

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



Compliance and Data Protection Department

Service Provider Accreditation

Accreditation Scheme

compliance.qcert.org



WORKSHOP CONTENTS ACCREDITATION



1. FRAMEWORK AND ACCREDITATION INTRODUCTION
2. ACCREDITATION OVERVIEW
3. ACCREDITATION VALUE PROPOSITION
4. ACCREDITATION LIFECYCLE AND ACHEIVEMENT
5. QUESTIONS AND ANSWERS

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



FRAMEWORK AND SCHEME INTRODUCTION

compliance.qcert.org



COMPLIANCE AND DATA PROTECTION (CDP) DEPARTMENT INTRODUCTION



The mandate of MOTC, which empowers CDP, is set within **Emiri Decree No. 16 of 2014** amended by **Emiri Decree No. 8 of 2016**.

Department under the Cyber security Sector of the:

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



Compliance and
Data Protection
(CDP) Department

Information Protection Regulatory
Affairs

Accreditation and Certification

Information Assurance

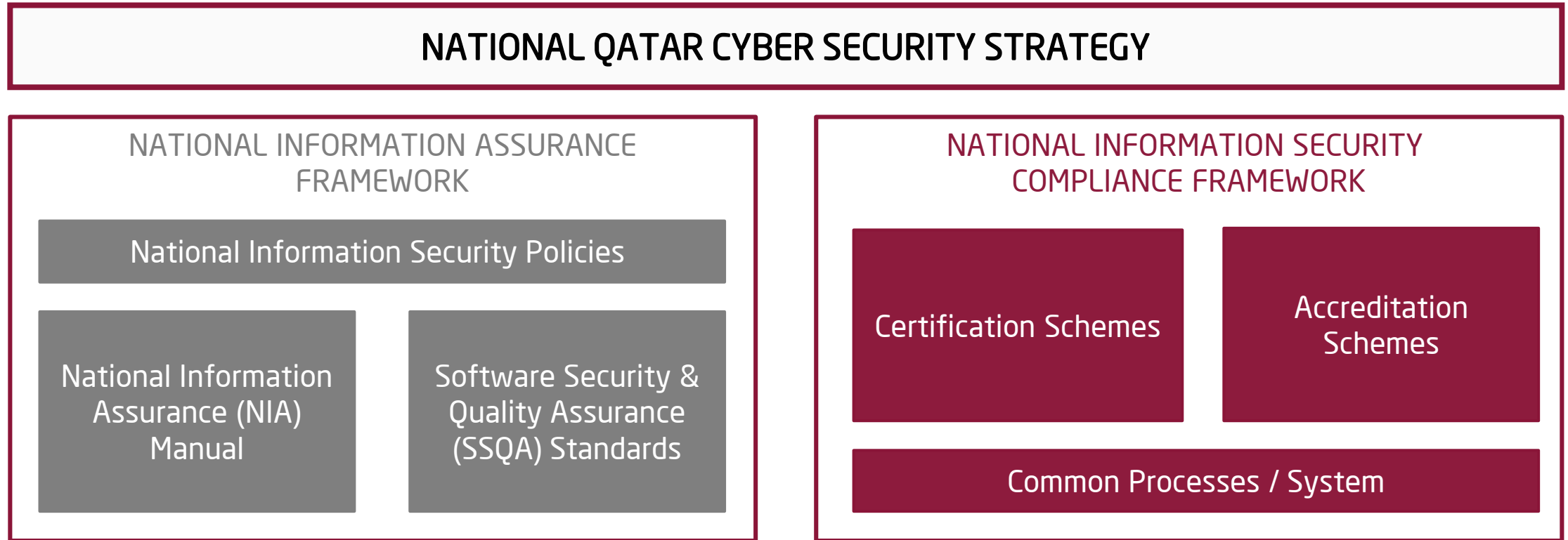
CYBERSECURITY STRATEGY

Qatar National Cyber Security Strategy (2014)

Establish a legal and regulatory framework to enable a safe and vibrant cyberspace.

National Information Assurance Framework (NIAF)
National Information Security Compliance Framework (NISCF).

NATIONAL INFORMATION SECURITY ASSURANCE FRAMEWORK OVERVIEW



To simplify the purposes of both frameworks, the intentions can be described as:

- The National Information Assurance Framework (NIAF) intends to drive and guide the achievement of security; while,
- The National Information Security Compliance Framework (NISCF) intends to validate and assure security.

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



ACCREDITATION OVERVIEW

compliance.qcert.org



DEFINITIONS



COMPLIANCE

Standards, specifications, regulations, or laws.

CERTIFICATION

NIA
COMPLIANT - امتثال

إطار آليات الامتثال للمعايير
الوطنية لأمن المعلومات
National Information Security
Compliance Framework

Formal procedure by which an authorized entity, assesses and verifies compliance, leading to a written attestation.

ACCREDITATION

SSQA • AUDIT •
ACCREDITED - معتمد

إطار آليات الامتثال للمعايير
الوطنية لأمن المعلومات
National Information Security
Compliance Framework

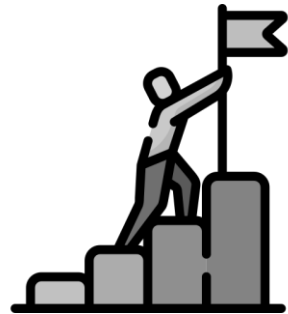
Assurance of an entity's competence in a specified subject or areas of expertise and their integrity

ACCREDITATION

“Accreditation is the formal recognition that an organization is competent to perform specific services, activities or tasks in a consistent, reliable and precise manner”.



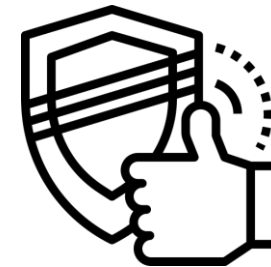
Impartial



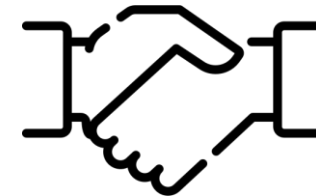
Objective



Transparent



Reliable



Trustworthiness

ACCREDITATION SERVICES



Advisory Services



Information security consulting and implementation services, excluding vulnerability assessment, penetration testing, security operations, and managed security services.



Audit Services



Audit services for Certification standards SSQA and NIA

CERTIFICATION SERVICES



NIA Standard



Certification for Information Security Management System

Government E-Service (SSQA)

