الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Audit Risk Procedure

[NCSA -NISCF-ACCR-AUD-NIA-SOP-AR]

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-AR
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 Risk 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 assessing audit risk 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 Risk 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

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 assessing audit risk.

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).

4. Standard Operating Procedure

4.1. Introduction

Audit risk allows the Accredited Service Provider for National Information Assurance (NIA) Audit to manage the NIA audit engagement effectively and efficiently as it allows to:

- Focus on the areas of greater risk without ignoring the low risk areas;
- Deploy audit resources where and when they are needed the most;
- Get the reasonable assurance that material Non-Conformities (NC) will be detected and reported during the audit;
- Limiting the audit procedures to the sufficient and adequate level to eliminate unnecessary audit procedure; and
- Reduce the audit calendar to the minimum required level.

Audit risk shall be re-evaluated during the NIA audit engagement. This re-evaluation occurs generally after the completion of the Design Effectiveness (DE) audit or when the Accredited Service Provider for NIA Audit discovers new significant elements that changes its understanding of the environment.

In reality, in these situations, it is the sub-components of the audit risk that are re-evaluated, that may or may not lead to an update of the detection risk, and therefore, the nature, extent and calendar of audit procedures to maintain the audit risk at a low acceptable level.

The detection risk level and the related the nature, extent and calendar of audit procedures to be conducted during an engagement depend from the objective of the audit (Please refer to the Technical Directive on Objectives and Audit Scope (NCSA-NISCF-CERT-NIA-TD-OAS-001) for more information on the objectives of the different audit engagements under the NIA Certification Service).

During subsequent audit(s) (i.e., Maintenance, scope expansion, Re-Certification…), the Accredited Service Provider for NIA Audit shall ensure that the relevant levels of the audit risk's sub-components assessed are still valid and updated if necessary (please refer to sections **4.3. Update of Audit Risk During an Engagement** and **4.4. Update of Audit Risk During Subsequent Audit(s))**.

4.2. Initial Audit Risk Assessment

Step ID	Step Description	Inputs	Outputs
SOP-AR-IARA-01	In application of requirements of section A.P.2.2.1. Audit Risk of the NISCF Audit Standard (NCSA-NISCF-AUD-STND), the Accredited Service Provider for NIA Audit shall perform an audit risk assessment. This assessment shall be performed at the scope level and shall be supported by clear and detailed explanation. The Accredited Service Provider for NIA Audit may decide to perform a more detailed audit risk assessment per business process or NIA domain. However, this approach is time-consuming and does not usually result in significantly different assessment from the audit risk assessment performed at the overall scope of audit level. The Accredited Service Provider for NIA Audit shall determine first the inherent risk related to the scope during the preliminary work activities. The Accredited Service Provider for NIA Audit shall assess the inherent risk at the assertions level which in the case of National Information Assurance (NIA) Certification are: • Confidentiality; • Integrity; and • Availability.	• Understanding of the audit environment	• Justified inherent risk level, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
	The Accredited Service Provider for NIA Audit shall start assessing the inherent risk level for the scope based on the NIA Certification Subject (Auditee)'s risk management document. However, this should not be considered as the only source of information to perform the evaluation and the Accredited Service Provider for NIA Audit should exercise professional judgment in assessing the inherent risk level. The Accredited Service Provider for NIA Audit shall determine the inherent risk by choosing a risk level (i.e., High, Medium or Low) with clear and detailed justification of the overall inherent risk level based on the inherent risk at the assertions level. The Accredited Service Provider for NIA Audit shall justify the chosen inherent risk level considering the NIA Certification Subject (Auditee)'s risk level definitions. If the NIA Certification Subject (Auditee) is using quantitative risk assessment, the Accredited Service Provider for NIA Audit shall translate the NIA Certification Subject (Auditee)'s quantitative scale to the defined levels in this procedure (i.e., High, Medium, Low) using **Table 4: Quantitative Inherent Risk Equivalency**. The Accredited Service Provider for NIA Audit shall not include in the justification of the inherent risk elements related to the engagement as these elements are part of the detection risk and do not align with the definition of inherent risk.		

