الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Audit Sampling

## [NCSA-NISCF-ACCR-AUD-NIA-SOP-SAMP]

### Standard Operating Procedure

National Cyber Security Agency (NCSA)

October 2024

V1.0

C0 – Public / PS1 – Non-Personal Data (Non-PD)

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

## Document Control

| Document Details | |
|---|---|
| **Document ID** | NCSA-NISCF-ACCR-AUD-NIA-SOP-SAMP |
| **Version** | V1.0 |
| **Classification & Type** | C0 – Public / PS1 – Non-Personal Data (Non-PD) |

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this Standard Operating Procedure, titled "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Audit Sampling – Standard Operating Procedure" - V1.0 - C0 – Public / PS1 – Non-Personal Data (Non-PD) , in order to provide the required steps and actions to be performed by the Accredited Audit Service Providers for the sampling during NIA Certification Audits, as part of National Information Security Compliance Framework (NISCF) Certification Services of the National Cyber Security Agency (NCSA).

NCSA 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 NCSA as the source and owner of the "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Audit Sampling – Standard Operating Procedure".

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

The authorization from NCSA 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.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# LEGAL MANDATE(S)

Based on Emiri Decree No 1 of year 2021, National Cyber Security Agency (NCSA) – National Cyber Governance and Cyber Assurance Affairs (NCGAA) is the entity responsible for issuing certificates for Technology and Information Security service providers and Certificates of Compliance with National Information Security standards and policies.

This document 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.

# Table of Contents

# Table of Tables



# Table of Figures



# Table of Equations

# 1. 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.

NCSA offers Audit Service Accreditation for Service Providers that are willing to participate in the delivery of audits related to NISCF's Services.

National Information Assurance (NIA) Certification is one of the NISCF's services that requires the reliance on Audit Service Providers.

Accredited Audit Service Providers shall comply with the steps and rules defined in this document when performing NIA Certification Audit. Conformance to this procedure is considered in the maintenance of the Audit Service Providers Accreditation.

# 2. Purpose and Scope

## 2.1. Purpose

This Standard Operating Procedure has been developed with the objective to instruct the Accredited Audit Service Providers for National Information Assurance (NIA) on the mandatory steps and method of sampling.

This Standard Operating Procedure shall be read in conjunction with the NISCF Audit Standard (NCSA-NISCF-AUD-STND) and NIA Audit Accreditation Standard (NCSA-NISCF-ACCR-AUD-NIA-STND).

## 2.2. Scope

This Standard Operating Procedure applies to all National Information Assurance (NIA) Certification Audits.

# 3. Terms and Definitions

The terminologies used in this document are consistent with the definitions provided in the NCSA-NISCF-ACCR-GTXD (General Taxonomy Document for National Accreditation - Public), NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public), NCSA-NISCF-ACCR-NIA-AUD-STND (NIA Audit Accreditation Standard) and the NCSA-NISCF-AUD-STND (NISCF Audit Standard - Public).

For the purpose of this document, the following verbs indicate:

| | |
|---|---|
| ***Appropriate*** | Suitable for or to. |
| ***Can*** | A modal verb that entail a possibility or capacity. |
| ***May*** | A modal verb that entail a permission. |
| ***Shall*** | A model verb that entail a requirement. |
| ***Should*** | A modal verb that entail a recommendation. |

# 4. Standard Operating Procedure

## 4.1. Sampling principles

The NIA Audit sampling approach is designed to cover the entirety of the scope of audit with a minimal number of samples that allow to reach the reasonable assurance needed.

These principles are:

- Layered sampling: The sampling approach detailed in this document is applied across the different layers of the scope. The different layers defined in this document are based on TOGAF © four primary architecture domains:

  i. Business Architecture: A layer inclosing the business processes composing the scope of the audit;

  ii. Data Architecture: A layer inclosing the information asset(s)[1] supporting the defined business processes;

  iii. Application Architecture: A layer inclosing the applications[2] used to interact with the information assets; and

  iv. Technology Architecture: A layer inclosing all the technological components.

- Full scope coverage (based on the audit objective): The sampling approach detailed in this document is designed to ensure that adequate sampling will allow to audit the entirety of the scope. However, not all the scope will be audited against all the audit criteria;

- Maximizing coverage: The sampling approach detailed in this document, calling for the Accredited Service Provider for NIA Audit to rely on professional judgment, aims at maximizing the coverage of information assets to be audited;

[1] As defined in the NIA Certification Scoping Standard, an information asset is "A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and utilized effectively. Information Assets can be processed in a physical (i.e., paper), digital (i.e., IT / OT) or cognitive (i.e., human knowledge) format." Information assets are not the containers (i.e., servers, routers, firewalls…) in which the information is processed.

