وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Compliance and Data Protection Department

NATIONAL INFORMATION ASSURANCE (NIA) COMPLIANCE

Compliance Certification Scheme Overview

compliance.qcert.org

Q-CERT

Classification: Public

Workshop Contents

1. FRAMEWORK AND SCHEME OVERVIEW

- Information Assurance Framework Overview
- The National Information Assurance (NIA) Policy
- NIA And SSQA Alignment

2. NIA STANDARDS AND COMPLIANCE

- Assessment Cycle
- Selecting An Accredited Service Provider
- Evidencing NIA Compliance
- Certification Fees & Enforcement

3. NIA CERTIFICATION

- Process Overview
- Scope Agreement & Administration Fees
- Accredited Service Provider Engagement & Scheduling Compliance Audits
- Assisting With Compliance Audits
- Questions And Answers

Classification: Public

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

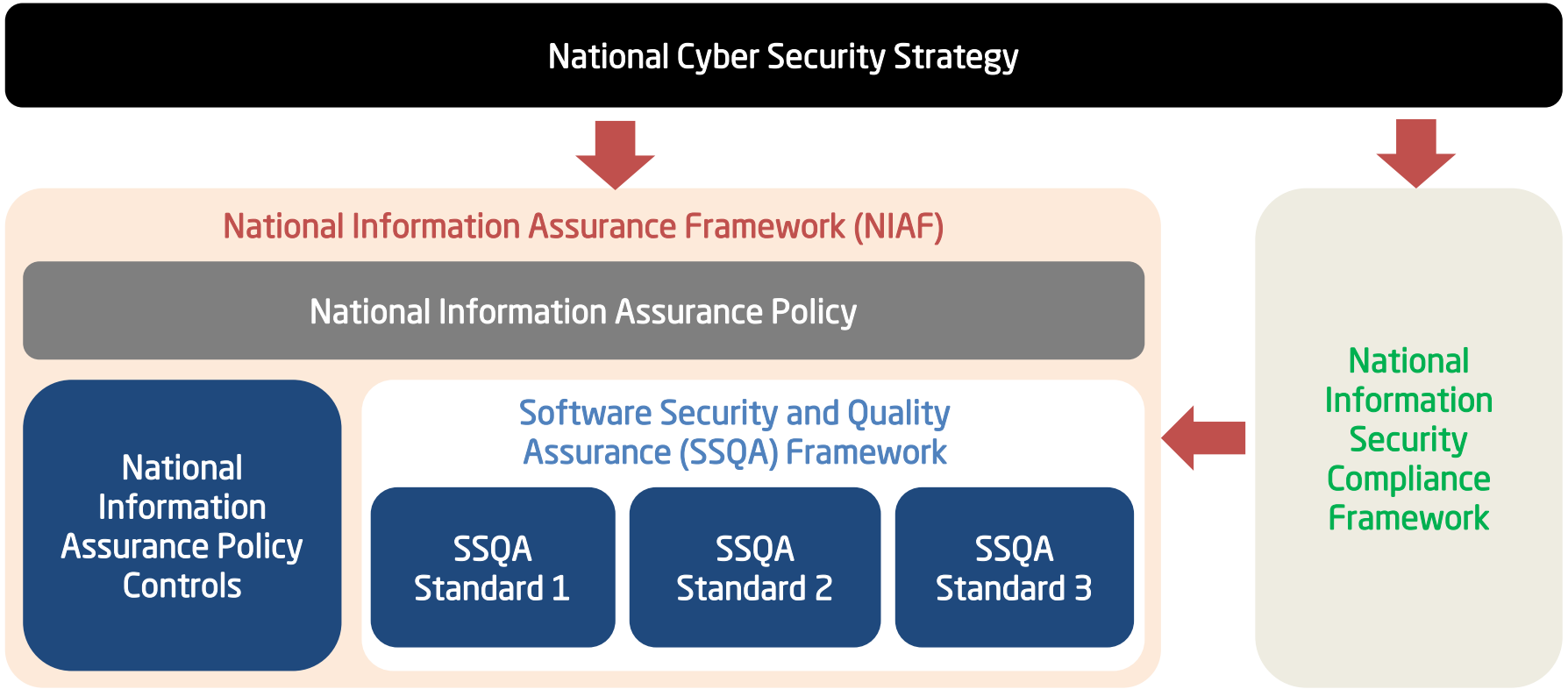
FRAMEWORK AND SCHEME OVERVIEW

compliance.qcert.org

Q-CERT

Classification: Public

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.**

compliance.qcert.org

Classification: Public

THE NATIONAL INFORMATION ASSURANCE (NIA) POLICY

The National Information Assurance compliance certification is based upon the NIA policy control set.

