider is granted a grace period of 180 calendar days from the date of notice or expiration, whichever comes soonest, to ramp down operations and provide adequate notification to service beneficiaries. The service provider is required to notify their service beneficiaries immediately, no later than 180 calendar days before the end of the grace period and adhere to the provisions outlined in Article 6.

Public Consultation

9. License transfer or sub-contracting

9.1 Transfer of license for service providers

The license issued by NCA to a Managed SOC service provider may not be assigned to another organization without obtaining NCA's written approval. Assignment is permitted for reasons including, but not limited to, mergers and acquisitions, or business transfers within a group company. Article 11.4 details the requirements for applying to transfer a license and the procedures related thereto.

9.2 Transfer of certification for individual staff

The SOC analyst certification issued by NCA may not be assigned to another individual or organization under any circumstances.

9.3 Sub-contracting

A licensed Managed SOC service provider may sub-contract the works thereof, under the following conditions:

9.3.1 All obligations arising from contracting remain the sole responsibility of the licensed service provider entering a sub-contracting arrangement.

9.3.2 All parties must document the sub-contracting arrangements within their internal company records.

9.3.3 Tier 1 licensed Managed SOC service providers servicing organizations covered by the scope of the National Policy for MSOCs are not permitted to sub-contract more than 30% of the total billed managed SOC services for a single beneficiary covered by the scope of the National Policy for MSOCs to other Tier 1 or Tier 2 sub-contractors.

9.3.4 Tier 1 licensed Managed SOC service providers servicing organizations covered by the scope of the National Policy for MSOCs are required to carry out due diligence and ensure that sub-contracted Tier 1 or Tier 2 licensed Managed SOC service providers fulfill the same minimum thresholds of employing certified SOC analysts, as stipulated in minimum requirements for Tier 1 licenses in Appendix C, when providing services for organizations covered by the scope of the National Policy for MSOCs. Sub-contracted Tier 2 licensed Managed SOC service providers are required

Public Consultation

to meet these minimum threshold conditions only for the services provided directly to the organizations covered by the scope of the National Policy for MSOCs, through the sub-contracting relationship.

Public Consultation

10 Certifications of SOC analysts and their renewal

10.1 Certification duration

The certification duration period for certified SOC analysts begins from the date of the staff member's certification issuance by NCA and expires exactly 3 years after.

10.2 Certification renewal

Certified SOC analysts may apply to renew their certification 90 calendar days before the certification expiration date and not later than 30 calendar days before the expiration date of the certification.

The approval to renew the SOC analyst's certification is subject to similar conditions of the issuance of new certificate, as well as the addition of professional development requirements as stipulated in Appendix C. The term of the new certification shall be the same as the validity period of the certificate upon its issuance.

10.3 Certification validity under different service provider employers

The certification for a SOC analyst will remain valid if that certified SOC analyst changes employer from a licensed Managed SOC service provider to another licensed Managed SOC service provider. The term of the certification shall be the same as the validity period of the certification upon its issuance.

Public Consultation

11. License and certification procedures

11.1 Procedures for obtaining a license

A service provider wishing to obtain a license to carry out managed SOC services, subject to the regulations in this document must submit an application to NCA and pay the new license application financial consideration as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix B. Service providers must fulfill and take note of the following conditions:

11.1.1 NCA may request further information or additional documents from the applicant service provider during the evaluation of its application. NCA reserves the right to reject applications that are incomplete or that do not include all supporting documents.

11.1.2 NCA shall issue its decision to approve or reject the application.

11.1.3 The NCA will award Managed SOC service providers with a provisional license, based on the tier license the service provider has applied for, upon approval of the application. NCA reserves the right to determine the provisional period of the license, at its discretion.

11.1.4 As stipulated in Appendix B, Managed SOC service providers are required to keep under their employment a mandated level of certified SOC analysts, who hold a valid NCA issued SOC analyst certification. If the Managed SOC service provider does not have such certified SOC analysts under employment, the Managed SOC service provider must hire and train apprentices that should obtain SOC analyst certification within the provisional license period, to meet the requirements set out in Appendix B and Appendix C.

11.1.5 Once the mandated level of certified SOC analysts has been reached, the Managed SOC service provider is required to notify the NCA and provide evidence of certification in line with the requirements set out in Appendix B and C. Upon receipt and verification, the NCA will convert the provisional license of the service provider into a full license.

11.2 Procedures for maintaining a license

Licensed Managed SOC service providers wishing to hold a license to provide Managed SOC services subject to the regulations in this document must pay the annual service financial consideration as

Public Consultation

stipulated in Appendix D, while fulfilling all the requirements set forth in Appendices B. In addition, Managed SOC service providers must fulfill the following conditions:

11.2.1 It is the licensed Managed SOC service provider's responsibility to duly verify that their employed staff members' certifications are valid and that the requirements of certified SOC analysts are met throughout the duration of the license.

