وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Compliance and Data Protection Department

Service Provider Accreditation

Accreditation Certification Scheme

compliance.qcert.org

Q-CERT

WORKSHOP CONTENTS AUDIT ACCREDITATION

MOTC

1. FRAMEWORK AND SCHEME INTRODUCTION

   Introduction To Compliance And Accreditation

   Information Assurance Framework Overview

   Compliance And Data Protection (CDP) Department Introduction

2. ACCREDITATION INITIATION

   Audit Accreditation Scheme

   Accreditation Lifecycle Overview

   Understanding The Process Of Accreditation

   Completing The Self-assessment & Providing Evidence

   Auditing Approach

   Accreditation Agreement And Audit Ethics

3. ACCREDITATION MANAGEMENT

   Maintaining Accreditation

   Conditions For Losing Accreditation

   Complaints And Appeals

   Questions And Answers

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

FRAMEWORK AND SCHEME INTRODUCTION

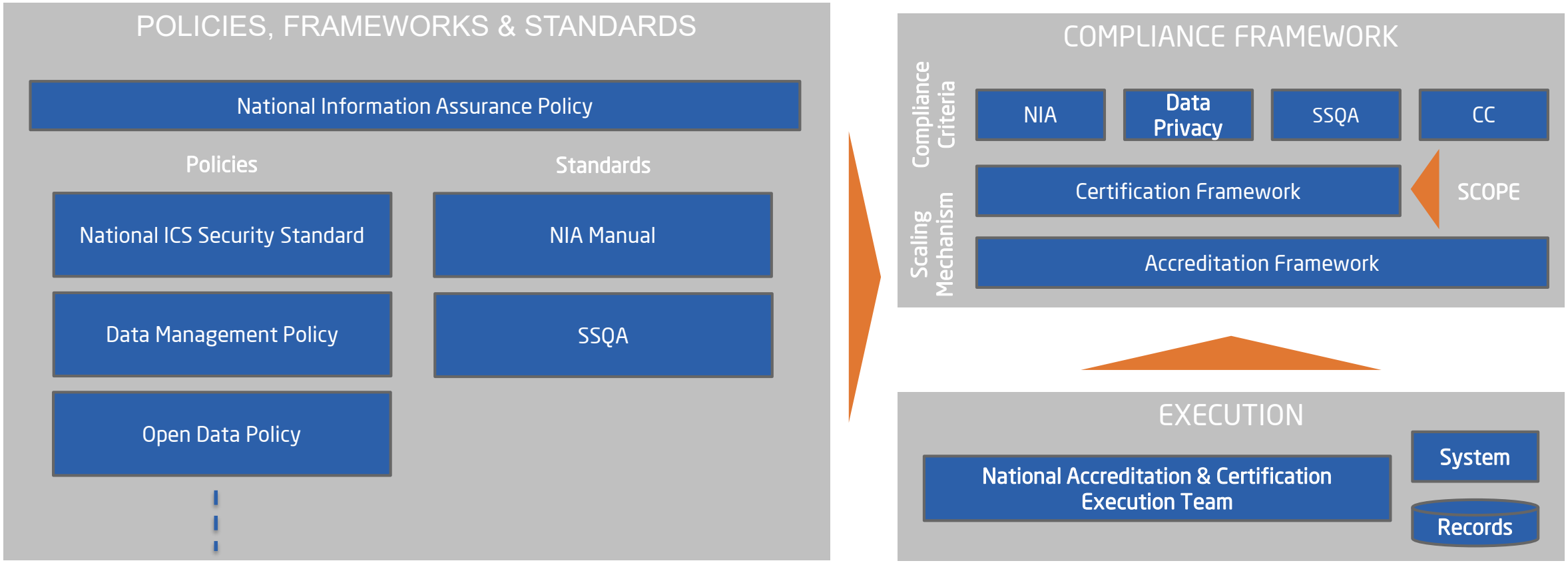
compliance.qcert.org

Q-CERT

INTRODUCTION TO COMPLIANCE AND ACCREDITATION

MOTC

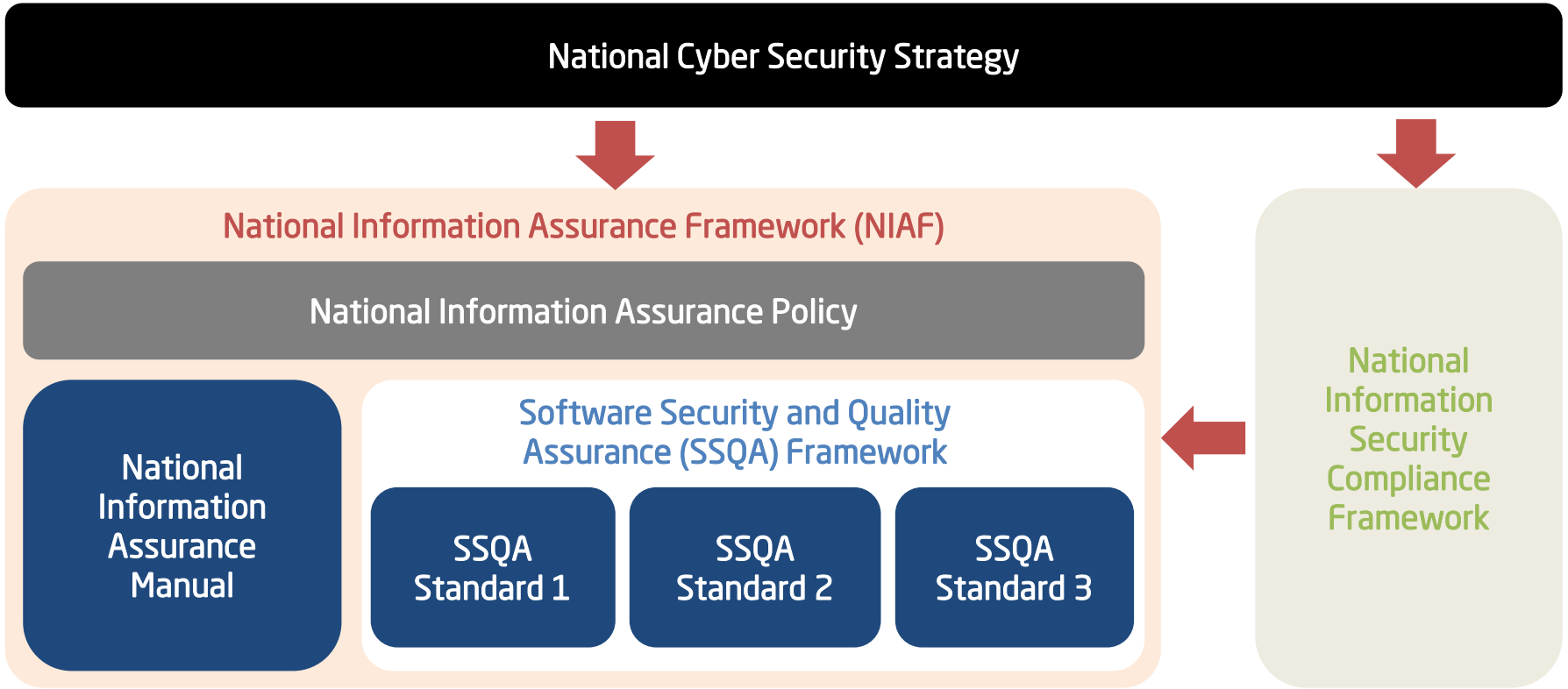
NATIONAL CYBER SECURITY STRATEGY



compliance.qcert.org

INFORMATION ASSURANCE FRAMEWORK OVERVIEW

MOTC



The Software Security And Quality Assurance (SSQA) Framework integrates into the National Information Assurance Framework (NIAF) to enhance digital services.

The National Information Security Compliance Framework (NISCF) assures the implementation of the NIAF controls.

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.**

compliance.qcert.org

COMPLIANCE AND DATA PROTECTION (CDP) DEPARTMENT INTRODUCTION

Our role is to support the National Information Assurance Framework (NIAF) by assuring the implementation of National Standards and Service Provider Capabilities.

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 No. 26 of 2018, the empowerment that provides the authority to supervise, regulate and develop the sector of Information and Communications Technology in the State of Qatar.