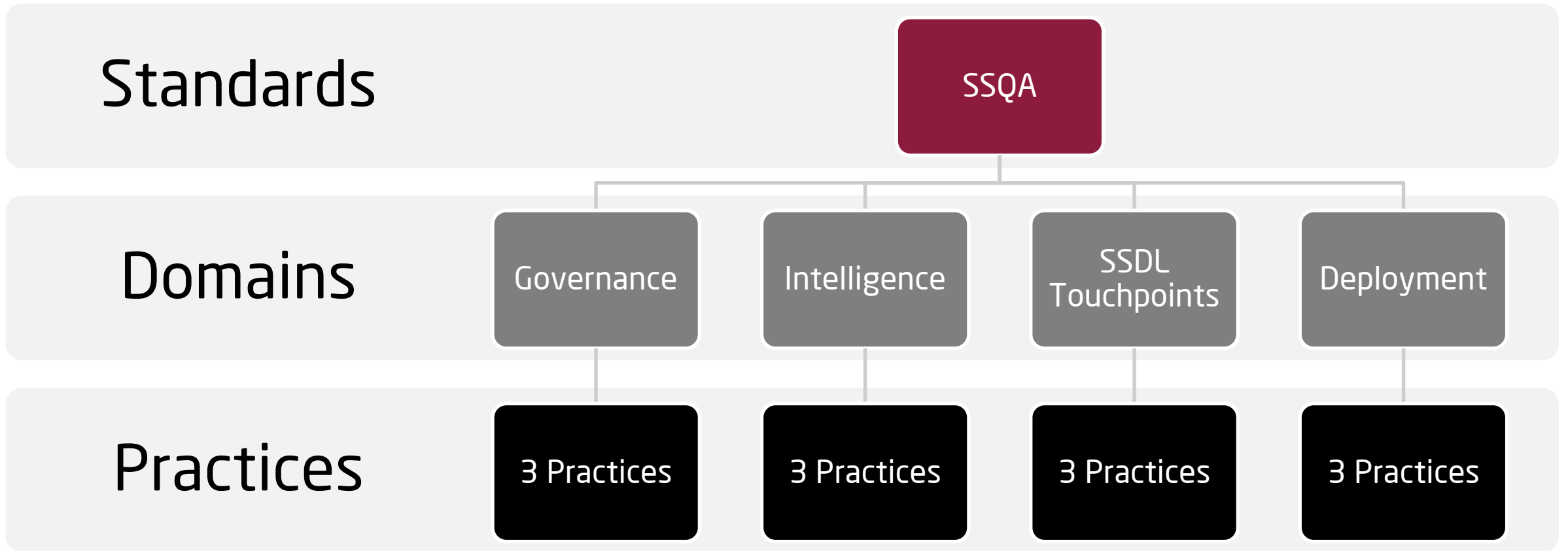


Certification of Government E-Services

NIA COMPLIANCE



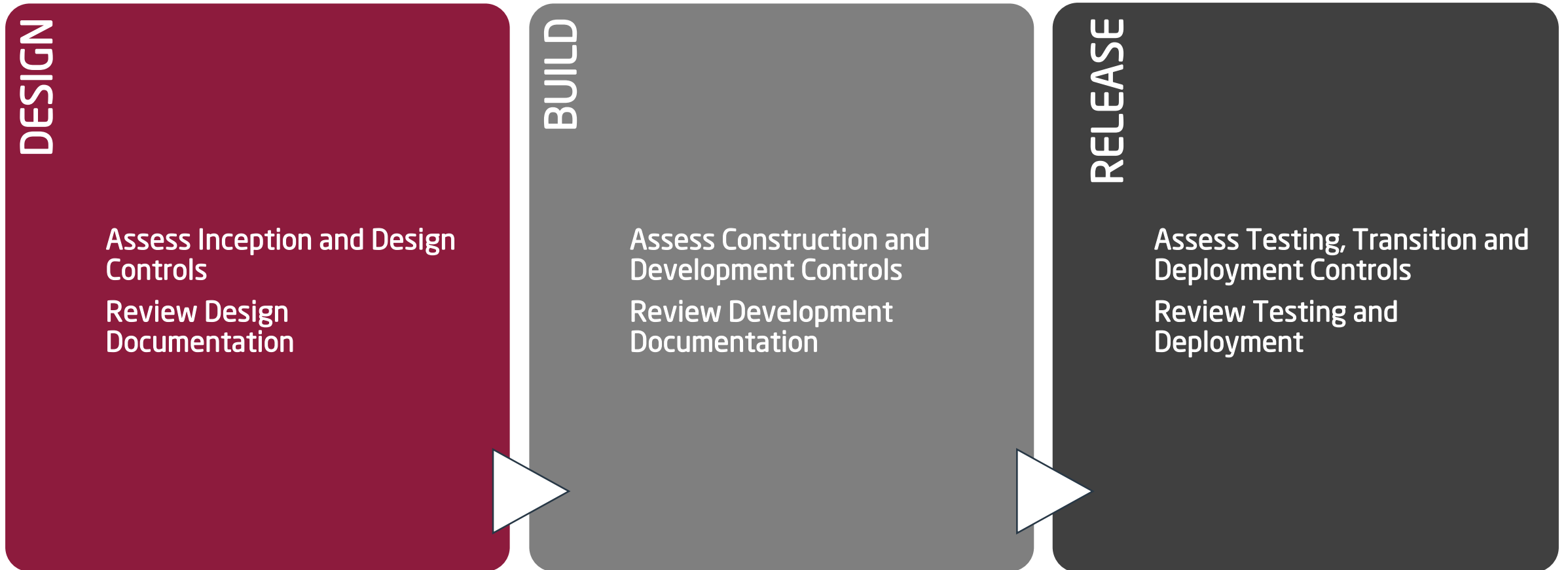
SSQA COMPLIANCE



SSQA COMPLIANCE



SSQA COMPLIANCE



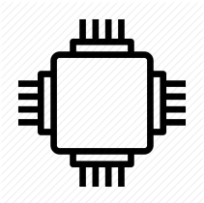
UPCOMING...

Upcoming Compliance



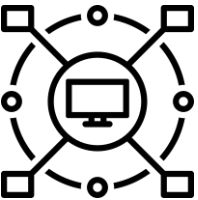
Personal Information Privacy Protection (PIPP)

Upcoming Certification Services



Common Criteria

Upcoming Accreditation Services



Security Operations Center (SOC) Services



Penetration Testing



Cloud Services

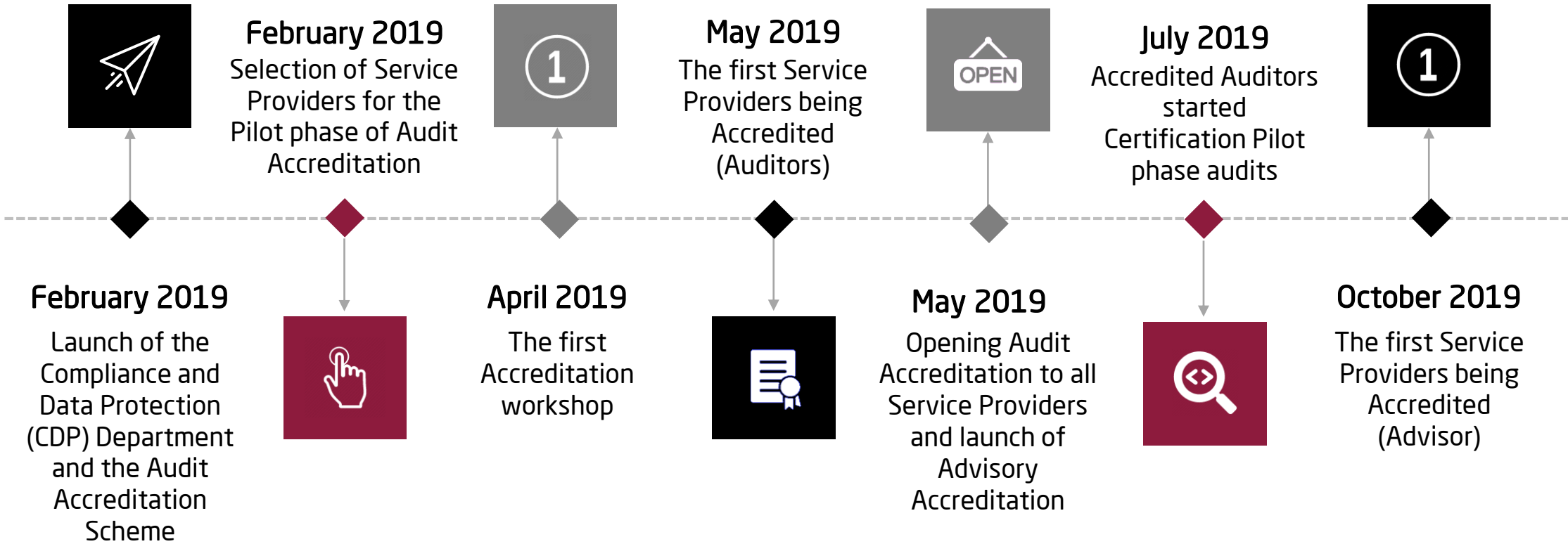
CERTIFICATION APPLICABILITY AND MANDATE



Type of Organisation	SSQA	NIA	PIPP	CC
Government Entities				
Semi-Government Entities				
Private (Large)				
Private (SMEs)				
Critical Sector Organisations (CSOs)				

Mandatory
 Applicable
 Future

TIMELINE



LIST OF ACCREDITED SERVICES PROVIDERS



Compliance and Data Protection

Home / Accreditation / Accredited Service Providers

List of Accredited Service Providers

Number:

Name:

Services:

Status:

Apply

Accr. Number	Name	Status	Expiry Date	Services
20029	Protiviti Member Firm Qatar LLC	Accredited	07 October 2022	Advisory
20028	Deloitte & Touche	Accredited	07 May 2022	SSQA Audit
00000	Ahmed Tawfik & Co Certified Public Accountants	Accredited	07 May 2022	SSQA Audit
20027	Deloitte & Touche	Accredited	07 May 2022	NIA Audit
20026	Ahmed Tawfik & Co Certified Public Accountants	Accredited	07 May 2022	NIA Audit

The Compliance and Data Protection (CDP) Department will maintain a listing of all Accredited Service Providers, allowing organizations to verify the status of Service Providers.