[2] Applications are used as interface between the data and the user (which can be a human or machine).

- Materiality and risk of material Non-Conformities (NC) consideration: The sampling approach detailed in this document is based on the materiality concept and risk of material Non-Conformities (NC)[3]; and
- Rotation among audits: The sampling approach detailed in this document calls for the rotation of the sampling performed at all architectural layers from audit engagement to another for the same scope[4].

The approach described in this document is a multistage sampling.

[3] For more information regarding the risk of material Non-Conformities, please refer to the Standard Operating Procedure on Audit Risk (NCSA-NISCF-ACCR-AUD-NIA-SOP-AR).
[4] For more information about rotation of samples between audits, please refer to the Standard Operating Procedure on Audit Work Program (NCSA-NISCF-ACCR-AUD-NIA-SOP-AWP).

## 4.2. Multistage Layered Sampling

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| SOP-SAMP-LS-01 | The Accredited Service Provider for NIA Audit shall use "adequate sampling" during NIA Audit in order to reach reasonable assurance of the conformity of the scope to NIA requirements (i.e., audit criteria) in a practical and economically feasible manner.<br><br>The Accredited Service Provider for NIA Audit shall sample the scope parts that will be audited against specific audit criteria.<br><br>The Accredited Service Provider for NIA Audit shall cover all the scope through sampling during initial Certification, scope expansion or Re-Certification audits.<br><br>In order to achieve adequate sampling, the Accredited Service Provider for NIA Audit shall determine which parts of the scope will be audited for each NIA domain.<br><br>As an example, please refer to **Figure 1: Adequate Sampling Example** that provides an example of adequate sampling for 7 of NIA domains covering the entirety of a scope composed by 3 business processes.<br><br>Generally, the number of business processes in a given scope does not equal the number of NIA domains.<br><br>If the number of NIA domains exceeds the number of business processes in the scope, the Accredited Service Provider for NIA | • Statement of Applicability (SoA)<br>• Information Assets Classification Register (IACR)<br>• Enterprise Architecture / OBASHI model<br>• Understanding of the audit environment | • Justified business architecture layer sample, documented in the working papers for recording sampling shared during the Accreditation |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | Audit shall use materiality (relative importance of the business processes) and professional judgment to audit the material business processes against a larger number of NIA domains.<br><br>In the example provided, business processes 1 and 2 are material which lead to their conformity being audited against 3 NIA domains each, while process 3 is audited against only 1 NIA domain.<br><br>If the number of NIA domains are equal or inferior to the number of business processes in the scope, the Accredited Service Provider for NIA Audit shall distribute the NIA domains evenly among the business processes in the scope. In this case, the allocation is based on professional judgement of the Accredited Service Provider for NIA Audit.<br><br>For certain NIA domains, the audit criteria might not be easily mapped to a business process in the scope. For example, the Governance Structure domain audit criteria are not linked directly to a business process or the underlying information assets supporting it. In such a case, the Accredited Service Provider for NIA Audit should audit the conformity to the audit criteria considering the entire scope.<br><br>The Accredited Service Provider for NIA Audit shall use professional judgment and rationale in determining the NIA domains for which it is not practical to link the business processes in the scope based | | |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | on the available documentation provided by the NIA Certification Subject (Auditee).<br><br>Similarly, other NIA domains can be more easily mapped to other items other than a business process. For example, Security Awareness domain audit criteria are easier to be audited for a business department or per Security Awareness session performed (as the underlying subject(s) matter would generally be the NIA Certification Subject (Auditee)'s staff and third-party resources) instead of auditing at a business process level. Mapping the Security Awareness domain audit criteria to a business process is achievable, however, this exercise might be time consuming and with little value for the NIA Certification Subject (Auditee).<br><br>Therefore, in all cases and before sampling and allocating the NIA domains to the business processes to be audited for these domains, the Accredited Service Provider for NIA Audit shall assess feasibility of the mapping of the audit criteria to business processes and determine if auditing an NIA domain at the scope or department level (which would cover by default more than one business process) is more viable option.<br><br>The Accredited Service Provider for NIA Audit shall document the rationale behind the selection of which part of the scope is to be audited against which NIA domain, based on materiality, feasibility | | |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | and adequacy of the supporting information assets to the NIA domain objective. | | |
