وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

National Information Security Compliance Framework – Audit Standard

[CDP-NISCF-AS-V1.0]

Standard - Audit Requirements and Guidelines for Certification Audits

Compliance and Data Protection Department

October 2019

V1.0

Public

compliance.qcert.org

Q-CERT

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

DISCLAIMER / LEGAL RIGHTS

Compliance and Data Protection (CDP) Department of Ministry of Transport and Communications (MOTC) has designed and created this publication, titled "National Information Security Compliance Framework – Audit Standard" - V1.0 - Public, as audit requirements and guidance for accredited service provider related to the National Information Security Compliance Framework (NISCF) certification audits.

CDP is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction, shall acknowledge MOTC and CDP as the source and owner of the "National Information Security Compliance Framework – Audit Standard".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the CDP and MOTC. CDP and MOTC shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from CDP and MOTC shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

LEGAL MANDATE(S)

Article 18 of the Emiri Decree no (4) for the Year 2016 setting the mandate of Ministry of Transport and Communications (hereinafter referred to as "MOTC") provides that MOTC has the authority to regulate and develop the sector of Information and Communications Technology 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

Based on Cabinet decision (26) for the year 2018, the Compliance & Data Protection Department (herein referred to as CPD) is entrusted by the Ministry of Transport and Communications (MOTC) as the competent authority, responsible for determining, in the public interest, the technical competence and integrity of organizations such as those offering assessments, testing and compliance services and the Issuance of Certifications those seeking certificates of compliance within the State of Qatar.

This standard has been prepared to take into consideration the current applicable laws of the State of Qatar. If 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.

REFERENCES

- [IAP-NAT-IAFW] Information Assurance Framework
- [IAP-NAT-DCLS] National Information Classification Policy
- [NIAF-SSQA-S-SSL1] SSQA Level 3 Software Security Standard
- [NIAF-SSQA-S-SSL2] SSQA Level 3 Software Security Standard
- [NIAF-SSQA-S-SSL2] SSQA Level 3 Software Security Standard

Table of Contents

Introduction **7**
Scope **7**
Terms and Definitions **8**
Chapter 1: Audit Requirements **10**
1. Audit Engagement Acceptance Due Diligence 10
2. Planning and Conducting Audit work 12
3. Audit Reporting and Closing 22
Chapter 2: Audit Guidelines **26**
1. Audit Engagement Acceptance Due Diligence 26
2. Planning and Conducting Audit work 26
3. Audit Reporting and Closing 31
Appendix A (normative): Audit Ethics / Code of Conduct **33**
1. Fundamental Principles 33
2. Conceptual framework 34
Appendix B (normative): National Information Security Compliance (NISCF) Audit Areas **37**
1. The National Information Assurance (NIA) Policy 37
2. Software Security and Quality Assurance (SSQA) 38

Introduction

The National Information Security Compliance Framework (NISCF) helps to support the achievement of Qatar's National Cyber Security Strategy; it complements Qatar's National Information Assurance Framework (including wider applicable information security legislation, regulation and standards) to establish safe and vibrant cyberspace.

Compliance is a continual process and one that relies on open relationships between the Accreditation Body, Certification Body, Service Providers, and, Clients. It requires establishing a cycle of verification and validation to assure the on-going quality of services and to remediate any changes that may affect upon those services.

Accreditation is the formal recognition that an organization is competent to perform specific services, activities or tasks in a consistent, reliable and precise manner. It must be performed impartially, and the process must remain objective, transparent and consistent to ensure reliability and trustworthiness.

The National Information Security Compliance Framework (NISCF) offers an Audit Service Accreditation for Service Providers interested in elevating quality assurance of Information and Communications Technology in the State of Qatar.

Service providers shall comply with the audit requirements defined in this standard for the purpose of Accreditation maintenance.

This document provides audit requirements (Chapter1: Audit Requirements), including the normative Appendices, as well as guidelines (Chapter2: Audit Guidelines).

Scope

This standard is mandatory to all accredited services providers that will engage on certification audits under the National Information Security Compliance Framework (NISCF).

Terms and Definitions

Audit;	systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
Audit criteria;	set of controls, policies, procedures or requirements used as a reference against which audit evidence is compared.
Audit evidence;	records, statements of fact or other information, which are relevant to the audit.
Audit findings;	results of the evaluation of the collected audit evidence against audit criteria on which conclusions of compliance or non-compliance is based on.
Audit Conclusion;	outcome of an audit, after consideration of the audit objectives and all audit findings.
Auditee;	organization or parts thereof being audited.
Auditor;	independent accredited service provider who conducts an audit.
Audit team;	one or more individuals planning, conducting and reporting an audit.
Audit team leader;	person part of the audit team that is responsible for the audit within the auditor's organization.
External experts;	persons or entities providing specific expertise to the audit team.
Scope;	subject matter of the certification.
Risk;	effect of uncertainty on objectives.
Population;	is the entire set of data from which the auditor wants to sample to reach a conclusion on the scope based on audit criteria.
Compliance;	fulfilment of a requirement.

Non-compliance;	non-fulfilment of a requirement.
Requirement;	statement defined in a policy, standard or manual as a compliance basis.
E-Service;	constitutes a service produced, provided or consumed through ICT and which is available on the Internet.

Chapter 1: Audit Requirements

1. Audit Engagement Acceptance Due Diligence

1.1. Due Diligence

1.1.1. The auditor shall perform due diligence before engaging with an audit client to check and evidence the compliance with fundamental principles of ethics and the conceptual framework provided in Appendix A: Audit Ethics / Code of Conduct.

1.1.2. The auditor shall have a reasonable expectation that the audit can achieve its objectives based on the scope and determine if there is any restrictions that need to be addressed.

1.1.3. The auditor shall have reasonable expectation that the auditee's management understands its obligations and responsibilities with respect to the provision of appropriate, relevant and timely information required to perform the engagement.

1.1.4. The auditor shall have reasonable expectation that the engagement can be completed in accordance with this standard and, where required, applicable regulations and result in a professional conclusion.

1.1.5. Before performing any audit activity, the auditor shall collect and document all non-compliance already identified by the auditee.

