



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

Request for Public Consultation on the Draft Regulatory Framework for Licensing Cybersecurity Compliance Assessment Services

TLP: White

Document Classification: [Public](#)



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

Contents

1	Introduction	4
2	Definitions	5
3	Framework Objectives	6
4	Framework Scope	7
5	Compliance Assessor Licensing Framework Methodology	9
6	Obligations under the license	10
7	Financial fees	13
8	License duration and renewal	14
9	License transfer or sub-contracting	16
10	Certification duration and renewal	17
11	License and certification procedures	18
12	General provisions	23
13	Appendices	24

1. Introduction

1.1. Background

The National Cybersecurity Authority (NCA) is the national entity in charge of cybersecurity in Saudi Arabia and the national reference in all 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.

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	Are governmental, private for-profit, private non-profit, or any other form of entity
Assessed organization	Refers to any organization in Saudi Arabia, whether government, private or non-profit, that undergoes an assessment of its compliance with NCA cybersecurity controls or other NCA regulations
Certification	A qualification process for cybersecurity individuals that intend to provide restricted cybersecurity services in Saudi Arabia, as determined by NCA
Cloud service provider (CSP)	Refers to organizations that provide cloud computing and data storage services
Compliance assessment	The evaluation of an organization’s level of compliance with NCA’s cybersecurity controls or other NCA regulations
Compliance assessment services provider	An organization that provides compliance assessment services in Saudi Arabia
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
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 in this framework
Service provider	An organization, private for-profit or non-profit, that provide a cybersecurity service, product, or solution in Saudi Arabia for the benefit of organizations and individuals

3. Framework Objectives

The purpose of introducing licensing regulation for cybersecurity compliance assessment service providers is to improve the cybersecurity posture at the national level by enhancing the level of maturity of organizations that conduct compliance assessments and contribute to developing the cybersecurity sector by creating a broader market for cybersecurity compliance assessments, in addition to laying the foundations for scalability by establishing an ecosystem for training and improving the quality of compliance assessments.

4. Framework Scope

There are four main components that are within the scope of this regulation: 1) NCA cybersecurity Regulatory Documents; 2) compliance assessments process, methodology, and contents; 3) compliance assessment services providers; and 4) assessed organizations. Below is a description of each component:

4.1. NCA cybersecurity Regulatory Documents

NCA's cybersecurity Regulatory Documents include, but are not limited to, the Essential Cybersecurity Controls (ECC), Critical Systems Cybersecurity Controls (CSCC), Cloud Cybersecurity Controls (CCC), and the specialized controls and standards which are, but are not limited to, the Organizations' Social Media Accounts Cybersecurity Controls, Telework Cybersecurity Controls (TCC), the Operational Technology Cybersecurity Controls (OTCC), National Cryptographic Standards (NCS) and Data Cybersecurity Controls (DCC). NCA reserves the right to publish additional general and specialized Regulatory Documents and to amend, modify, or delete any of them.

4.2. Compliance assessments process, methodology, and contents

The compliance assessment process includes, but is not limited to, conferring with the assessed organization CISO and executive leadership on the NCA cybersecurity controls or other NCA regulatory requirements being evaluated, visiting the assessed organization physical location to evaluate compliance, collecting artifacts, compiling artifacts and observations into a comprehensive compliance assessment report, drafting a comprehensive compliance assessment report, reviewing a draft version of the compliance assessment report with the assessed organization's CISO and executive leadership, and submitting the final compliance assessment report to NCA in a format and through a channel determined by NCA. The compliance assessment methodology is, but is not limited to, the practices and procedures that a compliance assessor must follow while carrying out the compliance assessment process. The compliance assessment content is, but is not limited to, the structure of the compliance assessment report, the criteria for admissible artifacts, and the criteria for determination of whether an assessed organization is compliant with a specific control. NCA reserves the right to define the process, methodology, and contents of compliance assessments in its entirety and make any amendments, modifications, or deletions therewith.

4.3. Compliance assessment services providers

The provisions of this framework shall apply to all service providers in Saudi Arabia that carry out cybersecurity compliance assessments of any NCA cybersecurity controls or other NCA regulatory requirements for all public and private organizations in Saudi Arabia. That is, all service providers that provide any cybersecurity compliance assessments of NCA cybersecurity controls or other NCA regulations to public and private organizations in Saudi Arabia, will require a license issued by NCA. Regarding the staff working for a service provider that intends to carry out cybersecurity compliance assessments, only those individual staff members that are directly carrying out the compliance assessment or carrying out any part of the compliance assessment process, as outlined below, are required to be certified as per the provisions of this framework.