| **SOP-SAMP-LS-02** | Once the Accredited Service Provider for NIA Audit selected the NIA domains that will be audited for each business process, it shall sample for each business process the information assets that will be audited.<br><br>The Accredited Service Provider for NIA Audit shall use materiality and professional judgement in determining the information assets sampled.<br><br>As generally information assets are processed through applications and using Information and Communication Technology (ICT) or Operation Technology (OT), the Accredited Service Provider for NIA Audit shall perform the sampling at the application and technology architectures that maximizes the coverage of the information assets (in application of the Maximizing coverage principle).<br><br>However, as not all information assets are processed through Information and Communication Technology (ICT) or Operation Technology (OT), the Accredited Service Provider for NIA Audit shall sample the information assets to be audited in paper-based format without considering the application or technology architectures. | • Statement of Applicability (SoA)<br>• Information Assets Classification Register (IACR)<br>• Enterprise Architecture / OBASHI model<br>• Understanding of the audit environment<br>• Output of SOP-SAMP-LS-01 | • Justified data architecture layer sample, documented in the working papers for recording sampling shared during the Accreditation |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | When information assets are processed in a paper-based format, the Accredited Service Provider for NIA Audit shall sample at least 5% (without exceeding 25 samples++) of the information assets supporting a given business process. | | |
| **SOP-SAMP-LS-03** | The Accredited Service Provider for NIA Audit shall sample one (1) application and one (1) technology component for each business process selected.<br>As explained in section step SOP-SAMP-LS-03, the selected application and technological component shall be based on the maximizing coverage principle; i.e., the Accredited Service Provider for NIA Audit shall select the application and technological component that process the maximum number of information assets supporting a given business process.<br>The Accredited Service Provider for NIA Audit shall consider the NIA domain and audit criteria objectives to be tested when selecting the technology component. | • Statement of Applicability (SoA)<br>• Information Assets Classification Register (IACR)<br>• Enterprise Architecture / OBASHI model<br>• Understanding of the audit environment<br>• Output of SOP-SAMP-LS-01 and SOP-SAMP-LS-02 | • Justified application and technology architecture layer sample, documented in the working papers for recording sampling shared during the Accreditation |
| **SOP-SAMP-LS-04** | When auditing the scope for conformity against an audit criterion, regardless of the sample being determined based on the business process – data – application – technology architectures layering or | • Statement of Applicability (SoA) | • Justified underlaying subject(s) |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | not, the Accredited Service Provider for NIA Audit shall determine clearly the underlying subject(s) matter (please refer to the NISCF Audit Standard (NCSA-NISCF-AUD-STND) for the definition of underlying subject(s) matter) to be audited for each audit criteria.<br><br>Based on the layered sampling decision made, the Accredited Service Provider for NIA Audit shall identify the population of underlying subject(s) matter) to be audited for each audit criteria.<br><br>The examples provided in **6.2.2. Layered Sampling Examples**, the layered sampling and the relation with the underlying subject(s) matter. These are only illustrative examples and shall not be used without exercising professional judgment from the Accredited Service Provider for NIA Audit.<br><br>The Accredited Service Provider for NIA Audit shall document in detail the whole approach and selection process for the layered sampling and identification the underlying subject(s) matter, as per the working papers for recording the sampling shared during the Accreditation. | • Information Assets Classification Register (IACR)<br>• Enterprise Architecture / OBASHI model<br>• Understanding of the audit environment<br>• Output of SOP-SAMP-LS-01, SOP-SAMP-LS-02 and SOP-SAMP-LS-03 | matter identified, documented in the working papers for recording sampling shared during the Accreditation |

*Table 1: Multistage Layered Sampling Standard Operating Procedure*

## 4.3. Operating Effectiveness (OE) Audit Sample Size

National Information Assurance (NIA) Certification audit requires the Accredited Service Provider for NIA Audit to use sampling as it is impractical to audit every underlying subject(s) matter for all audit criteria. National Information Assurance (NIA) requirements are suited for compliance testing or test of controls, which is an audit procedure designed to evaluate the Operating Effectiveness (OE) of controls in preventing, or detecting and correcting, material non-conformities (NC) to NIA requirements.

