Holland Quaestor

ASSOCIATION OF QUALITY
CORPORATE SERVICES PROVIDERS

Holland Quaestor SIRA Framework & Methodology for Trust Offices

Integer

Onafhankelijk

Betrouwbaar

Duurzaam

Professioneel

Contents

Definitions

Compliance Monitoring:
The ongoing process of evaluating the effectiveness of control measures and ensuring adherence to regulatory and organizational standards.

Control Measures:
Policies, procedures, and actions implemented to reduce or manage identified risks, ensuring they remain within acceptable limits.

De Nederlandsche Bank ("DNB")
The central bank and financial supervisory authority of the Netherlands responsible for integrity oversight for trust offices.

High-Risk Jurisdictions:
Geographic areas identified as having elevated risks of financial crime, corruption, or insufficient regulatory frameworks, necessitating enhanced due diligence measures.

Holland Quaestor ("HQ"):
The Dutch association of trust offices that represents the sector's interests and promotes compliance and integrity.

Impact:
Relates to the damage that can occur as a result of financial and economic crime. This could include the long or short-term effects of the criminal activities on the financial system, financial undertakings, the economy and society.

Inherent Risk:
The natural level of risk present before any control measures or mitigation strategies are applied.

Institution-Specific:
Tailored to the unique characteristics, risks, client base, and operational profile of the trust office, ensuring that risk assessments and controls are relevant and effective.

Integrity Culture:
The collective values, attitudes, and practices within an organization that prioritize ethical behaviour and adherence to compliance standards.

Integrity Risk (DNB):
Risk of insufficient compliance with what is prescribed by or pursuant to any statutory provision, as well as the risk of the trust office or its employees being involved in actions that are so contrary to what is deemed acceptable in social conduct according to unwritten law, that it could seriously damage trust in the trust office or in the financial markets.

Residual Risk:
The remaining level of risk after all control measures and mitigation strategies have been implemented.

Risk:
The likelihood that a threat will exploit a vulnerability, resulting in an event with potential impact or consequences.

Risk Appetite:
The level and types of risks a trust-office is willing to accept in pursuit of its objectives, expressed through policies, controls, and measurable limits.

Scenario:
A detailed description of how a specific risk could manifest, including the sequence of actions, decisions, or events, designed to assess and address vulnerabilities and threats within an organization.

Systematic Integrity Risk Analysis (SIRA):
A structured process used by trust offices to identify, assess, and mitigate integrity risks affecting business operations. The process involves risk identification, analysis, control measures, and ongoing monitoring and review.

Threats:
Arise from persons, groups of persons, or activities that can cause damage to, for example, a country, society, a financial undertaking and the economy. Threats are posed by criminals, terrorist groups, their facilitators, their funds and the activities that they undertake.

Vulnerabilities:
Make the realization of threats possible. Examples are weaknesses in the anti-money laundering and terrorist financing system, such as inadequate controls, or specific characteristics of a financial undertaking or sector, services or products.

Wet Toezicht Trustkantoren 2018 (“WTT 2018”):
The Dutch law regulating trust offices, requiring licensing and setting strict compliance standards to prevent financial crime.

1 Introduction

The Wtt 2018 requires trust offices, for the purpose of conducting their business with integrity and in a controlled manner, to periodically carry out an analysis of the integrity risks to sound business operations. Each identified risk from this analysis must be systematically reviewed, with specific adjustments or additions made to existing policies, operational procedures, and risk control measures. Trust offices have at least an annual process to review and update the organisation-wide integrity risk analysis.

The results of this organisation-wide analysis are recorded, but that document is often seen as a static document. The objective of the integrity risk analysis is to transpose the analysis into practical procedures and processes, showing why certain measures must be taken. The intention is also to actively respond to internal and external developments where new risks may arise and to revise that part of the integrity risk analysis. The integrity risk analysis is essentially about the result: awareness of risks and taking adequate control measures to manage the risks. It is therefore important that all relevant first- and second line employees as well as management are involved in the integrity risk analysis process and are informed about the outcomes.