4.4. Assessed organizations

Any organization in Saudi Arabia, whether public, private or non-profit, being assessed on its compliance with NCA cybersecurity controls or any other NCA regulations through an NCA defined compliance assessment is considered an “assessed organization.”

5. Compliance Assessor Licensing Framework Methodology

NCA is taking a phased approach with the licensing of compliance assessors in Saudi Arabia. NCA will introduce multiple, tiered licenses for compliance assessors. 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 carry out compliance assessments for NCA's cybersecurity controls or other NCA regulations within the scope of the application of this framework shall be required to obtain the relevant license, and its relevant staff that will directly carry out parts of the compliance assessment process, shall obtain the relevant certificate issued by NCA. Appendix A provides details on the structure of 4 types of licenses available based on the tier of assessed organizations and category of compliance assessments. Appendix B provides details on the minimum requirements for licensed compliance assessment services providers and staff.

NCA will introduce provisional licenses for the Tier 1-A license. NCA will waive the requirement for compliance assessment services providers to employ NCA certified compliance assessors. All other minimum requirements for service providers and their staff are binding. NCA will require holders of provisional licenses to convert provisional licenses to full licenses within 12 months or have their provisional licenses expire. NCA reserves the right to increase or decrease the duration period of provisional licenses at its discretion.

6. Obligations under the License

6.1. General obligations for licensed compliance assessor service providers

Any compliance assessment services provider that has obtained any of the four types of licenses issued by NCA for the carrying out of compliance assessments for NCA's cybersecurity controls or other NCA regulations, as stipulated in Appendices A and B, shall comply with the provisions of the Regulatory Framework for Compliance Assessors Licensing "this document", all relevant NCA regulatory provisions, the laws of Saudi Arabia, and the following obligations:

- 6.1.1 Comply with the regulations, acts, standards, decisions, and instructions related to cybersecurity in force in Saudi Arabia.
- 6.1.2 Carry out compliance assessments using the NCA methodology, as defined by NCA.
- 6.1.3 Meet license maintenance requirements for licensed compliance assessment services providers and their corresponding certified staff, in accordance with the license awarded, including but not limited to the terms stipulated in Appendix C.
- 6.1.4 Submit compliance assessments reports in NCA's approved format and through NCA's approved channel, such as Haseen or other as determined by NCA.
- 6.1.5 NCA to fulfill its mandate, roles, and responsibilities needs to conduct compliance assessments centrally for government and CNI organizations. The licensee must comply with the delivery model determined by NCA .
- 6.1.6 Shall not release cybersecurity data or information related to an assessed organization's compliance data or information on the Saudi cyber space with any entities, whether they are public or private entities, without obtaining written approval from the NCA.
- 6.1.7 Execute and adhere to any directions and circulars issued by the NCA regarding the compliance assessment of assessed organizations.
- 6.1.8 Notify NCA within 15 calendar days of any changes of information or any discovered inaccuracy in information, of an administrative nature, that has been reported to NCA.
- 6.1.9 Maintain accurate and complete records for a period of 5 years of compliance assessment applications and renewal applications, compliance assessments carried out, certified staff that carried out compliance assessments, any business organization

which delivers any part of the compliance assessment on behalf of the licensee, and any correspondence with NCA regarding compliance assessments and the maintenance of the licensed compliance assessment services provider's license.

- 6.1.10 Fully cooperate with NCA to carry out its oversight duties over licensed compliance assessment services providers and the compliance assessment process. In addition to the cooperation with NCA, facilitating its tasks and making available all possible resources of the licensed compliance assessment services provider to carry out the inspection process, including reviewing the systems of the licensed compliance assessment services provider and providing NCA with all the required documents and information that would confirm the licensed compliance assessment services provider's compliance with NCA's regulations. The information that NCA may request includes, but is not limited to:
- 6.1.10.1 Information related to financial performance, including revenue and sources, capital and sources, and training and development expenses.
 - 6.1.10.2 Information relating to compliance assessments conducted and the corresponding assessed organizations, including number and nature of assessed organizations, meetings and interactions with assessed organizations, and maintained records and archives of compliance assessments.
 - 6.1.10.3 Information relating to the licensed compliance assessment services provider's staff carrying out compliance assessments, including number of currently employed and active assessors, biographical information of assessors, and relevant certification information.
 - 6.1.10.4 Any evidence required by NCA that proves the licensed compliance assessment services provider's compliance with the obligations issued within this framework, and other regulations issued by the NCA and other relevant bodies.
- 6.1.11 Commitment to the local Saudi talent employment conditions stipulated by NCA and the relevant government authorities.