Compliance testing requires auditing the conformity of attributes (characteristics) that are defined by the NIA requirements. Attribute sampling method deals with the presence or absence of the attribute, and provides conclusions that are expressed in rates of incidence. This methodology is a statistical sampling approach using fixed sample size attribute or frequency-estimating sampling method based on Binomial distribution.

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| **SOP-SAMP-SS-01** | To determine the sample size for Operating Effectiveness (OE), the Accredited Service Provider for NIA Audit shall use **Table 11: Sample Sizes Table** and **Equation 1: Sample Size Formula for Medium Risk of Material non-Conformities (NC)** or **Equation 2: Sample Size Formula for High Risk of Material non-Conformities (NC)**. | • Risk of Material Non-Conformities<br>• Output of Output of SOP-SAMP-LS-01, SOP-SAMP-LS-02 and SOP-SAMP-LS-03 | • Justified sample sizes, documented in the working papers for recording sampling shared during the Accreditation |

*Table 2: Sample Size Standard Operating Procedure*

## 4.4. Samples Selection Method

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| SOP-SAMP-SSM-01 | An audit criterion in NIA can have one or multiple attributes to be audited.<br><br>Example of one attribute: CM 5. All associated system documentation is updated to reflect the change. The attribute testing: Is System documentation is updated to reflect change (Yes / No)?<br><br>Example of three attributes: CM 3. Document and approve all proposed changes through the relevant Change Management Committee?<br>• Attribute testing 1: Are all proposed changed documented (Yes / No)?<br>• Attribute testing 2: Are all proposed changed approved (Yes / No)?<br>• Attribute testing 3: Are all approvals provided by the relevant Change Management Committee (Yes / No)?<br><br>When performing an audit of an audit criterion for the sampled underlaying subject(s) matter, the Accredited Service Provider for NIA Audit shall audit all the attributes in the audit criterion. | • Statement of Applicability (SoA) | • Identified attributes to be audited per audit criterion |
| SOP-SAMP-SSM-02 | When selecting a sample from a population of underlying subject(s) matter, the Accredited Service Provider for NIA Audit | • Output of SOP-SAMP-SSM-01 | • Justified samples |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | shall ensure that the attribute that need to be verified in the sample is applied homogeneously across the population.<br><br>Generally, attributes coming from the same audit criterion should be homogeneous.<br><br>The Accredited Service Provider for NIA Audit shall determine the homogeneity of the population based on the Design Effectiveness (DE) audit.<br><br>By confirming population homogeneity, the Accredited Service Provider for NIA Audit should be able to select the same sample to test multiple attributes, reducing therefore the number sample requests.<br><br>When considering the homogeneity of a population to select a sample, the Accredited Service Provider for NIA Audit shall consider if the activities / processes / controls to be tested are performed the same way across:<br>• Departments;<br>• Systems; and<br>• Locations.<br><br>Also, within the audit criteria, the information security activities applied can follow multiple practices within the NIA Certification Subject (Auditee) that make them non-humongous. As an | | grouping for underlying subject(s) matter, documented in the working papers for recording sampling shared during the Accreditation |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | example, for audit criteria "AM 3 Access rights of a user or entity to create, read, update, delete or transmit an Organization's information assets SHALL be based on a matrix (hierarchical) model of rights defined by business rules established by the owners of that information.", the Accredited Service Provider for NIA Audit selected one (1) application "A4" and the supporting Operating System "OS4" of the application as one (1) technology component to be audited.<br><br>Fifteen (15) access have been granted to the application "A4" and two (2) access have been granted to the supporting Operating System "OS4" during the audit period. Assuming a risk of material Non-Conformities (NC) assessed as low, if the process to grant access to the application "A4" is different from the process of granting access to the supporting Operating System "OS4", homogeneity cannot be considered and the Accredited Service Provider for NIA Audit shall sample two (2) access granted for "A4" and one (1) access granted for "OS4" instead of just two (2) for both if the access granting process was homogeneous. | | |
| **SOP-SAMP-SSM-03** | To select a sample, the Accredited Service Provider for NIA Audit shall use one of the below techniques:<br><br>• Simple Random Sampling: The items in the population have equal chance to be included in the sample without any specific selection order; | • Output of SOP-SAMP-SS-01, SOP-SAMP-SSM-01 and SOP-SAMP-SSM-02 | • Justified selected samples of underlying subject(s) matter for |