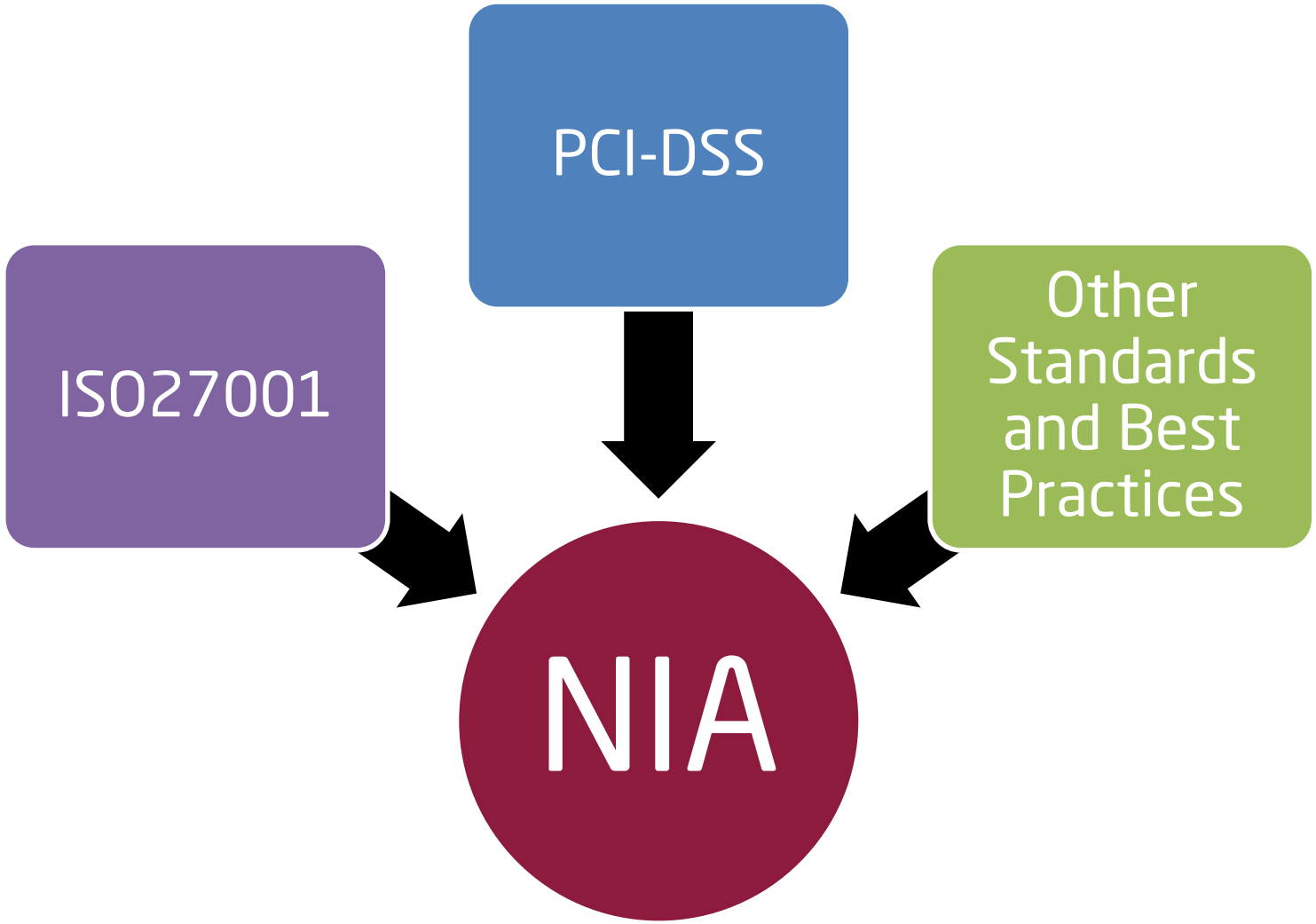
The controls, both baseline and recommended, are mapped upon ISO27001 as well as best practices and other standards such as PCI-DSS.

There are 26 domains, focusing on procedural activities and technology, and implementation is prioritized by a Business Impact Assessment (BIA).

The scope, alongside our Asset Classification Model determines the applicability of NIA controls.