6.2. General obligations for assessed organizations

Any assessed organization shall comply with the provisions of this framework, all relevant NCA regulatory provisions, the laws of Saudi Arabia, and the following obligations:

- 6.2.1. Comply with the regulations, acts, standards, decisions, and instructions related to cybersecurity in force in Saudi Arabia.
- 6.2.2. Contract only with an NCA licensed compliance assessment services provider for the purpose of conducting compliance assessments for the assessed organization in accordance with the restrictions of the license of the licensed compliance assessment services provider.
- 6.2.3. Report any faults by licensed compliance assessment services providers to the NCA.
- 6.2.4. Shall not contract with a different licensed compliance assessment services provider for the purposes of conducting the same compliance assessment within 6 months, unless approved by the NCA.
- 6.2.5. Ensure their critical third parties obtain compliance assessments from a licensed compliance assessment services provider.

7. Financial Fees

Licensed compliance assessment services providers are subject to the relevant financial fees requirements stipulated in Appendix D. Such financial fees includes, but is not limited to, financial fees for new license application, license renewal, and annual service. The NCA reserves the right to amend and/or cancel any or all financial fees stipulated in this document.

Financial fees requirements shall be due as soon as the payment invoice is issued. Licensed compliance assessment services providers and/or their staff are obligated to pay the financial fees on their due dates within 30 calendar days from the date of their issuance.

8. License Duration and Renewal

8.1 License Duration

Licensed compliance assessment services providers may provide compliance assessments as stipulated by their awarded license for the duration of 5 years. The license duration period for licensed service providers begins from the date of the service provider's license issuance by NCA and expires exactly 5 years after. This period is not inclusive of the provisional license period.

8.2 License renewal and conditions

Licensed compliance assessment services providers may apply to renew their license. Renewal applications shall be submitted within 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 absolute discretion and may be rejected.

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

8.3 Cancellation of license

Licensed compliance assessment services providers may elect to cancel their license by submitting a request in writing to NCA. NCA shall review the request and inform the licensed compliance assessment services provider of its decision and any requirements or obligations that must be satisfactorily fulfilled towards NCA or any other parties before implementing the request.

All financial fees 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 compliance assessment services 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 absolute 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.

8.4 Restrictions upon license expiration, cancellation, or revocation

Compliance assessment services providers are not permitted, under any circumstances, to carry out compliance assessments upon the expiration, cancellation, or revocation of the compliance assessment services provider's license. If a compliance assessment services provider's license expires, cancels, or is revoked during an ongoing compliance assessment, the compliance assessment services provider should cease carrying out the compliance assessment and inform the assessed organization immediately.

9. License transfer or sub-contracting

9.1 Transfer of license for service providers

The license issued by NCA to a compliance assessment services provider may not be assigned to another organization without obtaining NCA's written approval. The NCA shall take into consideration certain applications in cases of mergers and acquisitions or business transfers within a group company. This document details the requirements for applying to transfer a license and the procedures related thereto.

9.2 Transfer of certification for individual staff

The certification for staff assessors issued by NCA may not be assigned to another individual or organization under any circumstances.

9.3 Sub-contracting

A licensed compliance assessment services providers may sub-contract the works thereof, under the following conditions:

- 9.3.1 All obligations arising from licensing remain the sole responsibility of the licensed wishing to enter a sub-contracting arrangement.
- 9.3.2 All parties must make note of the sub-contracting arrangements in the compliance assessment report and within their internal company records.
- 9.3.3 Compliance assessment services providers may only sub-contract from other licensed compliance assessment services providers within the category they hold a license for. Therefore, Tier 1-A may only sub-contract from Tier 1-A and Tier 2-A licensed service providers and or staff. The same hold true for all license types.
- 9.3.4 Any Tier 1-A or Tier 1-B service provider that wishes to sub-contract another service provider must seek approval from the NCA.
- 9.3.5 Any Tier 1-A or Tier 1-B service provider that wishes to sub-contract a Tier 2-A or Tier 2-B service provider, respectively, must seek approval from the NCA, as well as ensure the Tier 2 sub-contractor holds a valid license, and that the Tier 2 sub-contractor's certified staff are Saudi citizens.
- 9.3.6 Any Tier 2-A or Tier 2-B service provider may sub-contract other licensed Tier 2 service providers without NCA approval.