ACCREDITED SERVICE PROVIDERS

MOTC



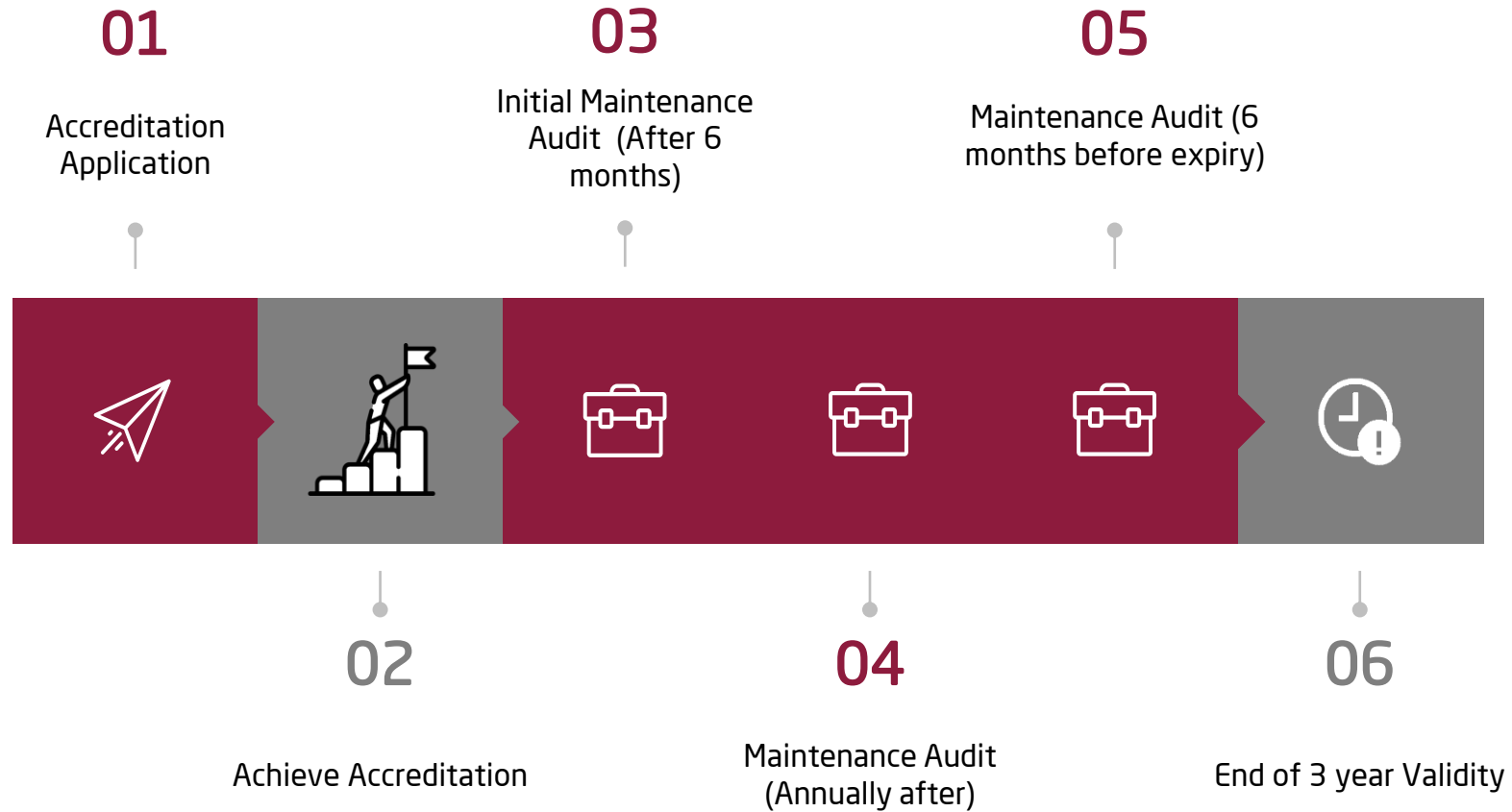
AHMED TAWFIK & CO.
Certified Public Accountants

ACCREDITATION BLOCKS

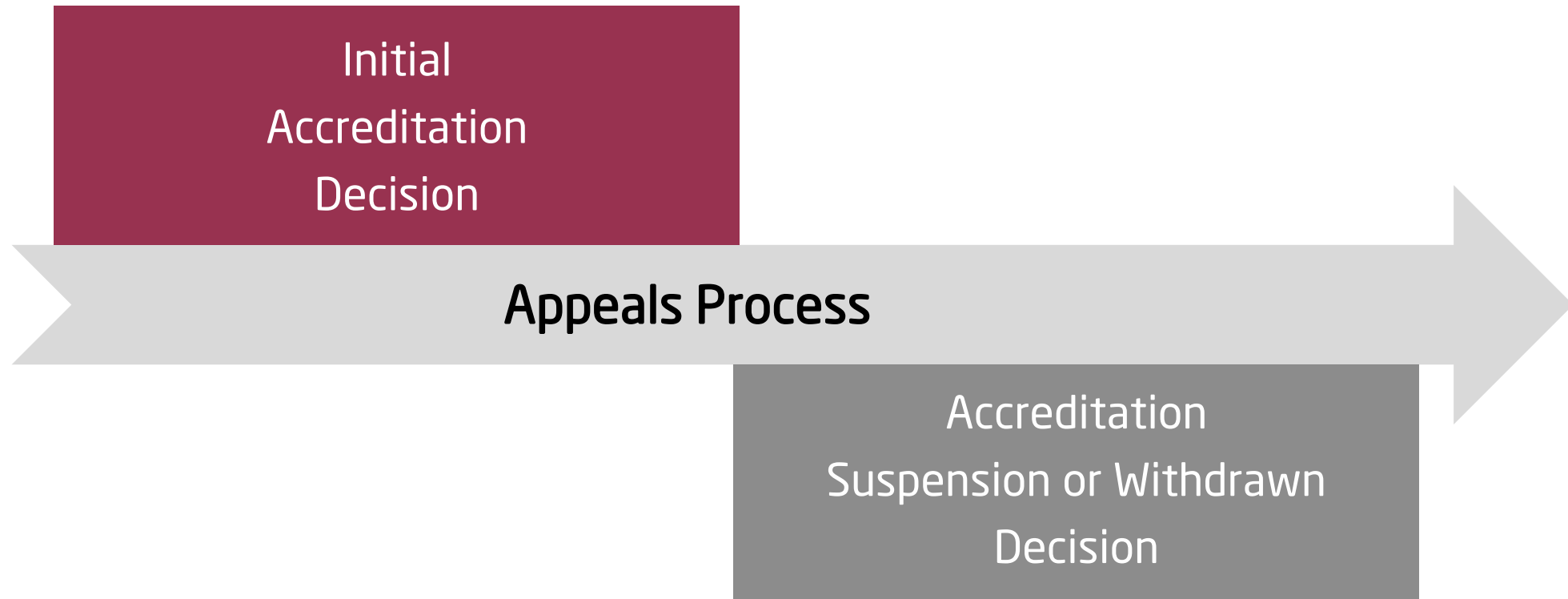


SELF-ASSESSMENT	VALIDITY	MAINTENANCE
<p>Accreditation is granted after successfully pass a self-assessment. The self-assessment requires the Service Provider to confirm its compliance with all the provisions of the self-assessment and provide evidence of it</p>	<p>Accreditation certificate will be Valid for a period of three (3) years, subject to successful accreditation maintenance cycle</p>	<p>Accreditation will be maintained through a Combination of Scheduled and Unscheduled Audits</p>