Compliance and Data Protection (CDP) Department

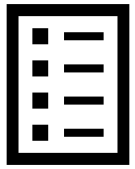
- Information Protection Regulatory Affairs
- Accreditation and Certification
- Information Assurance

compliance.qcert.org

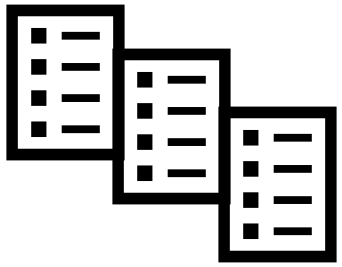
CDP'S COMPLIANCE SERVICES

MOTC

Standards



NIA Standard



SSQA Standard(s)

Compliance Certifications

NIA

- Organization-focused compliance approach
- Aligned with ISO27001

SSQA

- System or Service-focused compliance approach
- Aligned with BSIMM7

compliance.qcert.org

APPLICABILITY AND MANDATORY REQUIREMENTS

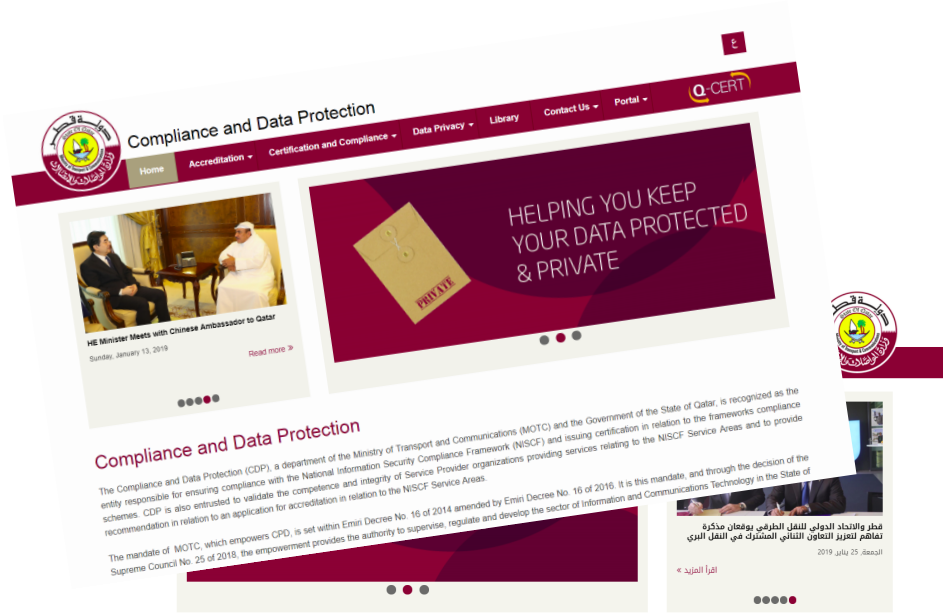
MOTC

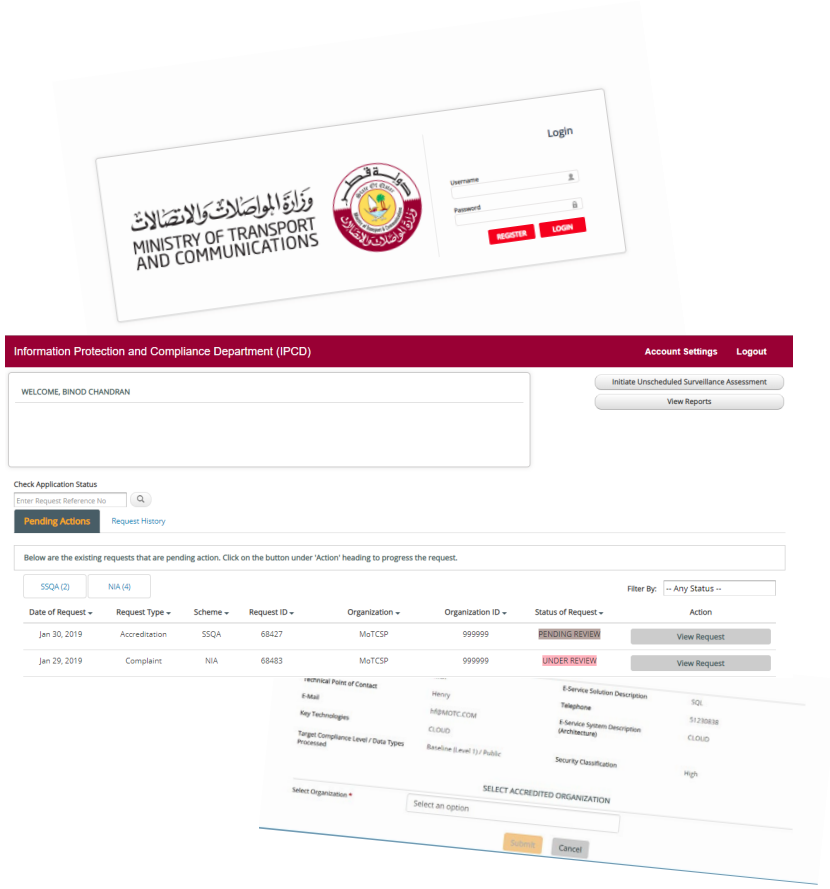
Organisation Type	SSQA	NIA	PIPP	CC
Government Entities	✓	✓	✓	✓
Semi-Government Entities	✓	✓	✓	✓
Private (Large)		✓	✓	
Private (SMEs)		✓	✓	
Critical Sector Organisations (CSOs)	✓	✓	✓	✓

Mandatory
Applicable
Future

compliance.qcert.org

CDP'S COMPLIANCE PORTAL AND HELPDESK





إدارة الامتثال وحماية المعلومات

تتولى وزارة المواصلات والاتصالات (MOTC) مسؤولية الإشراف على إدارة الامتثال وحماية المعلومات باعتبارها، فيما يخص الصالح العام، الجهة المعنية المسؤولة عن تحديد الكفاءة الفنية والنزاهة للمؤسسات التي تقدم خدمات التقييم والاختبار والامتثال، وعن إصدار التصديقات للمؤسسات الساعية إلى الحصول على تصديق الامتثال في دولة قطر.

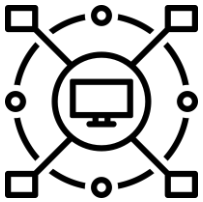
بناءً على القرار الاميري رقم 16 لعام 2014 و المعدل بالقرار الاميري رقم 8 لعام 2016 و بالإضافة الى قرار مجلس الوزراء رقم 25 لعام 2018 بتعديل الهيكل التنظيمي لوزارة المواصلات والاتصالات تختص الوزارة بتنظيم وتطوير والإشراف على قطاع تكنولوجيا المعلومات والاتصالات وحماية البنية المعلوماتية التحتية بدولة قطر و ضمان الامتثال للمعايير الوطنية للأمن السيبراني بما يتوافق مع متطلبات أهداف التنمية الوطنية.

compliance.qcert.org

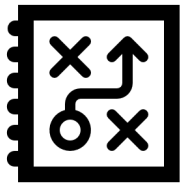
CDP'S FUTURE GROWTH

MOTC

Accredited Service Areas



Security Operations Center (SOC) Services



Penetration Testing

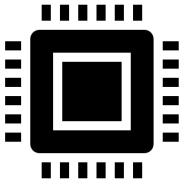
Cloud Services

Advisory Services

Compliance Schemes

Personal Information Privacy Protection (PIPP)