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| | • Systematic Sampling: The first sampled item will be selected based on a random number ranging between one (1) and a number (k) equivalent to the population divided by the sample size. After the selection of the first item in the sample, the other items in the sample will be selected at a fixed interval equal to the number (k); or<br>• Stratified Sampling: The items in the population are classified into non-overlapping homogeneous sub-groups (Strata), then select a sample from each Strata. The number of items sampled in each Strata is not necessarily equal, however, the total of the items sampled from all Strata shall be equivalent to the determined sample size. | | each audit criterion, documented in the working papers for recording sampling shared during the Accreditation |

*Table 3: Samples Selection Standard Operating Procedure*

## 4.5. Extrapolation

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| SOP-SAMP-EXR-01 | Extrapolation of the results of the audit of a sample to the entire population is not a linear process.<br><br>The Accredited Service Provider for NIA Audit shall use **Table 12: Extrapolation Table** and **Equation 3: Extrapolation Formula** to perform the extrapolation of the results of a sample on the entire population.<br><br>For certain situations and based on the small sample size selected, only one (1) error or exception detected in the sample is sufficient to conclude on the Operating Effectiveness (OE) of an audit criterion as having a Non-Conformity (NC). This is emphasized further when the risk of material Non-Conformities (NC) is defined as low, as it is not expected to find any exception or error in the population, yet alone in the small sample selected. | • Population of underlying subject(s) matter<br>• Identified attributes to be audited per audit criterion<br>• Output of SOP-SAMP-SSM-03<br>• Errors and exceptions identified in the samples | • Operating Effectiveness (OE) audit extrapolation justified and supported by detailed findings and evidence per attribute |

*Table 4: Extrapolation Standard Operating Procedure*

## 4.6. Conclusion

| Step ID | Step Description | Inputs | Outputs |
|---|---|---|---|
| **SOP-SAMP-CN-01** | When auditing a sample, the Accredited Service Provider for NIA Audit shall assess the conformity attributes. Therefore, when a NIA control include multiple attributes to be audited, the conclusions and extrapolations shall be made on the sum of all attributes. | • Output of SOP-SAMP-EXR-01 | • Aggregated Operating Effectiveness (OE) audit extrapolation justified and supported by detailed findings and evidence per audit criterion |
| **SOP-SAMP-CN-02** | The Accredited Service Provider for NIA Audit shall conclude on that the scope is having an Operating Effectiveness (OE) Non-Conformity (NC) only when the extrapolated error rate for the population of the underlying subject(s) matter equals or exceeds 10%. | • Output of SOP-SAMP-CN-02 | • Operating Effectiveness (OE) audit conclusions justified and supported by detailed findings and evidence |

*Table 5: Conclusion Standard Operating Procedure*

# 5. Compliance and Enforcement

## 5.1. Compliance Process

All applicants to NISCF's NIA Audit Accreditation Services and Accredited Service Provider for NIA Audit by NCSA shall conform with the rules defined in this Standard Operating Procedure.

## 5.2. Roles and Responsibilities

National Cyber Governance and Assurance Affairs (NCGAA) is responsible for enforcing and monitoring conformance to this Standard Operating Procedure.

## 5.3. Transitioning and effective date

### 5.3.1. *Effective date*

This Standard Operating Procedure is effective from January 1, 2025.

### 5.3.2. *Transition period*

The Accredited Service Provider for NIA Audit shall apply this Standard Operating Procedure for audit(s) related to new NISCF Certification requests submitted starting from January 1, 2025.

The Accredited Service Provider for NIA Audit shall apply this Standard Operating Procedure for Maintenance, Re-Certification audits and any other audit related to issued NISCF Certificate of Compliance, occurring after January 1, 2025.

Existing Accredited Audit Service Providers at the time of the publication of this Standard Operating Procedure shall make the necessary updates to conform with this Standard Operating Procedure before January 1, 2025.

Any new request for NISCF Audit Accreditation shall be in conformance with this Standard Operating Procedure from the date of publication.

## 5.4. Exceptions and deviations

### 5.4.1. *Exceptions to Policy Statements*

Exceptions to this Standard Operating Procedure shall only be defined by the National Cyber Security Agency (NCSA) and / or any NCSA's organizational structure that has been given the authority over the NISCF or the Accreditation Services.