ACCREDITATION LIFECYCLE

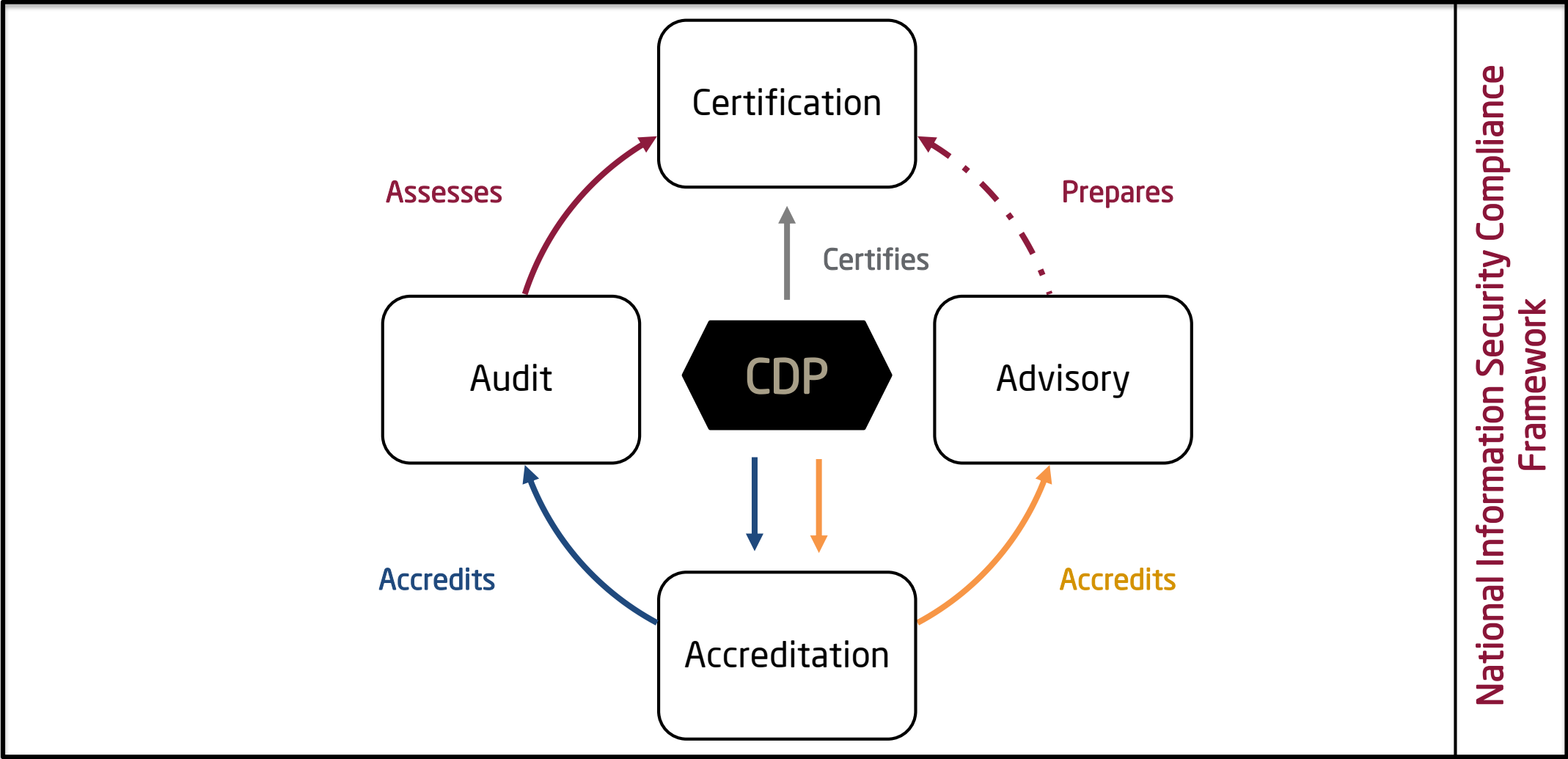


ASSURANCE AND IMPARTIALITY



NISCF SCHEMES INTEGRATION

National Information Assurance Framework



National Information Security Compliance Framework

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS

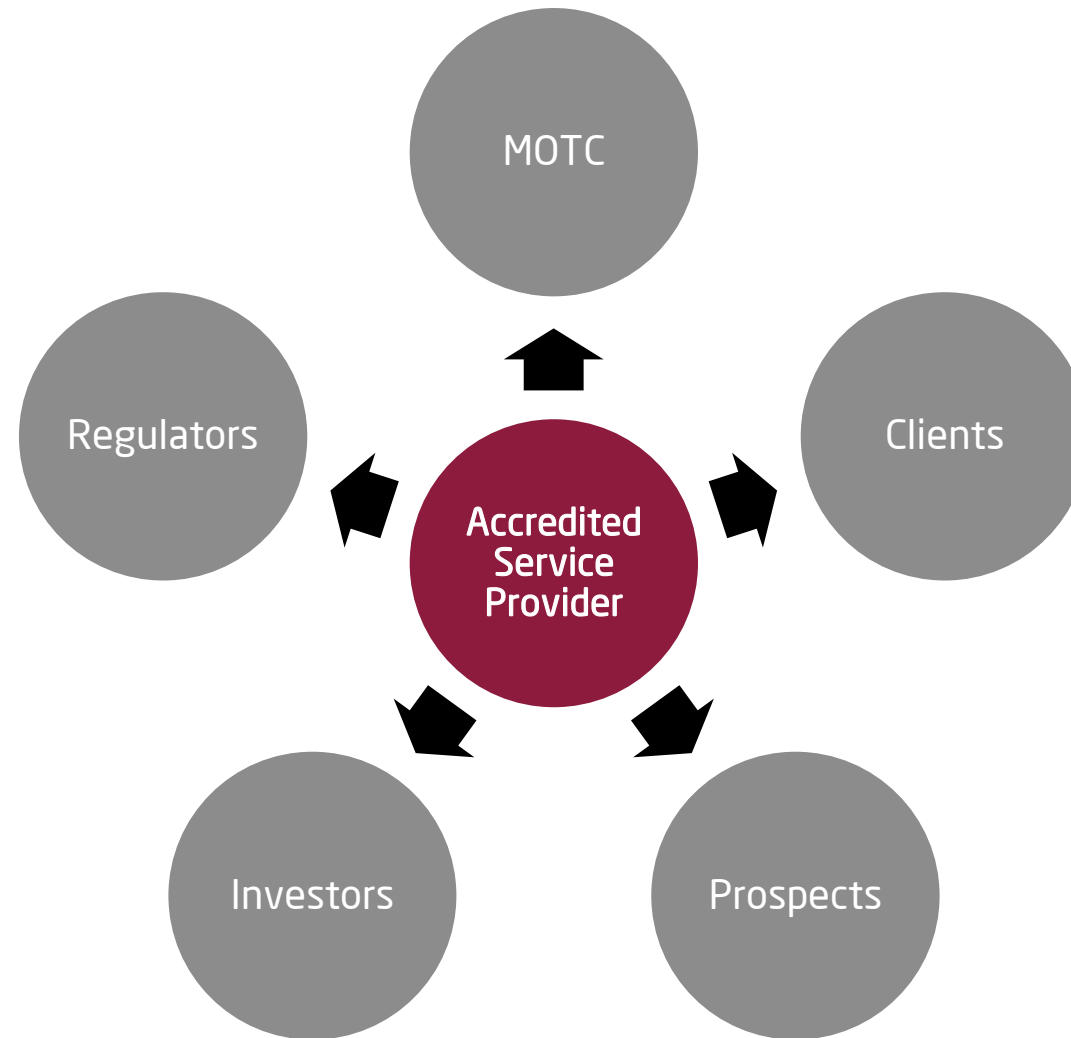


ACCREDITATION VALUE PROPOSITION

compliance.qcert.org



ACCREDITATION INTEGRATED LANDSCAPE



PURPOSE OF ACCREDITATION



ACCREDITATION BENEFITS



PRIVILEGED ACCESS

Provides access to closed market for Certification audit engagements



NEW OPPORTUNITIES

Provides Accredited Service providers additional marketing opportunities



THE BIG LEAGUE

Provides any Service Provider to be considered and recognized by top companies



PREFERRED

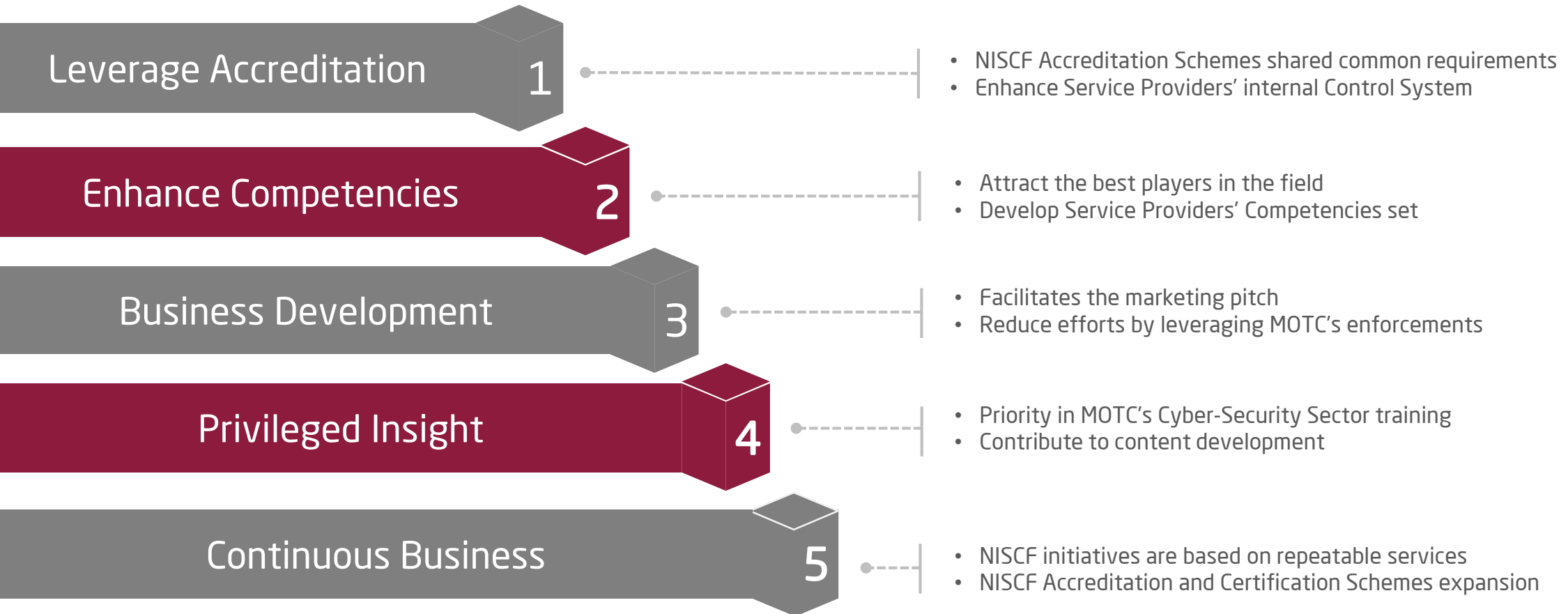
Gives a preferred Service Provider status, once accredited



EXPOSURE

Provides higher exposure by being listed on the CDP website

ACCREDITATION ADDED VALUE



ACCREDITATION AWARD

The accreditation certificate awarded following successful application provides a point-in-time reference to an Organization's compliance with the NISCF accreditation requirements for a specific service area.

The Compliance and Data Protection Department maintains a listing of all Accredited Service Providers, allowing organizations to verify the status of Service Providers.

Compliance and Data Protection

Home Accreditation Certification and Compliance Data Privacy Library Contact Us Portal

Home / Accreditation / Accredited Service Providers

List of Accredited Service Providers

Number Name Services

Status

Apply

Accr. Number	Name	City	Status	Expiry Date	Services
--------------	------	------	--------	-------------	----------

Q-CERT | وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

ACCREDITATION
CERTIFICATE

THIS IS TO ATTEST THAT

XYZ Company Name

has met the accreditation requirements of the National Information Security Compliance Framework to provide independent audit services in relation to the National Information Assurance (NIA) certification.