Baseline Controls are mandatory (subject to applicability)

compliance.qcert.org



Classification: Public

NIA AND SSQA ALIGNMENT

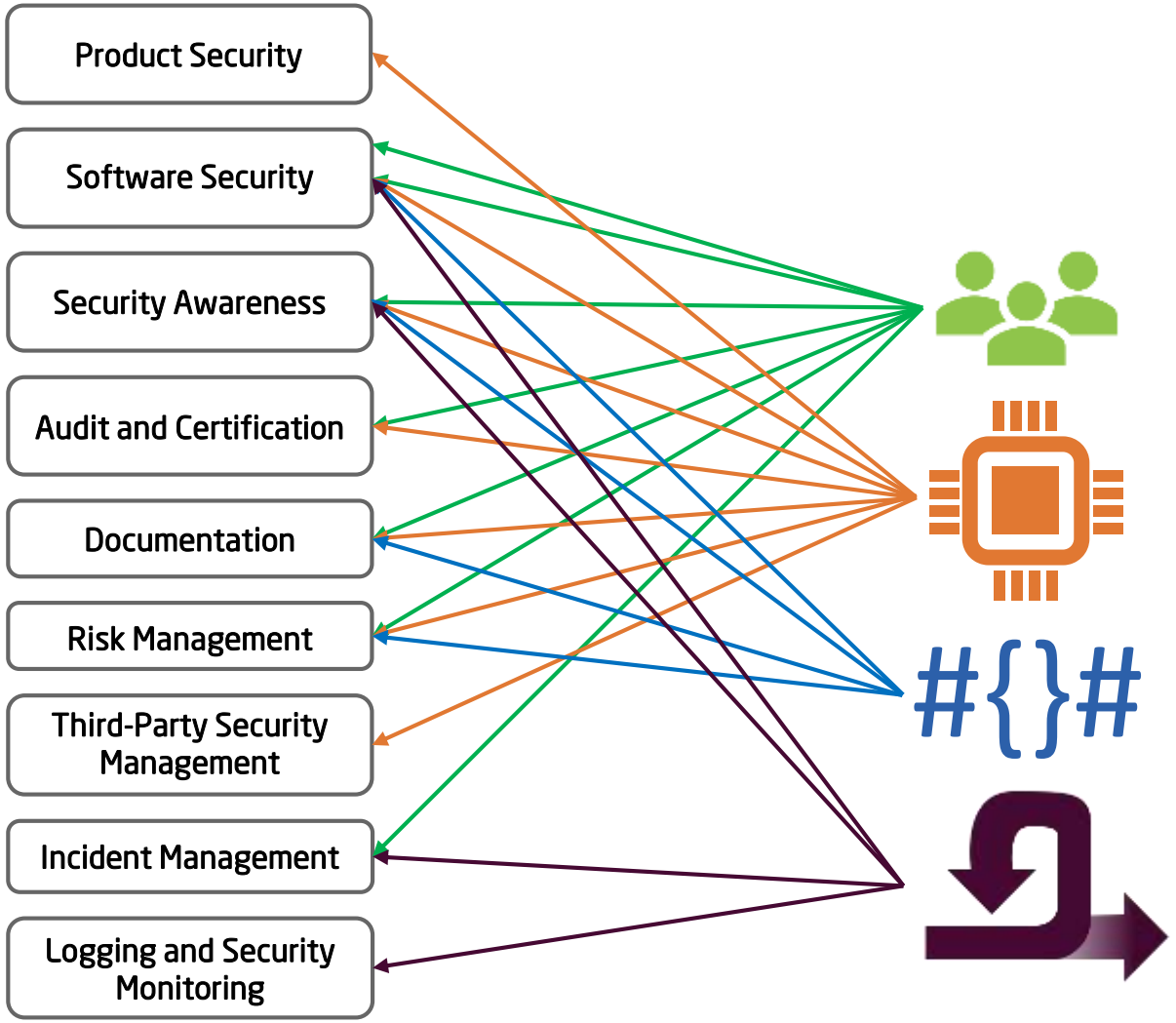
The Software Security and Quality Assurance (SSQA) Standard, central to our e-services certification, is based upon an industry standard BSIMM7.

This introduces 113 controls address 4 Domains:

- Governance,
- Intelligence,
- SSDL Touchpoints; and,
- Deployment.

The controls enhance many of the NIAP domains.

compliance.qcert.org



Each Domain is comprised of 3 Practices, creating a total of 12 Practices:

- Strategy and Metrics
- Compliance and Policy
- Training
- Attack Models
- Security Features and Designs
- Standards and Requirements
- Architecture Analysis
- Code Review
- Security Testing
- Penetration Testing
- Software Environment
- Configuration Management and Vulnerability Management

Classification: Public

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

NIA STANDARDS AND COMPLIANCE

compliance.qcert.org

Q-CERT

Classification: Public

THE NIA COMPLIANCE ASSESSMENT CYCLE

Registration & Scope Submission

- The organization registers using the Compliance Portal and submits documentation, including:
  - Certification Scope, -
  - Information Security Policy,
  - Business Impact Analysis,
  - Assets Classification Register,
  - Statement of Applicability, and,
  - Compliance Roadmap.

Scope Agreement and Auditor Selection

- The Compliance and Data Protection(CDP) department review the certification scope.
- If the certification scope is appropriate, the applicant is then able to engage an Accredited Service Provider to plan and complete the audit activity.