### 5.4.2. *Deviation process from Policy Statements*

Deviation from Standard Operating Procedure steps shall be formally authorized in writing by the National Cyber Security Agency (NCSA).

### 5.4.3. *Sanctions*

National Cyber Security Agency (NCSA) reserves the right to not accept NISCF Accreditation Services requests and / or suspend or withdraw Certificates of Accreditation or any other Certificates, Credentials or Licenses provided by NCSA from applicants to NISCF's NIA Audit Accreditation Services and Accredited Service Provider for NIA Audit that do not conform with the requirements defined in this Standard Operating Procedure.

National Cyber Security Agency (NCSA) reserves the right to impose any monetary or procedural sanctions in virtue of the authority that has been granted to NCSA, through laws and regulations.

# 6. Annexes

## 6.1. Acronyms

| | |
|---|---|
| ***AM*** | Access Control Security |
| ***CM*** | Change Management |
| ***DR*** | Data Retention & Archival |
| ***IACR*** | Information Assets Classification Register |
| ***IM*** | Incident Management |
| ***NC*** | Non-Conformities. |
| ***NCGAA*** | National Cyber Governance and Assurance Affairs. |
| ***NCSA*** | National Cyber Security Agency. |
| ***NIA*** | National Information Assurance |
| ***NISCF*** | National Information Security Compliance Framework. |
| ***OE*** | Operating Effectiveness. |
| ***PH*** | Physical Security |
| ***PS*** | Personnel Security |
| ***SOA*** | Statement of Applicability |

## 6.2. Tables, Graphs and Figures

### 6.2.1. Adequate Sampling Example

| Scope \ NIA domains | Change Management | Access Control Security | Media Security | Risk Management | Cryptographic Security | Network Security | Security Awareness |
|---|---|---|---|---|---|---|---|
| Process 1 | X | | X | | X | | |
| Process 2 | | X | | | | X | X |
| Process 3 | | | | X | | | |

*Figure 1: Adequate Sampling Example Figure*

### 6.2.2. Layered Sampling Examples

| Example 1 | | | | | | |
|---|---|---|---|---|---|---|
| **Audit criteria** | DR 5 "Archived data retains it classification markings and is secured accordingly" | | | | | |
| **Selected business process** | P4 | | | | | |
| **Information assets** | D3, D7, D8, D12 and D15 | | | | | |
| **Applications** | A7 | | | A11 | | |
| **Technology components** | T13 | T14 | T16 | T13 | T17 | T20 |
| **Underlying Subject Matter** | Archived data in T13[5] | | | | | |

*Table 6: Example 1 of Layered Sampling*

[5] In this example archived data is not accessible through the business applications. The Accredited Service Provider for NIA Audit identified that T13 supports both applications and therefore based on the principle coverage selected the archived data in T13 as population to be audited.

| Example 2 | |
|---|---|
| **Audit criteria** | PS 5 "Conduct adequate screening to ascertain the integrity of prospective candidates for employment and contractors (including sub-contracted workers). The Organization may further extend this exercise to existing employees as deemed necessary to satisfy conditions arising out of factors such as but not limited to "Change of employee responsibilities" or "Suspicion raised on the conduct of an employee". |
| **Selected business process** | P12 |
| **Information assets** | NA |
| **Applications** | NA |
| **Technology components** | NA |
| **Underlying Subject Matter** | Candidates to finance department[6] |

*Table 7: Example 2 of Layered Sampling*

| Example 3 | |
|---|---|
| **Audit criteria** | PH 4 "Implementation of a "clean desk" and "clean screen" policy". |
| **Selected business process** | P6 |
| **Information assets** | NA |
| **Applications** | NA |
| **Technology components** | NA |
| **Underlying Subject Matter** | Offices 1,2 and 4 in location A and offices 2, 4 and 5 in location B[7] |

*Table 8: Example 3 of Layered Sampling*

[6] The process P12 is under the sole responsibility of the finance department within the NIA Certification Subject (Auditee). The Accredited Service Provider for NIA Audit identified that it will be easier to focus of all candidates of the finance department as it will be faster than investigating which candidates would have to work within process P12 boundaries which will require from the NIA Certification Subject (Auditee) an analysis of the cases that does not add value to the NIA Certification Subject (Auditee).