Certification Body: **Compliance and Data Protection (CDP) Department**
Certificate ID: **A/NIA/2019/98765**
Issuance Date: **07-FEB-2019**

This certificate supersedes any previous accreditation bearing an earlier effective date. This accreditation will remain valid for three years from the date of issuance, unless invalidated through suspension or withdrawal of accreditation.

NIA ACCREDITED • AUDIT • معتمد - إطار آليات الامتثال للمعايير الوطنية لأمن المعلومات National Information Security Compliance Framework

Erg. Dena Al-Abdella
Compliance and Data Protection Director
Cyber Security, MOTC

Signed on behalf of the Compliance and Data Protection (CDP) Department, Ministry of Transport & Communications (MOTC), State of Qatar

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



ACCREDITATION LIFECYCLE

compliance.qcert.org



ACCREDITATION LIFECYCLE OVERVIEW



Achieving Accreditation



Maintaining Accreditation



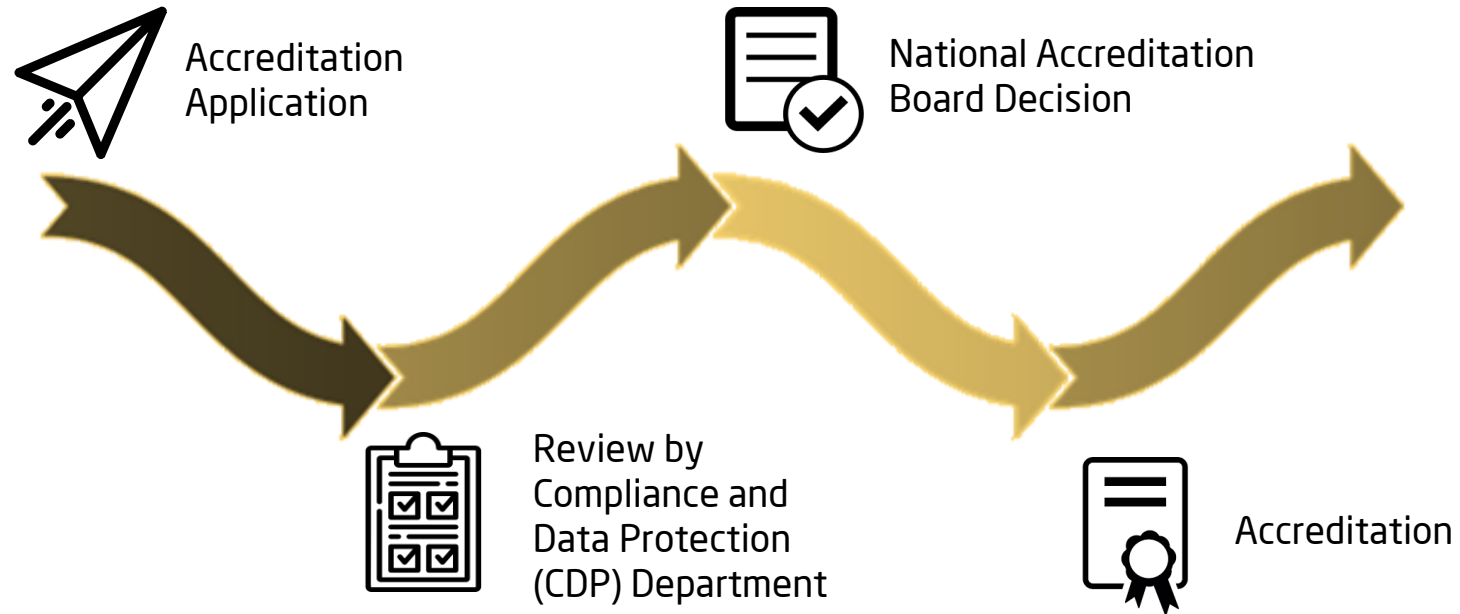
Accreditation revocation



Complaints and Appeals



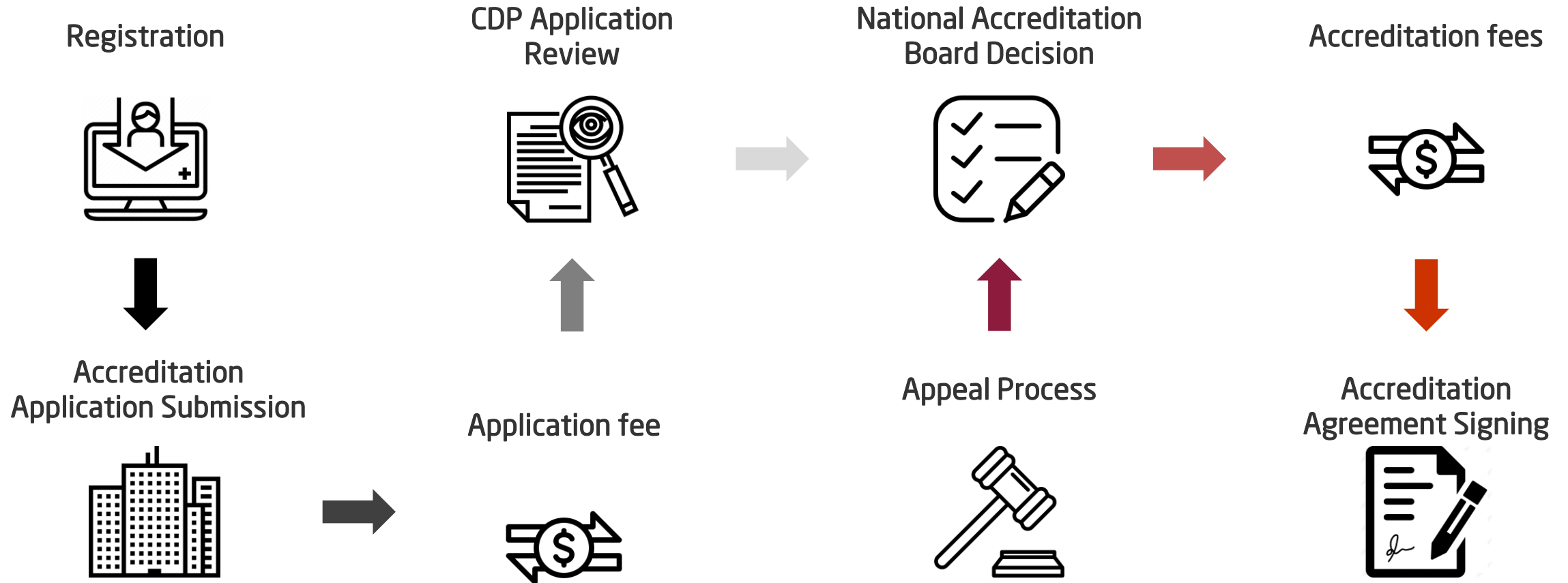
ACHIEVING ACCREDITATION JOURNEY



ACCREDITATION APPLICATION REQUIREMENTS



ACHIEVING ACCREDITATION DETAILED



FEES



- All fees in relation to Accreditation and Certification are waived until 01 January 2020. This includes all Application and Maintenance Fees.