Assess Controls Evidence

- The Accredited Service Provider defines the audit schedule and the audit process begins.
- An audit of the controls against the scope is conducted, with evidence reviewed and findings documented.
- An assessment report is produced documenting the audit activity and the findings.

Audit Reporting

- The Compliance and Data Protection (CDP) department review the audit report submitted by the Accredited Service Provider
  - If successful CDP provide the applicant with the NIA Compliance Certificate
  - If unsuccessful, the applicant is advised of the outcome and of their right to appeal or re-apply.

The process enabling applicants to achieve certification consists of four key activities:

- **Registration & Scope Submission** – The Constituent provide organizational details and submits prospective Assessment Scope & other documents
- Scope Agreement and Auditor Selection – CDP review the scope and agree the appropriateness of the assessment scope and chosen assessor
- Assess Controls Evidence – The assessor evaluates system compliance development against the controls and compiles a report
- Audit Reporting – CDP communicate the Certification Decision following review of the Assessment Report

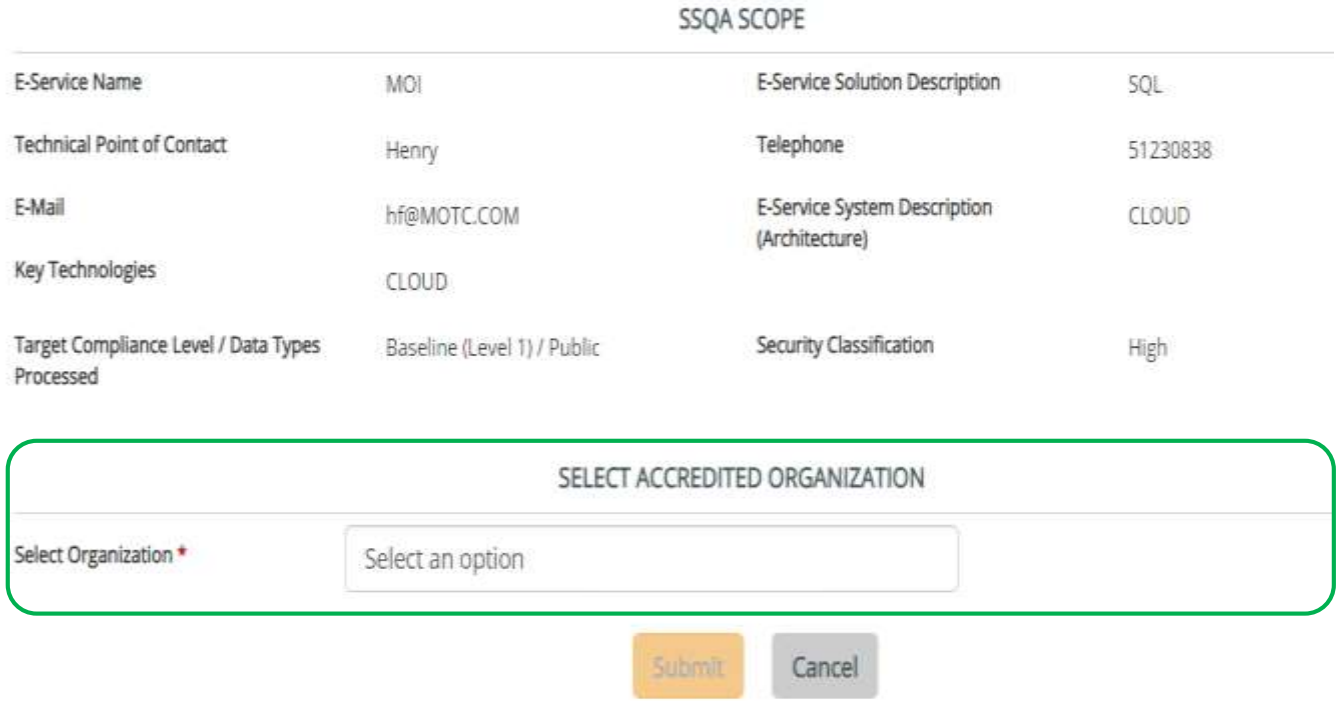
compliance.qcert.org

Classification: Public

SELECTING AN ACCREDITED SERVICE PROVIDER

Applicants 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) Compliance Scheme or the Software Security and Quality Assurance (SSQA) Compliance Scheme.