10. Certification duration and renewal

10.1 Certification duration

Certified staff assessors, as stipulated in Appendix B, may provide compliance assessments as stipulated by their certification while under the employment of a licensed compliance assessment services provider for the duration of 2 years. The certification duration period for certified staff assessors begins from the date of the assessor's certification issuance by NCA and expires exactly 2 years after.

10.2 Certification renewal and conditions

Certified staff assessors may apply to renew their certification. Renewal applications shall be submitted within 90 calendar days before the expiration date of the certification and no later than 30 calendar days before the expiration date of the certification. Applications received by NCA outside of this window are under NCA's absolute discretion and may be rejected.

Unless otherwise specified, the approval to renew the certification for staff assessors is subject to similar conditions to that of a new certification application. The term of the certification upon renewal shall be the same as the validity period of the certification upon its issuance.

10.3 Certification validity under different service provider employers

The certification for a certified staff assessor will remain valid if that certified staff assessor changes employer from a licensed compliance assessment services provider to another licensed compliance assessment services provider. The term of the certification shall be the same as the validity period of the certification upon its issuance.

10.4 Restrictions upon certification expiration

Certified staff assessors are not permitted to initiate a compliance assessment or participate in an ongoing compliance assessment upon the expiration of the assessor's certification.

Certified staff assessors are not permitted to initiate a compliance assessment or participate in an ongoing compliance assessment upon the expiration of the assessor's certification.

11 License and certification procedures

11.1 Procedures for obtaining a license

Service providers wishing to obtain a license to carry out compliance assessments subject to the regulations in this document must submit an application to NCA and pay the new license application financial fees as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix B for consideration. In addition, service providers must fulfill 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 Upon approval of the application, NCA will award the service provider with a provisional license based on the type that the service provider submitted its application. As stipulated in Appendix B and Appendix C, service providers are required to hold and maintain a license in addition to keeping under their employment competent staff that are also required to hold and maintain a staff-level certification of the same type in order to fulfill the requirements to carry out compliance assessments as stipulated under this framework. The service provider must then provide evidence that it has under its employment fully certified individual staff members who hold the same type of license the service provider has under provisional status.
- 11.1.4 Upon the completion of full certification of at least 50% of the service provider's compliance assessment staff members, NCA will convert the provisional license of the service provider into a full license within 5 working days of the certification issuance date.
- 11.1.5 As stipulated in Article 5, in the interest of precipitating development of an ecosystem of compliance assessors NCA will suspend the requirement for Tier 1-A service providers and their staff members to complete NCA General compliance assessor training courses and pass the NCA General compliance assessor exams within the time period stipulated in Article 11.6.3. NCA will extend the period to convert provisional licenses to full licenses for Tier 1-A service providers to 12 months.

11.2 Procedures for maintaining a license

Licensed compliance assessment services providers wishing to hold a license to carry out compliance assessments subject to the regulations in this document must pay the annual service financial fees as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix C. In addition, service providers must fulfill the following conditions:

- 11.2.1 The certified individual staff members of the licensed compliance assessment services provider shall fulfill all the individual staff member certification maintenance requirements set forth in Appendix C. In order for the licensed compliance assessment services provider to be compliant with the maintenance requirements of its individual staff members, at least one certified service provider staff member must fulfill the maintenance requirements as stipulated in Appendix C. It is the licensed compliance assessment services provider's responsibility to duly verify that their employed staff members' certifications are valid.
- 11.2.2 Failure to comply with license maintenance requirements on the service provider level subjects the service provider to a violation as determined by NCA, under its absolute discretion.

11.3 Procedures for renewing a license

Licensed compliance assessment services providers wishing to renew a license to carry out compliance assessments subject to this framework must submit a renewal application and pay the license renewal financial fees as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix B. In addition to the following:

- 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 The licensed compliance assessment services provider applicant for a license renewal must have under their employment at least one individual staff member that holds and maintains a valid, staff-level certification of the same type in order to fulfill the requirements to carry out compliance assessments as stipulated under this framework.
- 11.3.3 NCA shall issue its decision to approve or reject the application.