ACCREDITATION LIFECYCLE OVERVIEW



Achieving Accreditation



Maintaining Accreditation



Accreditation revocation



Complaints and Appeals



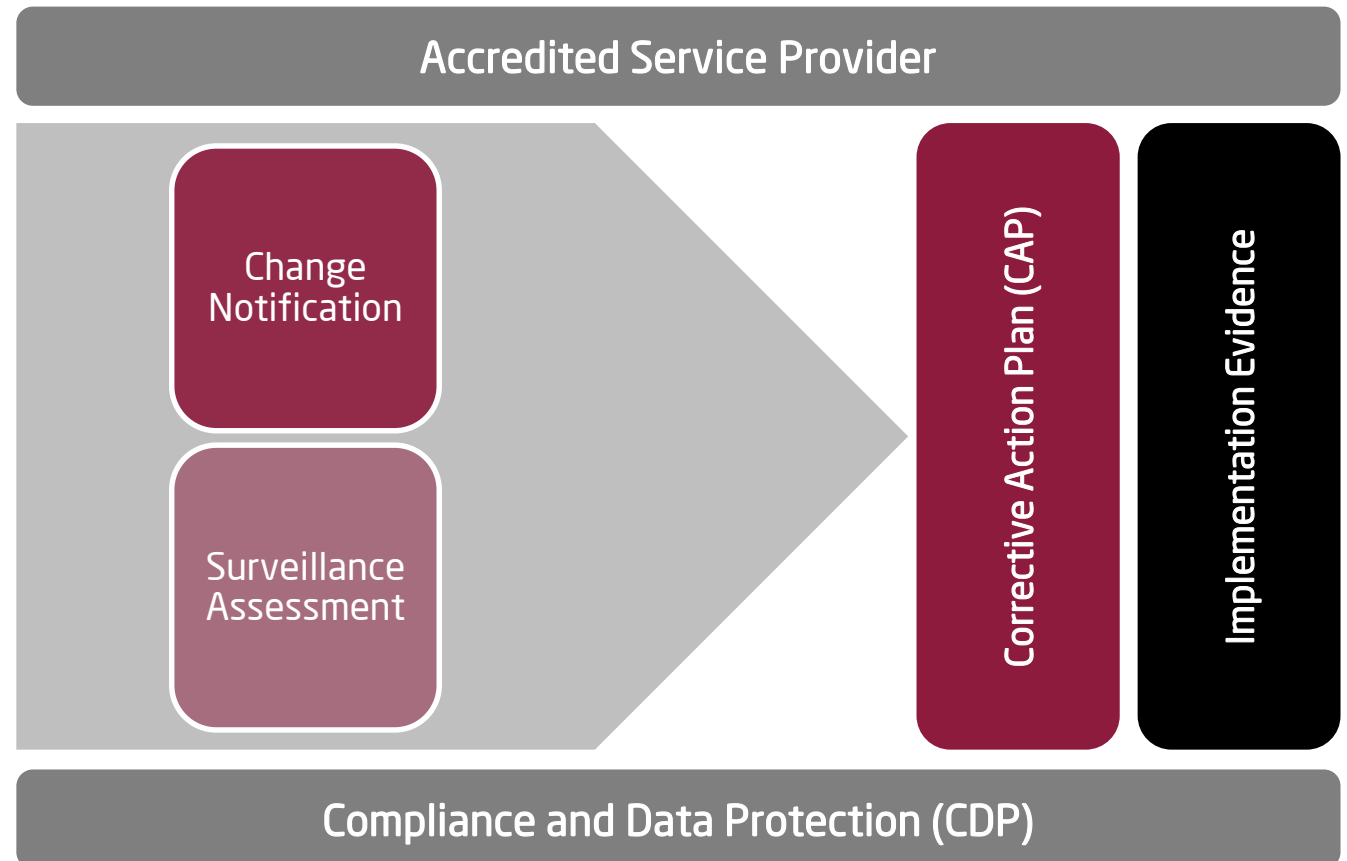
MAINTAINING ACCREDITATION

This is achieved through a combination of scheduled and random surveillance audits.

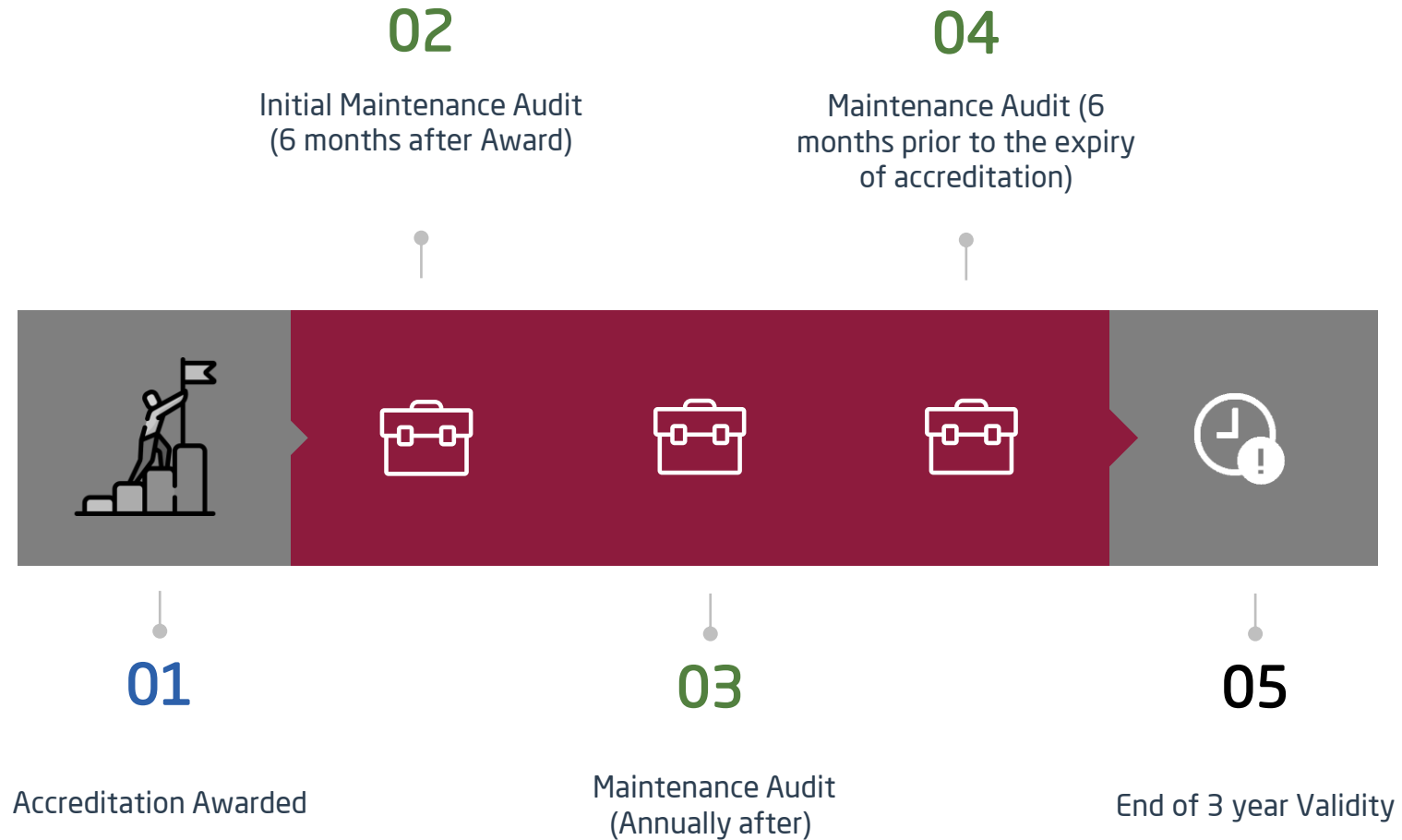
The Corrective Action Plan (10) calendar days following notification of the non-conformity.

The remediation time-frame varies dependent upon the severity of the non-conformity.

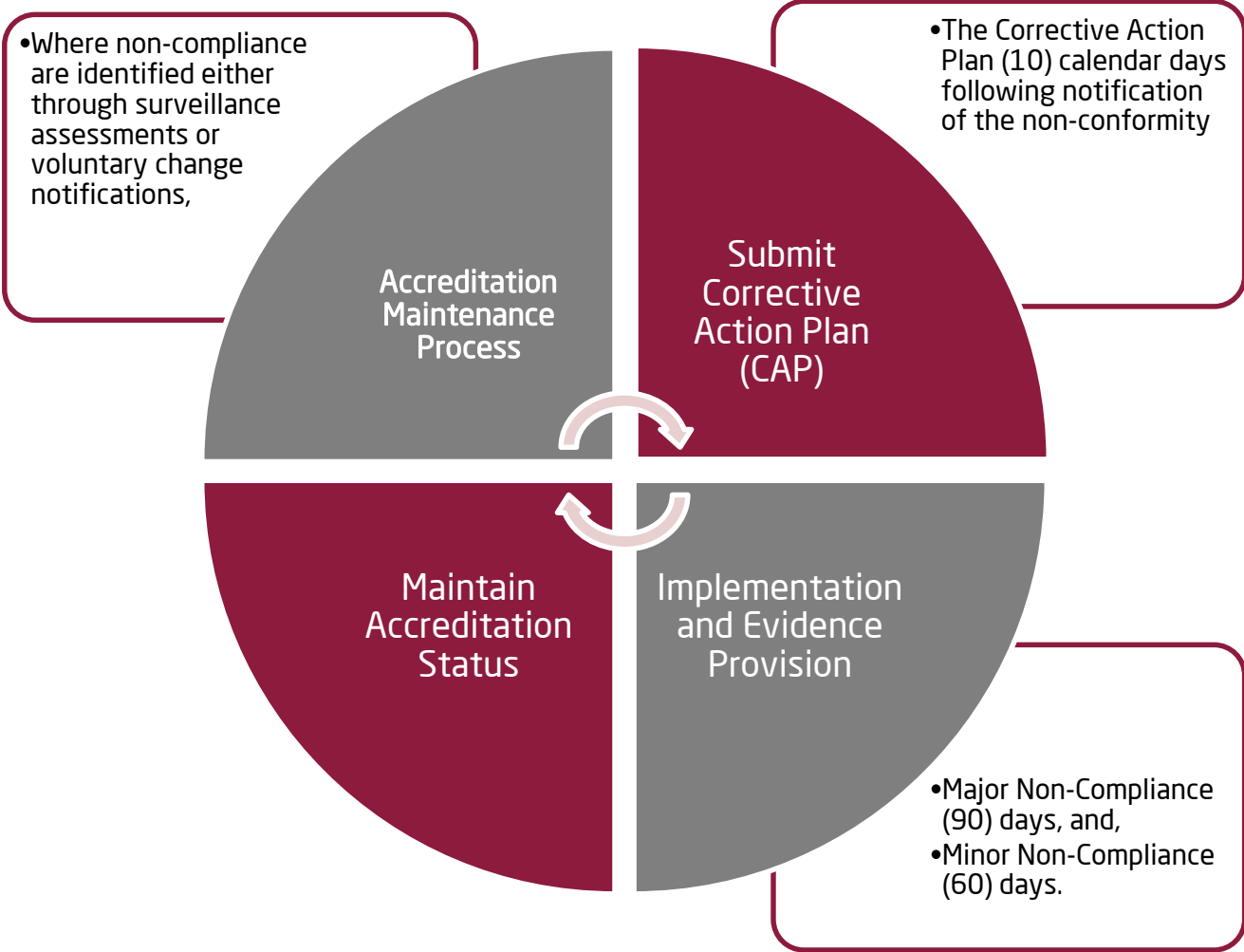
- Major Non-Compliance (90) days, and,
- Minor Non-Compliance (60) days.