Common Criteria



compliance.qcert.org

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

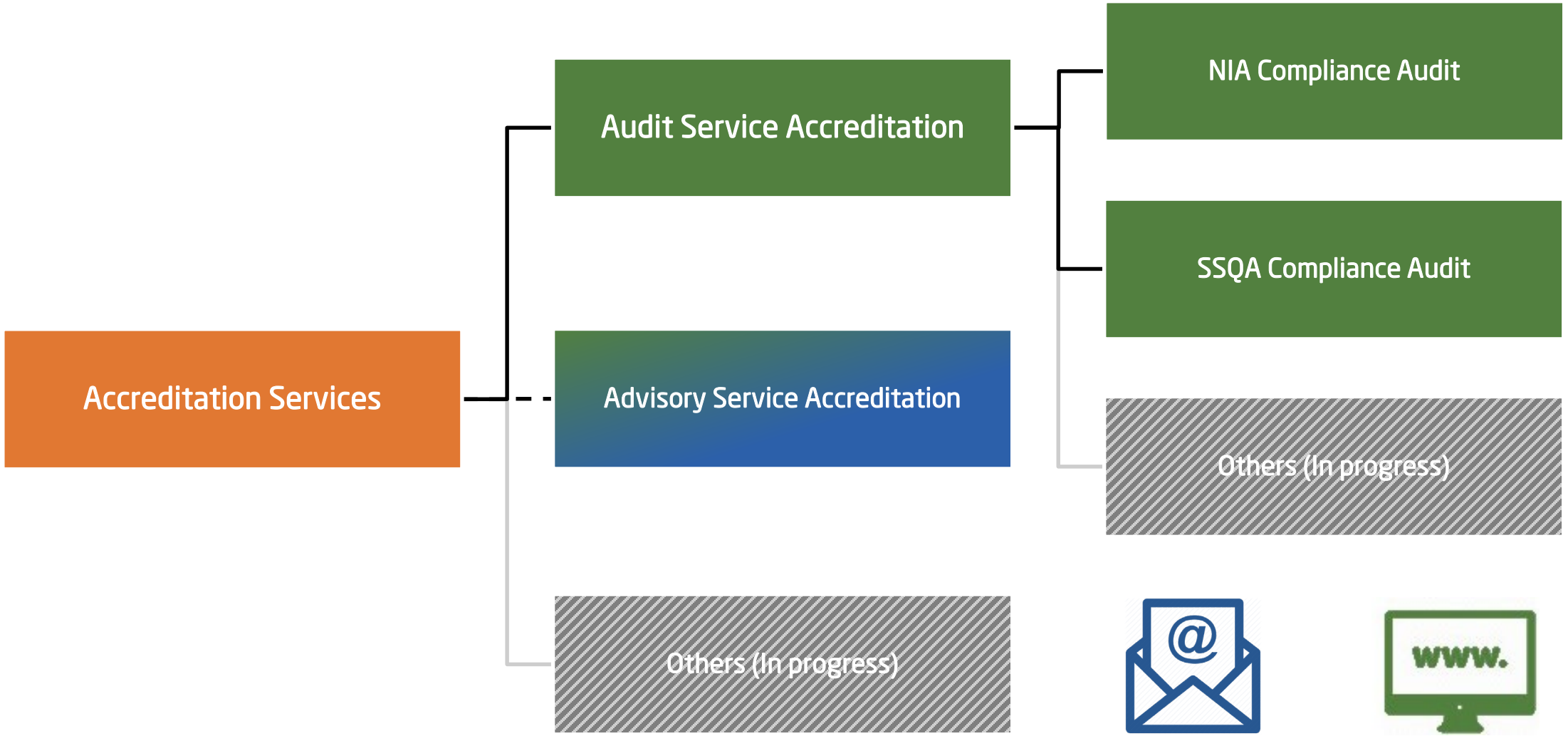
ACCREDITATION INITIATION

compliance.qcert.org

Q-CERT

CDP'S ACCREDITATION SERVICES

MOTC



ACCREDITATION BENEFITS

MOTC

PRIVILEGED ACCESS

Provides access to closed market for Assessment & Certification

NEW OPPORTUNITIES

Provides Accredited Service providers additional marketing opportunities

THE BIG LEAGUE

Provides smaller businesses access to the Government sector

PREFERRED

Provides preferred supplier status, once accredited

EXPOSURE

Provides higher exposure by being listed on the CDP website

ACCREDITATION LIFECYCLE OVERVIEW

MOTC

Achieving Accreditation:
Prior to becoming and Accredited Organization, Applicant Organizations must provide a completed Application Pack (and scheme specific fees) to facilitate the evaluation of accreditation suitability and to determine an accreditation outcome.

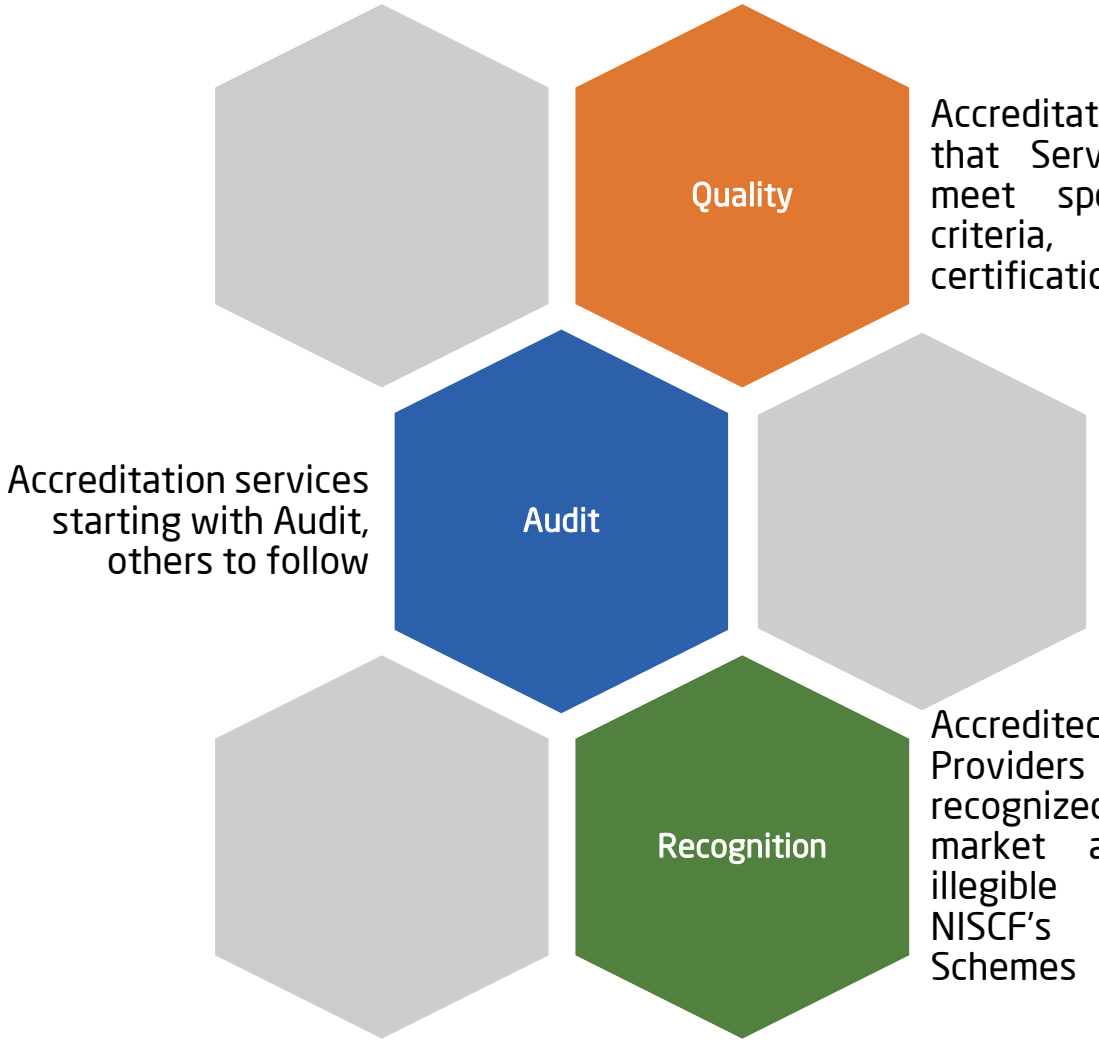
Complaints and Appeals:
Applicant Organizations or Accredited Organizations may experience dissatisfaction or confusion in relation to an Accreditation Decision, a non-compliance or the suspension or withdrawal of accreditation and may complain or appeal against decisions or findings concerning accreditation.

Maintaining Accreditation:
Accredited Organizations are subject to scheduled (and random) surveillance assessments to ensure continuing compliance with accreditation requirements and the maintenance of high-quality certification assessment services.