11.4 Procedures for transferring a license

Licensed compliance assessment services providers wishing to transfer a license must submit a written request to NCA stating the reason and circumstances for the transfer request, while fulfilling all license maintenance requirements set forth in Appendix C and stipulated in Article 11.2. In addition, service providers must fulfill the following conditions:

- 11.4.1 The licensed compliance assessment services provider applying for a transfer of a license 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 impact on the existing clients, specifically but not limited to assessed organizations, of the service provider.
 - 11.4.1.4 The purpose and rationale for transferring the license.
 - 11.4.1.5 Basic financial information about the parties involved in the transaction.
- 11.4.2 Upon acknowledging receipt of the written request from the service provider, the NCA shall 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 compliance assessment services providers wishing to cancel a license to carry out compliance assessments subject to this framework 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 licensed compliance assessment services provider of its decision and any requirements or obligations that must be met. Service providers are expected to fulfill the requirements under the license as stipulated in this document until the effective date of cancellation.

11.6 Procedures for obtaining a certification

Individuals wishing to obtain a certification to carry out compliance assessments subject to the regulations in this document must submit an application to NCA and pay the new certification application financial fees as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix B for consideration, in addition to fulfilling the following conditions:

- 11.6.1 NCA may request further information or additional documents from the applicant 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 provide provisional approval or rejection of the application.
- 11.6.3 In order to proceed to a full certification, applicants will then be expected to enroll in an NCA General compliance assessor training courses, complete the courses according to its curricular requirements, and pass the NCA General compliance assessor exams, within 90 calendar days from the date of receiving preliminary approval from NCA.
- 11.6.4 Upon successful completion of the NCA General compliance assessor training courses and passing the NCA General compliance assessor exams, NCA will convert the provisional certification of individual staff members into a full certification of passing the NCA General compliance assessor exams.

11.7 Procedures for maintaining a certification

Certified staff assessors wishing to hold a certification to carry out compliance assessments subject to the regulations in this document must fulfill all the requirements set forth in Appendix C.

11.8 Procedures for renewing a certification

Individual staff members wishing to renew a certification to carry out compliance assessments subject to this framework in this document must submit a renewal application to the NCA and pay the certification renewal financial fees as stipulated in Appendix D, while fulfilling all the requirements set forth in Appendix B and having maintained all the requirements set forth in Appendix C. In addition, individual staff members must take note of the following:

- 11.8.1 NCA may request further information or additional documents from the applicant individual staff member during the evaluation of its application. NCA reserves the right to reject applications that are incomplete or that do not include all supporting documents.
- 11.8.2 NCA reserves the right to require renewing applicants to once again complete the NCA General compliance assessor training courses and pass the NCA General compliance assessor examinations.
- 11.8.3 NCA shall issue its decision to approve or reject the application within 10 working days.

11.9 Procedures for resolving the dispute as to assessment results

Licensed compliance assessment services providers and/or assessed organizations agree to use their respective best efforts to resolve any disputes that may arise resulting from a compliance assessment. In cases of dispute as to assessment results, all parties of the dispute shall submit their concerns in writing to the NCA through its approved channels accompanied by all the above-mentioned relevant documents. The submission should also specify the name and particulars of the licensed compliance assessment services provider and/or its staff, the name and particulars of the assessed organization, identify the compliance assessment report, and state the reasons for the concern, amongst other details.

12. General provisions

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

13. Appendices

Appendix A: Taxonomy of NCA issued Cybersecurity Compliance assessment services provider Licenses

NCA will issue 4 license types, which are based on 2 tiers and 2 categories, as specified in the tables below:

Tier	Description
Tier 1 (Gov org & CNIs)	Tier permitting compliance assessment services provider to conduct compliance assessments for all organizations, including government organizations and private sector organizations owning, operating, or hosting CNIs.
Tier 2 (Other organizations)	Tier permitting compliance assessment services provider to conduct compliance assessments for only other organizations that are not classified as government organizations or private sector organizations owning, operating, or hosting CNIs.