MAINTAINING ACCREDITATION CYCLE



MAINTAINING ACCREDITATION



ACCREDITATION LIFECYCLE OVERVIEW



Achieving Accreditation



Maintaining Accreditation



Accreditation revocation

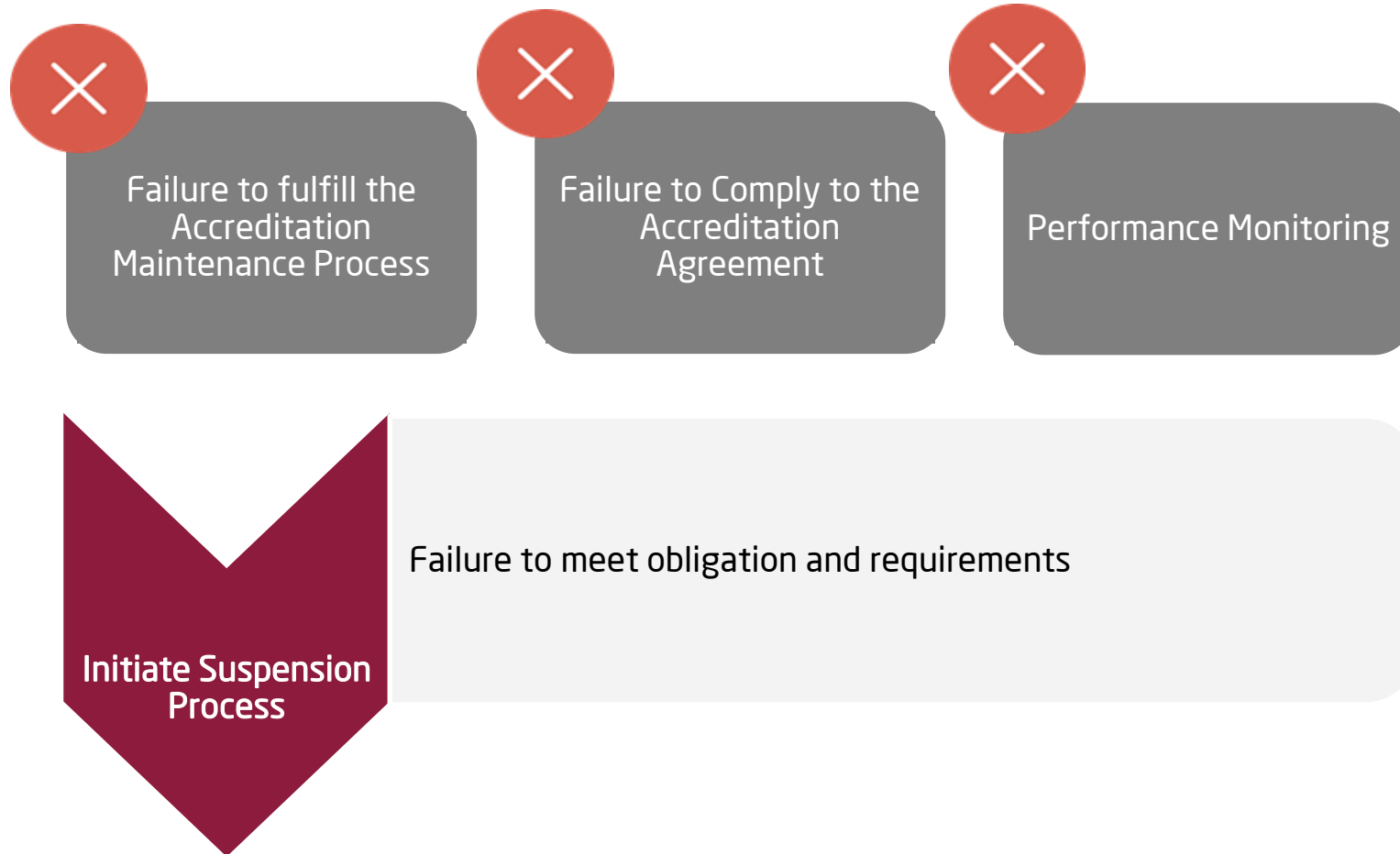


Complaints and Appeals



CONDITIONS TO ACCREDITATION REVOCATION

Accredited Organizations are required to address compliance concerns identified through either:

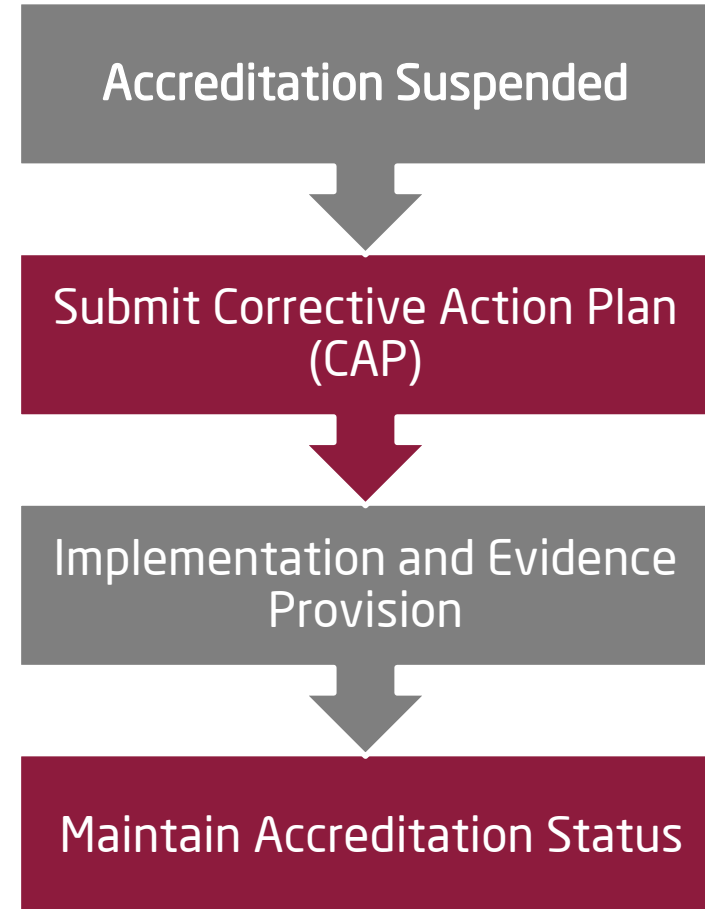


ADDRESSING COMPLIANCE CONCERNS

Where non-compliance are identified, appropriate remediation will be necessary to maintain accreditation.

To ensure the suitable remediation of identified non-conformities;

- The Accredited Service Provider will be required to submit a **Corrective Action Plan (CAP)**, agreed with CDP,
- And provide **Implementation Evidence** that provides assurance to CDP of the suitable and complete remediation of concerns.
- Non-Compliance Corrective Action Plan and Implementation Evidence not received or agreed within timeframe the revocation process is Initiated.



ACCREDITATION REVOCATION PROCESS OVERVIEW

Failure to address compliance concerns from the suspension process will lead to the revocation of accreditation.



- Accredited Organization is notified of Suspension (including detail of issues leading to the suspension)
- During the Suspension timeframe (not exceeding six-months), the Accredited Organization is unable to perform new certification assessments but may continue with 'in-flight' assessments or pre-authorized assessments.



- If the issue (and it's Root Cause) are not remediated within the 6-month suspension window, through the implementation of an agreed Corrective Action Plan and the provision of suitable Implementation Evidence, the Accreditation of the Third-Party will be withdrawn.
- In instance of Accreditation Withdrawal, the affected Third-Party may appeal the withdrawal or re-apply for accreditation.

ACCREDITATION LIFECYCLE OVERVIEW



Achieving Accreditation



Maintaining Accreditation



Accreditation revocation



Complaints and Appeals



COMPLAINTS

Complaints are categorised and reviewed by the **CDP**.

The complainant is advised of the review outcome and advised of their right to appeal.



APPEALS



Level 1 Appeal

- Committee of individuals from CDP without any conflict of interest

Level 2 Appeal

- Review by The Appeal Review Board (Level 2) If decision at level 1 was not satisfactory.

ACCREDITATION LIFECYCLE OVERVIEW



Achieving Accreditation



Maintaining Accreditation



Accreditation revocation



Complaints and Appeals



وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



ACHIEVING ACCREDITATION

compliance.qcert.org



ACCREDITATION SERVICES



Advisory Services



Information security consulting and implementation services, excluding vulnerability assessment, penetration testing, security operations, and managed security services.

