وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Cyber Security Guidelines for Defining NIAP Scope Statements

Version 1.1

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: June 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	August 2017
1.1	MOTC Logo & Branding Changed	June 2018

Table of Contents

Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This guideline has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Introduction

The Ministry of Transport & Communication (MoTC) has issued the National Information Assurance Policy (NIAP) V2.0. The policy is mandatory for compliance by the government sector and strongly recommended for the critical sector organizations.

In line with the objectives of the Cybersecurity department of MoTC, to drive the adoption of NIAP, this document is a step in this direction to help agencies choose the right scope statement in pursuit of NIAP compliance.

The main purpose of setting the ISMS (information security management system) scope is to define which information you intend to protect

Audience

Any agency that has initiated a plan to comply with NIA Policy V2.0

Guidelines:

The journey towards establishing an Information Security Management System is in some ways challenging for established organizations as it entails reengineering existing processes or introducing new processes to comply with the security requirements, ditto for organizations that are huge in terms of the line of business it does, sheer size and locations. It is extremely important that in such cases Agencies carefully develop a roadmap for compliance. The compliance journey should be broken down into small scopes that are practical, manageable and aligned as per the criticality needs of the business.

Alignment to NIAP Compliance Roadmap

Agencies should ensure that the scope chosen by them, aligns to the NIAP Compliance roadmap agreed by the agency with MoTC. The scope statement should reflect in entirety the desired scope of work and the milestone as defined in the NIAP Compliance roadmap.

Smaller scope does not mean an easier job.

The agency has to ensure that within the selected scope, all the relevant controls are applied. The agency will have to regulate information that flows out to or in from areas that are outside the scope. This in itself may become tricky and as such is not recommended for smaller organizations.

Exclusion of controls has nothing to do with the ISMS scope.

Scope limitation, does not in any way mean controls limitation. The agency cannot for e.g. say we will apply all controls, except Network and Access Management. The agency should document all exclusions in the Statement of Exception with valid justifications, vetted by the senior management of the agency. E.g. The agency could state that a certain Legacy system cannot be hardened, because no support exists or that certain controls have not been implemented as they are due for upgrade / replacement etc.

The agency can exclude the controls only if there are no risks nor requirements, which would require the implementation of those controls

Mapping the Scope

One of the effective ways to identify what is in the scope is the OBASHI methodology. A methodology for mapping and developing how IT systems relate to organizational operations (OBASHI stands for Ownership, Business Processes, Applications, Systems, Hardware, and Infrastructure).
The OBASHI methodology provides a framework and method for capturing, illustrating and modeling the relationships, dependencies and data flows between business and Information technology (IT) assets and resources in a business context.
It is a formal and structured way of communicating the logical and physical relationships and dependencies between IT assets and resources (Ownership, Business Processes, Applications, Systems, Hardware, and Infrastructure) to define the business services of a modern enterprise.

This is not the only method, and may not necessarily the best method for your specific ISMS.

Some other options include using graphical representation. This might be suited for small agencies. The agency can draw draw the processes that are included in ISMS scope within a circle, and then outside of this circle draw the processes that are provided from outside of your scope. By *processes*, we mean the main business processes within your scope

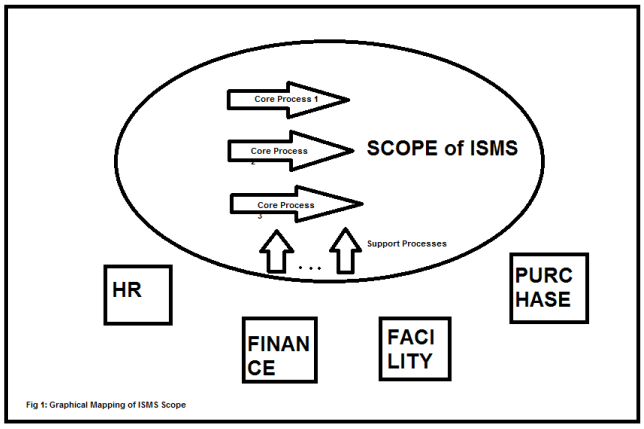

Fig 1: Graphical Mapping of ISMS Scope

The next step after determining the boundaries are to identify the interfaces that is the input and output of these processes and how they relate to each other in order to protect them better.

For smaller organization, it is usually easy and safe to include the whole organization. This includes all its people, processes, systems and physical locations. This is usually suited for organizations with single office, small head count and very limited service offerings.

Scope Examples

The following statement and examples are to provide guidance to agencies in choosing and framing their scope statement in pursuit of NIAP compliance. The following examples are by no means the only syntax / format and agencies can choose to re-write / re-draft their scope statements.

Generic Scope Statement:

The scope of the <Agency>'s ISMS applies to the provision of <agency function / services> in accordance with the <Agency's> NIAP Compliance Plan version ____ dated _____ and Statement of Exception, version _____ Dated …….

The ISMS is compliant to the National Information Assurance Policy [NIAP] V2.0, issued by the Ministry of Transport and Communication. It covers the Assurance of <Agency's> information assets and business activities.

The scope includes staff, assets and third parties that support the agency function.

Scope Definition Related to Agency's Org Structure

The scope of the <Agency>'s ISMS applies to the provision of information assets and business activities of <XYZ> Sector / Directorate in accordance with the <Agency's> NIAP Compliance Plan version ____ dated _____ and Statement of Exception, version _____ Dated …….

The ISMS is compliant to the National Information Assurance Policy [NIAP] V2.0, issued by the Ministry of Transport and Communication. It covers the Assurance of <Agency's> information assets and business activities.

The scope includes staff, assets and third parties that support the agency function.

Scope Definition related to Agency's Services

Example 1

The scope of the <Agency>'s ISMS applies to the provision of <Agency's e-Services> in accordance with the <Agency's> NIAP Compliance Plan version ____ dated _____ and Statement of Exception, version _____ Dated …….

The ISMS is compliant to the National Information Assurance Policy [NIAP] V2.0, issued by the Ministry of Transport and Communication. It covers the Assurance of <Agency's> information assets and business activities.

The scope includes staff, assets and third parties that support the agency function.

Example 2

The development, operation, administration and maintenance of the e-Services (listed below) provided by the Agency, in accordance with the <Agency's> NIAP Compliance Plan version ____ dated _____ and Statement of Exception, version _____ Dated …….

List of e-Services in Scope

1. ABC
2. XYZ
3. Etc.

Example 3

The Information Security Management System (ISMS) applies to the provision of the listed services to internal and external customers of <Agency> in accordance with the <Agency's> NIAP Compliance Plan version ____ dated _____ and Statement of Exception, version _____ Dated …….

Scope Definition Related to Agency's Locations

As stated in the <Agency's> NIAP Compliance Plan version ____ dated _____ and Statement of Exception, version _____ Dated ……. the Information Security Management System (ISMS) encompasses <Agency>'s Information Technology Division Office, Data Centre, and WAN infrastructure, covering business activities relating to the provision of operation, maintenance and management of corporate IT services.