Step ID	Step Description	Inputs	Outputs
SOP-AR-IARA-02	Once the inherent risk is determined, justified and documented, the Accredited Service Provider for NIA Audit shall assess the control risk. Similar to the inherent risk, the Accredited Service Provider for NIA Audit shall assess the control risk during the preliminary work activities. The control risk level is determined based on the Accredited Service Provider for NIA Audit assessment of the design of the controls selected and implemented by the NIA Certification Subject (Auditee) to address the inherent risks. The Accredited Service Provider for NIA Audit shall determine during the preliminary work, based on the environment understanding the overall approach, the controls selected and implemented by the NIA Certification Subject (Auditee) to address the inherent risks at the assertions level. The Accredited Service Provider for NIA Audit shall use professional judgment to determine if the selected controls and how they have been designed and implemented will allow the NIA Certification Subject (Auditee) to prevent, detect or correct at the right time the inherent risks. Based on this evaluation, the Accredited Service Provider for NIA Audit should be in a position to select the control risk level using **Table 5: Control Risk Level Indicators**.	• Understanding of the audit environment	• Justified control risk level, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
	The Accredited Service Provider for NIA Audit shall use **Table 5: Control Risk Level Indicators** assuming that the control risk is high. Based on evidence gathering at the planning stage, the Accredited Service Provider for NIA Audit shall reduce the control risk level when evidences show that the mentioned indicators or factors exist and that the Accredited Service Provider for NIA Audit, based on its professional judgment evaluate that these evidences are effective in addressing the inherent risks. If the indicators stated in front of the control risk level "High" are not existent in the scope, this generally indicates that the Information Security Management System has not been implemented by the NIA Certification Subject (Auditee) and that the audit would not achieve its objectives. The Accredited Service Provider for NIA Audit can include additional factors to be checked to be able to reduce the control risk from one level to the other. In such cases, the Accredited Service Provider for NIA Audit shall have a standardized and approved audit risk management methodology and related working papers that shall be submitted during its Accreditation application. Similar to inherent risk level selection, the Accredited Service Provider for NIA Audit shall justify the chosen control risk level.		

Step ID	Step Description	Inputs	Outputs
	The Accredited Service Provider for NIA Audit may decide to reduce the control risk level, even when all the mentioned indicators or factors are not evidenced within the scope based on its professional judgment and other justification factors. In this case, the Accredited Service Provider for NIA Audit shall have clear and detailed justification. The Accredited Service Provider for NIA Audit shall not reduce the control risk level based on the fact it will implement additional audit procedures as these elements are not related to the NIA Certification Subject (Auditee)'s ability to address the inherent risks.		
SOP-AR-IARA-03	The Accredited Service Provider for NIA Audit shall determine the level of risk of material Non-Conformities (NC) based on **Figure 1: Risk of Material Non-Conformities (NC) Matrix**.	• Output of SOP-AR-IARA-01 and SOP-AR-IARA-02	• Justified risk of material Non-Conformities (NC) level, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
SOP-AR-IARA-04	The Accredited Service Provider for NIA Audit shall manage the detection risk by implementing appropriate and sufficient audit procedures to keep the audit risk at a low acceptable level. Please refer to the NIA Audit Work Program Standard Operating Procedure (NCSA-NISCF-ACCR-AUD-NIA-SOP-AWP) and NIA Sampling Standard Operating Procedure (NCSA-NISCF-ACCR-AUD-NIA-SOP-SAMP) for more information on audit response to risk of material Non-Conformities (NC). The Accredited Service Provider for NIA Audit shall explain in details how the nature, extent and calendar of audit procedures that are planned to be conducted will ensure that the detection risk is low enough to maintain the audit risk at a low acceptable level. The Accredited Service Provider for NIA Audit shall in its justification map the audit work program, including the testing scripts to the risk areas identified for risk of material Non-Conformities (NC).	• Output of SOP-AR-IARA-03 • Nature, extent and calendar of audit procedures • Audit work program	• Justified detection risk level, documented in the working papers for recording the audit risk assessment shared during the Accreditation
SOP-AR-IARA-05	The audit risk shall always be kept at a low acceptable level. The minimization of the detection risk and the justification provided at the detection level shall lead to the audit risk level justification. The Accredited Service Provider for NIA Audit should account for a margin of error between the level of detection risk. **Figure 2: Audit Risk** is an illustrative representation of the interactions among the risk of material Non-Conformities (NC), detection risk	• Risk of material Non-Conformities (NC) • Output of SOP-AR-IARA-03 and SOP-AR-IARA-04	• Justified audit risk kept at a low acceptable level, documented in the working papers for