Audit Services



Audit services for Certification standards
SSQA and NIA

ACCREDITATION APPLICATION REQUIREMENTS



ACCREDITATION APPLICATION REQUIREMENTS

- Officially appoint a Single Point of Contact (SPOC), who shall be responsible for maintaining the link and all communication between the Parties.
- Ensure that the SPOC is familiar with all the Accreditation Requirements and ensures that all such requirements comply with the provisions of CDP.
- Ensure that the SPOC acts in a manner that does not compromise the integrity of the accreditation application process and that the applicant complies with the provisions of CDP.



ACCREDITATION APPLICATION REQUIREMENTS



- Submitting the Application package to the CDP through the Compliance and Data Protection (CDP) portal:

 - (New applicants will need to register a new account before continuing with the application process).
- Application package must be complete and submitted by the Single Point of Contact (SPOC) in the prescribed format
(Existing account holders should first ensure that the contact details for the account is accurate).

 - Application form must be accompanied by a Self-Qualification Questionnaire in respect to part 2: Staff information on the Service Provider Accreditation Application form.
- Service provider Self-assessment form; contains assessment controls of the relevant accreditation standard

 - This should be contingent on meeting all eligibility criteria, and all requested evidence must be provided on submission.

ACCREDITATION SELF-ASSESSMENT AREAS

The assessment area (s) contains assessment controls of the relevant accreditation service and should be contingent on meeting all eligibility criteria, and all requested evidence must be provided on submission.



Legal and contractual Requirements



Structural Requirements



Resource Requirements



Information Requirements



Process Requirements

AUDIT ACCREDITATION SPECIFIC ASSESSMENT AREAS





ACCREDITATION SELF-ASSESSMENT (SAMPLE)



	Control Description	Identify documentation and sections as applicable	Assessment (Compliance and Data Protection Department)	
		(Service Provider to provide details & evidence)	Suggested Evidence	Comments (Official use)
1	Requirement for Service Provider a			
b	Legal and Contractual Matters			
c	The Service Provider shall be a legal entity, or a defined part of a legal entity, such that it can be held legally responsible for all its audit and assessment activities in relation to the National Information Security Compliance Framework (NISCF) and related Certification Schemes.			
1.1.2	The Service Provider shall have a legally enforceable agreement for the provision of audit and assessment activities to its client.			
1.2	Management of Impartiality			
1.2.1	The Service Provider shall have top management commitment to impartiality in audit and assessment activities, providing a publicly accessible statement outlining that it understands the importance of impartiality in carrying out audit and assessment activities, manages conflicts of interest and ensures the objectivity of its audit and assessment activities.			

a. Requirement b. sub-category of Requirement c. Control to fulfill the requirement

ACCREDITATION SELF-ASSESSMENT (EVIDENCING)

	Description	Identify documentation and sections as applicable	Assessment (Compliance and Data Protection Department)	
		(Service Provider to provide details & evidence)	Suggested Evidence	Comments (Official use)
1	Requirement for Service Provider			
1.1	Legal and Contractual Matters			
1.1.1	The Service Provider shall be a legal entity, or a defined part of a legal entity, such that it can be held legally responsible for all its audit and assessment activities in relation to the National Information Security Compliance Framework (NISCF) and related Certification Schemes.	Refer Commercial Registration 2018-2019 attached	 Commerical Registration	
1.1.2	The Service Provider shall have a legally enforceable agreement for the provision of audit and assessment activities to its client.	All engagements with clients are government by a contract ('engagement letter'). There are standard legally enforceable terms and conditions, which are further customized for each countries laws and regulations, and these terms and conditions are included in the engagement	 Approved Legal Agreement	
1.2	Management of Impartiality			
1.2.1	The Service Provider shall have top management commitment to impartiality in audit and assessment activities, providing a publicly accessible statement outlining that it understands the importance of impartiality in carrying out audit and assessment activities, manages	Refer to below link to publicly accessible website, with statement from outlining independence policies and commitment to impartiality.	https://www2.sp.com/glob/en/pages/independence.html	

ADVISORY ACCREDITATION SPECIFIC ASSESSMENT AREAS





ACCREDITATION SELF-ASSESSMENT (SAMPLE)



Ref	Description	Identify documentation and sections as applicable (Service Provider to provide details & evidence)	Suggested Evidence
1.3	Liability and Financing		
1.3.1	The Service Provider shall be able to demonstrate that it has evaluated the risks arising from its Implementation Services and that it has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates.		Professional Indemnity
1.3.2	Please provide the latest audited* financial statements of your firm. *Only applicable where it is a statutory requirement for the firm to have audited financial statements.		Financial Statements

ACCREDITATION SELF-ASSESSMENT (EVIDENCING)

Ref	Description	Identify documentation and sections as applicable (Service Provider to provide details & evidence)	Suggested Evidence
1.3	Liability and Financing		
1.3.1	The Service Provider shall be able to demonstrate that it has evaluated the risks arising from its Implementation Services and that it has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates.	XYZ Company has Professional Indemnity Insurance to liabilities arising from operations and the geographic areas in which it operates.	 Professional Liability Insurance -
1.3.2	Please provide the latest audited* financial statements of your firm. *Only applicable where it is a statutory requirement for the firm to have audited financial statements.	Please refer to financial Audit statements for reference	 XYZ Company Financial Report - 20

ACCREDITATION SELF-ASSESSMENT OVERVIEW



General Accreditation requirements	Audit Specific Requirements	Advisory Specific Requirements
<ul style="list-style-type: none">- Legal & Contractual- Management of Liability- Liability and Financing- Organizational Structure- Competence- Personnel Evaluation- Record- Outsourcing- Public Information- Confidentiality	<ul style="list-style-type: none">- Impartiality- Safeguarding Impartiality- External Experts- Exchange With Clients- Audit Plan- Audit Program- Evidencing	<ul style="list-style-type: none">- Financing- Control Environment- Project management- Information security management

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



QUESTIONS AND ANSWERS SESSION

compliance.qcert.org



CDP'S COMPLIANCE PORTAL AND HELPDESK



CDP's main points of contacts:

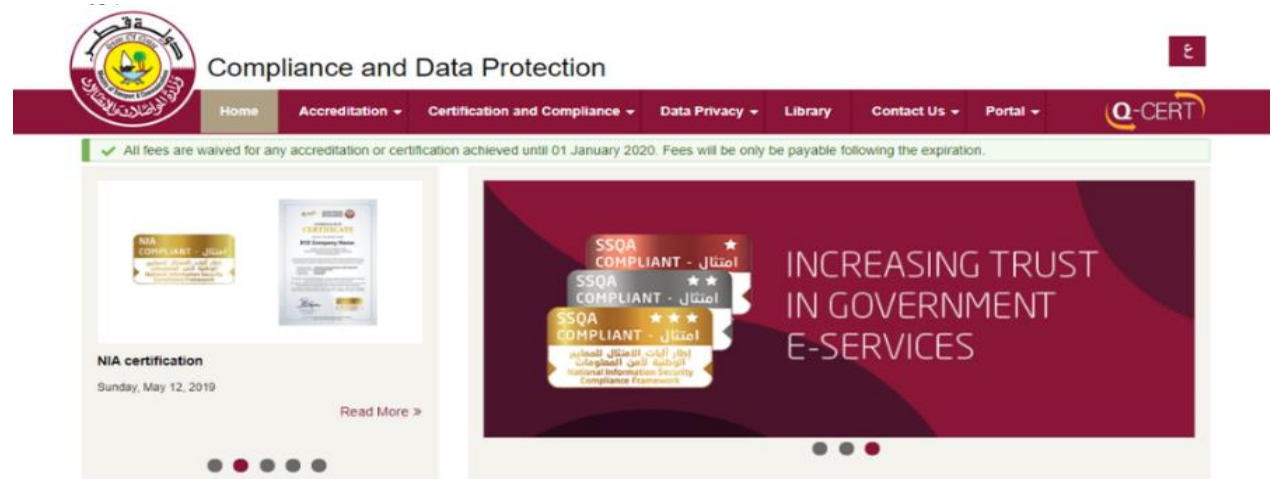
Website: compliance.qcert.org

CDP Portal: compliance-portal.qcert.org

Email: cdp@motc.gov.qa

24hrs Phone lines: +974 4499 5399
email: cdpHelpdesk@motc.gov.qa for support inquiries

compliance.qcert.org



Compliance and Data Protection Department

The Compliance and Data Protection (CDP), a department of the Ministry of Transport and Communications (MOTC) and the Government of the State of Qatar, is recognized as the entity responsible for ensuring compliance with the National Information Security Compliance Framework (NISCF) and issuing certification in relation to the frameworks compliance schemes. CDP is also entrusted to validate the competence and integrity of Service Provider organizations providing services relating to the NISCF Service Areas and to provide recommendation in relation to an application for accreditation in relation to the NISCF Service Areas.

The mandate of MOTC, which empowers CDP, is set within Emiri Decree No. 16 of 2014 amended by Emiri Decree No. 8 of 2016. It is this mandate, and through the decision of the Cabinet - decision No. (26) of 2018, the empowerment provides the authority to supervise, regulate and develop the sector of Information and Communications Technology in the State



وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



Thank You

P.O. Box 2304, Doha, Qatar
T +974 4499 5399
CDP@motc.gov.qa
compliance.qcert.org