1.2. Acceptance Documentation

1.2.1. The auditor shall produce evidence of their proficiency and independence compliance assessment against the fundamental principles and the conceptual framework provided in Appendix A: Audit Ethics / Code of Conduct.

1.2.2. The auditor shall produce evidence of performing due care to ensure that the audit will meet the defined expectations.

1.2.3. The formal acceptance of the engagement shall be documented and signed by the auditor and the auditee. Authorized persons, who could legally engage the responsibility of the auditor and the auditee, shall sign this document.

1.2.4. The audit engagement documentation shall state that the audit report shall only be used for the certification purpose by the auditor and shall not be communicated to any other entity other than the CDP without the notification and approval of the auditee.

1.2.5. The audit engagement documentation shall have a clear statement of the scope (list the processes in the scope and reference of the certification submission ID).

1.2.6. The audit engagement documentation shall state that the audit is for the purpose of NISCF Certification scheme, as defined by the CDP in the NISCF, and that the audit will be conducted in compliance with this standard audit requirement.

1.2.7. When accepting an engagement, the auditor shall communicate to the CDP within 10 working days from the signature, the engagement document and the evidence of acceptance diligence.

1.3. Independent Quality Control Reviewer (IQCR)

1.3.1. The auditor shall designate for each audit engagement an Independent Quality Control Reviewer (IQCR).

1.3.2. IQCR shall:

- Check the compliance of auditor and audit team with the Appendix A: Audit Ethics / Code of Conduct of this standard;
- Review key audit documentation:
  - Audit Engagement Acceptance Evidence;
  - Planning documentation, including audit team assignment and communication;
  - Findings and conclusions over high-risk area identified during the audit planning; and
  - Audit report.
- Check:
  - How significant problems brought to light by the audit team in terms of audit approach, audit criteria interpretation, evidence gathering, and audit conclusions have been solved; and
  - The appropriateness of the audit conclusions expressed in the audit report.
- Ensure that acceptance due diligence over the audit team and organization, the auditee and the scope have been performed before formal acceptance of the engagement.

1.3.3. The IQCR shall possess the adequate management and technical skills and experience to be capable to perform a meaningful quality control review.

1.3.4. The IQCR shall have enough authority within the accredited audit firm to be capable of imposing professional judgment.

2. Planning and Conducting Audit work

2.1. General approach

2.1.1. The auditor shall plan and perform a certification audit in two phases:
- Design Assessment: Considered as preliminary assessment; and
- Operating Effectiveness Assessment: Considered as final assessment.

2.1.2. During design assessment, the auditor shall verify that controls have been designed, documented, approved and communicated to relevant parties.

2.1.3. The auditor shall plan and perform the design assessment based on interviews, on-site observations and documentation reviews.

2.1.4. During operating effectiveness assessment, the auditor shall verify the implementation and effectiveness of the designed controls.

2.1.5. The operating effectiveness assessment shall be performed on-site.

2.1.6. The auditor shall determine an audit period that represents the operation timeframe of controls to be audited. For more scheme specific details on this section, please refer to Appendix B: National Information Security Compliance (NISCF) Audit Areas.

2.1.7. In some situations, where the scope has been certified against standards aligned with the National Information Security Compliance Framework (NISCF) policies and standards. In these situations, the auditor shall assess the usefulness and appropriateness of reports issued by the other non-NISCF auditor and shall consider any significant findings reported.

2.2. Preliminary work

2.2.1. Establishing Contact with Auditee

2.2.1.1. The auditor shall establish contact with the auditee to:
- Define communication and escalation channels with the auditee;
- Request access to relevant information for planning purposes; and
- Arrange for the audit including the schedule.

2.2.2. Understanding the auditee and its environment

2.2.2.1. The auditor shall gain and document an understanding of the auditee and its environment, including and not limited to:

- Industry, regulatory, and other external factors;
- Nature of the auditee's organization, including the auditee's risk exposure, appetite and risk assessment methods; and
- Objectives, strategies, and the related organizations risks that could affect the compliance against the standards of the certification scheme.

2.2.2.2. The auditor shall understand the context of the implementation of the audit criteria by the auditee, including the identification of the implementation team.

2.2.2.3. If Accredited Advisors by the CDP helped the auditee to govern, plan, build, implement or review compliance implementation, the auditor shall communicate that to the CDP during the preliminary reporting.

2.3. Audit Planning

2.3.1. Approach to Planning

2.3.1.1. The auditor shall plan prior to each audit the nature, extent and schedule of audit activities.

2.3.1.2. The auditor shall not use a risk assessment approach to manage the audit scope and shall take it from a compliance angle; compliance to specific standards or set of controls with inflexible application for the scope defined by the auditee.

2.3.1.3. Materiality shall be used only to determine and balance the audit procedures workload for compliance criteria defined in the scope or in the compliance scheme standards (subject matter areas).

2.3.1.4. Materiality shall not be used to reduce or expend the scope of work, or to question the controls to be tested as required by the compliance scheme standards or defined by the auditee for the scope.

2.3.1.5. The auditor shall only collect justification and statements of exclusion for any deviation from the compliance scheme standards. For more scheme specific details on this section, please refer to Appendix B: National Information Security Compliance (NISCF) Audit Areas.

2.3.2. Using Audit Risk in planning

2.3.2.1. If the auditor uses a risk-based approach for planning the audit, the auditor shall manage the audit engagement to reduce audit risk to a low acceptable level.

2.3.2.2. Inherent risk shall be set high; as for information security audit potential effect of errors generally impact critical business systems.

2.3.2.3. The auditor shall assess the control risk as high unless the design of controls defined in the scope or in the compliance scheme standards have been evaluated as effective.