Losing Accreditation:
Where a large volume of minor complaints (or a major complaint) focus on an Accredited Organizations, or where a Surveillance Assessment or Change Notification indicate non-conformance with accreditation requirements, accreditation may be suspended and later withdrawn.

INTRODUCTION TO AUDIT ACCREDITATION SCHEME

MOTC



Accreditation ensures that Service Providers meet specific quality criteria, before any certification audit

Accreditation services starting with Audit, others to follow

Accredited Service Providers will be recognized in the market as the only illegible auditors for NISCF's Certification Schemes

ACCREDITATION PILLARS

SELF-ASSESSMENT

Accreditation is granted after successfully pass a self-assessment aligned with ISO 17021: Conformity assessment – Requirements for bodies providing audit and certification of management systems

VALIDITY

Accreditation certificate will be Valid for a period of three (3) years, subject to successful accreditation maintenance annually

MAINTENANCE

Accreditation will be maintained through a Combination of Scheduled and Unscheduled Audits

ETHICS AND CONDUCT

Accredited Auditors will follow the agreed on CDP's Code of Conduct and Audit Ethics

SUPPORT

Accreditation is Supported by resources available (Guidelines, checklists...) on our website and through our teams within the Compliance and Data Protection (CDP)

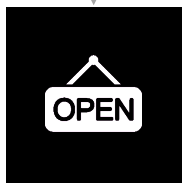
AUDIT ACCREDITATION STATE

February 2019
Launch of the Compliance and Data Protection (CDP) Department and the Audit Accreditation Scheme

February 2019
Selection of Service Providers for the Pilot phase of Audit Accreditation

April 2019
The first Service Providers being Conditional Accredited Auditors

April 2019
The first Accreditation workshop and open Audit and Advisory Accreditation



PILOTING THE SCHEMES

MOTC

Public Prosecution
NIA Certification

MOTC Government e-services
SSQA Certification

Conditional Accredited Auditors

AHMED TAWFIK & CO.
Certified Public Accountants

Deloitte.

ACCREDITATION PROCESS FOR AUDIT SERVICE PROVIDERS

MOTC

Accreditation Application Submission

CDP Application Review

Appeal Process

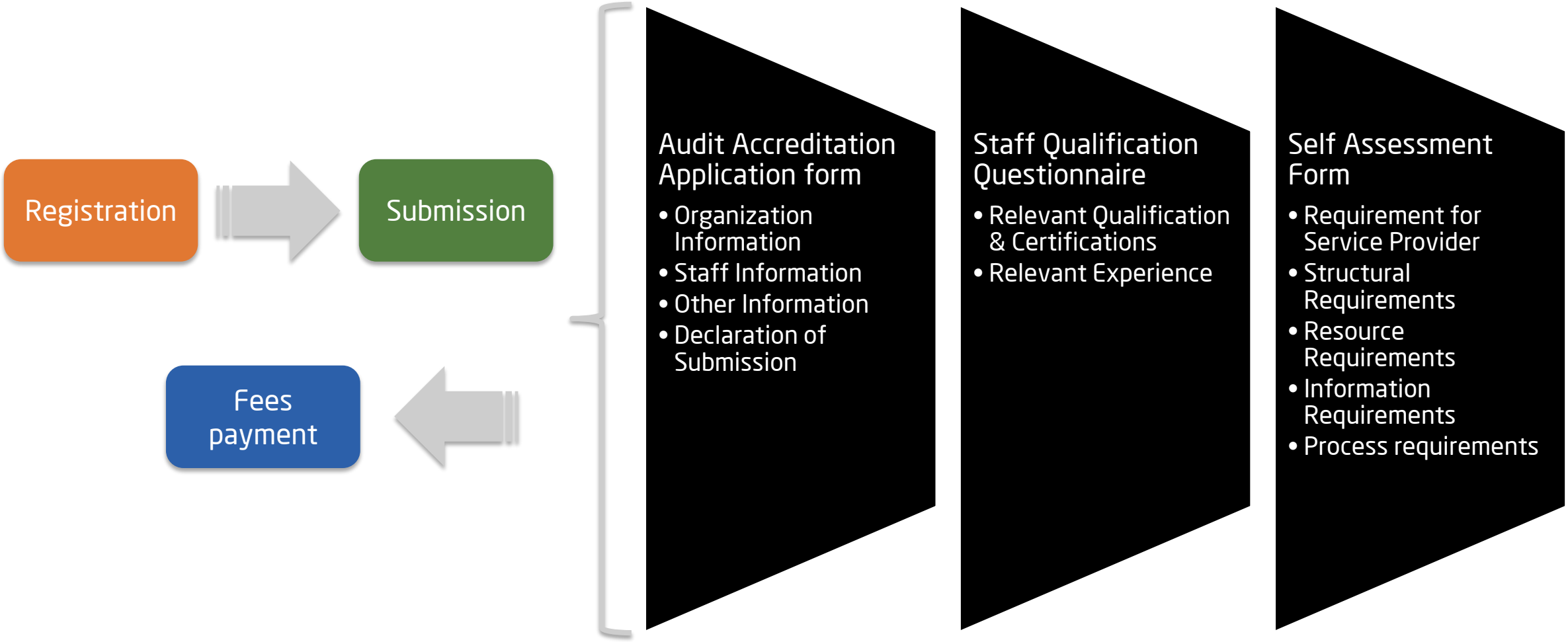
Accreditation Committee Approval

Accreditation & Maintenance

compliance.qcert.org

ACCREDITATION APPLICATION SUBMISSION

MOTC



وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

SELF-ASSESSMENT FULFILMENT DISCUSSION

compliance.qcert.org

Q-CERT

NON-DISCLOSURE AGREEMENT

After registration and prior to submit any submission, the registered service providers will be invited to the CDP office for a kick-off meeting.

Answer interrogations

Live contact between representatives

Sign an NDA for evidence submission

COMPLETING THE SELF-ASSESSMENT & PROVIDING EVIDENCE

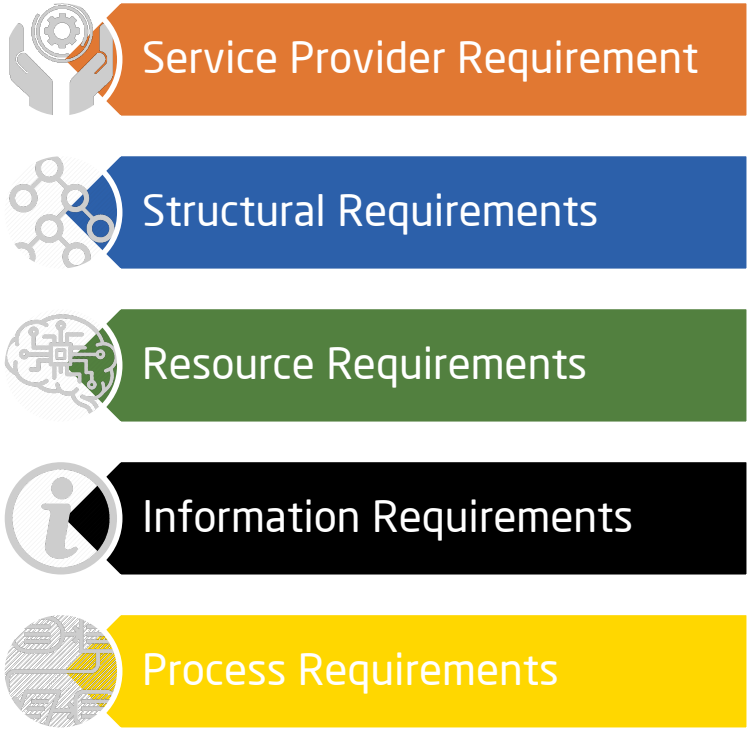
MOTC

The first step in the Accreditation application process, the Service Provider must submit information relating to the business and provide a completed Self-Assessment, outlining compliance with the National Information Security Compliance Framework (NISCF) accreditation requirements.

The Accreditation Application Form requires that Service Providers identify the Service Areas (NIA, SSQA Audit) for which accreditation is desired.

The self-assessment should be supported by evidence. This is critical for the submission.