Category	Description
A - General	Category permitting compliance assessment services provider to conduct compliance assessments of general NCA cybersecurity controls or other NCA regulations, such as the ECC, CCC, and CSCC
B - Specialized	Category permitting compliance assessment services provider to conduct compliance assessments for specialized NCA cybersecurity controls or other NCA regulations, such as the operational technology cybersecurity controls (OTCC)

License types issued by NCA for cybersecurity compliance assessors

License Tier	Category	
	A - General	B - Specialized
Tier 1 (Gov org & CNIs)	<p>Tier 1-A Permits compliance assessment services provider to conduct compliance assessments of general NCA cybersecurity controls or other NCA regulations for all organizations, including government organizations and private sector organizations owning, operating, or hosting CNIs.</p>	<p>Tier 1-B Permits compliance assessment services provider to conduct compliance assessments of specialized NCA cybersecurity controls or other NCA regulations for all organizations, including government organizations and private sector organizations owning, operating, or hosting CNIs.</p>
Tier 2 (Other organizations)	<p>Tier 2-A Permits compliance assessment services provider to conduct compliance assessments of general NCA cybersecurity controls or other NCA regulations for only other organizations that are not classified as government organizations or private sector organizations owning, operating, or hosting CNIs.</p>	<p>Tier 2-B Permits compliance assessment services provider to conduct compliance assessments of specialized NCA cybersecurity controls or other NCA regulations for only other organizations that are not classified as government organizations or private sector organizations owning, operating, or hosting CNIs.</p>

Appendix B: Minimum requirements to qualify for NCA issued Cybersecurity Compliance Assessment Licenses

In order to be qualified for NCA issued cybersecurity compliance assessment licenses, compliance assessment services providers shall meet the minimum requirements. Moreover, compliance assessment services providers must meet the minimum requirements of employing certified staff who hold certifications of the same tier and category. Certifications can be obtained individually. However, certified assessors must be employed by a licensed service provider in order to carry out a compliance assessment.

The minimum requirements to qualify for Tier 1-A and Tier 2-A general licenses and certifications are stipulated below:

License Tier	Minimum requirements for service providers	Minimum requirements for staff certification
Tier 1 - A	<p>General Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> ● Be legally registered in the KSA and its HQ located in the KSA ● Satisfy requirements for foreign ownership influence ● Comply with all NCA controls (such as ECC, etc.) and satisfy an NCA inspection ● If service provider uses cloud service provider (CSP), CSP must also comply with all NCA controls (such as ECC, etc.) ● Employ minimum of 30 assessors ● Have available minimum of 10M SAR capital 	<p>General Certified Staff Assessor must:</p> <ul style="list-style-type: none"> ● Have Saudi citizenship ● Hold University degree in IT, OT, Cybersecurity, or related field ● Have 5 years of experience in IT, OT, Cybersecurity, or related field ● Complete NCA General compliance assessor training courses ● Pass NCA General compliance assessor exams

Tier 2 - A	General Licensed Compliance assessment services provider must: <ul style="list-style-type: none">● Be legally registered in the KSA● Comply with all NCA controls (such as ECC, etc.) and satisfy an NCA inspection● Employ minimum of 1 assessor	General Certified Staff Assessor must: <ul style="list-style-type: none">● Have a valid Saudi residency● Hold University degree in IT, OT, Cybersecurity, or related field● Have 3 years of experience in IT, OT, Cybersecurity, or related field● Complete NCA General compliance assessor training courses● Pass NCA General compliance assessor exams
-------------------	---	--

The minimum requirements to qualify for Tier 1-B and Tier 2-B specialized licenses are stipulated below:

License Type	Minimum requirements for service providers	Minimum requirements for staff certification
Tier 1 - B	<p>Specialized Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> ● Be legally registered in the KSA and its HQ located in the KSA ● Satisfy requirements for foreign ownership influence ● Comply with all NCA controls (such as ECC, etc.) and satisfy an NCA inspection ● If service provider uses cloud service provider (CSP), CSP must also comply with all NCA controls (such as ECC, etc.) ● Employ minimum of 10 CS domain specialists with a minimum of 5 assessors ● Have minimum of 3M SAR capital 	<p>Specialized Certified Staff Assessor must:</p> <ul style="list-style-type: none"> ● Have Saudi citizenship ● Hold University degree in IT, OT, Cybersecurity, Assessment or related field ● Have 5 years of experience in IT, OT, Cybersecurity, or related field ● Complete NCA General compliance assessor training courses) ● Complete NCA Specialized compliance assessor training courses ● Pass NCA General compliance assessor exams ● Pass NCA Specialized compliance assessor exams
Tier 2 - B	<p>Specialized Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> ● Be legally registered in the KSA ● Comply with all NCA controls (such as ECC, etc.) and satisfy an NCA inspection ● Employ minimum of 1 assessor 	<p>Specialized Certified Staff Assessor must:</p> <ul style="list-style-type: none"> ● Have a valid Saudi residency ● Hold University degree in IT, OT, Cybersecurity, or related field ● Have 3 years of experience in IT, OT, Cybersecurity, Assessment or related field ● Complete NCA General compliance assessor training courses ● Complete NCA Specialized compliance assessor training courses ● Pass NCA General compliance assessor exams ● Pass NCA Specialized compliance assessor exams