Purpose

The purpose of this guideline is to support trust offices to implement a SIRA that identifies, analyses, and mitigates integrity risks within the risk appetite of the trust institution. This updated version aims to make SIRA more practical and accessible, also taking into account the regulatory expectations for the employees in the first line, for its application.

Target Audience

The intended readers include trust office staff, compliance officers, senior management, and other stakeholders in risk management, members of Holland Quaestor and other interested parties.

Documents

The SIRA Guidelines consists of three parts:

- This **SIRA Framework & Methodology** is the **main document** provides theoretical foundations.
- The **SIRA Practical Guideline** is a **practical document** will include detailed examples and tools for SIRA implementation,
- The **SIRA Scenario Overview i**s a sheet of **common scenarios and examples** of mitigating measures that trust office employees may encounter in their daily practice and help trust offices to complete their analysis.

Survey

To further improve the SIRA guidelines and understand what aspects are most valuable to trust offices, Holland Quaestor conducted a survey among trust offices in 2024. This survey gathered insights on areas for improvement in the SIRA process and highlighted the aspects most important to members. The findings from this survey have been incorporated into this guidance to further align the SIRA framework with practical needs of participating institutions and to improve its usability for trust offices.

2 Purpose of the Integrity Risk Analysis

The primary purpose of the SIRA is to identify and assess potential integrity risks that could impact the trust office's operations and reputation. The analysis should be realistic and relevant to the trust office's specific risk landscape.

This process is structured as a **continuous review cycle** that aligns with DNB's Sira Good Practices four recommended steps:

1. **Risk identification (paragraph 3)**
2. **Analysis and risk categorization (paragraph 4)**
3. **Assessment and risk measures (paragraph 5)**
4. **Monitoring and updating (paragraph 6)**

A trust office will often already consider the possible risks concerning risk factors such as clients, third parties, employees, delivery channels, countries or services. However, by doing this in a structured way and by making this a continuous process and recording the results, the firm will ensure that reflecting on the risks is 'ingrained' in everyday processes and done intrinsically. This means, for example, that if first line employees point out that the transaction behaviour of a few clients has changed, this will not only be assessed for those clients, but that a broader analysis is made if a new risk occurs structurally.

Effective risk identification is the cornerstone of a robust integrity risk analysis. This involves not only detecting obvious risks, such as unusual transaction patterns or regulatory changes, but also anticipating **emerging risks** that could arise due to shifts in the business environment or new service offerings. For example, the firm should examine patterns over time, scrutinize anomalies in client behaviour, and assess dependencies on third parties to identify risks proactively. Furthermore, categorizing risks based on their origin — be it operational, reputational, or strategic — ensures that no potential threats are overlooked. By prioritizing this phase, the trust office can establish a comprehensive understanding of its risk landscape, forming a solid foundation for subsequent mitigation strategies.

By involving all relevant employees in **risk identification** process, an internalized, integer culture can be implemented within the trust office which is embedded across all levels of the organization. This means that from the first line all employees who have client contact or handle and assess client documents and transactions, such as employees of the finance, legal, tax, and office support departments who are aware of all activities and risks, are actively involved. Management, compliance and risk management have an essential role.

Ultimately, the integrity risk analysis serves as a steering document for the full organization and for management for guidance and determination of control actions to take in certain scenarios.