Accreditation is scheme specific and the Applicant 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 on the Compliance and Data Protection (CDP) department website which enabling the validation any asserted accreditations.

compliance.qcert.org

Classification: Public

EVIDENCING NIA COMPLIANCE

- As part of the assessment process an, Independent, Accredited Service Provider evaluates the implementation of controls within the context of a defined audit scope.
- If, following the assessment, it is determined that all applicable controls have been implemented, a certificate of compliance is issued by the Compliance and Data Protection (CDP) department.
- The compliance certificate demonstrates alignment of a given organization or asset, specified by the compliance scope, with the applicable controls of the NIA standard.
  Compliance is determined at a point-in-time and relates specifically to the outlined audit scope.
- Any changes to the evaluated asset that materially alters impacts the applicability of the controls will invalidated the compliance certificate and require re-assessment.

compliance.qcert.org

Classification: Public

CERTIFICATION FEES & ENFORCEMENT

Certification Fees

Both, Certification and Accreditation require the payment of fees to cover the administrative (and operational costs) for running the accreditation and certification services.

Fees are due around three distinct activities

- During the Application Phase,
- Upon award of Certification or Accreditation; and,
- During any maintenance or Re-instatement period.

The fee values necessary at each point have yet to be agreed and will be released following the conclusion of the Pilot Activities and prior to the end of the compliance grace period.

compliance.qcert.org

Compliance Enforcement

Evidencing compliance with the NIA and SSQA standards is mandatory for the government sector. NIA 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.

Classification: Public

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

NIA CERTIFICATION

compliance.qcert.org

Q-CERT

Classification: Public

NIA CERTIFICATION PROCESS OVERVIEW

MOTC

CERTIFICATION PROCESS

The National Information Assurance (NIA) certification process is designed to promote the enhancement of information security management across an organization, to ensure that information is processed securely.

As part of the National Information Security Compliance Framework (NISCF), the effective and appropriate implementation of NIA controls will be mandatory for many organizations; however, it is recommended as good practice also for all.

The NIA certification is provided following the independent audit of an organization, by Accredited Service Providers, within the context of a defined Assessment Scope that specifies the boundaries of the compliance effort.

The audit is completed through a combined document review and on-site verification activity.

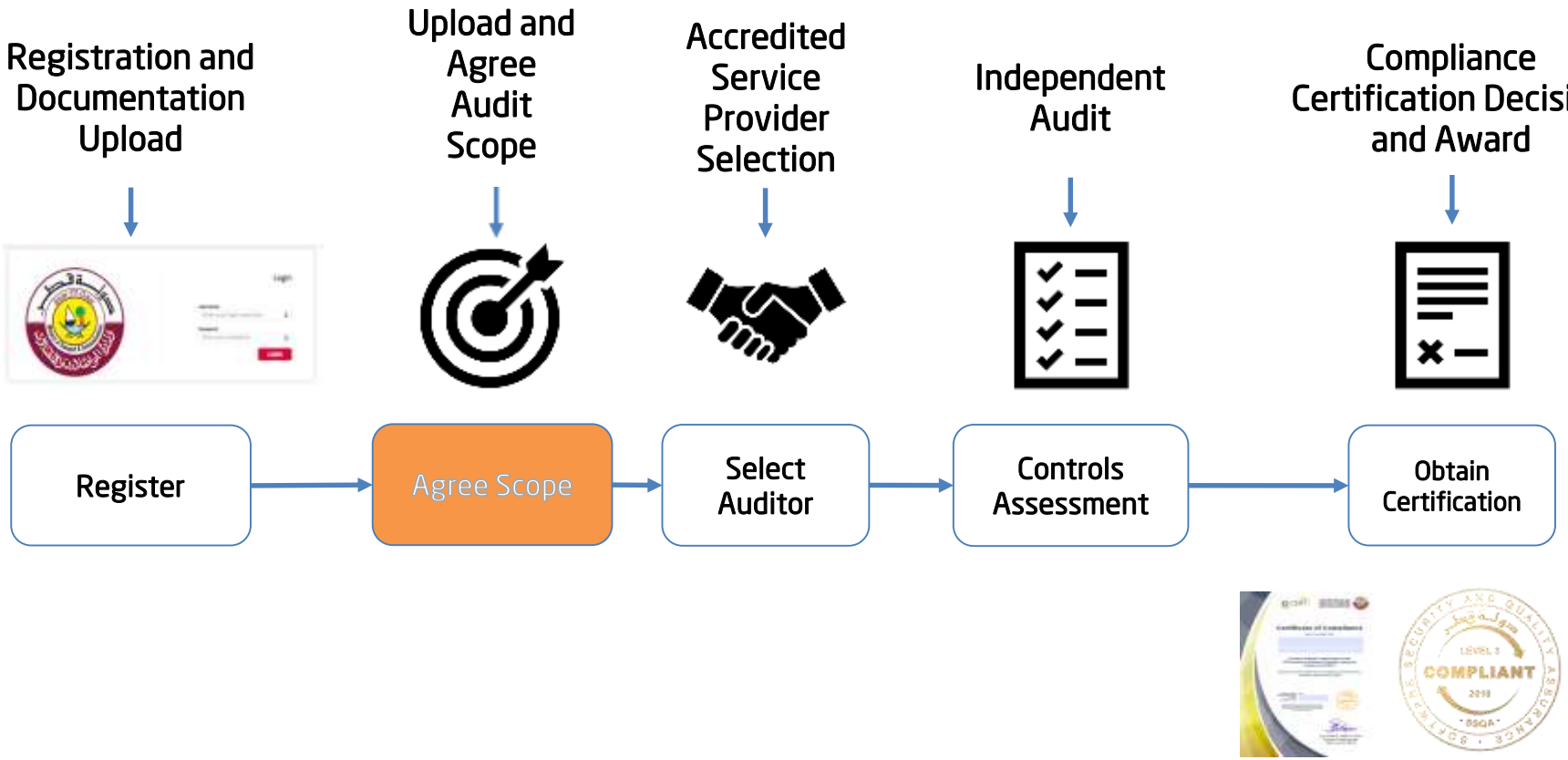
KEY ARTEFACTS :