11.2.2 Failure to comply with license maintenance requirements by the licensed Managed SOC service provider, including the staff certification requirements, subjects the Managed SOC service provider to a violation as determined by NCA, under its discretion.

11.3 Procedures for renewing a license

Licensed Managed SOC service providers wishing to renew a license to provide licensed managed SOC services subject to the regulations in this document must submit a renewal application, in line with this document, and pay the license renewal financial consideration as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix B. In addition, licensed Managed SOC service providers must fulfill and take note of the following conditions:

11.3.1 NCA may request further information or additional documents from the applicant service provider during the evaluation of its application. NCA reserves the right to reject applications that are incomplete or that do not include all supporting documents.

11.3.2 NCA shall issue its decision to approve or reject the application.

11.4 Procedures for transferring a license

Licensed Managed SOC service providers wishing to transfer a license to provide licensed Managed SOC services subject to the regulations in this document must submit a written request to NCA stating the reason and circumstances for the transfer request, while fulfilling all the maintenance requirements set forth in Appendix B. In addition, licensed Managed SOC service providers must fulfill the following conditions:

Public Consultation

11.4.1 The licensed Managed SOC service provider applying for a transfer of a license and the organization applying for the transfer must include the following information in the transfer request:

11.4.1.1 Identification of all parties involved in the transfer process.

11.4.1.2 A description of the nature of the operation for which the transfer is requested.

11.4.1.3 The purpose and rationale for transferring the license.

11.4.1.4 Basic financial information about the parties involved in the transaction.

11.4.1.5 A complete list of current service beneficiaries and any possible impact to Managed SOC services being provided.

11.4.1.6 Updated company information on sub-contractors and licensed SOC analysts within the new organization.

11.4.2 NCA shall upon receipt of the written request from the licensed Managed SOC service provider implement any of the following actions:

11.4.2.1 Unconditionally agree to the transfer.

11.4.2.2 Conditional approval of the transfer with additional terms or actions required by NCA.

11.4.2.3 Reject the request for transfer.

11.5 Procedures for cancelling a license

Licensed Managed SOC service providers wishing to cancel a license to provide licensed Managed SOC services subject to the regulations in this document must submit a written request to NCA stating the desire for cancellation and the desired effective date. NCA will process the cancellation request, determine an effective date of cancellation, and inform the service provider of its decision and any requirements or obligations that must be met. Licensed Managed SOC service providers are expected to fulfill their obligations under the license as stipulated in this document until the effective date of cancellation. Licensed Managed SOC service providers must actively support their service beneficiaries in migrating to a different provider. Licensed Managed SOC service providers might charge their own cost for migration support to their service beneficiaries. The burden of proof regarding applicable cost is on the licensed Managed SOC service provider.

Public Consultation

11.6 Procedures for obtaining a SOC analyst certification

Individuals wishing to become a certified SOC analyst, must submit an application to NCA, pay the new certification application financial consideration as stipulated in Appendix D while fulfilling all the requirements set forth in Appendix C for consideration.

Individuals must fulfill the following conditions:

11.6.1 NCA may request further information or additional documents from the individual applying for the SOC analyst certificate during the evaluation of its application. NCA reserves the right to reject applications that are incomplete or that do not include all supporting documents.

11.6.2 NCA shall issue its decision to approve or reject the application.

11.7 Procedures for maintaining SOC analyst certification

The certified SOC analysts shall fulfill all the certification maintenance requirements set forth in Appendix C and are responsible to renewing their certification before expiry. These individuals must fulfill 40 hours of professional development per year, and submit evidence of completion for the last 3 years along with the renewal application, in line with the requirements set out in Appendix C.

11.8 Procedures for renewing SOC analyst certification

Certified SOC analysts wishing to renew their certification must submit a renewal application to the NCA and pay the certification renewal financial consideration as stipulated in Appendix D, while providing evidence that they fulfill the maintenance requirements set out in Appendix C. Individuals must take note of the following:

11.7.1 NCA reserves the right to require renewing applicants to once again complete the NCA SOC certification examination in line with the requirements set out in Appendix C.

11.7.2 NCA shall issue its decision to approve or reject the application.

Public Consultation

12 General provisions

NCA reserves the right to amend, modify, and/or delete any part of the framework, at its discretion.