[7] The process P6 is processed in specific offices in two different locations. The Accredited Service Provider for NIA Audit identified that it will be easier to focus on the location as the objective of the audit criteria is targeting physical spaces.

| Example 4 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Audit criteria** | AM 20 "Passwords are changed at least every 90 days" | | | | | | | | | | |
| **Selected business process** | P3 | | | | | | | | | | |
| **Information assets** | D3 | D7 | | D9 | | | D10 | D13 | D14 | D15 | |
| **Applications** | A2 | | | A3 | | | A5 | | | | |
| **Technology components** | T1 | T2 | T4 | T2 | T3 | T4 | T2 | T5 | T6 | | |
| **Underlying Subject Matter** | A5 and T2[8] | | | | | | | | | | |

*Table 9: Example 4 of Layered Sampling*

| Example 5 | | | | | |
|---|---|---|---|---|---|
| **Audit criteria** | IM 8 "Report all Critical incidents to NCSA within two (2) hour of incident identification." | | | | |
| **Selected business process** | P2 | | | | |
| **Information assets** | D2 | D3 | D5 | D6 | D7 |
| **Applications** | A1 | | | | |
| **Technology components** | T1 | T3 | T15 | | |
| **Underlying Subject Matter** | Incidents impacting A1 and T3[9] | | | | |

*Table 10: Example 5 of Layered Sampling*

[8] Based on the principle of maximizing coverage, the Accredited Service Provider for NIA Audit identified that the audit criteria will be audited on A5 and T12.

[9] The Accredited Service Provider for NIA Audit identified that incidents are classified per IT assets impacted or potentially impacted, which made it easier to select the population for the audit criteria to be selected at the IT assets level supporting the business process P2.

### 6.2.3. Sample Sizes Table and Formulas

| Nature of Control | Population Size | Extent of audit procedure based on risk of material Non-Conformities (NC) | | |
|---|---|---|---|---|
| | | Low | Medium | High |
| Manual | 500< | 6 | Formula S | Formula S' |
| Manual | [251;500] | 5 | 25 | Formula S' |
| Manual | [51;250] | 3 | 15 | 25 |
| Manual | [11;50] | 2 | 3 | 9 |
| Manual | [1;10] | 1 | 2 | 3 |
| Automated | 1=< | 1 | 1 | 1 |

*Table 11: Sample Sizes Table*

Below are the formulas mentioned in the table, where "N" is the population size:

$$S= N/(1+((N-1)/31.130))$$

*Equation 1: Sample Size Formula for Medium Risk of Material non-Conformities (NC)*

$$S'= N/(1+((N-1)/58.982))$$

*Equation 2: Sample Size Formula for High Risk of Material non-Conformities (NC)*

### 6.2.4. Extrapolation Table and Formula

| Nature of Control | Population Size | Extrapolation for at least 1 error found in the sample based on the risk of material Non-Conformities (NC) | | |
|---|---|---|---|---|
| | | Low | Medium | High |
| Manual | 500< | Non-Conformity | Formula E | Formula E |
| Manual | [251;500] | Non-Conformity | Formula E | Formula E |
| Manual | [51;250] | Non-Conformity | Formula E | Formula E |
| Manual | [11;50] | Non-Conformity | Non-Conformity | Formula E |
| Manual | [1;10] | Non-Conformity | Non-Conformity | Non-Conformity |
| Automated | 1=< | Non-Conformity | Non-Conformity | Non-Conformity |

*Table 12: Extrapolation Table*

$$E = ((x / n) + (1.28 * \text{Square Root } (((x / n) * (1 - SP)) / n))) * N$$

*Equation 3: Extrapolation Formula*

- N = N = The entire population size
- SP: SP = x / n
  - i. x = Number of observed errors in the sample
  - ii. n = Sample size

## 6.3. Reference

Emiri Decree No 1 of year 2021

President of National Cyber Security Agency (NCSA) Decision No 3 of year 2022

NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public)

NCSA-NISCF-ACCR-GTXD (General Taxonomy Document for National Accreditation - Public)

NCSA-NISCF-ACCR-GPNA (General Policy for National Accreditation - Public)

NCSA-NISCF-CERT-GPNC (General Policy for National Certification - Public)

NCSA-NISCF-CERT-SMSC (Standard for Management Systems Certification - Public)

NCSA-NISCF-ACCR-SNA (Standard for National Accreditation - Public)

NCSA-NISCF-AUD-STND (NISCF Audit Standard - Public)

NCSA-NISCF-ACCR-AUD-NIA-STND (NIA Audit Accreditation Standard - Public)

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# End of Document