Step ID	Step Description	Inputs	Outputs
	and the audit risk to allow for better understanding and should not be taken as accurate, in scale representation.		recording the audit risk assessment shared during the Accreditation

Table 1: Initial Risk Assessment Standard Operating Procedure

4.3. Update of Audit Risk During an Engagement

Step ID	Step Description	Inputs	Outputs
SOP-AR-UARDE-01-A	Following the Design Effectiveness (DE) audit, the Accredited Service Provider for NIA Audit shall have a better and more thorough understanding of the controls in place and how they are designed by the NIA Certification Subject (Auditee) to address the risks to Confidentiality, Integrity and Availability. It is expected that if the preliminary work activities are performed in conformance with the NISCF Audit Standard and if the NIA Certification Subject (Auditee) provides all necessary information required by the Accredited Service Provider for NIA Audit, that the understanding of the controls in place by the Accredited Service Provider for NIA Audit would not change significantly from post preliminary work to post Design Effectiveness (DE) audit. However, there can be situation(s) where this better and more thorough understanding gained during Design Effectiveness (DE)	• Design Effectiveness (DE) audit results	• Justified updated control risk level, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
	audit can provide indication that an update to the control risk level needs to be performed. When update is required, the Accredited Service Provider for NIA Audit shall re-assess the control risk based on the better understanding gain through Design Effectiveness (DE) audit and provide justification and explanation of the new level of control risk. The Accredited Service Provider for NIA Audit shall also provide explanation on the reasons that led to inability to gain the same understanding during the preliminary work.		
SOP-AR-UARDE-01-B	At any moment during the audit engagement, if the Accredited Service Provider for NIA Audit discovers new or existing significant factors that changes its understanding of the audit environment, the Accredited Service Provider for NIA Audit shall assess the impact of these factors on the audit risk. The Accredited Service Provider for NIA Audit shall determine which sub-component of the audit risk is impacted by the newly discovered factors and re-assess the risk level as per the requirements defined in this Standard Operating Procedure. If the new factors that have been discovered by the Accredited Service Provider for NIA Audit are existing factors (i.e., existed prior to the Accredited Service Provider for NIA Audit conducting the preliminary work), the Accredited Service Provider for NIA Audit	• Updated understanding of the audit environment	• Justified updated inherent risk, control risk or detection risk level, documented in the working papers for recording the audit risk assessment shared during

Step ID	Step Description	Inputs	Outputs
	shall provide an explanation on the reasons that led to non-discovery of these significant factors during the preliminary work as part of the update to the audit risk update. New significant factors discovered do not necessarily require to change the sub-components of audit risk levels. The Accredited Service Provider for NIA Audit shall evaluate the impact of these new factors and determine following the steps defined in this procedure if changes to the risks levels is required.		the Accreditation

Table 2: Audit Risk Update During an Engagement Standard Operating Procedure

Updating the audit risk sub-components levels during an audit engagement may occur based on the described situations in steps SOP-AR-UARDE-01-A and / or SOP-AR-UARDE-01-B. The update may result in more audit procedure required to maintain the audit risk at low acceptable level.

Even though it should not be expected during an audit engagement, but the update of the audit risk sub-components levels can result in less audit procedure to be conducted. This is an exceptional situation permitted only when during the preliminary work activities, the Accredited Service Provider for NIA Audit adopted an approach that is too conservative that resulted in unnecessary audit procedures to be planned. In such a situation, the Accredited Service Provider for NIA Audit shall document in details the reasons that led to adopting such approach as additional audit procedures lead to additional budget and time for the NIA Certification Subject (Auditee) to complete its NIA Certification request or maintenance.

In all cases, the Accredited Service Provider for NIA Audit shall document in detail the justification of the change to the audit risk sub-components levels impacted and the required changes to the audit work program and nature, extent and calendar of the audit procedures based on these changes to maintain the audit risk at a low acceptable level.