Public Consultation

13 Appendices

Appendix A

Additional Information on the services provided by MSOCs

Managed services aim to monitor the cybersecurity state in the technical ecosystem of the beneficiary, with the objective of early detection of cyber threats, discovering how they occur, and providing comprehensive recommendations on how to address them and take the necessary measures to contain them. The business model includes a contract between the beneficiary and the managed services provider, to take full responsibility for cybersecurity monitoring activities including operations, staff and systems. Such services are provided remotely. The following is a description of key services provided by MSOCs:

1. Continuous Threat Monitoring and Detection

This service includes providing (24/7) continuous and real-time monitoring of the beneficiary's technical ecosystem (including its networks and systems), and early detection of cyber threats and attacks. It also includes issuing alerts triggered through monitoring and detection tools that use several detection methods, including detection use-cases, Indicators of Compromise, and Detection rules. Additionally, this services includes classifying alerts based on its severity, issuing instant alerts on threats targeting beneficiary, and developing executive and technical reports on the state of cybersecurity by managing and activating cybersecurity monitoring and detection tools.

2. Threat Analysis and Investigation

This service includes analyzing and investigating detected threats, linking several events and putting them into the context of the beneficiary's ecosystem. It also supports the beneficiary in identifying accurate alerts related to real cyber incidents, and identifying false alerts based on a systematic method in analyzing all threats. Through this service, the beneficiary will be provided with anlytical reports that include full analysis of cyber incidents' and alerts' root causes. Additionally, this service includes several capabilities, including sweeping, threat hunting, and the ability to analyze and investigate cases reported by the service provider.

Public Consultation

3. Threat Containment

This service includes providing comprehensive and effective recommendations to the beneficiary, including how to contain and neutralize cyber threats, which can be applied by the beneficiary's internal teams to control the risk of detected cyber attacks, threats and incidents.

Depending on the scope of work and service level agreement, this service may include the service provider performing the containment of cyber threats -if possible- and implementing the necessary measures for that, including isolating endpoints targeted by threats and attacks from the beneficiary's system.

Public Consultation

Appendix B

Taxonomy and Minimum Requirements of NCA issued Managed SOC Licenses

NCA will issue 2 license tiers as per the permissions in the table below. Licenses will be issued to service providerswith operations in Saudi Arabia. The specifications are:

License	Description
Tier 1 (Gov org & CNIs)	Permitting service provider to provide Managed SOC services for all organizations, including government organizations and private sector organizations owning, operating, or hosting CNIs.
Tier 2 (Other organizations)	Permitting service provider to provide managed SOC services for only other organizations that are not classified as government organizations or private sector organizations owning, operating, or hosting CNIs.

In order to qualify for NCA issued managed SOC licenses, service providers will have to meet minimum requirements at the service provider level. Moreover, service providers will have to employ SOC analysts who will also have to have pass a certification exam and hold a valid certification.

The minimum requirements to qualify for Tier 1 and Tier 2 Managed SOC licenses are stipulated below:

License	Minimum requirements for Managed SOC service providers
Tier 1	1. Managed SOC service provider must be legally registered with HQ in Saudi Arabia. 2. Managed SOC service provider must satisfy requirements for local ownership. 3. Managed SOC service provider must satisfy localization requirements which stipulate that all physical facilities, staff, and data must be kept in Saudi Arabia. 4. Managed SOC service provider must provide all the SOC services as defined in Appendix A.

Public Consultation

	5. Managed SOC service provider must present an annual certificate provided by an NCA licensed compliance assessor to demonstrate the compliance with all requirements detailed in the NCA ECC, CCC, and any other relevant NCA cybersecurity controls and standards, as deemed by NCA (enforced after provisional period). 6. Managed SOC service provider is required to ensure that its KSA based IT service providers also comply with ECC, CCC, and any relevant NCA cybersecurity controls and standards, as deemed by NCA, with a compliance assessment conducted by an NCA licensed compliance assessor (enforced after provisional period). 7. Managed SOC service provider must comply with all NCA technical requirements defined in the National Standard for Managed SOC Services and obtain a certificate from an NCA licensed compliance assessor (enforced after provisional period) or satisfy an NCA inspection. 8. Managed SOC service provider must offer 24/7/365 Managed SOC services. 9. Managed SOC service provider must employ a minimum of 30 SOC analysts. 10. Managed SOC service provider is required to employ Certified SOC analysts to carry out Managed SOC related services, and meet the following thresholds among staff carrying out Managed SOC related services (enforced after provisional period): 10.1 At least 10 SOC Cybersecurity Defense Analysts II; and 10.2 At least 5 SOC Cybersecurity Defense Analysts III. 11. Managed SOC service provider must submit a "Cybersecurity Program of Managed SOC Service Providers" report that will be referenced in service agreements with service beneficiaries. 12. Managed SOC service provider must present a 5-year business plan that includes, but is not limited to, 13.1 Managed SOC service provider vision and market strategy, 13.2 Pro forma financial statements for 5 years of operations, 13.3 Human capital and technical capacity investment roadmap and targets, and 13.4 Demonstration on how previous investments have been used to develop SOC capabilities. 13. Managed SOC service provider must have either: 14.1 Capital to cover the next two years in investments as stipulated in the Managed SOC service provider business plan; 14.2 Or 100 million SAR. 14. Managed SOC service provider must show proof of funds covering, above and beyond the investment capital requirement stipulated above, a minimum of 18