- **Assessment Scope –** The Assessment Scope establishes the outlines the boundaries of the controls audit.
- **Certification Assessment Report -** The Assessment Report documents the observed implementation of NIA controls applicable to the scope and any observed non-conformances.
- **Compliance Certificate –** The Compliance Certificate indicates the compliance with the NIA controls within the context of the documented scope.

compliance.qcert.org

Classification: Public

SCOPE AGREEMENT & ADMINISTRATION FEES



When applying for certification, Applicants must provide a clear scope to identify the audit boundaries.

This scope document includes a:

- **Information Security Policy** – Clarifying the direction of information security across the organization,
- **Business Impact Analysis (BIA)** - determining the effects of an information security incident,
- **Information Asset Classification Register** – rating assets to identify the applicable controls that help mitigate identified risks
- **Statement of Applicability** – Bringing together the assets, impacts and controls to ensure risk is mitigated to an acceptable level; and,
- **Compliance Roadmap** – Outlining the organizations approach and commitment towards organizational compliance.

Following submission the Compliance and Data Protection (CDP) department conduct a review to ensure key business areas are prioritized and, once approved, the CDP will request the Schemes Administration Fee.

Classification: Public

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

EXERCISE 1: SCOPE FULFILMENT

compliance.qcert.org

Q-CERT

Classification: Public

NIA DOCUMENTS OVERVIEW

To start the certification process, the following documents are requested after registering on the compliance portal.

✓ Scope	Identifying the audit boundaries.
✓ Information Security Policy	Clarifying the direction of information security across the organization.
✓ Business Impact Analysis (BIA)	Determining the effects of an information security incident.
✓ Information Asset Classification Register	Rating assets to identify the applicable controls that help mitigate identified risks.
✓ Statement of Applicability (SoA)	Bringing together the assets, impacts and controls to ensure risk is mitigated to an acceptable level.
✓ Compliance Roadmap	Outlining the organizations approach and commitment towards organizational compliance.

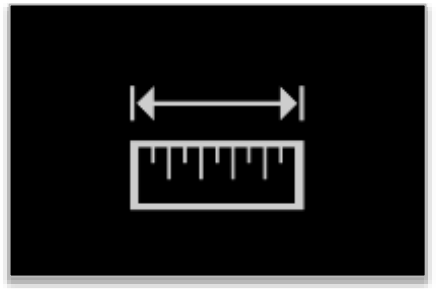
NIA Scope Document

Classification: Public

BUSINESS IMPACT ANALYSIS (BIA)

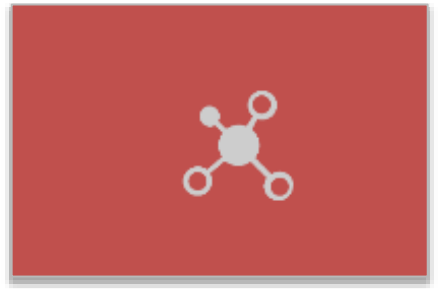
To help developing a certification scope, a BIA must be completed which will help define a certification scope. The BIA should help prioritize the NIA implementation.

When submitting a the mandatory BIA document, what information need be considered to ensure a comprehensive BIA ?



Assessment method

Outline a repeatable assessment procedure



Impact factors

Identify the impact factors (internal, external, economic…)

Impact values

Determine the impact values of a loss or degradation

Impact ranking

Prioritize impacts based on scores

compliance.qcert.org

Classification: Public

BUSINESS IMPACT ANALYSIS (BIA)

The following details could be provided as part of a comprehensive BIA document.

Process	Customer	NICP Priority	Owner	Impact on Reputation	External Impact	Internal Impact	Legal Impact	Economic Impact	Impact Value

Classification: Public

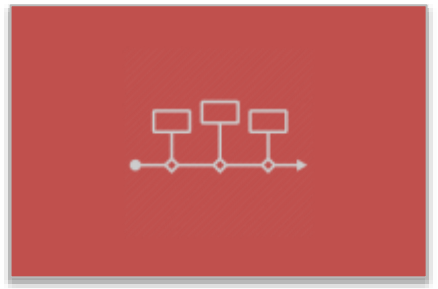
COMPLIANCE ROADMAP

The compliance roadmap is a commitment that the organization makes, to achieve full organizational compliance against NIA.