4.4. Update of Audit Risk During Subsequent Audit(s)

Step ID	Step Description	Inputs	Outputs
SOP-AR-UARSA-01-A	During the planning of Maintenance, the Accredited Service Provider for NIA Audit shall confirm that inherent and control risks levels identified during the most recent previous audit are still valid, in order to determine an adequate detection risk level based on the Maintenance objective. If there is evidences that inherent and control risks levels changed due to changes in the scope, this should normally indicate changes that require to be audited to ensure their conformity with the audit criteria (please refer to the Maintenance Objective as defined in section A.P.6.2. Rest of Audit Process of the NISCF Audit Standard and in the Technical Directive on Objectives and Audit Scope (NCSA-NISCF-NIA-TD-OAS-001)). Therefore, the Accredited Service Provider for NIA Audit shall adapt detection risk and ensure that the audit work program covers the audit of changes occurred to the scope against the audit criteria to maintain the audit risk at low acceptable level. Generally, due to the limited scope of work during Maintenance, it is not expected to have changes to the audit risk sub-components levels after confirmation during the preliminary work as per the requirements defined in section A.P.6.2. Rest of Audit Process of the NISCF Audit Standard.	• Updated understanding of the audit environment	• Justified updated or confirmed audit-risk sub-components levels, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
SOP-AR-UARSA-01-B	During scope expansion audit planning (either part of Maintenance or special audit), the Accredited Service Provider for NIA Audit shall confirm the inherent and control risks levels. For scope expansion, it is generally expected that inherent risks changes (as new business processes and information assets are included in the expanded scope), therefore, the Accredited Service Provider for NIA Audit shall evaluate and determine the adequate inherent level for the expansion part of the scope. Depending on the differences in the inherent risks between the certified scope and the expansion part subject of the audit of the scope expansion, the control risk level may need to be updated. The Accredited Service Provider for NIA Audit should also consider the integration between; the already certified scope and the expansion part subject of the audit of the scope expansion, before deciding to update the control risk level identified during the latest previous audit. This integration may consider factors such centralization of cyber security controls and processes, and differences in inherent risk scenarios, impact and likelihood levels between the two scopes. Based on the determined risk of material Non-Conformities (NC), the Accredited Service Provider for NIA Audit shall manage the detection risk to maintain the audit risk to an acceptable low level based on the objective of the audit as per the requirements	• Updated understanding of the audit environment of the certified scope • Understanding of the audit environment of the expansion part subject of the audit of the scope expansion	• Justified updated or confirmed audit-risk sub-components levels, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
	defined in section A.P.6.2. Rest of Audit Process of the NISCF Audit Standard and in the Technical Directive on Objectives and Audit Scope (NCSA-NISCF-NIA-TD-OAS-001).		
SOP-AR-UARSA-01-C	During Re-Certification audit planning, the Accredited Service Provider for NIA Audit shall confirm that the inherent risk and control risks levels determined during the most recent previous audit are still valid. If the risk of material Non-Conformities (NC) level is maintained as the same as during the initial NIA Certification audit or the last Re-Certification audit, the Accredited Service Provider for NIA Audit can adopt the same detection risk level by applying similar audit procedures and audit work program considering the rotation requirements (please refer to NIA Audit Work Program Standard Operating Procedure (NCSA-NISCF-ACCR-AUD-NIA-SOP-AWP)). If there is evidence that the inherent or control risks levels shall be updated, the Accredited Service Provider for NIA Audit shall re-assess the risk levels and determine the risk of material Non-Conformities (NC). Based on the determined risk of material Non-Conformities (NC), the Accredited Service Provider for NIA Audit shall manage the detection risk to maintain the audit risk to an acceptable low level based on the objective of the audit as per the requirements defined in section A.P.6.2. Rest of Audit Process of the NISCF Audit	• Updated understanding of the audit environment of the certified scope	• Justified updated or confirmed audit-risk sub-components levels, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Step ID	Step Description	Inputs	Outputs
	Standard and in the Technical Directive on Objectives and Audit Scope (NCSA-NISCF-NIA-TD-OAS-001).		
SOP-AR-UARSA-01-D	During the planning of a special audit for reinstatement following suspension, the Accredited Service Provider for NIA Audit shall confirm that inherent and control risks levels identified during the most recent previous audit are still valid, in order to determine an adequate detection risk level based on the special audit objective. If there is evidence that changes to the inherent and control risks levels are identified, the Accredited Service Provider for NIA Audit shall re-evaluate the risk of material Non-Conformities (NC) based on these changes. Based on the determined risk of material Non-Conformities (NC), the Accredited Service Provider for NIA Audit shall manage the detection risk to maintain the audit risk to an acceptable low level based on the objective of the audit as per the requirements defined in section A.P.6.2. Rest of Audit Process of the NISCF Audit Standard and in the Technical Directive on Objectives and Audit Scope (NCSA-NISCF-NIA-TD-OAS-001).	• Updated understanding of the audit environment of the certified scope	• Justified updated or confirmed audit-risk sub-components levels, documented in the working papers for recording the audit risk assessment shared during the Accreditation

Table 3: Audit Risk Update During Subsequent Audit(s) Standard Operating Procedure

When the Accredited Service Provider for NIA Audit conducting a subsequent audit is not the same as the Accredited Service Provider for NIA Audit that conducted the initial NIA Certification audit or the latest previous audit, the new Accredited Service Provider for NIA Audit shall conduct risk assessment as per the steps defined in the section **4.2. Initial Audit Risk Assessment**.

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

DE	Design Effectiveness
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

6.2. Tables, Graphs and Figures

6.2.1. Inherent Risk Equivalency Table

Range of percentage of the NIA Certification Subject (Auditee) quantitative scale	Equivalent inherent risk levels
[0% - 33%]	Low
[34% - 66%]	Medium
[67% - 100%]	High

Table 4: Quantitative Inherent Risk Equivalency

6.2.2. Control Risk Level Indicators Table

Indicators / Factors to be checked to clear the risk level	Control risk Level
• Information Security Policies, Standard Operating Procedures and processes as required by NIA • Risk Management documentation • Clear roles and responsibilities to Cyber Security activities	High
• Clear mapping between processes in the scope, their supporting information assets, the risks related to these assets and the controls selected and implemented to address those risks • Communication of the Information Security Policies to the relevant stakeholders • Clear assignment of positions and roles related to Cyber Security and acknowledgment of the responsibilities	Medium
• KGI and KPI are defined for the controls • Independent review of the design and operating efficiency of the controls is performed • Optimization of the controls through performance management in place • Automation of the operation of controls	Low