Assessment Sections



SERVICE PROVIDER REQUIREMENT

MOTC

Legal

To be held legally responsible for all its audit and assessment activities in relation to the NISCF, the service provider shall be a legal entity, or a defined part of a legal entity.

Impartiality Management

The service provider shall have a commitment to impartiality in audit that is publically shared and have processes and mechanisms to identify, analyze and document the possibilities that could harm its impartiality.

- Impartiality, independence or any other ethics quality as an organization value
- Acceptance of audit engagement procedure
- Annual independence declaration and assessment for employees and joiners

Liability Management

The service provider shall have evaluate the risks arising from audit activities related to the NISCF and provides evidence of adequate coverage of the potential liabilities arising from it.

STRUCTURAL REQUIREMENTS

MOTC

Organizational Structure

The service provider shall have a documented organizational structure, clear roles, responsibilities and management authorities. It shall have a clear identification of the top management having overall authority and responsibility over audit activities (development of policies, supervision of the implementation, performance of audits and compliance assessment, contractual arrangements...).

- Organization chart
- Job descriptions
- Committee charter

Safeguards Committee

The service provider structure shall safeguard the impartiality of the activities and have a committee that develops, maintains, advices and review the impartiality compliance through the organization.

- Segregation of duties matrix
- Committee charter for safeguarding impartiality

RESOURCE REQUIREMENT

MOTC

Competence

The Service Provider shall have processes to ensure that its personnel have appropriate knowledge relevant to the compliance schemes and auditing. Processes shall also determine competence criteria for the personnel involved in the management and performance of audits and for initial and on-going monitoring of competence and performance.

- Job description and requirements
- Evaluation templates with competence criteria for joiners
- Skill gap assessment and training program for the NISCF's audit schemes
- Audit personnel evaluation policy

Involvement In Audits

The service provider shall have sufficient personnel (skills and number) to plan, perform, review and deliver an audit specific to the NISCF. The service provider shall demonstrate that processes are in place to enable audit team selection to achieve and demonstrate effective auditing, identify training needs and monitor performance of all personnel involved.

- Standard audit team structure
- NISCF audit activity plan and capacity assessment
- Skill gap assessment and training program for the NISCF's audit schemes
- Audit personnel evaluation policy
- Skills balance sheet for individuals and the whole audit team performing NISCF's schemes
- End of engagement evaluation process, templates and bottom-up evaluation sheets

RESOURCE REQUIREMENT

External Experts

The Service Provider shall require external auditors and external technical experts to have a written agreement by which they commit themselves to comply with applicable policies and procedures as defined by the Service Provider.

- Standard contract of engaging external auditor or technical experts
- Procedure of communication with external auditors or technical experts on applicable procedures and policies

Record

The service provider is required to have an up-to-date personnel records.

- Employees general ledger
- Subcontractors catalogue
- Skills balance sheet for individuals and the whole audit team performing NISCF's schemes

Outsourcing

The service provider is required to have a process in which it describes the conditions under which outsourcing may take place and have a legally enforceable agreement covering the agreement.

- Employees general ledger and subcontractors catalogue
- Skills balance sheet for individuals and the whole audit team performing NISCF's schemes

INFORMATION REQUIREMENTS

MOTC

Public Information

Information provided by the Service Provider to any client or to the marketplace, including advertising, shall be accurate and not misleading.

Confidentiality

The service provider shall have safeguards in place that achieve confidentiality of information obtained or created during NISCF's audits.

- Provisions on standard engagement letter and contracts
- Communication procedure for official communication channels
- Access management policy and procedures
- Encryption and device management procedures
- NDA for employees

Exchange With Clients

The service provider shall have defined standard mechanisms for exchanging information with its clients.

- Provisions on standard engagement letter and contracts

PROCESS REQUIREMENTS

Programme

An audit programme for the full compliance scheme shall be developed to clearly identify the audit activities required to demonstrate that the client fulfils the requirements for compliance to the selected standard(s).

Plan

The auditing procedure of the service provider shall include a planning phase that includes determining the nature, timing and extent of audit activities. The auditing procedure shall also take into account the scope validation.

- Standard audit plan template
- Preliminary work and scope confirmation audit work activities
- Planning procedure or tool documentation
- Audit manual

Evidencing

The service provider shall defined information (evidence) collection methods.

- Audit programme
- Audit manual

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

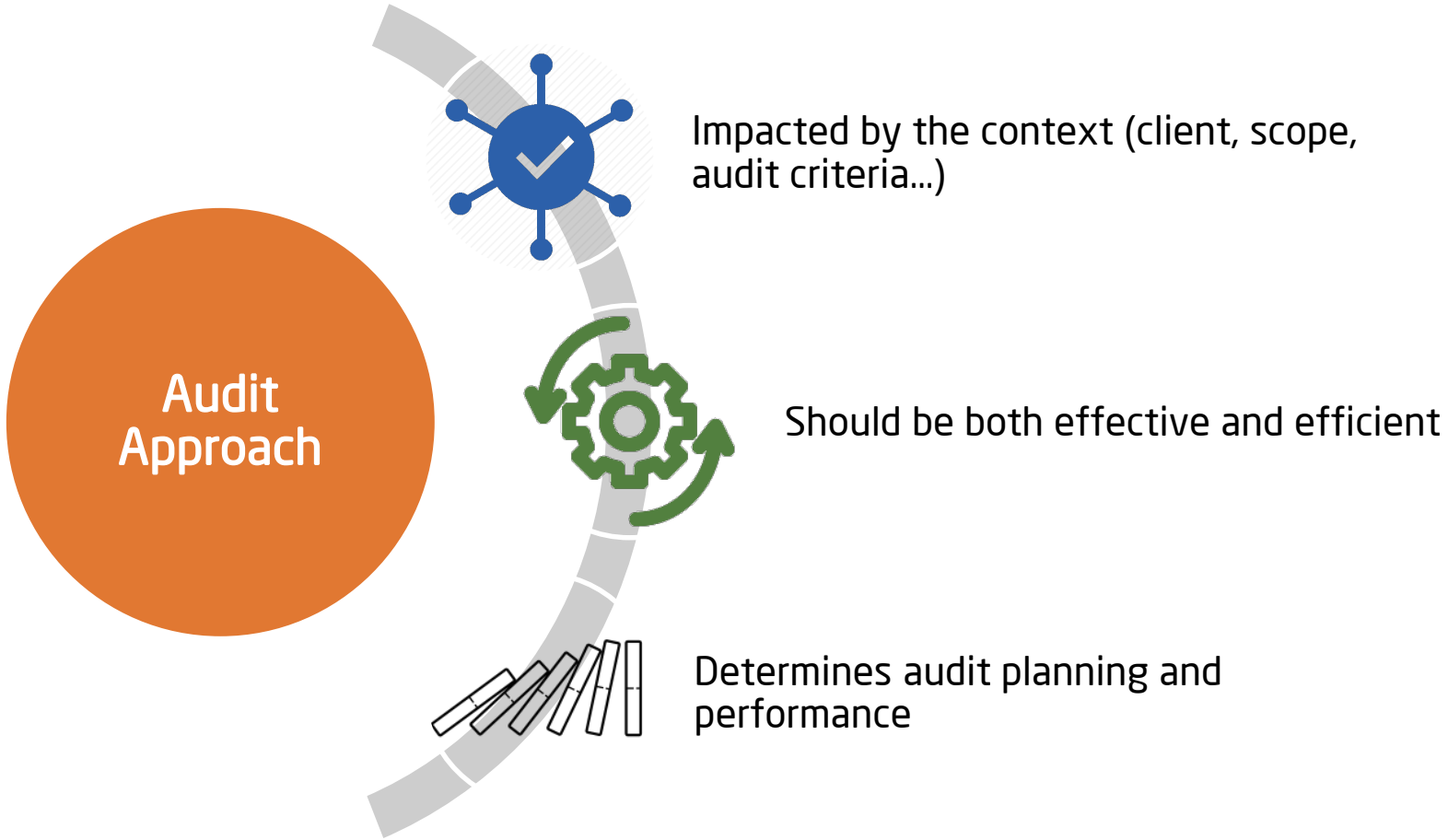
ACCREDITATION INITIATION (CONT'D)

compliance.qcert.org

Q-CERT

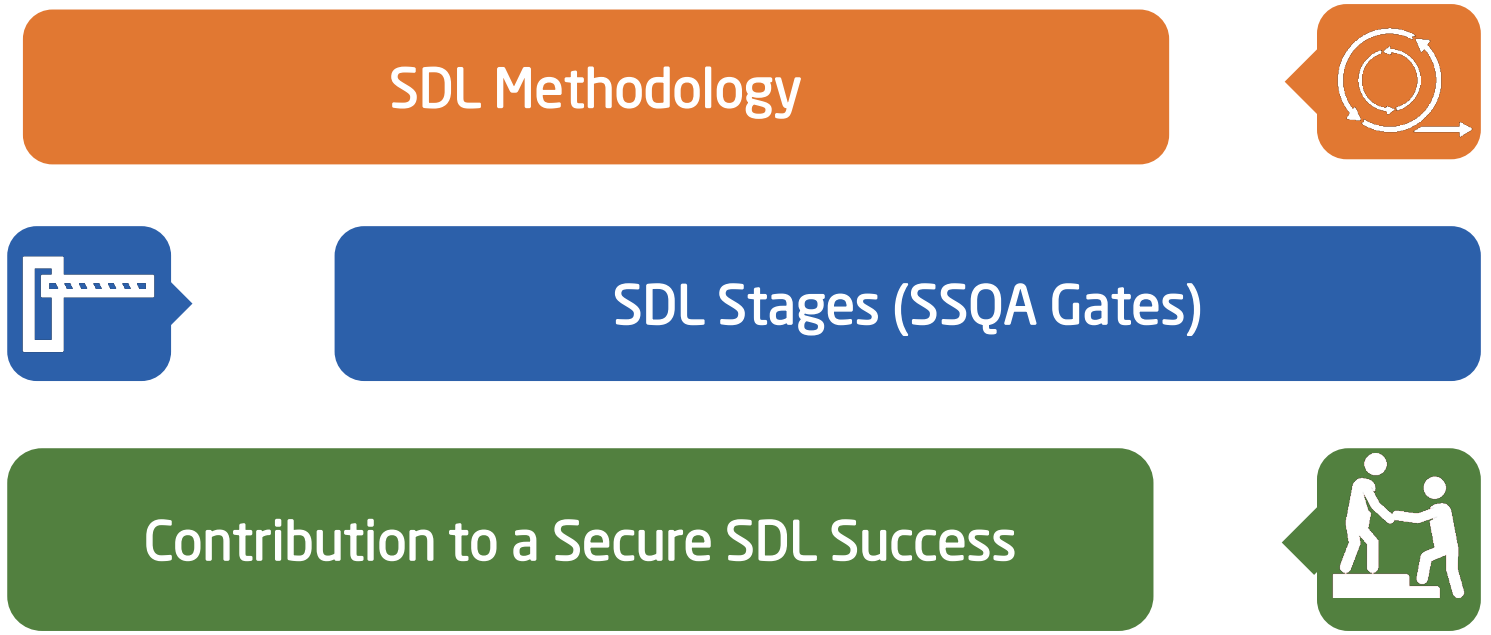
AUDIT APPROACH

The audit approach is the strategy used by an Service Provider to conduct an audit.



SSQA SPECIFICS FOR AUDIT APPROACH

The audit criteria have an impact over the audit approach. For Software Security and Quality Assurance (SSQA) certain specific considerations have to be taken into account.



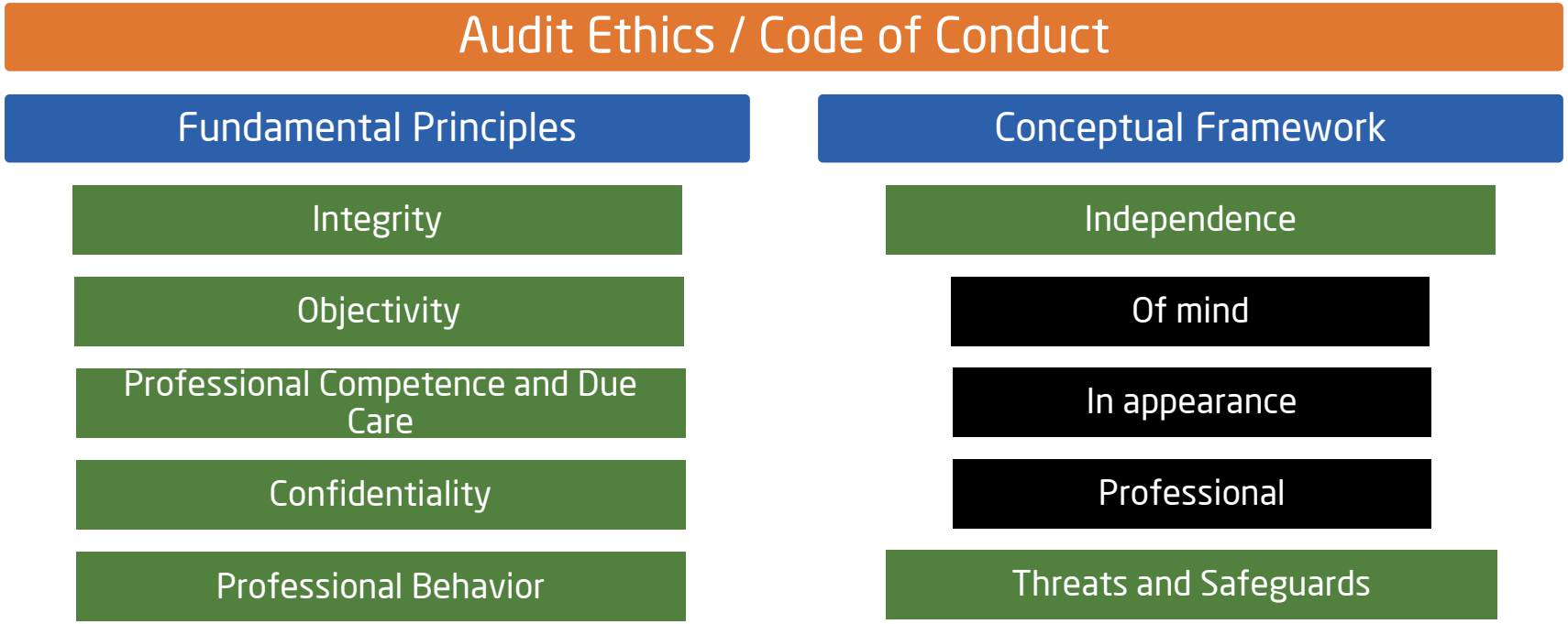
ACCREDITATION AGREEMENT

Once the accreditation submission has been reviewed and accepted by the CDP, the service provider and the CDP sign an accreditation agreement. That agreement highlights or redirects to all the requirements during the accreditation period.

Obligations and Responsibilities of the Service Provider	Comply with the terms of the accreditation agreement, including the expectations of the Code of Conducts and Audit Ethics
	Co-operate to enable the CDP to monitor the suitability of the Service Provider for Accreditation (grant it access to personnel and documents)
	Have enforceable arrangements with its clients that commit them to provide on request, access to CDP representatives to assess the Service Provider's performance
	Notification of any circumstances which may affect the Service Provider's ability to comply with the accreditation agreement
	Claim accreditation only with respect to the scope for which it has been granted accreditation and not use its accreditation in such a manner as to bring accreditation into disrepute
	Maintain high standards and act with integrity at all times

AUDIT ETHICS

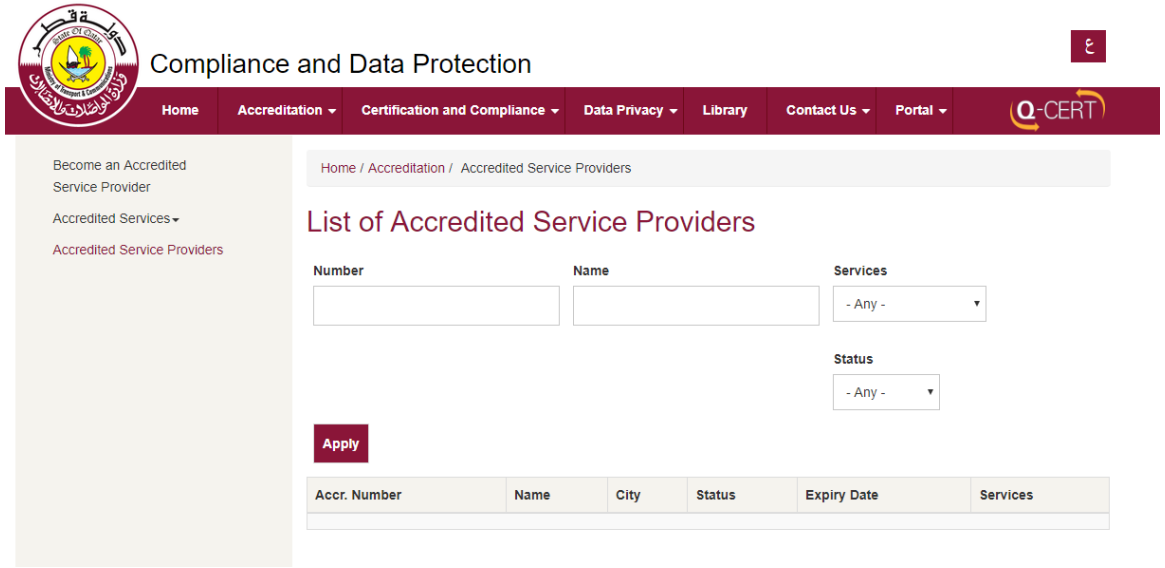
CDP's Code of Conduct is mandatory for accredited service providers as a condition of the accreditation agreement. It is composed with two blocks.



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 will maintain a listing of all Accredited Service Providers, allowing organizations to verify the status of Service Providers.



compliance.qcert.org

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

ACCREDITATION MANAGEMENT

compliance.qcert.org

Q-CERT

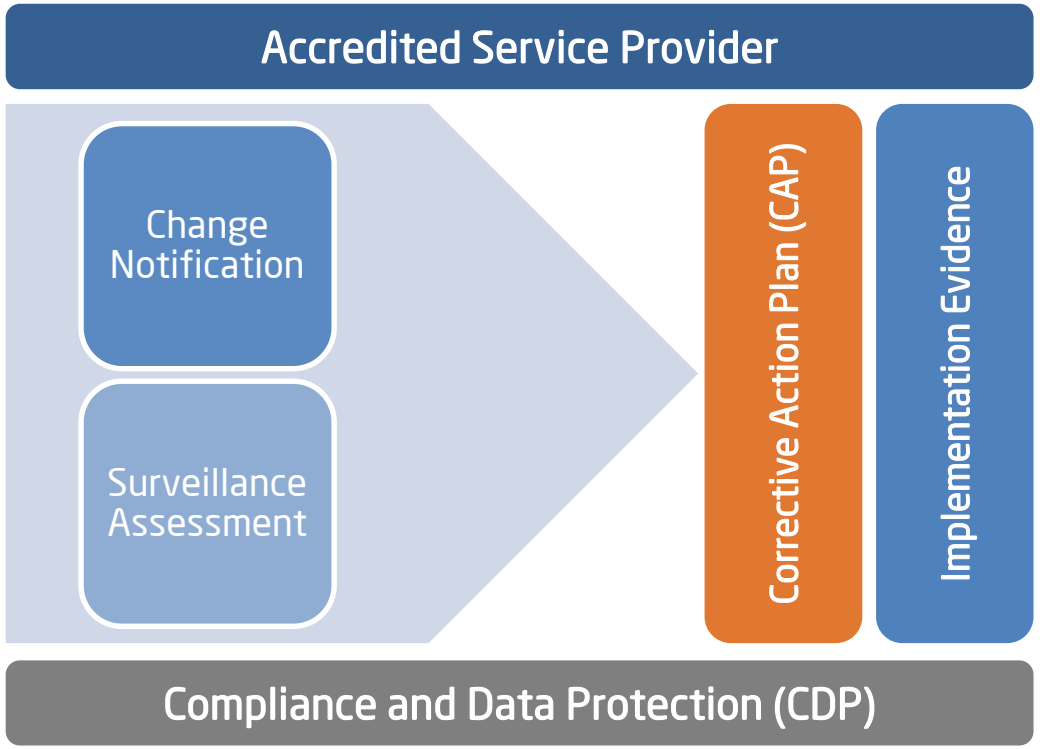
ACCREDITATION LIFECYCLE OVERVIEW

MAINTAINING ACCREDITATION

Once accreditation has been awarded, Service Providers enter the Accreditation Maintenance Process through which ongoing compliance with the National Information Security Compliance Framework (NISCF) accreditation requirements must be assured.

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

- Surveillance Assessments 6-months following the award of accreditation, annually thereafter and 6 months prior to the expiry of accreditation.
- Accredited Service Provider are required to notify the CDP of any changes which may result in a non-compliance requirements.

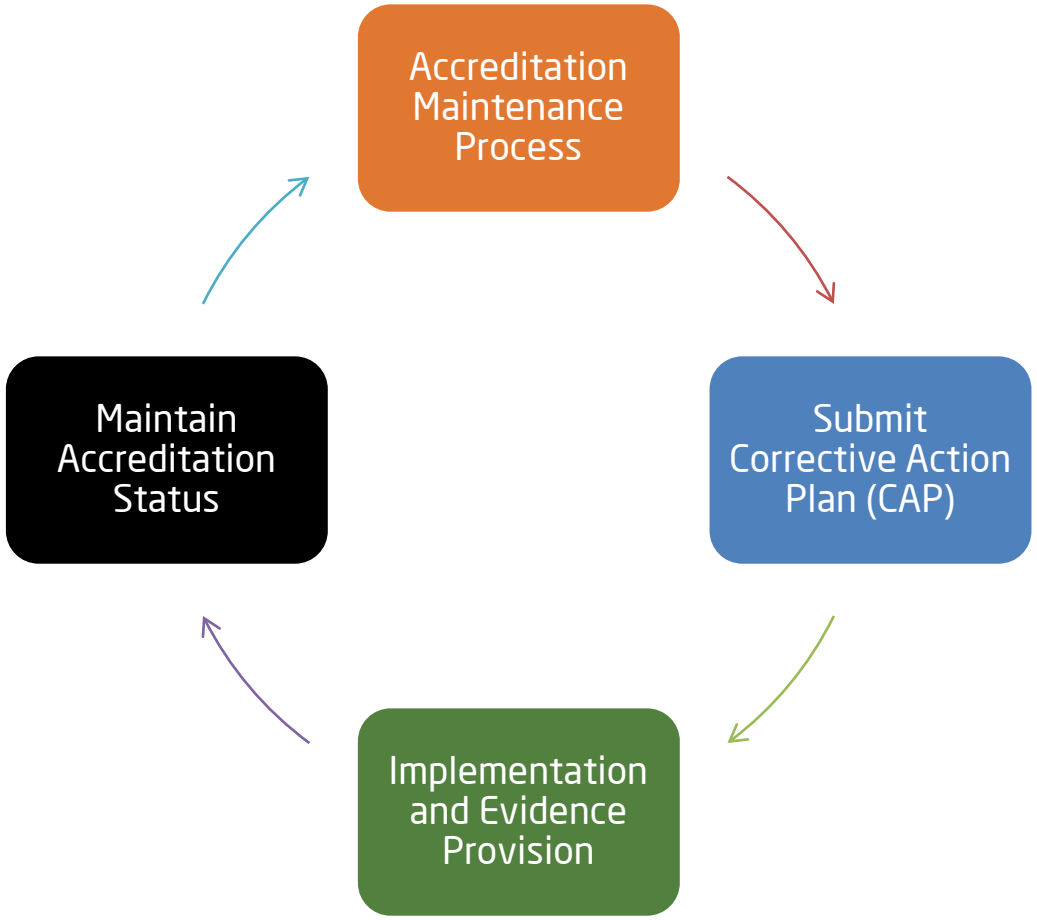


MAINTAINING ACCREDITATION

Where non-compliance are identified either through surveillance assessments or voluntary change notifications, 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.

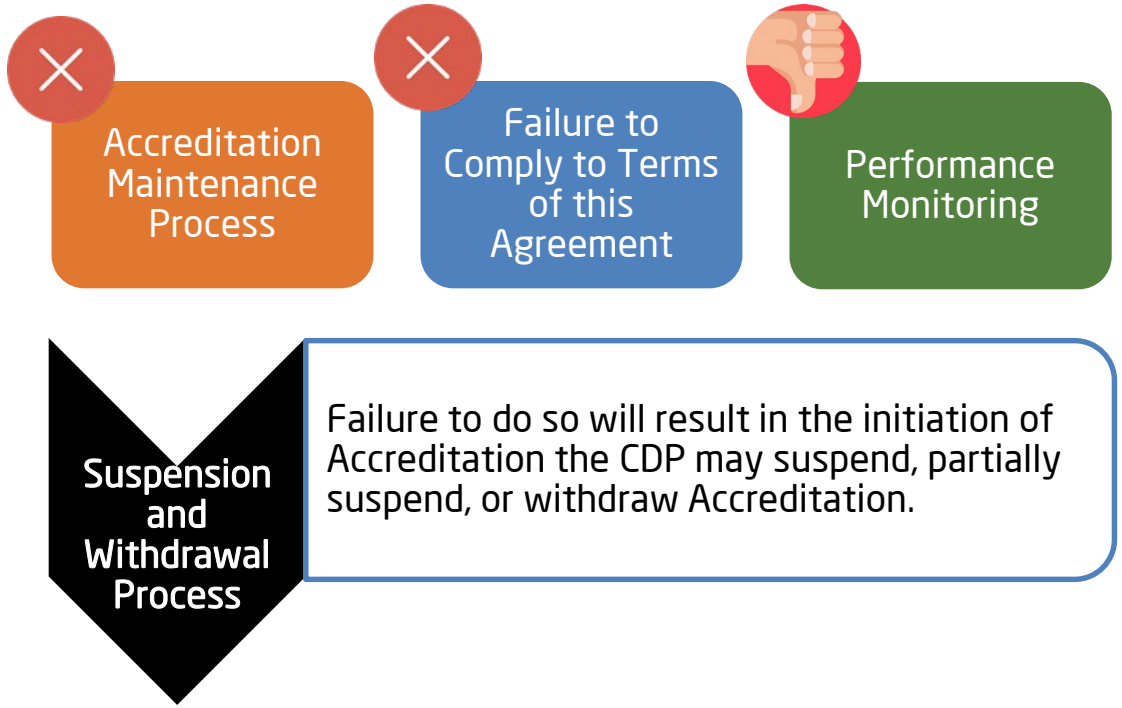


CONDITIONS FOR LOSING ACCREDITATION

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

- Failure to comply with Accreditation Maintenance Process,
- Failure to comply with the requirements or other terms of this Agreement; or
- Performance-related observations.

Failure to do so the CDP may suspend, partially suspend, or withdraw Accreditation,



CONDITIONS FOR LOSING ACCREDITATION

While accreditation is suspended, the entity cannot undertake new certification assessments and must address the identified compliance concerns.

Failure to address compliance concerns will result in the withdrawal of accreditation.

Suspension and Withdrawal Initiated

- Non-Compliance Corrective Action Plan and Implementation Evidence not received or agreed within timeframe
- Failure to comply with the requirements or other terms of this Agreement.
- Performance-related concerns.

Accreditation Suspended

- Accredited Organization is notified of Suspension (including detail of issues leading to the suspension)
- During the Suspension timeframe (not exceeding 6-months), the Accredited Organization is unable to perform new certification assessments but may continue with 'in-flight' assessments or pre-authorized assessments.

Accreditation Withdrawal

- 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.

COMPLAINTS

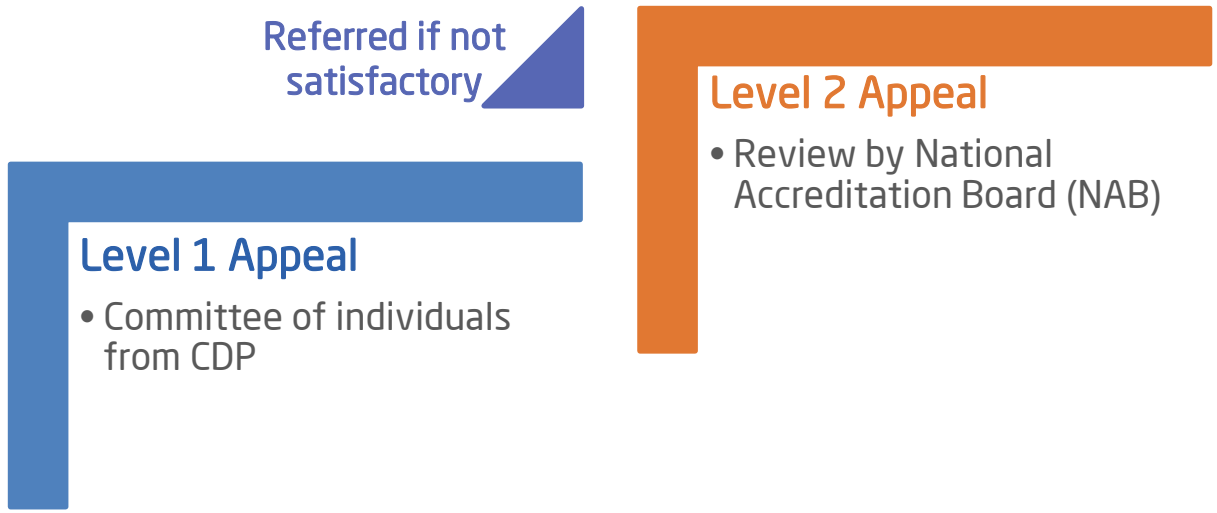
Complaints are categorised and reviewed by the CDP to validity and investigated if necessary.

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

APPEALS

Level One (1) Appeal Hearing shall be heard by a committee of individuals from CDP (who have no conflicting interests).

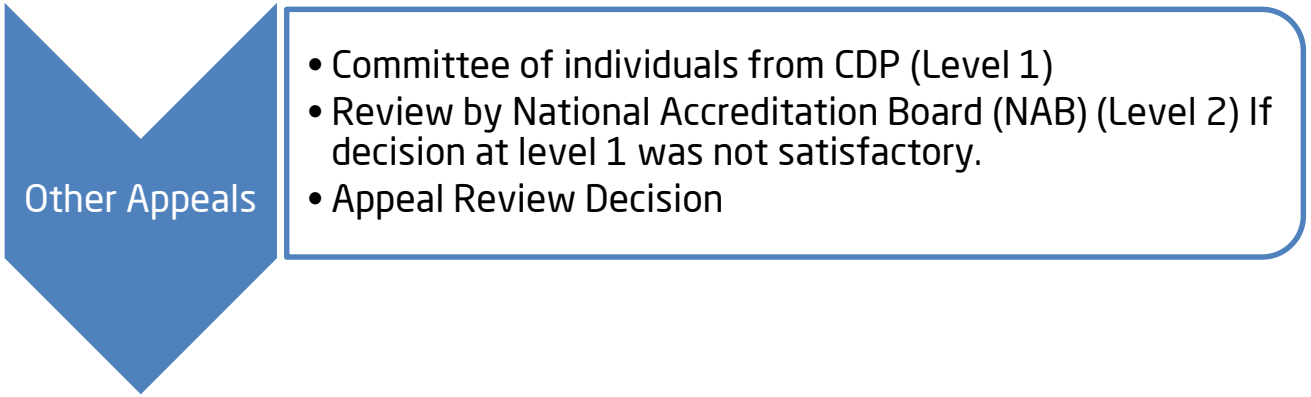
A Level Two (2) Appeal Hearing shall be heard by a committee of individuals from the National Accreditation Board (NAB) (who have no conflicting interests).



APPEALS

Appeals relating to an Accreditation Decision or an Accreditation Non-Conformance are heard by the National Accreditation Board (NAB) through a Level Two (2) Appeal Hearing.

All other Appeals are first reviewed by CDP at a Level One (1) Appeal Hearing.



وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

QUESTIONS AND ANSWERS SESSION

compliance.qcert.org

Q-CERT

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

Q-CERT