Public Consultation

	months of operating expenses as stipulated in the Managed SOC service provider's business plan.
Tier 2	1. Managed SOC service provider must be legally registered in Saudi Arabia. 2. Managed SOC service provider must provide at least one of the Managed SOC services as defined in Appendix A. 3. Managed SOC service provider must present an annual certificate provided by an NCA licensed compliance assessor to demonstrate the compliance with requirements detailed in the NCA ECC, CCC, and any other relevant NCA cybersecurity controls and standards, as deemed by NCA (enforced after provisional period). 4. Managed SOC service provider must comply with all NCA technical requirements defined in the National Standard for Managed SOC Services. 5. Managed SOC service provider must offer 24/7/365 Managed SOC services. 6. Managed SOC service provider is required to employ at least 7 Certified SOC analysts (enforced after provisional period). 7. Managed SOC service provider must submit a "Cybersecurity Program of Managed SOC Service Providers" report that will be referenced in service agreements with service beneficiaries. 8.

In order to maintain NCA issued Managed SOC licenses, Managed SOC service providers will have to maintain the above-mentioned requirements at the organizational and staff level throughout the duration of the license in order to be in compliance with this framework.

Public Consultation

Appendix C

Minimum Requirements for NCA issued Certification for SOC Analysts

NCA will certify individuals to become SOC Analysts at three levels. Certifications will only be awarded to individuals residing in Saudi Arabia. Individuals will also have to meet the minimum requirements at their corresponding certification level.

The minimum requirements to qualify for SOC Analysts certifications are stipulated below:

Certification Level	Minimum requirements for individuals

Level I	SOC Cybersecurity Defense Analyst I
	• Saudi residency.
	• Meet the Knowledge, Skills, and Abilities for the job role as specified by the Saudi Cybersecurity Workforce Framework (SCyWF).
	• Either of the requirements below:
	  ○ Minimum of one year of experience working as an analyst or administrator in a cybersecurity or network role, or
	  ○ University degree in IT, Cybersecurity, Data Science or related field
	  ○ Complete NCA SOC Cybersecurity Defense Analyst training course (40hrs).
	• Pass NCA SOC Cybersecurity Defense Analyst examination.

Level II	SOC Cybersecurity Defense Analyst II
	• Saudi residency.
	• Meet the Knowledge, Skills, and Abilities for the job role as specified by the Saudi Cybersecurity Workforce Framework (SCyWF).
	• Either of the requirements below:
	  • 3 years of experience working as an analyst in a SOC with a recognized Cybersecurity provider
	  • Held a valid SOC Cybersecurity Defense Analyst I certification in good standing for at least 3 years
	  • Hold one or more of the Cyber Defense Certifications
	• Pass NCA SOC Cybersecurity Defense Analyst examination.

Public Consultation

Level III	SOC Cybersecurity Defense Analyst III
	• Saudi residency.
	• Meet the Knowledge, Skills, and Abilities for the job role as specified by the Saudi Cybersecurity Workforce Framework (SCyWF).
	• Either of the requirements below:
	  ◦ 6 years of experience working as an analyst in a SOC with a recognized Cybersecurity provider
	  ◦ Held a valid SOC Cybersecurity Defense Analyst II certification in good standing for at least 3 years
	  ◦ Hold one or more of the Cyber Defense Certifications
	• Pass NCA SOC Cybersecurity Defense Analyst examination.

In order to maintain NCA issued cybersecurity SOC Analyst certifications, individuals will have to meet maintenance requirements on an annual basis. Evidence of completion will need to be submitted for the certification renewal process every 3 years, and the maintenance requirements are stipulated below:

	Certification Maintenance requirements for individuals
All Levels	Completion of 40 hours of professional development annually (includes cybersecurity courses, attendance of cybersecurity conferences, and other cybersecurity learning and development activity as deemed relevant by NCA)

Public Consultation

Appendix D

Schedule of financial consideration for NCA issued Managed SOC Service Provider Licenses and SOC Analyst Certifications

In order to maintain NCA issued Managed SOC service provider licenses, service providers and/or their corresponding staff will have to pay the following financial consideration in return for services provided by the NCA. NCA reserves the right to amend, modify, and delete any or all financial consideration stipulated in the schedule of financial consideration.

Financial consideration requirements for Managed SOC service providers			
	New license application	License renewal application	Annual service financial consideration
Tier 1	1,000,000 SAR	1,000,000 SAR	5% of annual revenues (enforced after the provisional period)
Tier 2	50,000 SAR	50,000 SAR	5% of annual revenues (enforced after the provisional period)

Financial consideration requirements for SOC analysts	
	New or renew certification application
Level I	1000SAR
Level II	3000SAR
Level III	5000 SAR

Public Consultation

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority