وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Compliance and Data Protection Department

SOFTWARE SECURITY AND QUALITY ASSURANCE (SSQA) COMPLIANCE

Compliance Certification Scheme Overview

compliance.qcert.org

Q-CERT

WORKSHOP CONTENTS SSQA CERTIFICATION

MOTC

1. **FRAMEWORK AND SCHEME OVERVIEW**
   Introduction To Compliance And Accreditation

   Certification Enforcement

   Information Assurance Framework Overview

   Augmenting the National Information Assurance Policy

   SSQA Scheme Rationale

2. **SSQA STANDARDS AND COMPLIANCE**
   SSQA Standards Structure

   Simplifying Compliance Through Tiered Standards

   SSQA Standards Assessment Gates

   Evidencing Compliance

3. **SSQA CERTIFICATION**

   SSQA Certification Processes

   SSQA Compliance Certification Process - Overview

   Certification Scope Agreement & Administration

   Accredited Service Provider Engagement & Scheduling Compliance Audits

   Selecting An Accredited Service Provider

   Assisting with Compliance Assessments & Compliance Assessment Ownership

   SSQA Assessment Cycle

   Questions and Answers

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

FRAMEWORK AND SCHEME OVERVIEW

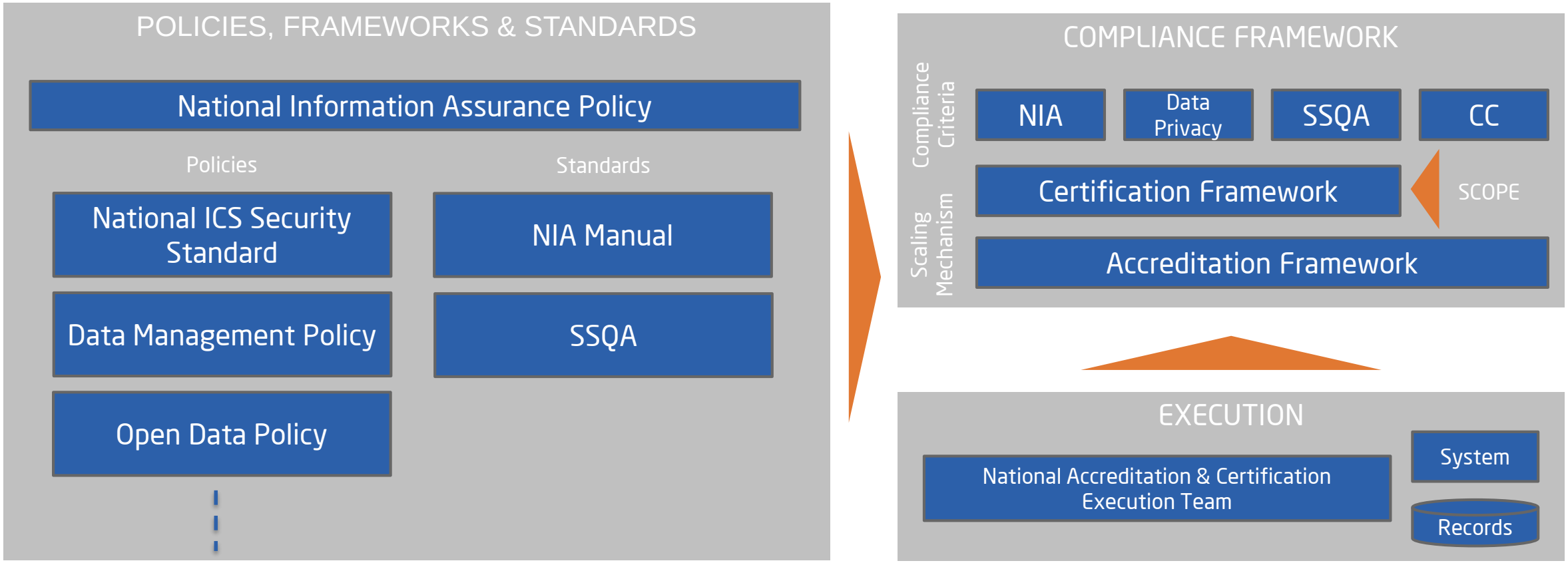
compliance.qcert.org

Q-CERT

INTRODUCTION TO COMPLIANCE AND ACCREDITATION

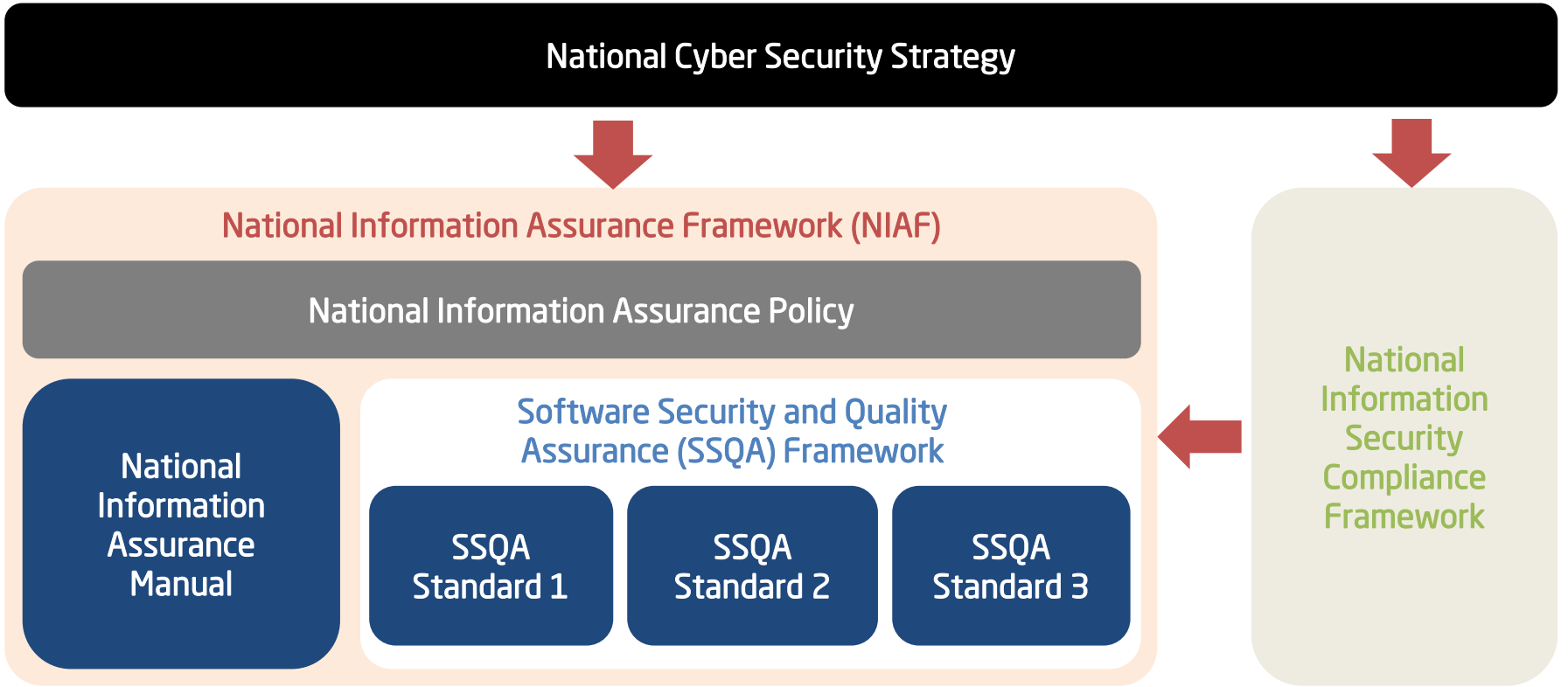
MOTC

NATIONAL CYBER SECURITY STRATEGY



compliance.qcert.org

INFORMATION ASSURANCE FRAMEWORK OVERVIEW



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.**

CERTIFICATION ENFORCEMENT

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

Mandatory
Applicable

Evidencing compliance with the NIA and SSQA standards is mandatory for the government sector. SSQA compliance may be extended to other organizations at a later stage. The Compliance and Data Protection (CDP) department will be following-up with organizations to ensure compliance where this applies.

Although compliance may be mandatory, a grace period will be available as the department recognizes the difficulties initiating new projects within an existing budgetary model.

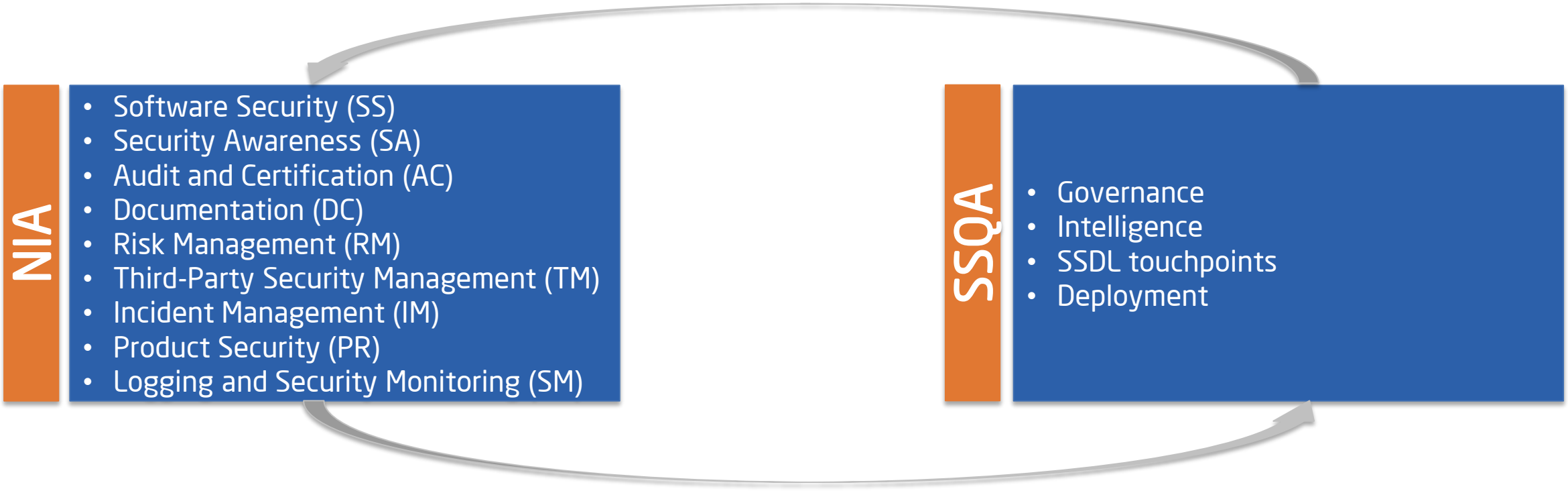
The end-date of the grace period will be announced following the conclusion of the Pilot Activities to enable appropriate planning across all impacted organizations.

compliance.qcert.org

AUGMENTING THE NATIONAL INFORMATION ASSURANCE FRAMEWORK

The Software Security and Quality Assurance (SSQA) Framework, built upon the BSIMM standard, provides a complimentary addition to the existing control set of the National Information Assurance Manual (NIAM).

The National Information Assurance Policy (NIAP) and the National Information Assurance Manual (NIAM) facilitates Software Security and Quality Assurance (SSQA) Framework by providing a favourable frame for Secure Software Development.



SSQA SCHEME RATIONALE

High Availability

- Widely used information
- Frequent transactions

Critical Data

- Financial
- Personal Sensitive
- Government

Critical Functions

- To citizens
- To businesses
- To other government services

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

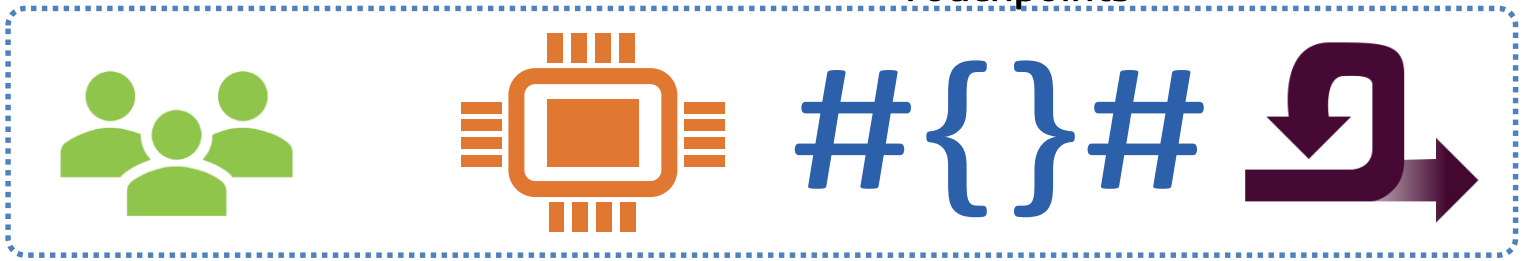
SSQA STANDARDS AND COMPLIANCE

compliance.qcert.org

Q-CERT

SSQA STANDARDS STRUCTURE

- Based upon the industry standard BSIMM7
- Controls across four (04) Domains
- Each Domain is comprised of 3 Practices, for a total of 12 Practices



Governance	Intelligence	SSDL Touchpoints	Deployment
• Strategy and Metrics; • Compliance and Policy; and, • Training.	• Attack Models; • Security Features and Designs; and, • Standards and Requirements.	• Architecture Analysis; • Code Review; and, • Security Testing.	• Penetration Testing; • Software Environment; and, • Configuration Management and Vulnerability Management.

SIMPLIFYING COMPLIANCE THROUGH TIERED STANDARDS

MOTC

Level 1

- Must meet the "requirements" of SSQA Standard 1

The MINIMUM STANDARDS EXPECTED CONTROLS for SSQA provide the first (bronze) level of compliance and represent the minimum consideration to security required for all E- Services.

Level 2

- Must meet the "requirements" of SSQA Standard 1 and 2

The RECOMMENDED STANDARDS CONTROLS for SSQA provide a second (silver) level of compliance and represent the an intermediate level of assessment based on desired level of compliance and E-Service classification.

Level 3

- Must meet the "requirements" of SSQA Standard 1,2 and 3

The ENHANCED STANDARDS CONTROLS provide a third (gold) level of compliance and represent the highest level of assessment based on desired level of compliance and E-Service classification.

compliance.qcert.org

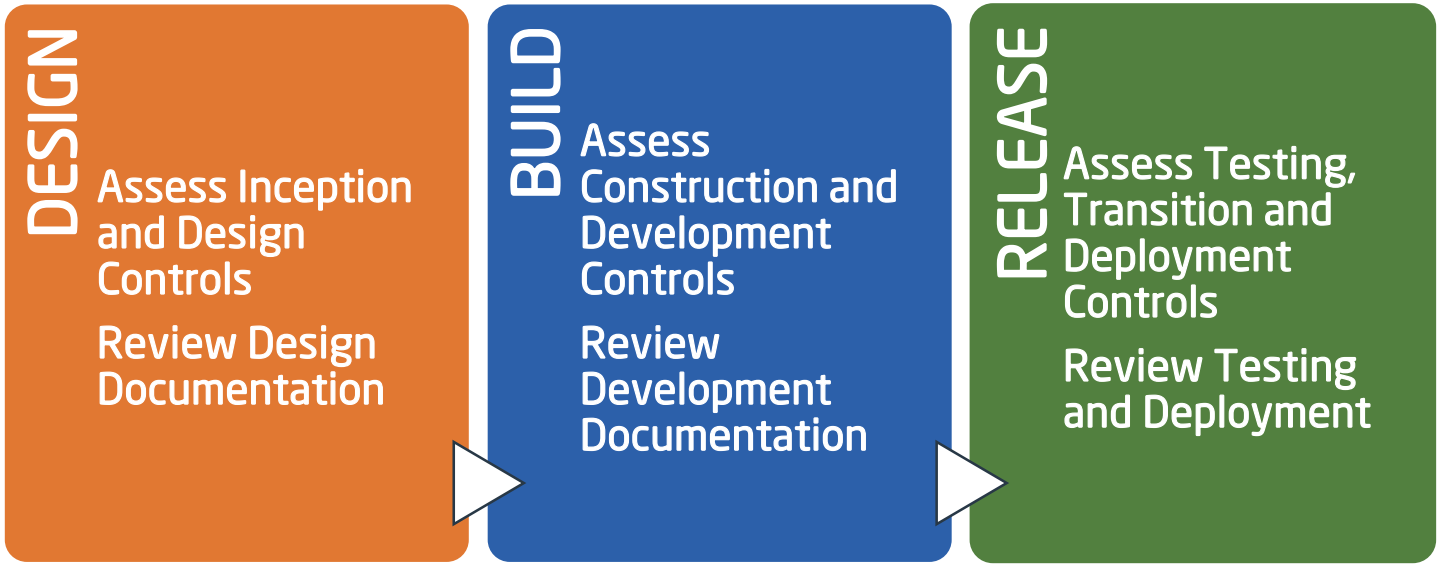
SSQA STANDARDS ASSESSMENT GATES

MOTC

ASSESSMENT ACTIVITIES:

The assessment of the Software Security and Quality Assurance (SSQA) controls are performed at 3 checkpoints, the Design, Build and Release assessment gates.

Each assessment gate provides an opportunity for the Accredited Service Provider to audit the implementation of controls from the **Baseline**, **Intermediate** and **Enhanced** control sets that are relevant to the current System Development Lifecycle (SDL) stage.



SSQA STANDARDS ASSESSMENT GATES

MOTC

DESIGN — High-level security and business risks

- Project Charter and Project Definition Document
- Project Management Plan

BUILD — Light security and functional testing

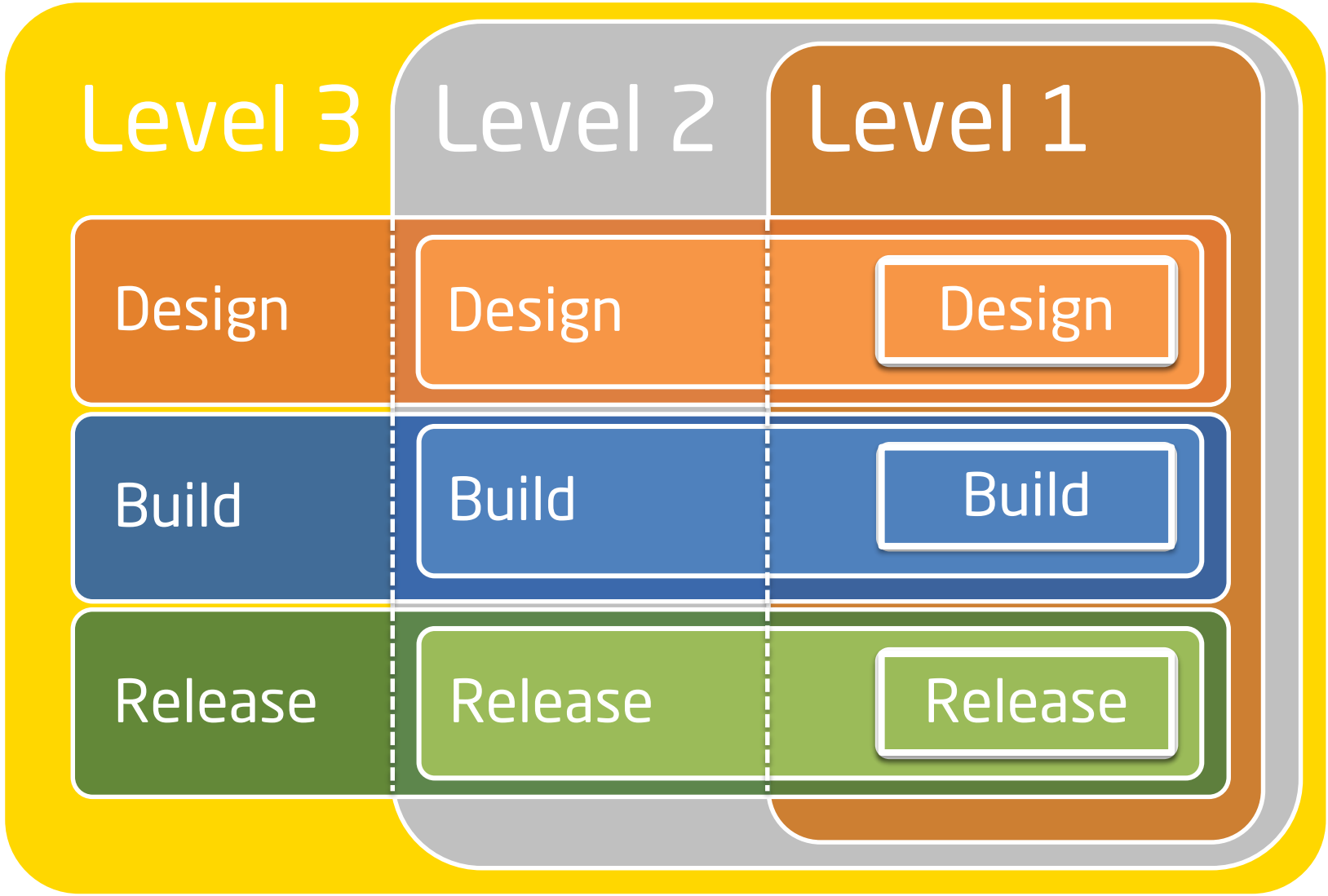
- Updated or Developed Security Documentation
- High-Level Use and Abuse Test Cases

RELEASE — Evaluation within the organization's operation environment

- Security Authorization Sign-Off & Risk Acceptance, and,
- Compliance Authorization Sign-Off and Risk Acceptance.

ASSESSING COMPLIANCE WITH SSQA STANDARDS

MOTC



compliance.qcert.org

EVIDENCING COMPLIANCE

- As part of the assessment process an, Independent, Accredited Service Provider evaluates the implementation of controls (at a specified level) within the context of a defined system and related development activities.
- If, following the assessment, it is determined that the controls (relevant to the specified target compliance level) have been achieved, a certificate of compliance is issued by the Compliance and Data Protection (CDP) department.
- The compliance certificate demonstrates alignment of a given system, specified by the compliance scope, with specific controls relevant to the documented compliance target. Compliance is determined at a point-in-time and relates specifically to the outlined system scope.
- Any changes to the system that materially alter the service or design will invalidated the compliance certificate and require re-assessment.

compliance.qcert.org

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

SSQA CERTIFICATION

compliance.qcert.org

Q-CERT

CERTIFICATION PROCESSES FOR THE SSQA SCHEME

MOTC

SSQA CERTIFICATION PROCESS

The certification process provides a structured process for the independent assessment of Constituent systems, by an Accredited Service Provider, against a defined control set.

Systems that adequately demonstrate the implementation of Software Security and Quality Assurance (SSQA) for a target assessment level will be eligible for certification upon completion of an independent assessment by an Accredited Service Provider.

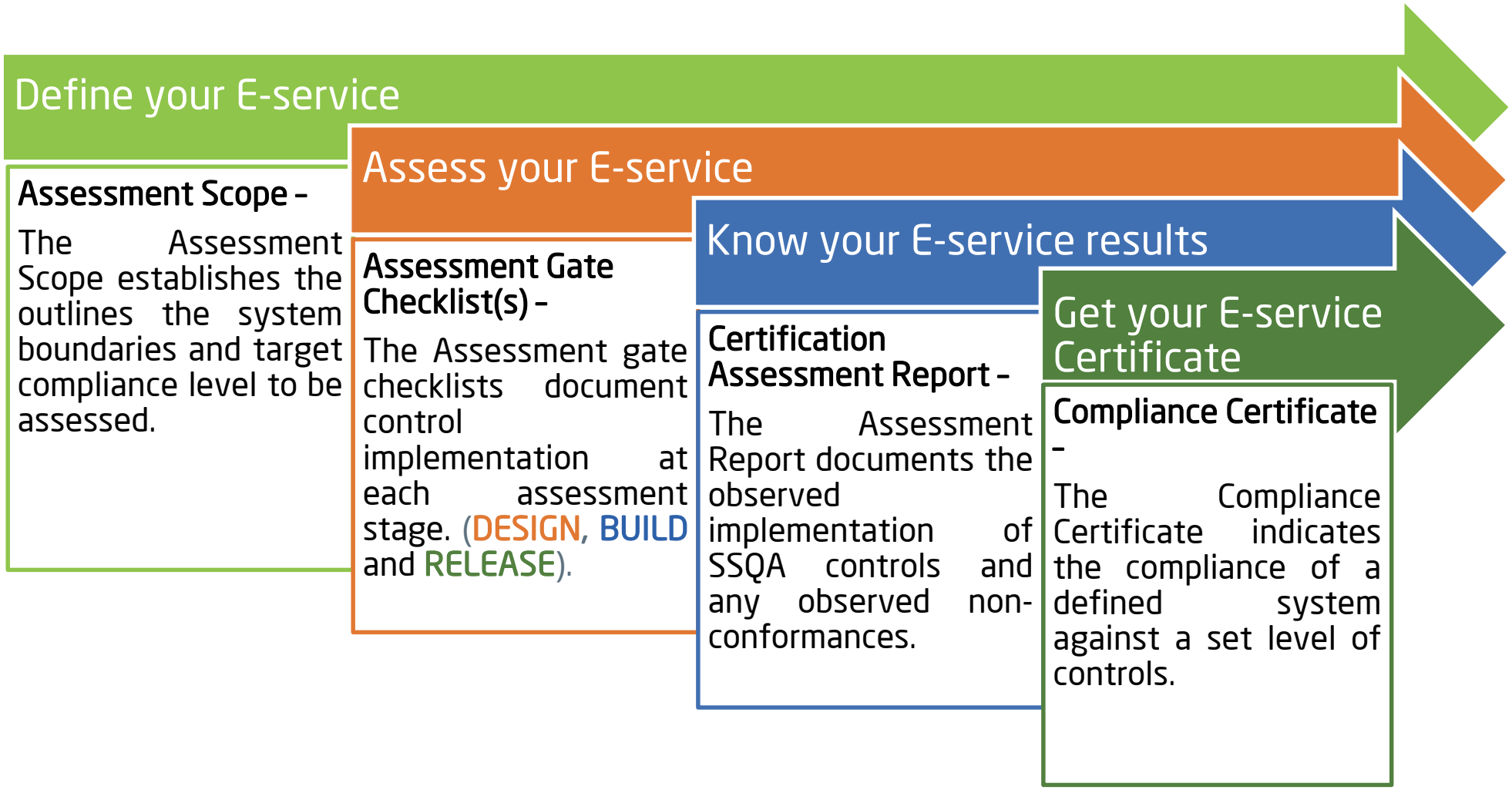
Systems assessments performed against the lowest control tier may be conducted using a self-assessment approach, however the results of the assessment will be reviewed in depth by the CDP Team prior to the ward of certification.

SSQA GATE PROCESS

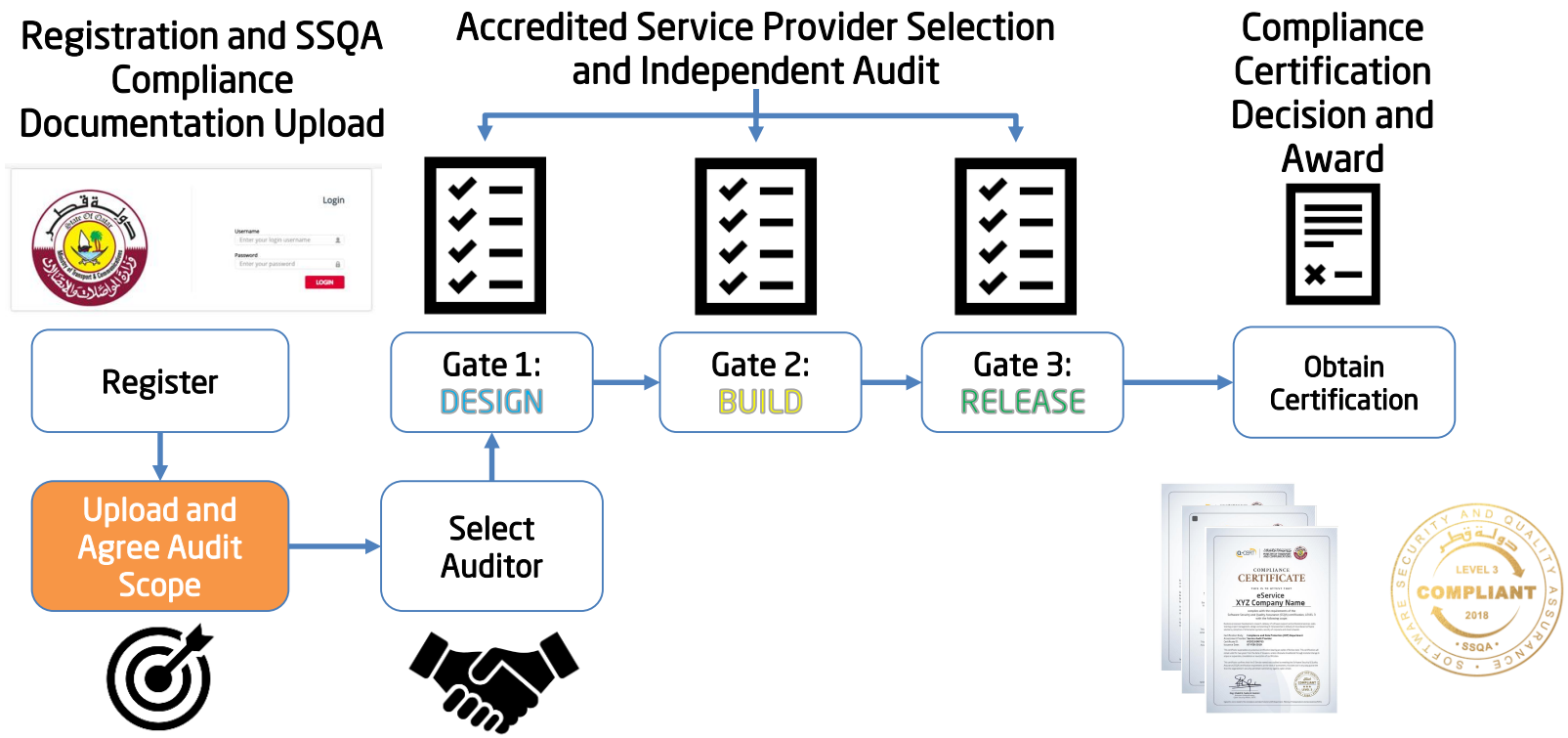
The gate assessment process provides a structured approach providing through-development assessment.

This approach ensures the on-going consideration of security throughout the development lifecycle and enables the assessment of controls at relevant stages of the Systems Development Lifecycle (SDL).

SSQA COMPLIANCE CERTIFICATION PROCESS - OVERVIEW



CERTIFICATION SCOPE AGREEMENT & ADMINISTRATION



When applying for certification, the scope of the certification assessment must be clearly understood.

The Scope document captures key information regarding the assessment environment, such as the type of information that is being processed and core processes.
The scope must also outline the target compliance level to be assessed.

Following submission, the Certification Scope Document is reviewed by the Compliance and Data Protection (CDP) department to ensure the appropriateness of the assessment boundaries and compliance level.

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

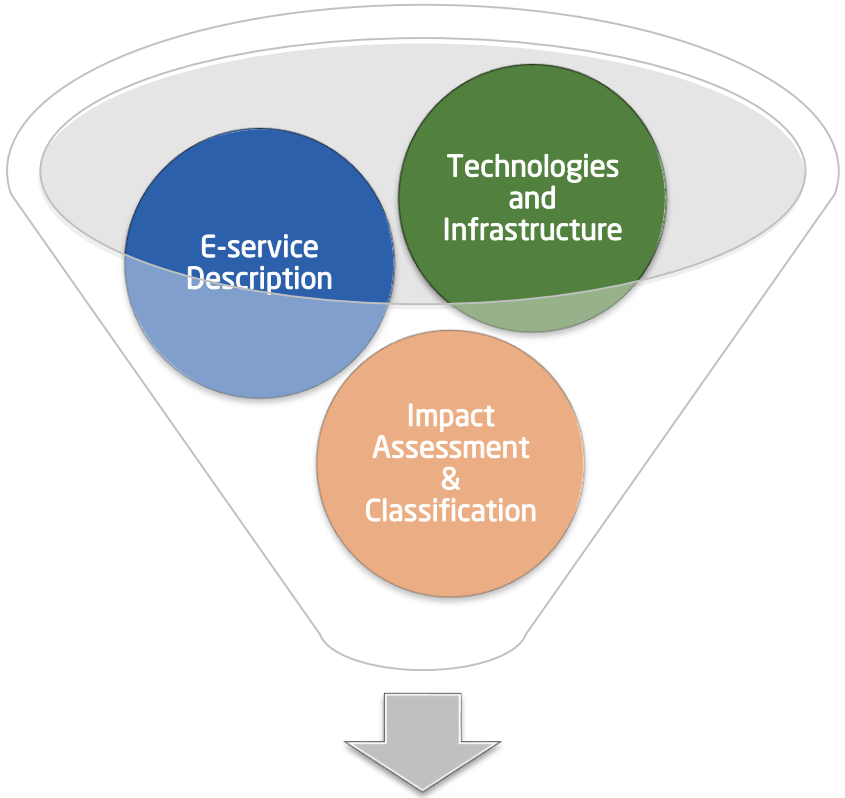
SCOPE FULFILMENT DISCUSSION

compliance.qcert.org

Q-CERT

SSQA ASSESSMENT SCOPE

To start the certification process after registration, an assessment scope of your E-service should be submitted. This scope submission should give a comprehensive and clear identification of your E-service and the SSQA level of compliance associated with.



SSQA Assessment Scope

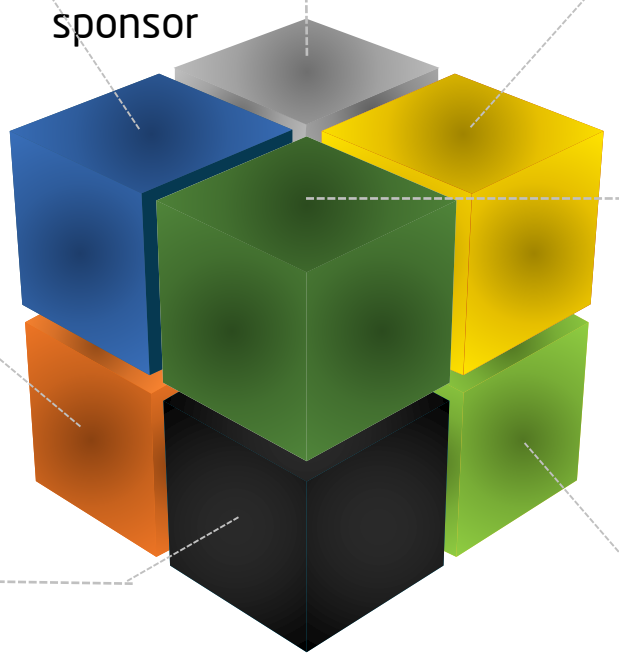
SSQA E-SERVICE DESCRIPTION

The assessment scope is mainly driven by the E-service reason of existence and the environment it sits into. So when providing detailed information about your E-Service and its environment, the following information should be considered:

E-Service Name, ownership & sponsorship :
An identification that sets the E-Service from any other one and clear ownership and sponsor

E-Service Data Management:
A description of the data being managed by the E-Service in entrance, processing, storage and display

E-Service Customer:
A detailed identification of the E-Service end users (as end client and service management users)



E-Service Environment:
A description the development and running environments

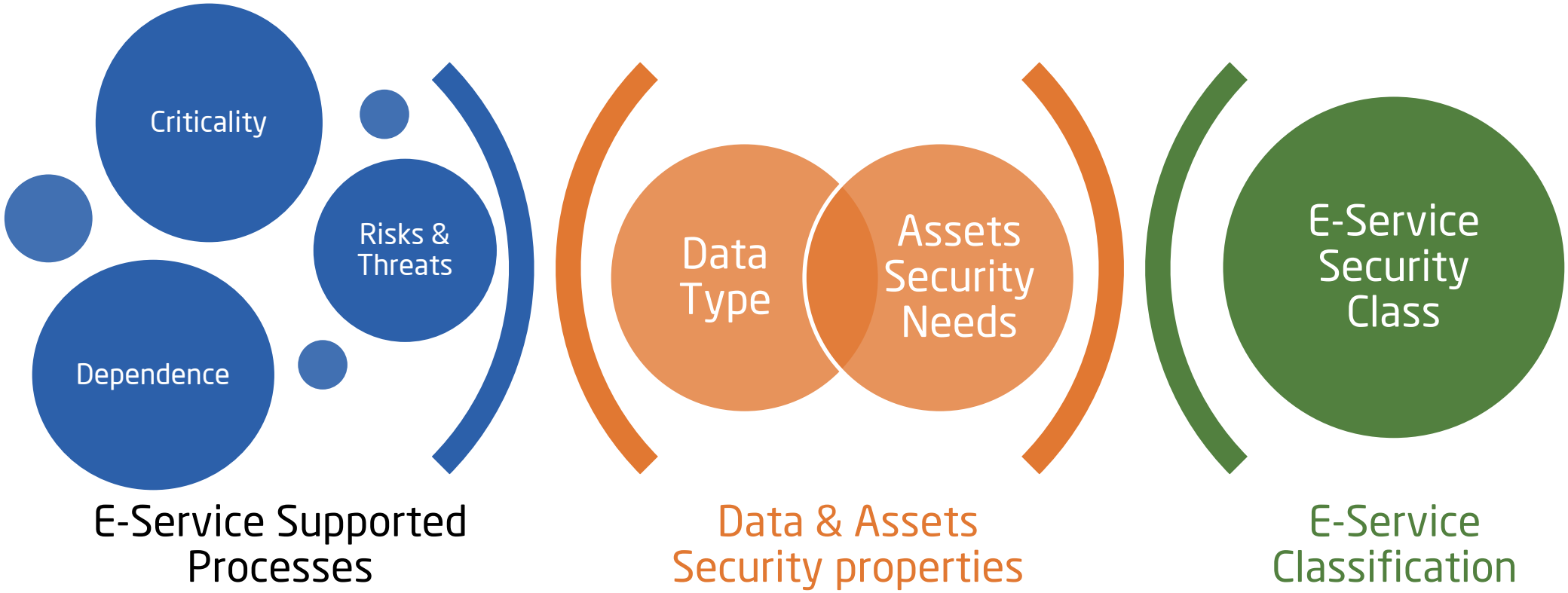
E-Service Trigger and Purpose:
The reason behind the creation of the E-Service and a high level description of the goals the E-Service is intended to achieve

E-Service Landscape:
A description of relationships with other services, systems or entities

E-Service Project:
The roadmap, time to market and the E-Service state of progress at the scope submission time

E-SERVICE CLASSIFICATION

The security controls over the System Development Life Cycle need to be aligned with the criticality of the E-Service. This criticality forms a base for the security class the E-Service has to comply with.



ENSURING SECURE SYSTEMS DEVELOPMENT

MOTC

Your E-Service is enabled by a set of technologies and resides within an infrastructure. The use of certain technologies, hardware or underlying systems could bring to the table vulnerabilities and open the door to new threats.

WEB

Giving various information on your E-Service Web Application by answering question about:

- Web Services;
- Coding language;
- Hosting environment...

INFRASTRUCTURE

You should provide information related to the infrastructure:

- Accessibility;
- Live hosts and their location;
- Operating Systems;
- Database Systems;
- Network Segmentation...

INTEGRATION

Providing information about potential API usage gives you and the CDP better view of the security implication based on:

- Association to PCI;
- REST or SOAP;
- Number of API calls;
- Authentication requirements...

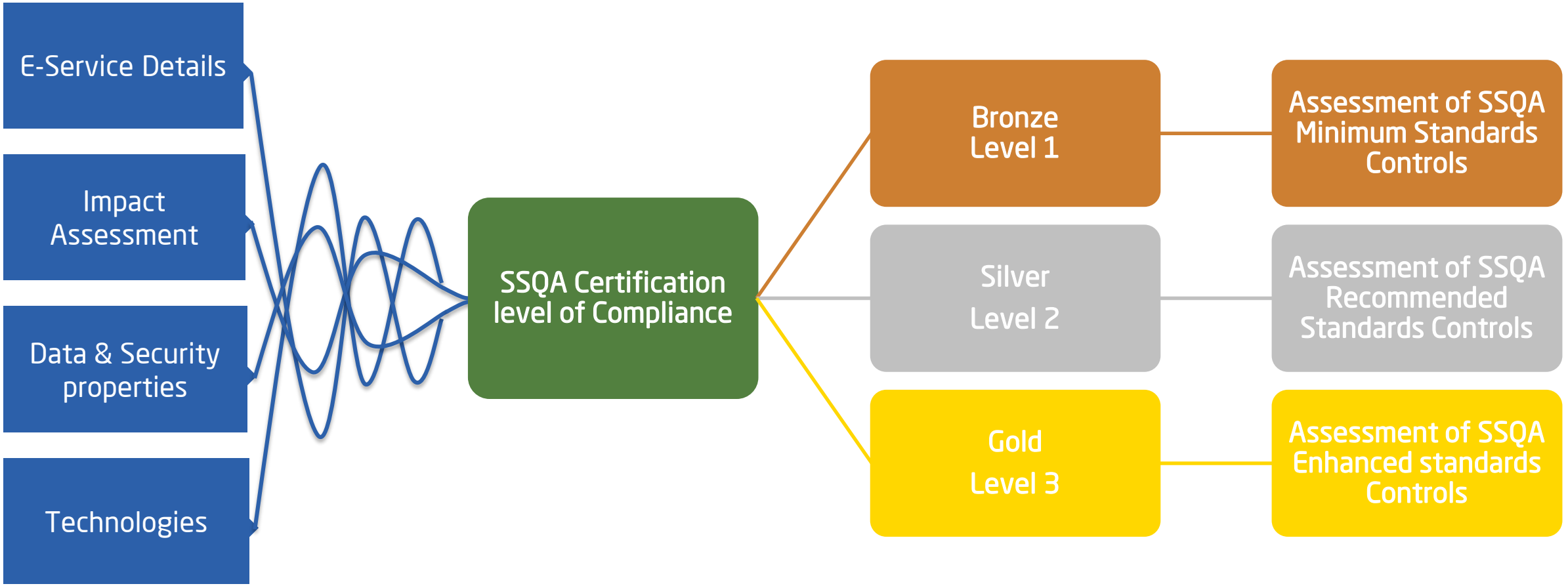
MOBILE

E-Service through mobile app needs different security considerations depending on:

- Platform & OS;
- Types of apps
- Authentication;
- Communication means...

LEVELS OF COMPLIANCE

Confidence in your E-Service is based on the Assurance given to stakeholders. The SSQA Certification level of compliance should give the adequate Assurance level.



compliance.qcert.org

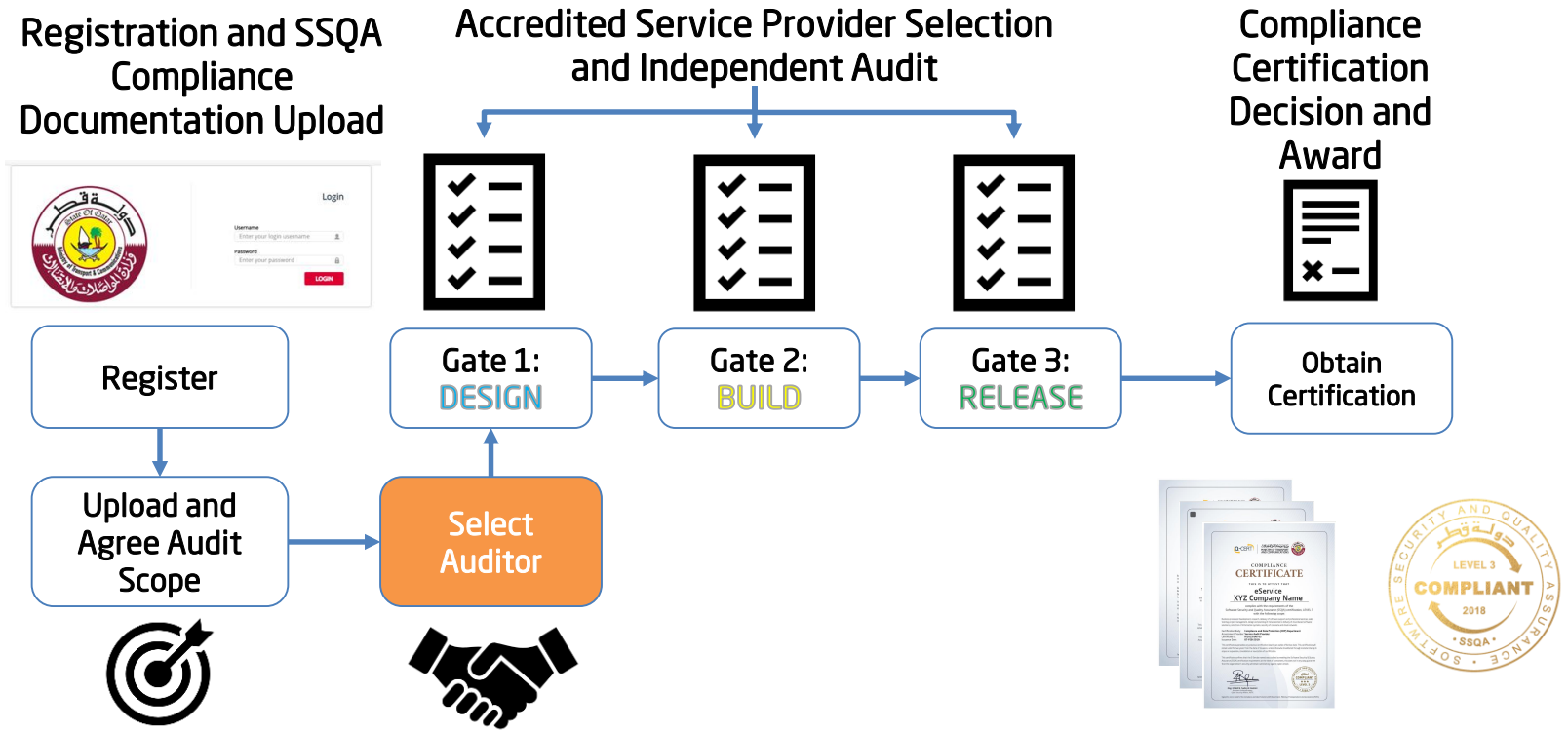
وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

SSQA CERTIFICATION (CONT'D)

compliance.qcert.org

Q-CERT

ACCREDITED SERVICE PROVIDER ENGAGEMENT & SCHEDULING COMPLIANCE AUDITS



When the scheme-specific Admin Fee has been received, an Accredited Service Provider may be selected to perform the Compliance Assessment.

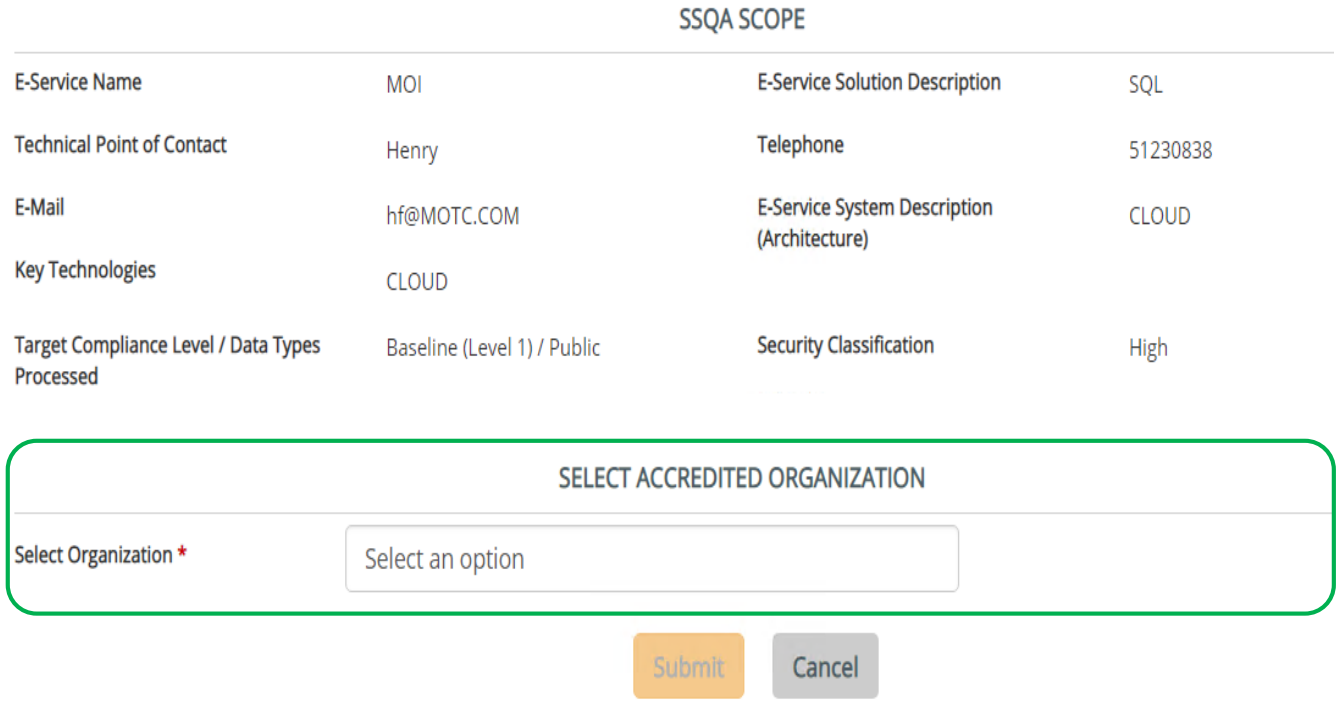
It is critical to work with the Accredited Service Provider to enable the completion of compliance assessments. This means providing insight into the systems development process to agree the best approach and dates for assessments.

The approach taken to assess systems developed using an Agile development methodology will be different to that of a Waterfall-based project and, if the assessment is performed too early, it will be difficult to evidence compliance.

SELECTING AN ASSESSMENT SERVICE PROVIDER

Constituents must ensure that only accredited Service providers are engaged for assessment services.

An Accreditation Certificate is awarded to Service Providers to authorize specific activities relating to the National Information Security Compliance Framework (NISCF) and it's related schemes (such as the National Information Assurance (NIA) Scheme or the Software Security and Quality Assurance (SSQA) Scheme).



Accreditation is scheme specific and the Constituent should ensure that the Service Provider is authorized (through the accreditation) to provide the assessment service in relation to the specific scheme for which compliance is sought.

A list of accredited Service Providers is maintained by the Compliance and Data Protection (CDP) department which enabling the validation any asserted accreditations.

compliance.qcert.org

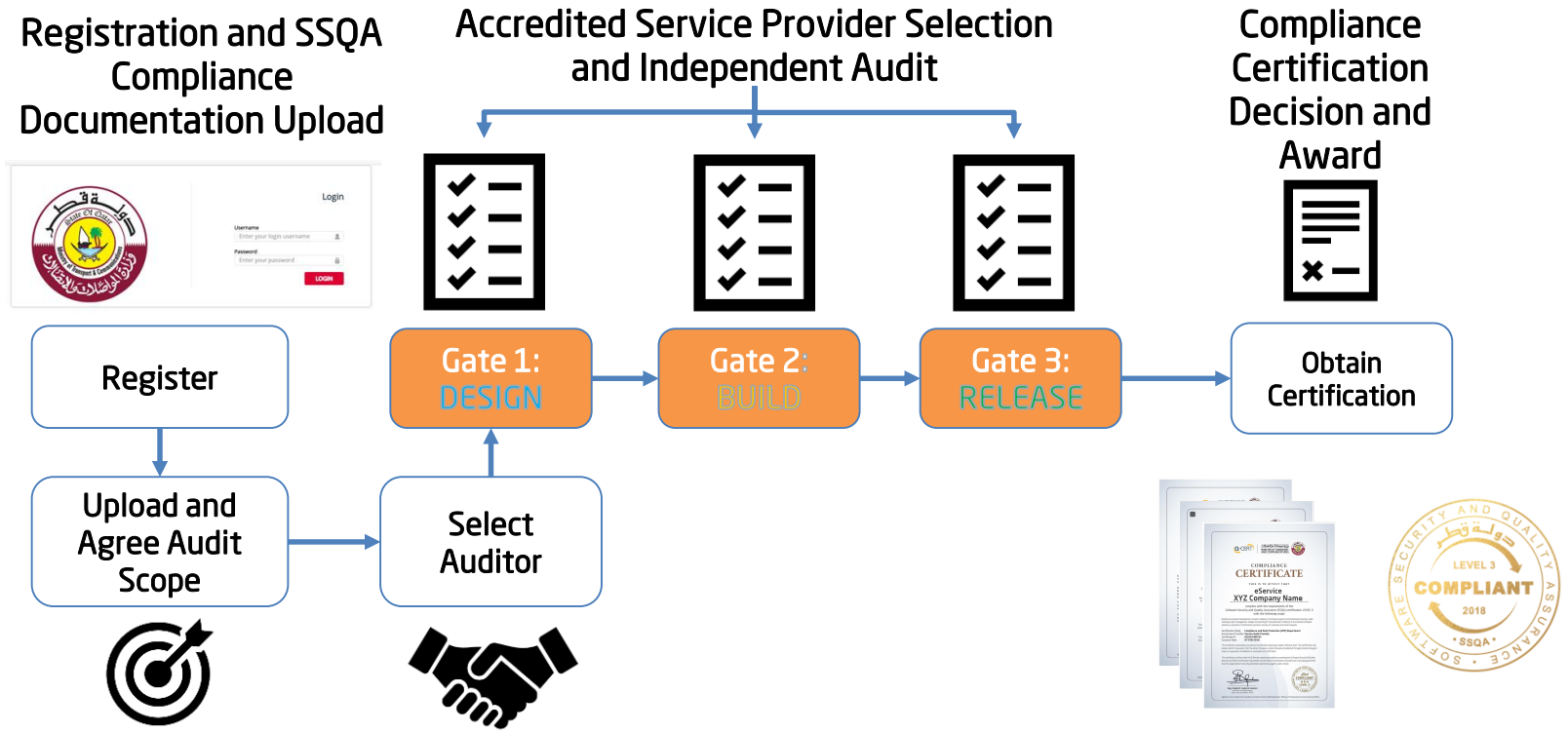
COMPLIANCE ASSESSMENT OWNERSHIP

Regardless of the development approach, the ownership of the compliance assessment process is the E-Service owner.

Approach (Development, hosting…)	Ownership	
	Accountable	Responsible
In-House / Internal	E-Service Owner	E-Service Owner
Outsourced	E-Service Owner	Service Provider/E-Service Owner

- Responsible – person who performs an activity or does the work.
- Accountable – person who is ultimately accountable and has Yes/No/Veto.

ASSISTING WITH COMPLIANCE ASSESSMENTS



Throughout the assessment process, the Compliance and Data Protection (CDP) department may evidence in support of the findings or comments asserted by a Service Provider (or Constituent in the case of self-assessment).

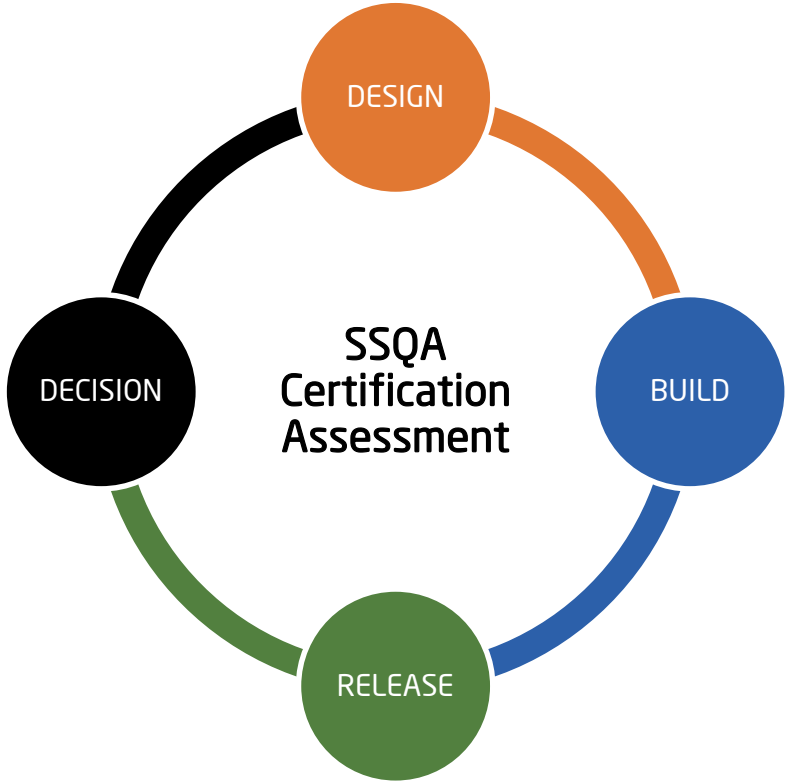
The request for documentation is put forward to ensure the continuing high-standards of service provision amongst Accredited Service Providers and to maintain the integrity of compliance certification.

SSQA ASSESSMENT CYCLE

The Software Security and Quality Assurance (SSQA) Framework Certification Assessment is performed through 4 key activities, these include the 3 Gate Assessments (DESIGN, BUILD and RELEASE) and the final Assessment Report.

DESIGN Assessment Gate:
- Initial delineation of business requirements in terms of confidentiality, integrity, and availability;
- Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information; and,
- Determination of any privacy requirements.

SSQA Assessment Report:
The assessment report submitted to the Compliance and Data Protection (CDP) department to evaluate the compliance of a Constituents system with the target controls.



BUILD Assessment Gate:
- Conduct the risk assessment and use the results to supplement the baseline security controls,
- Analyze security requirements,
- Design security architecture, and,
- Develop system security documentation.

RELEASE Assessment Gate:
- Integrate the information system into its environment,
- Plan and conduct testing of security controls,
- Conduct an operational readiness review,
- Manage the configuration of the system; and,
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls.

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