When creating a the mandatory Compliance Roadmap for NIA certification, what type of information is considered relevant to have a clear overview of the commitment to organizational certification ?

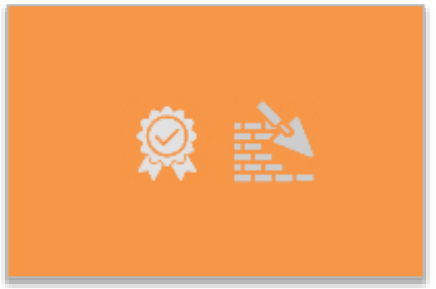
Current vs Target

Provide a snapshot of current state and the end state



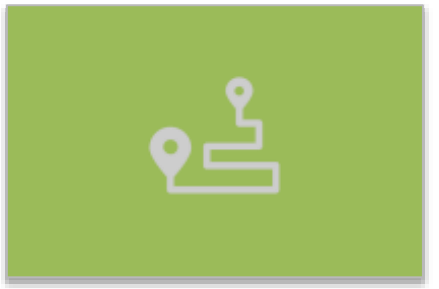
Timeline

Provide a clear calendar for achieving organizational compliance



Implementation vs Certification

Providing an overview of implementation and certification progress



Roadmap rationale

Provide background surrounding the implementation priorities

compliance.qcert.org

Classification: Public

COMPLIANCE ROADMAP

The following template is what could be a comprehensive Compliance Roadmap.

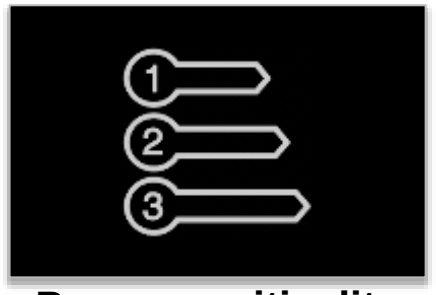
Criticality	Process	Implementation current state	Certification current state	Stage 1 (2019)		Stage 2 (2020)		Stage 3 (2021)	
				Implementation Target	Certification Target	Implementation Target	Certification Target	Implementation Target	Certification Target
High	A	✓	☒	✓	✓	✓	✓	✓	✓
High	D	✓	☒	✓	✓	✓	✓	✓	✓
Medium	B	☒	☒	✓	☒	✓	✓	✓	☒
Low	E	☒	☒	☒	☒	☒	☒	✓	✓
Low	C	☒	☒	☒	☒	☒	☒	✓	☒

Classification: Public

SCOPE

The scope declaration is mandatory. It may include either the whole organization, specific functions or processes.

When drafting your NIA Certification scope document, what information need to be taken into consideration ?



Process criticality and context

Scope relevant regarding the internal and external context of the Agency

Stakeholder requirements

Scope that satisfies the information needs of the CDP

Boundaries and dependencies

Scope that clearly states the boundaries of the certification

Authoritative considerations

Scope considers wider legal regulatory security requirements

Classification: Public

SCOPE

The following table is what could be a part of a comprehensive NIA certification scope document.

Process	Organizational boundary	Physical Boundary	Logical Boundary	Other legal requirements impacting information security	Scope inclusion statement
	IT department	HQ	local network	Privacy law	In
		HQ & call centre	local network & external Call Centre		In
			local network & hosting software service provider	SOX	Out

Classification: Public

INFORMATION ASSET CLASSIFICATION REGISTER

Information security is the preservation of confidentiality, integrity and availability of information assets regardless of its format.

When providing the Information Asset Classification Register, what information may be considered relevant to give an overview of the information assets criticality and the scope they supporting ?

Link to processes

Link the assets with the processes in the scope

Aggregate security level

Determine the security level needed for each asset based on its information security criteria

Asset information

Provide enough details about the information asset to give a clear understanding of its role

Responsibilities

Provide information about the ownership and custodian of the assets

compliance.qcert.org

Classification: Public

INFORMATION ASSET CLASSIFICATION REGISTER

The following table is what could be a comprehensive Information Asset Classification Register.

Process	Asset ID	Asset description	Business unit	Asset owner	Asset status	Location	Asset category	Asset custodian	Type of data	Availability	Integrity	Confidentiality	Aggregate security level
							Digital Asset Business Data Base Software Source Code Non Digital Asset Servers People Assets network Devices Desktops Laptops Media Support Utilities		Sensitive Customer Data Personal Data Personal Sensitive Data National Security Data				

Classification: Public

STATEMENT OF APPLICABILITY (SOA)

Statement of Applicability (SoA) translates all the risk analysis and information classification outputs into applicable controls.