2.3.3. Documenting the Audit Planning

2.3.3.1. The audit plan shall be appropriate to the objectives and the scope of the audit. The audit plan shall at least include or refer to the following:

- Audit objectives;
- Compliance criteria;
- Scope to be audited;
- Information assets in the scope (systems, applications, database etc.) to be audited and the nature and extent of audit work to be done over them;
- Interviews plan;
- Information request list;
- Audit work program including testing procedures to be performed;
- Procedures to be used to verify and validate the information collected and their use as audit evidence;
- Tools needed for gathering evidence, performing tests and information for reporting;
- Time budget, resources allocation, schedule of on-site and off-site audit activities;
- Audit calendar and timeline;
- The roles and responsibilities of the different audit team members; and
- Defined deliverables, their audience and their usage.

2.3.3.2. When changes in circumstances occur, the audit planning shall be reviewed and updated accordingly.

2.3.3.3. Based on the work-performed results, the audit planning shall be reviewed and updated to ensure audit objectives achievement.

2.3.3.4. The auditor shall review and update if necessary the audit planning based on the preliminary assessment results and the corrective action plan prepared by the auditee to address exceptions and errors of the design controls.

2.3.3.5. Often, when using a single document to plan an audit, the required information could be provided in different documents (Risk Assessment Matrix, Audit Work Program, Interview Plan, Requested list of documents etc.) and referenced in the audit plan. In such case, the auditor shall make clear cross-referencing between documents.

2.3.3.6. The auditor shall provide to the CDP the audit planning evidence and all the supporting documents at the start of the audit and every time the audit planning is updated.

2.3.4. Audit Timeline

2.3.4.1. The auditor shall have a procedure to determine the time required to plan and accomplish a complete and effective audit based on the certification scheme.

2.3.5. Audit Teams Composition and Assignment

2.3.5.1. The auditor shall have a procedure to select, affect and exclude the audit team members, considering the competence and skills needed for the audit.

2.3.5.2. Auditor shall consider using the work of other experts for the engagement.

2.3.5.3. To determine the required audit team members and the composition, the auditor shall consider:

- Audit context (objectives, scope, criteria and deadlines);
- The competencies, knowledge and skills needed to achieve the objectives of the audit;
- Regulatory or contractual requirements;
- Language used to communicate with the auditee and between team members; and
- Previous experience of the audit team members with the auditee and its systems or similar ones.

2.3.6. Communication of audit team tasks

2.3.6.1. The audit team leader shall communicate with the team about the audit engagement objectives, their roles and responsibilities in the audit and the key success factors.

2.3.6.2. The audit team leader shall assign to each team member specific processes, functions, sites, areas to perform audit activities. The assignment shall consider the needed competence,

the effectiveness of resources allocation and roles and responsibilities of the members within the team.

2.3.7. Communication of audit plan

2.3.7.1. Regardless of the audit planning evidence form, the auditor shall provide the CDP with the audit planning evidence and all the supporting documents before conducting audit work.

2.3.7.2. The auditor shall communicate at the beginning of the audit to the auditee:

- Interviews plan;
- Information request list;
- Audit calendar and timeline; and
- Defined deliverables, their audience and their usage.

2.4. Conducting Audit

2.4.1. Conducting the Opening Meeting

2.4.1.1. The audit team leader shall organize and hold an on-site formal opening meeting with the auditee's management and those responsible for the functions or processes part of the audit scope

2.4.1.2. The auditor shall document the opening meeting and shall include the following:

- Listing of the participants and their roles in the audit;
- The confirmed audit scope;
- Presentation of the audit plan;
- Agree on dates of progress and closing meetings;
- Channels that will be used for communication between the audit team and the auditee, including the language used and reporting rules;
- Presentation of the needed resources by the audit team from the auditee and confirmation of their availability;
- Presentation and acknowledgement of security procedures that the audit team needs to comply with;
- Reminder that the audit team representing the auditor are responsible for the plan and execution of audit activities; and
- Methods, procedures and tools that will be used for sampling, Computer Assisted Audit Techniques (CAATs) and vulnerability assessments.

2.4.2. Scope and Documented Information Review

2.4.2.1. The auditor shall review the scope documentation provided during the certification submission and shall collect any other document that seems essential to verify that:

- The defined scope of the engagement enables conclusion on the subject matter and addresses any restrictions;
- The underlying logical and physical information assets defined are complete and cover the whole scope; and
- The scope relevance has not been impacted by any significant change in the internal or external environment of the organization since its validation by the CDP.

For more scheme specific requirements for this section, please refer to Appendix B: National Information Security Compliance (NISCF) Audit Areas*.*

2.4.2.2. If the auditor detects any situation that could, in his judgment, question the scope, the auditor shall inform formally the auditee and the CDP of such situation and provide justification of his judgment.

2.4.2.3. The auditor shall conduct all necessary interviews, perform on-site inspections and collect all necessary documents (policies, procedures, guidance, contracts, registers…) to be able to conclude on the design of every control applied to the scope during the documented information review phase.

2.4.3. Preliminary audit reporting

2.4.3.1. The auditor shall submit a preliminary reporting on the design of controls using the Preliminary Assessment Checklists provided by the CDP.

2.4.3.2. The CDP could share with the auditor after the start of the engagement, recommendations and comments about missing and incomplete information requested during the scope submission. The auditor shall perform the requested tasks and report the result to the CDP as part of the preliminary reporting.

2.5. Audit Tracking

2.5.1. The auditor shall track, periodically, the audit progress in a documented format.

2.5.2. The audit team leader shall periodically communicate the progress of the audit and report identified issues and challenges to the auditee in accordance with the agreed communication framework.

2.5.3. When information collected indicates that there is a significant threat occurring or that the audit objectives cannot be attained, the auditor shall report to the auditee and, if required, to the Compliance and Data Protection (CDP) the situation to determine appropriate action to be taken. The auditor shall report the outcome of the action taken to the CDP based on an agreed reporting timeline.

2.6. Audit Evidence, Findings and Conclusions

2.6.1. Evidence

2.6.1.1. Information for the audit objectives, scope and audit criteria shall be collected by means of that are verifiable.

2.6.1.2. Evidence shall be collected by:

- Interviews;
- Documentation review;
- On-site inspection; and
- Testing procedures.

2.6.1.3. The auditor shall corroborate evidence from multiple sources.

2.6.1.4. Only information that is verifiable shall be accepted as audit evidence.

2.6.1.5. Audit evidence leading to audit findings shall be recorded.

2.6.1.6. When evidence is collected based on documentation and records review, the auditor shall use artifacts to ensure that the information collected is complete and accurate, either by collecting directly or by collecting evidence over Information Produced by Entity.

2.6.1.7. The auditor shall obtain sufficient and appropriate evidence that enables to make reasonable audit conclusions.

2.6.1.8. The auditor shall consider the source, nature (written, oral, visual or electronic), authenticity (presence of digital or manual signatures, date/time stamps), and relationships between evidences.

2.6.1.9. The auditor shall consider the independence and qualifications of the source and provider of the audit evidence.

2.6.1.10. When the auditor is not able, to obtain sufficient audit evidence, the auditor shall report to the auditee management, and if necessary, to those charged with auditee governance and to the CDP in accordance with the auditee's procedures.

2.6.2. Record management

2.6.2.1. If during the collection of evidence, the auditor becomes aware of any new or changed circumstances or risks, the auditor shall address these accordingly in the audit plan.

2.6.2.2. The auditor shall collect, use, manage and protect information collected from the auditee in accordance with NIA Policy and Manual, the auditee's classification, labelling and security policies and other applicable laws and regulations. It is the auditee responsibility to protect data before sharing it with the auditor.

2.6.2.3. If the auditor receives from the auditee sensitive information that is not intended to be used in the audit, the auditor shall communicate it to the auditee management such situation and destroy the shared information as per the auditee's procedures.

2.6.2.4. The auditor shall retain audit evidence for the duration of one recertification cycle of two years after the audit closure.

2.6.2.5. The auditor shall provide to the CDP any evidence requested at any time during the audit engagement or during the retention period of two years.

2.6.2.6. The auditor shall destroy all the evidence in a secure manner at the end of the retention period unless it is required by the law to retain them for a long period.

2.6.2.7. Documents pertaining to the audit shall be retained or destroyed by agreement between the participating parties and in accordance with NIA requirements, this Standard, the auditor's audit procedures and agreed upon procedures with the auditee.

2.6.2.8. Unless required by law, the audit team and the person managing the audit shall not disclose information collected during the audit to any other party without the formal approval of the auditee.

2.6.3. Sampling

2.6.3.1. When using sampling methods to draw a conclusion on the entire population, the auditor shall only use statistical sampling.

2.6.3.2. When determining sample size, the auditor shall consider:

- Sampling risk;
- The number or amount errors that would be acceptable; and
- Errors expectation on the sample.

2.6.3.3. The auditor shall verify that the population to be sampled is complete for the objective and scope of the audit.

2.6.3.4. Analysis of the results of non-statistical sampling (haphazard or judgmental) shall be restricted to a description of the results of analyzing the sample.

2.6.3.5. If the projected errors in the population exceeds the tolerable error rate, the auditor shall reassess the sampling risk. If the auditor finds that the risk is unacceptable, the auditor shall consider extending the audit work and increasing the sample size.

2.6.3.6. Where findings are based on sampling, the auditor shall assess if errors detected in the whole population will exceed the tolerable error rates by comparing the projected error on the entire population error to the defined tolerable error rates. For more detail on tolerable error rate, please refer section 2.6.6 Conclusions.

2.6.4. Use of external experts

2.6.4.1. The auditor shall assess the adequacy of using external experts during audit planning. This includes:

- Evaluating the independence and objectivity of the other experts; and
- Assessing their proficiency, competencies, experience, resources and the use of quality control procedure in their work.

2.6.4.2. The auditor engaging external experts shall gain an understanding of the scope of work, approach, timing and use of quality control processes of the external experts work and shall define the level of review necessary to be performed to the expert work in the audit.

2.6.4.3. The auditor shall review the methodology, audit program, work papers and final report of the external experts by assessing that their work was appropriately planned, supervised, documented and reviewed and determine the appropriateness and sufficiency of the audit evidence provided by them, and to which extent the external expert's work can be used and be relied on.

2.6.4.4. The auditor shall determine whether the work of external experts will be relied upon and incorporated directly or referred to separately in the report.

2.6.4.5. The auditor shall also determine the impact of the external experts' findings and conclusions on the audit objectives and assess if any additional work is required to achieve the audit objectives.

2.6.5. Findings

2.6.5.1. The auditor shall consider any errors found and errors that could arise because of control non-compliance to determine and document any finding.

2.6.5.2. Exceptions and errors shall be discussed with the auditee to make sure that the findings are understood, and the supporting evidence are accurate.

2.6.5.3. The auditor shall record all audit findings based on specific requirements of the audit criteria and shall state in a clear manner the exceptions and errors with the associated detailed evidence.

2.6.6. Conclusions

2.6.6.1. The audit team under the audit team leader supervision shall:

- Assess against the audit objectives the audit findings and relevant information collected supporting the findings;
- Build agreed audit conclusions;
- Identify, record and present any follow-up actions to be performed; and
- Review the audit work program to make sure it was appropriate to the audit objectives and identify all necessary modification if it is otherwise.

2.6.6.2. The auditor shall conclude on each control on two different levels:

- Design level; and
- Operating effectiveness level.

2.6.6.3. For each control in the audit criteria, the auditor shall conclude and report on both levels, unless it is deemed impractical. Each level shall be reported as either:

- Compliant; or
- Compliant with opportunities for improvements; or
- Non-compliant.

2.6.6.4. To conclude on the design level, the auditor shall use professional judgment to determine if the design is compliant with the standard (audit criteria) requirements.

2.6.6.5. To conclude on operating effectiveness, the auditor shall use the tolerable error rates defined by the CDP and provided on the final assessment checklists.

2.6.6.6. The auditor shall communicate to the auditee all identified errors or exceptions (including controls on which minimal design flaws or operating deviation or have been identified but still assessed and reported as compliant).

2.6.6.7. If compensating controls have been identified, the auditor shall report controls with a conclusion status of non-compliant or compliant with opportunities of improvement as:

- The same status of compliance when the compensating controls are ineffective; and
- Compliant, when the compensating controls are fully effective and the auditor shall provide explanation and justification of how the compensating controls address the assessed control non-compliance.

2.6.6.8. The auditor shall always conclude as non-compliant, a control with errors or exceptions when they have been overridden by management resulting in fraud or illegal acts.

3. Audit Reporting and Closing

3.1. Audit completion meeting

3.1.1. The audit team leader shall record and hold a formal completion meeting, where attendance shall be recorded, with the auditee's management and those responsible for the functions or processes audited.

3.1.2. The completion meeting shall also include the following elements:

- Presenting that the audit evidence collected can be based on a sample and therefore introducing an element of uncertainty;
- Clearly present and validate all findings;
- Reminder of the method of reporting required by this standard and the timeframe for the final report; and
- Collect information on the timeframe necessary for the auditee to present a corrective action plan for exceptions and errors reported.

3.1.3. The auditor shall communicate to the CDP in 10 working days after it has been held the evidence of the completion meeting with the auditee.

3.2. Subsequent Events

3.2.1. The auditor shall inquire with the auditee's management as to whether they are aware of any subsequent events, through to the date of auditor's report, that would have a material effect on the audit report.

3.2.2. In such situation, the auditor shall present in the audit report, in a clearly distinctive section, a description of the events, the consequences (verified or potential) on the scope, the information assets, the findings and conclusions of the audit.

3.3. Audit Report

3.3.1. The Auditor shall provide a written report for each audit to the auditee and the CDP.

3.3.2. The audit report shall include the following:

- Introduction: In which the auditor shall present:
  - The audit criteria, audit objectives and scope;
  - Clear title that distinguish the report from any other potential reporting that is not governed by this standard;
  - State the recipients of the report as required by this standard and according to the terms of engagement;
  - The scope of the certification audit; and
  - The key persons that have been interviewed or consulted for the purpose of the audit.
- The audit report shall also state whether a follow-up on the previous audit is included or not;
- A summary of the nature, extent and the schedule of audit activities performed and the audit team members responsible for these activities;
- Issues, restrictions or limitations encountered during the audit;
- Findings summary: Overall compliance status;
- Detailed audit findings:
  - Audit findings, evidence or evidence reference in the audit work papers and conclusions associated with all compliance controls;
  - The impacted information assets and their classification; and
  - Management response for each finding.
- Generic audit recommendations given for findings reported; and
- Date of the audit report.

3.3.3. An authorized person, who could legally engage the responsibility of the auditor, shall sign the audit report.

3.3.4. The report constitutes the only and final deliverable that the auditor shall communicate to the auditee.

3.3.5. Along the audit report, the auditor shall communicate to the CDP the final assessment-reporting checklist related to the certification scheme provided by the CDP.

3.4. Closing

3.4.1. The audit is closed when the CDP make a certification decision on the scope based on the audit report and the auditee corrective action plan. The auditor could be asked by the CDP to reopen the audit to perform additional audit work. In such situation, the auditor shall perform the requested work and report to the CDP the findings within the defined timeframe.

3.4.2. The action plan shall include the following information:

- Link to audit findings;
- Management approval of the action plan;
- Information asset impacted and its classification;
- The criticality, priority and complexity of the action;
- Type of the correction; and
- Duration and deadline of the action.

3.5. Surveillance audit

3.5.1. For certification schemes that are subject to maintenance, the auditor shall make follow-up activities to ensure the adequacy, effectiveness and timeliness of actions taken by management to correct errors and exceptions that have been detected for a scope certified by the CDP.

3.5.2. The auditor shall collect and review the corrective action plan to address the detected exceptions and errors.

3.5.3. Before the starting the follow-up audit activities, the auditor shall collect an implementation report from the auditee. This report shows the implementation status of the communicated corrective action plan.

3.5.4. The auditor shall communicate to the CDP the implementation report before starting the follow-up audit activities.

3.5.5. If, during a surveillance audit engagement, the auditor finds that the corrective actions reported as 'implemented' had in fact not been implemented, the auditor shall communicate this to the appropriate level of management and those charged with governance.

3.5.6. The auditor shall inform the CDP in the surveillance audit report of such situation, even if the auditee implemented the corrective actions before the auditor surveillance report issuing.

3.5.7. Planning, performing and reporting a surveillance audit shall be done following the requirements defined in this standard for a certification audit.

Chapter 2: Audit Guidelines

1. Audit Engagement Acceptance Due Diligence

The auditor could use an acceptance checklist to document acceptance due diligence. Such a checklist can treat of following:

- Client management integrity;
- Competency and resources assessment to perform the audit; and
- Conflict of interest checking.

For more clarity, the auditor should include the following in the audit engagement document:

- The obligations and responsibilities of the accredited auditor;
- The obligations and responsibilities of the auditee;
- Confidentiality requirements or reference to the NDA;
- Liability of the engagement; and
- The terms of agreement (specific agreements decided between both parties that are not part of the audit process).

2. Planning and Conducting Audit work

2.1. Audit Planning

2.1.1. Approach to Planning

In planning, materiality should only be used to determine the nature, schedule and extent of audit activities for each audit criteria defined in the scope or in the compliance scheme standards.

The assessment of what is material is a matter of professional judgement by considering the effect and/or the potential effect on the scope.

The auditor should establish a materiality to determine the audit work by considering:

- Confidentiality, availability and integrity of information assets;
- Degree of criticality and risk to business and data impact on the scope; and
- Compliance with laws and regulations.

The materiality assessment should include:

- The nature of information collected, processed and stored;
- IT Infrastructure;

- Architecture design;
- Software and applications;
- Information Security operations procedures;
- Production, development and test environments; and
- Information security and privacy laws and regulations.

2.1.2. Using Audit Risk in planning

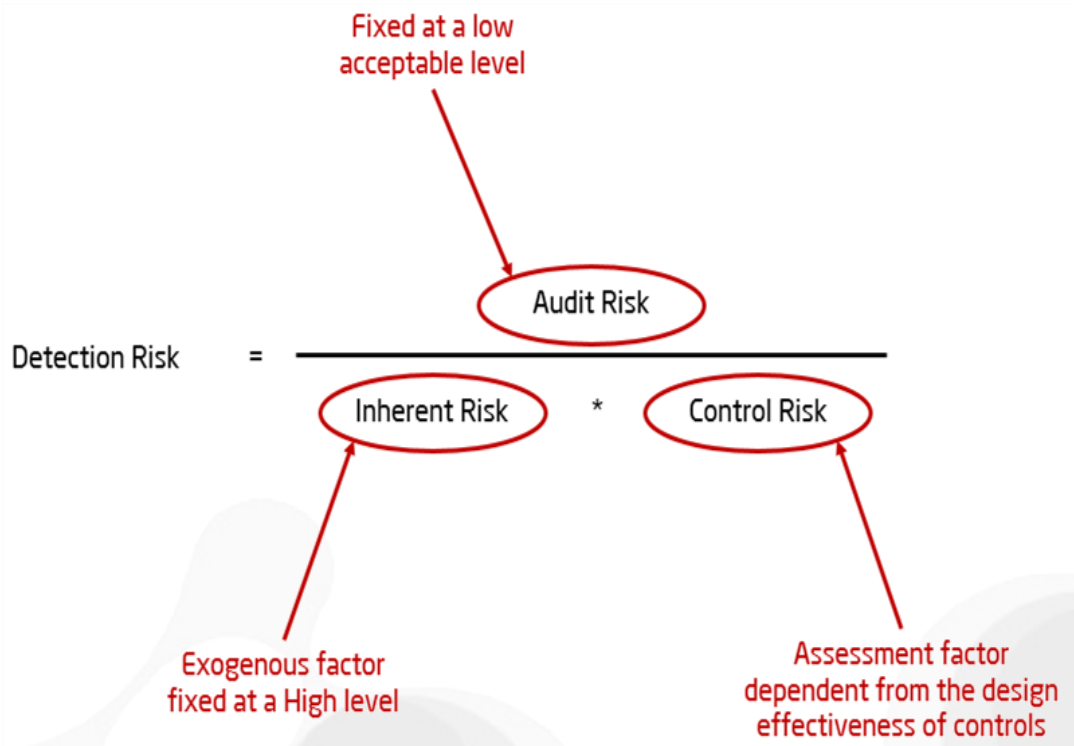
The audit risk refers to the risk of reaching an incorrect conclusion based upon audit findings.

The three components of audit risk are:

- Inherent risk (Exogenous factor to the auditor); Inherent risk is the fact that an audit area is susceptible to material errors (leading to non-compliance) when not taking into consideration auditee's existing controls;
- Control risk (Assessment factor by the auditor); Control risk is the risk that a material errors (leading to non-compliance) could occur and will not be prevented, detected and corrected at the right time by auditee's existing controls; and
- Detection risk (Endogenous factor to the auditor); is the risk that auditors' testing procedures will not detect an exceptions or errors.

The higher the assessment of inherent and control risk, the lower should be the detection risk and the more audit evidence should be obtained from the performance of tests on operating effectiveness.

The audit risk model is best understood through a mathematical formula. However, this formula is just presented for illustrative purpose and does not reflect the accurate relation between the audit risk components. The output of the formula is the detection risk, as it is the only factor that the auditor controls (related to his work).



A relationship exists between audit risk and materiality. This relationship is inverse. The higher the audit risk, the lower the materiality should be set. The lower the audit risk, the higher the materiality can be set. It means for higher audit risk (but still at acceptable level), the auditor needs to extent his audit work procedures on less important information assets and processes.

2.1.3. Documenting the Audit Planning

The method and documentation used for planning may differ from one auditor to another. Since planning is affected by changes and audit work findings, it is expected from the auditor to have various version of the audit planning evidencing the changes occurred to the audit approach and plan during the whole audit.

2.1.4. Audit Timeline

The auditor should consider the following to determine audit timeline:

- The applicable controls of the compliance criteria;
- Size, context and complexity of the auditee;
- Laws and regulatory requirements;
- In-house and outsourced activities within the scope;

- Previous audit findings; and
- Geographical position of the audit sites.

2.1.5. Audit Teams Composition and Assignment

To achieve audit objectives, the auditor may need technical experts, translators, and interpreters who will work under the auditor's direction. Where translators or interpreters are used, they should be selected in a manner, so they do not influence the audit.

2.1.6. Scope and Documented Information Review

Outside of the documents submitted during the scope, the auditor should review any other document necessary to understand the entity and its environment, the scope and the implementation of the compliance criteria including but not limited to management system documents and records, enterprise architecture as well as previous audit reports.

2.2. Audit Evidence, Findings and Conclusions

2.2.1. Evidence

During evidence gathering, the auditor should consider:

- The time and cost needed to collect and exploit the evidence compared to the sufficiency of already collected evidence in reducing audit risk;
- Importance of the information asset being evaluated; and
- The future availability of evidence that may not be exploitable after a certain period.

Procedures used to gather evidence vary based on the information system being audited, the timing, scope and objectives of the audit as well as the auditor judgement.

Evidence can be collected using manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both.

The following methods should be considered to collect audit evidence:

- Inquiry and confirmation of information from the relevant persons that manage and/or own the assets and processes being assessed;
- Observation of procedure or process being performed or physical items;
- Examination of internal or external documents, tapes and records;
- Analytical procedures on which the auditor examines relationships within the data or between the data and other relevant information (fluctuations, trends and inconsistent relationships);

- Manual or CAAT recalculation/computation of arithmetical and mathematical accuracy of documents or records;
- Re-performance of tasks that were originally executed by the information system or by a person to compare the results; and
- Other generally accepted methods as for example, social engineering, act as a mystery guest or conduct ethical intrusion testing.

2.2.2. Sampling

Audit generally implies that the auditor does not examine all the information available as it may be impractical (needs too much time to audit all information) and conclusions are made using audit sampling.

The auditor should select an audit sample, perform audit testing and evaluate sample results to obtain enough and appropriate evidence to form a conclusion.

In audit sampling design, it is important to consider:

- Purpose of the sample;
- Sampling unit;
- Population;
- Sampling risk and sample size;
- Tolerable error rates defined by the CDP;
- Underlying expected distribution (chi-squared, binomial, normal, exponential…);
- Subpopulations or subgroups; and
- Outliers and unusual items.

Sampling risk is the possibility that the auditor's conclusion based on a sample would be different from the conclusion that the auditor would have made if the entire population were tested by to the same audit procedure.

This is where the auditor assess that an error or exception is unlikely to be present when, in fact, the testing of the entire population would have led to an error or exception detection. This is either because of the sample is not representative of the population or because the extrapolation method used was not appropriate.

Based on the control risk and inherent risk, the auditor will choose the sample size based on errors expectation to be present in the population. In that case, a larger sample should be selected compared to when no error is expected. This will enable the auditor to conclude if the actual errors in the population would be inferior to the defined tolerable error rates by the CDP.

Smaller sample sizes are justified when the population is expected to be error free.

To estimate the expected error in a population, the auditor should consider:

- Inherent risk and control risk assessments;
- Error levels identified in previous audits; and
- Changes in the auditee procedures or individuals performing the control being tested.

Sampling methods can be divided into two sampling categories:

- Statistical sampling methods:
  - Simple random sampling where all items in the population have an equal chance of selection;
  - Systematic sampling that selects items using a fixed interval between selections and where the first selection has a random start within the interval range; and
  - Stratified random sampling where items are grouped together in subgroups and in each subgroup have a known, non-zero chance of selection based on random or systematic sampling use.
- Non-statistical sampling methods:
  - Haphazard sampling where the auditor selects the sample without following a predefined path and avoiding any conscious bias or predictability; and
  - Judgmental sampling where the auditor use judgment to target certain items in the population.

3. Audit Reporting and Closing

3.1. Completion meeting

The purpose of the completion meeting is to present and validate with the auditee audit findings and conclusions.

The auditee will be given the opportunity for asking questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client should be discussed and resolved where possible.

3.2. Subsequent Events

Events sometimes occur, after the scope being tested but before the date of the auditor's report, which have a material effect on the scope and therefore require adjustment or disclosure in the audit report. These occurrences are referred to as subsequent events.

The auditor should consider information about subsequent events that comes to their attention during the audit. However, the auditor has no responsibility to detect subsequent events.

3.3. Audit report

Each finding in the audit report should be presented with the audit evidence (screen shots, table of exceptions detected, source documents used…) or if it is impractical state the evidence reference in the audit work papers of the auditor.

Recommendation should be preceded by a presentation of the finding and followed by the auditee's response to the recommendation. If the auditee response is too lengthy to be included in the body of the report, a summary of the response should be included in the report with the complete response attached to it (i.e., Appendices).

It is recommended to also mention the dates and places when and where the audit work was performed, if not yet mentioned with the summary of the work performed.

Appendix A (normative): Audit Ethics / Code of Conduct

This Code of Conduct has been prepared to outline the broad principles of legal and ethical conduct embraced by the Compliance and Data Protection (CDP) department. It is not a complete list of legal or ethical questions that may be faced during accreditation, and, therefore, this shall be used together with professional and sound judgment.

1. Fundamental Principles

1.1. Integrity

1.1.1. The auditor shall be straightforward and honest in professional relationships. Integrity also implies fair dealing and truthfulness.

1.1.2. The auditor shall not be associated with reports, returns, communications or other information where they believe that the information:

- Contains a materially false or misleading statement;
- Contains statements or information furnished recklessly; or
- Omits or obscures information required to be included where such omission or obscurity would be misleading.

1.2. Objectivity

1.2.1. The auditor shall not compromise professional or business judgment because of bias, conflict of interest or the undue influence of others. The auditor may be exposed to situations that may impair objectivity. It is impracticable to define and prescribe all such situations.

1.2.2. Relationships that bias or unduly influence the professional judgment of the auditor shall be avoided.

1.3. Professional Competence and Due Care

1.3.1. The auditor shall maintain professional knowledge and skill at the level required to ensure that clients or employers receive competent professional service.

1.3.2. The auditor shall act diligently in accordance with applicable CDP's technical and professional standards.

1.3.3. Competent professional service requires the exercise of sound judgment in applying professional knowledge and skill in the performance of such service. The auditor shall maintain

professional competence, continuous awareness and an understanding of relevant technical professional and business developments.

1.4. Confidentiality

1.4.1. The auditor shall refrain from disclosing outside the accredited service provider confidential information acquired during or for purpose of certification audits related to the NISCF without proper and specific authority or unless there is a legal or professional right or duty to disclose.

1.4.2. The auditor shall refrain from using confidential information acquired during or for purpose of certification audits related to the NISCF for personal advantage or the advantage of third parties.

1.4.3. The auditor shall maintain confidentiality of information within accredited service provider and subcontracting organizations.

1.4.4. The auditor shall take all reasonable steps to ensure that staff under its control and persons from whom advice and assistance is obtained respect the auditor's duty of confidentiality.

1.4.5. The need to comply with the principle of confidentiality continues even after the end of relationships between an auditor and the auditee.

1.5. Professional Behavior

1.5.1. The auditor shall comply with relevant laws and regulations and avoid any action that may bring discredit to the accredited service provider, the auditee or the CDP.

1.5.2. In marketing and promoting itself, the auditor shall not bring the CDP's audit accreditation service into disrepute. The auditor should be honest and truthful and should not:

- Make exaggerated claims for the services they can offer, the qualifications they possess, or experience they have gained; or
- Make disparaging references or unsubstantiated comparisons to the work of others.

2. Conceptual framework

2.1. The CDP's fundamental principles of audit ethics and code of conducts for auditors are built upon the independence pillar. As the work of auditor is used for issuing certification of compliance, which is a public interest matter, the audit team member, the auditor and even the firm network it potentially related shall be independent of the auditee.

2.1.1. Independence of Mind

2.1.1.1. The auditor shall have a state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, allowing an individual to act with integrity, and exercise objectivity and professional skepticism.

2.1.2. Independence in Appearance

2.1.2.1. The auditor shall avoid of facts and circumstances that are so significant that a reasonable and informed third party, having knowledge of all relevant information, including safeguards applied, would reasonably conclude an auditor's, or a member of the audit team's, integrity, objectivity or professional skepticism had been compromised.

2.1.3. Professional independence

2.1.3.1. Many different circumstances or combinations of circumstances may be relevant in assessing threats to independence. It is impossible to define every situation that creates a threat to independence and to specify the appropriate action. Therefore, the auditor shall identify, evaluate and address threats to independence.

2.1.3.2. The auditor shall apply the conceptual framework approach to:

- Identify threats to independence;
- Evaluate the significance of the threats identified; and
- Apply safeguards, when necessary, to eliminate the threats or reduce them to acceptable levels.

2.1.3.3. When the auditor determines that appropriate safeguards are not available or cannot be applied to eliminate threats or reduce threats to an acceptable level, the auditor shall eliminate the circumstance or relationship creating the threats or decline or terminate the audit engagement.

2.1.4. Threats and Safeguards

2.1.4.1. The auditor shall avoid or manage the following circumstance or relationship that may create threat to its independence or the audit team members:

- Self-interest: The threat that a financial or other interest will influence the auditor judgement or behavior inappropriately;
- Self-review: The threat that the auditor will not appropriately evaluate the results of a previous judgement made or service performed by them or by another individual within the audit function, on which the auditor will rely when forming a judgement as part of performing the current engagement;

- Advocacy: The threat that the auditor will promote an auditee's position to the point that professional objectivity is compromised;
- Familiarity: The threat that due to a long or close relationship with the auditee, the auditor will be too sympathetic to the interests of the auditee or will be too accepting of the auditee's work, views or arguments;
- Intimidation: The threat that the auditor will be deterred from acting with integrity and objectivity because of actual or perceived pressures, including attempts to exercise undue influence over the auditor;
- Bias: The threat that the auditor will, as a result of political, ideological, social, psychological or other convictions, take a position that is not objective; and
- Management participation: The threat that results from the auditor taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit or assurance engagement.

2.1.4.2. When any conflict or impairment between the auditor and the auditee is detected, the auditor shall take all the safeguards necessary to minimize the potential impact.

2.1.4.3. The auditor also shall immediately inform the CDP of the conflict and the safeguards it has put in place.

2.1.4.4. If a third party informs the CDP of a conflict or impairment of an auditor or one of its audit team members regarding an engagement, the auditor shall justify to the CDP, which will open an investigation, how the preventive controls implemented by the auditor did not detect the conflict.

2.1.4.5. Under the conceptual framework, the auditor shall apply safeguards that address the facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat.

2.1.4.6. Safeguards that shall be considered by the auditor include but are not limited to:

- Suspension of the engagement;
- Exclude from the engagement the conflicted person;
- Make sure that the conflicted person will not interact with the subject of conflict if it is deemed to be kept in the engagement;
- Make sure that the work performed by the conflicted auditor is thoroughly reviewed or re-performed by an individual who was not a member of the audit team; and
- Confiscate the audit tools of the conflicted person.

Appendix B (normative): National Information Security Compliance (NISCF) Audit Areas

1. The National Information Assurance (NIA) Policy

1.1. General approach

1.1.1. The certification audit covers a defined past timeframe called audit period. For NIA certification audits, the audit period shall cover the duration from the NIA compliance implementation date for the scope (defined in the compliance roadmap) until the starting date of the audit.

1.1.2. However, for practical reason this period shall not exceed 12 months.

1.1.3. In addition, the timeframe between the implementation of NIA and the starting date of the certification audit for a defined scope may be not long enough to produce sufficient and appropriate evidence (tracks, occurrence, logs, requests, changes...) to enable the auditor to have a true and fair representation of the operating effectiveness of the implemented controls. While this depends purely on the frequency of a control being used to protect, detect or correct information security related events, the audit period shall not be shorter than 3 months.

1.2. Scope and Documented Information Review

1.2.1. The National Information Assurance (NIA) Certification Audit starts after the validation of the scope by the CDP. As part of the preliminary work, the auditor shall review the NIA scope documentation and assess the relevancy of the approved certification at the time of the beginning of the audit. At this stage, the auditor shall not question the scope (the controls applicable defined in the scope via the Statement of Applicability).

1.2.2. The auditor shall ensure that the auditee is applying all necessary controls required by the NIA Manual following the NIA Policy. The auditor shall check the completeness of the controls regarding the rules of selection defined with the NIA Policy and Manual and verify that any deviation from that (Non-applicable baselines controls or the absence of additional controls based on the security classification) is justified.

1.2.3. The auditor shall collect and analyze the following documents to assist in understanding the scope and preparing for an effective audit:

- Scope document;
- Compliance Roadmap;
- Business Impact Analysis (BIA);
- Information Asset Classification Register;
- Statement of Applicability (SoA);
- Information Security Policy;
- Enterprise Architecture;
- Information security Policy, Manuals, Procedure and Process documents;
- Risk management documentation;
- Previous audit reports (internal & external).

2. Software Security and Quality Assurance (SSQA)

2.1. General approach

2.1.1. The auditor shall plan, perform and report the audit of each completed gate of system development and giving input that allows corrections to be made before the next phase of the development.

2.2. Understanding the auditee and its environment

2.2.1. The auditor shall gain an understanding of the E-Service, assess risk, and take into consideration of controls of SSQA standard(s). While planning the review of the System Development Lifecycle (SDL) of E-Service, the auditor shall consider:

- The technology, complexity, objectives and intended usage of the E-Service;
- Skill and experience of the project team;
- The SSQA standard level chosen (Standard 1, 2 or 3);
- The formal SDL methodology (Agile or Waterfall) and customized process design adopted if any;
- Risks that are likely to affect the SDL Process;
- Any concerns or issues perceived by the client;
- The current SSQA Gate (Design, Build or Release);
- Any prior review of the earlier SSQA stages of the E-Service;
- Any prior SDL reviews of similar E-Service;
- Any other risk assessments/reviews by the auditors that have a bearing on the proposed review; and
- The skill and experience level of the auditors available and the possibility of getting competent external assistance where necessary.

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

End of Document