Table 5: Control Risk Level Indicators

6.2.3. *Risk of Material Non-Conformities (NC) Matrix*

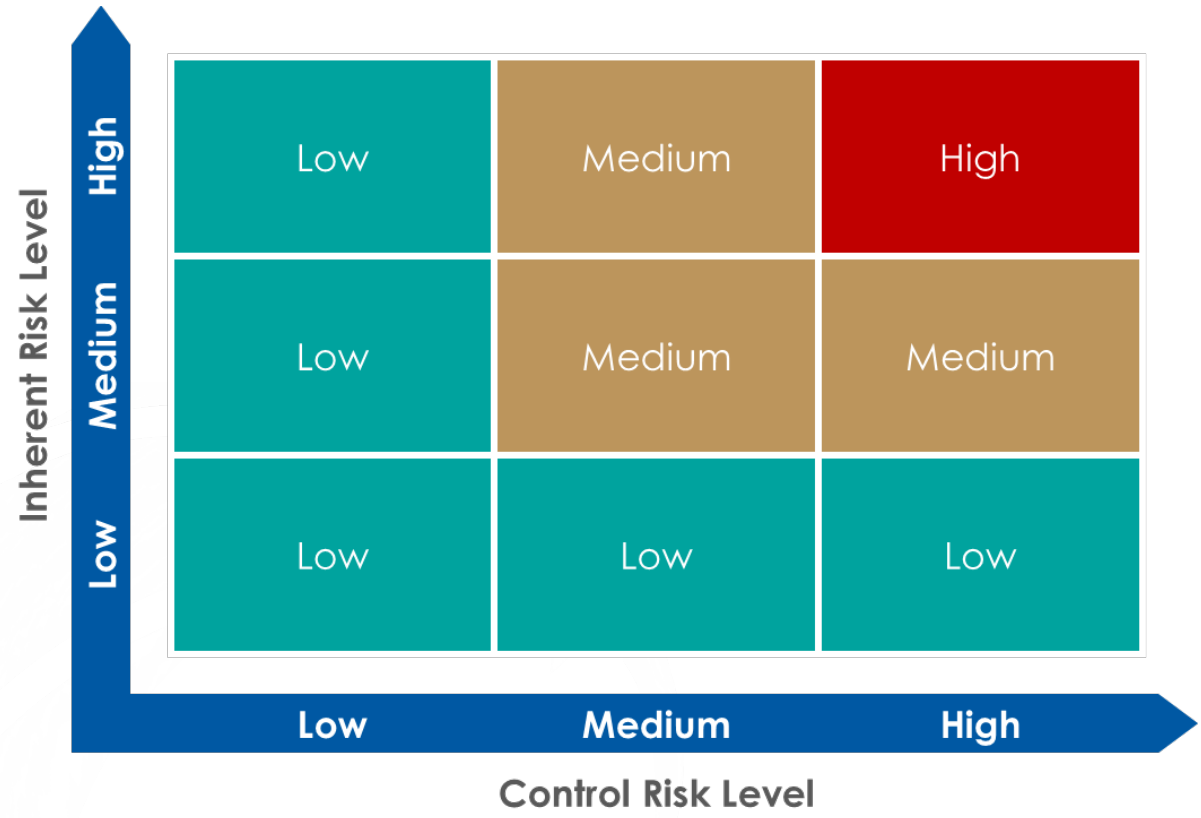

Figure 1: Risk of Material Non-Conformities (NC) Matrix

6.2.4. Audit Risk Figure

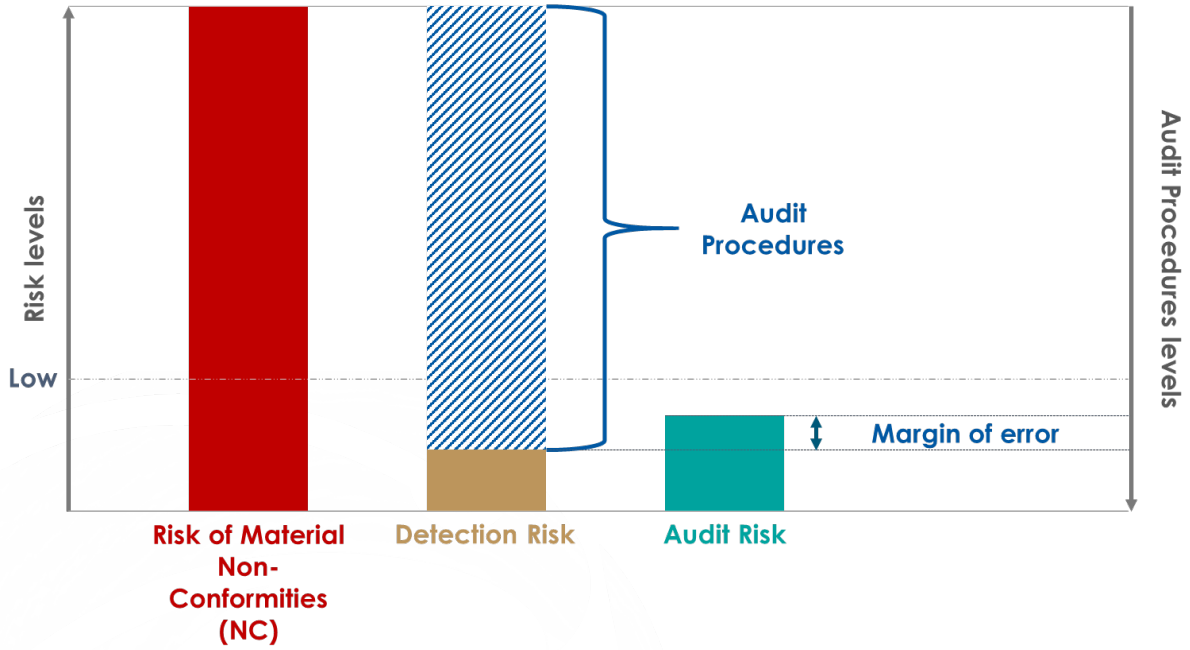

Figure 2: Audit Risk

End of Document