When providing a SoA, what type of information may be provided to present a clear translation of the BIA document and Information Asset Classification Register into controls ?

Status of implementation

For NIA Manual controls provide a status of their applicability

compliance.qcert.org

Justification of exclusion

This information can be looked at a summary of a statement of exception

Selection reasons

Controls can be implemented for different reasons, where's why

Controls addressing

How controls are linked to risks addressed, assets protected and processes supported

Classification: Public

STATEMENT OF APPLICABILITY (SOA)

The following template is what could be a comprehensive Statement of Applicability (SoA).

Control ID	Control description	Control status	Justification (including justification for exclusion)	Reasons for selection		Results of risk assessment	Process impacted
				NIA Base requirement	Other information security legal requirement		

Classification: Public

INFORMATION SECURITY POLICY (ISP)

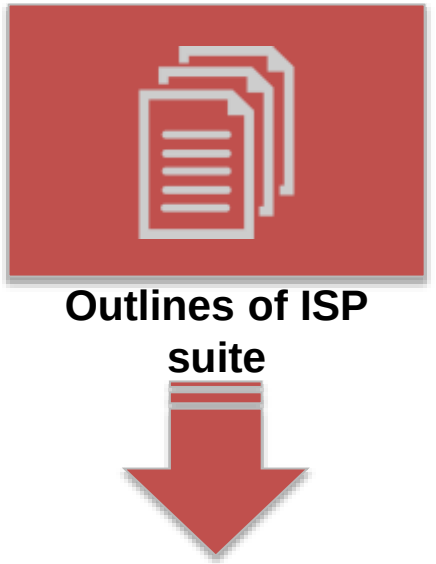
Information security policy (ISP) is a set of policies issued by an organization to ensure that all information technology users within the organization's boundaries comply with rules and guidelines related to the security of the information.

When submitting the ISP document, what information may be considered in the ISP ?

Global ISP document

Submitting the high level Global ISP document

compliance.qcert.org

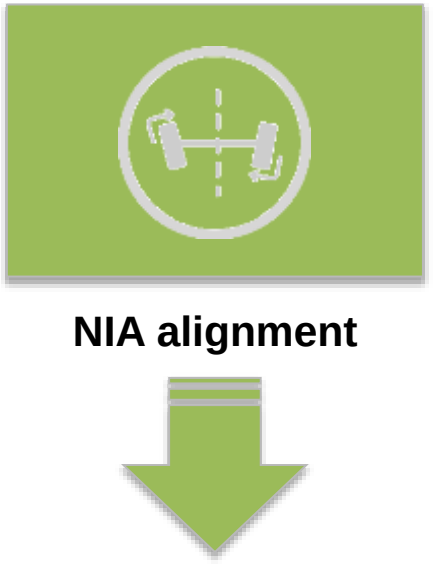


Outlines of ISP suite

Global ISP should give outlines on lower level information policies (topic-specific)

Commitment & direction

Global ISP includes a commitment to satisfy applicable requirements related information security



NIA alignment

It’s always good to check if the Agency’s ISP covers all NIA domain objectives

Classification: Public

ACCREDITED SERVICE PROVIDER ENGAGEMENT & SCHEDULING COMPLIANCE AUDITS

MOTC

Registration and Documentation Upload

Upload and Agree Audit Scope

Accredited Service Provider Selection

Independent Audit

Compliance Certification Decision and Award

Register → Agree Scope → Select Auditor → Controls Assessment → Obtain Certification

Following agreement of the certification scope, applicants will be required to may select an Accredited Service Provider to perform the Compliance Assessment).

Please note that we recommend the completion of any necessary tendering activities prior to selecting the Accredited Service Provider.

Following selection, the Applicant will work with the Accredited Service Provider to plan the audit activity and to ensure the completion and accuracy of planned compliance assessments.

compliance.qcert.org

Classification: Public

ASSISTING WITH COMPLIANCE AUDITS

Registration and Documentation Upload

Upload and Agree Audit Scope

Accredited Service Provider Selection

Independent Audit

Compliance Certification Decision and Award

Register → Agree Scope → Select Auditor → Controls Assessment → Obtain Certification

The Accredited Service Provider will complete the compliance assessment through combined document review and on-site audit.
This requires the availability of any necessary evidence, stakeholders and facilities (as agreed during any audit planning activity), in a timely manner.

The Compliance and Data Protection (CDP) department may request copies of evidence to ensure the continuing high-standards of service amongst Accredited Service Providers and to maintain the integrity of compliance certification.

compliance.qcert.org

Classification: Public

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Questions and Answers Session

compliance.qcert.org

Q-CERT

Classification: Public

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

Classification: Public