Appendix C: Maintenance requirements for NCA issued Cybersecurity Compliance assessment services provider Licenses

In order to maintain NCA issued cybersecurity compliance assessment licenses, compliance assessment services providers will have to meet maintenance requirements at the company and staff level.

The maintenance requirements for all 4 types of licenses are stipulated below:

License Type	Minimum requirements for service providers	Minimum requirements for certified staff
Tier 1 - A	<p>General Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> • Be legally registered in the KSA and its HQ located in the KSA • Maintain foreign ownership influence requirements • Compliance with all NCA controls (such as ECC, etc.) • If the company uses cloud service provider (CSP), CSP must maintain compliance with all NCA controls (such as ECC, etc.) 	<p>General Certified Staff Assessor must:</p> <ul style="list-style-type: none"> • Maintain Saudi citizenship • Maintain valid CISA, or ISO27001 Lead Auditor, or CRISC or industry equivalent certification • Completion of required hours of professional development annually (includes cybersecurity courses, attendance of cybersecurity conferences, and other cybersecurity learning and development activity as deemed relevant by NCA)*
Tier 2 - A	<p>General Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> • Maintain legal registration in the KSA • Compliance with all NCA controls (such as ECC, etc.) 	<p>General Certified Staff Assessor must:</p> <ul style="list-style-type: none"> • Maintain Saudi residency • Completion of required hours of professional development annually (includes cybersecurity courses, attendance of cybersecurity conferences, and other cybersecurity learning and development activity as deemed relevant by NCA)*
Tier 1 - B	<p>Specialized Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> • Be legally registered in the KSA and its HQ located in the KSA 	<p>Specialized Certified Staff Assessor must:</p> <ul style="list-style-type: none"> • Maintain Saudi citizenship • Maintain valid required certification

	<ul style="list-style-type: none"> ● Maintain foreign ownership influence requirements ● Compliance with all NCA controls (such as ECC, etc.) ● If company uses cloud service provider (CSP), CSP must maintain compliance with all NCA controls (such as ECC, etc.) 	<ul style="list-style-type: none"> ● Completion of required hours of professional development annually (includes cybersecurity courses, attendance of cybersecurity conferences, and other cybersecurity learning and development activity as deemed relevant by NCA)*
Tier 2 – B	<p>Specialized Licensed Compliance assessment services provider must:</p> <ul style="list-style-type: none"> ● Maintain legal registration in the KSA ● Compliance with all NCA controls (such as ECC, etc.) 	<p>Specialized Certified Staff Assessor must:</p> <ul style="list-style-type: none"> ● Maintain Saudi residency ● Completion of required hours of professional development annually (includes cybersecurity courses, attendance of cybersecurity conferences, and other cybersecurity learning and development activity as deemed relevant by NCA)*

* Holders of more than one certification (e.g. Tier 1-A and Tier 1-B) can apply the completion of the required hours of professional development to all certifications for the purposes of certification maintenance.

Appendix D: Schedule of financial fees for NCA issued Cybersecurity Compliance assessment services provider Licenses

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

Financial fees requirements for service providers			Financial fees requirements for staff		
	New license application	License renewal application	Annual service financial fees	New certificate application	Certificate renewal application
Tier 1 – A	500,000 SAR	Same as new license application financial fees	50,000 SAR	10,000 SAR	Same as new certification application financial fees
Tier 1 – B	250,000 SAR	Same as new license application financial fees	25,000 SAR	7,000 SAR	Same as new certification application financial fees
Tier 2 – A	20,000 SAR	Same as new license application financial fees	No financial fees	2,000 SAR	Same as new certification application financial fees
Tier 2 – B	20,000 SAR	Same as new license application financial fees	No financial fees	2,500 SAR	Same as new certification application financial fees



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