3 Risk identification process

Preparation and identification

In preparation, trust offices should use the HQ SIRA practical guidance. In addition, external and internal developments and several sources of information shall be assessed, such as:

- National (NL) and Supranational Risk Assessments (EU)
- Authorities such as FATF, AMLC
- Relevant EU or NL regulatory developments
- (internal) audits, compliance findings, incident and alert recordings, FIU and incident reports
- Items regarding operations such as insights in control effectiveness, trends analysis

- New products, services, technologies (including AI)
- Relevant DNB guidelines and best practices documentation and formal measures;
- Relevant court cases.
- Upcoming legislation
- Relevant DNB guidance, best practices and publication such as DNB Integriteitstoezicht in beeld

DNB Guidance: Following DNB's SIRA guidance's (DNB Sira Good Practices 2015 and the Consultatieversie "DNB SIRA Good Practices 2024), an organizational overview (will be at the end of this section) and identified risk scenarios help assess inherent risks. The suggested SIRA Good Practices can serve as a guidance during the preparation of the organizational overview and of the risk scenario. The identification process in the DNB consultation good practices is focussed on the creation of the organisational overview and based on that data, scenarios are created / updated. In previous DNB guidelines it included the evaluating the likelihood of risk occurrence and potential impacts. Likelihood may be based on occurrence frequency, and impact considers financial, reputational, regulatory and internal damage. Controls are assessed based on audit and compliance reports and DNB findings, identifying control gaps and net risks to inform additional necessary measures.

Relation between Risk Appetite and Risk Analysis

When developing a risk analysis, the trust office examines which risks can be accepted, which must be avoided or can be reduced by taking (additional) control measures. It is also necessary to formulate an "integrity risk appetite".

The risk appetite defines the amount of risk the trust office is willing to accept in pursuit of its strategic objectives and operational goals. The formulation of the risk appetite in a risk appetite statement and the development of the risk analysis are interconnected, but the processes can be independent. If a trust office is prepared to accept certain risks as part of its business strategy, it will be evident from the risk appetite. Through the risk analysis process, the trust office can then examine the extent of the measures needed to mitigate those risks to a level within the risk appetite.

The trust office formulates a risk appetite for the level and type of risk that the trust office regards as appropriate to execute its strategy, mission and core business. By testing the outcomes of the integrity risk analysis against the integrity risk appetite, the firm decides whether to accept, control, or avoid the identified risks. The integrity risk appetite will usually be a qualitative statement, for example that:

- the trust office wants to avoid measures by the regulator,
- clients or UBOs from certain countries are not to be accepted,
- tax integrity risks can be accepted with certain clients, but must be in line with the fiscal risk appetite and this is to be assessed for each client,
- there is no appetite for transactions with aggressive tax planning,
- limitations on clients with PEPs from high-risk countries as controls measures are difficult to include,
- there is no appetite for products that are made with child labour, or unacceptable activities from a social propriety point of view.

Risk appetite needs to be measurable. Otherwise, there is a risk that statements become void. A risk appetite usually has a framework that defines the tolerance of risk levels such as low, moderate, high or very high. Also, risk tolerance could be used, for example that

- no more than 20% of the customer base can consist of UBOs from high-risk countries,
- there is a maximum to the number of clients from certain countries,

- domicile-only services are only provided in case of administration services and viewing rights, on bank accounts to ensure proper transaction monitoring,
- there should be no more than 2 days backlog with regard to handling transaction monitoring alerts.

The risk appetite will have to be reviewed regularly. It is a logical part of the business strategy and business operations. For example, if a trust office is planning to provide a new type of service, the office will automatically consider, when developing that service, which risks can be accepted or which risks cannot be accepted or in case the risk is new, whether the risk appetite statement has to be updated. Considering the risks, the risk tolerance, the risk scenarios and how the risks have to be managed is a continuous process where the risk appetite and the risk analysis meet.

The integrity risk analysis considers the risks that can actually occur and how these risks are managed. If the risk appetite already specifies what can be accepted, it will become clear during the risk analysis process whether a risk falls within the boundaries of the risk appetite.

Organisational overview

An organizational overview is a document that serves as the foundation for identifying relevant integrity risks and ensures that the risk assessment process is tailored to the trust office's actual operations, structure, and service offerings.

For Dutch trust offices, the IRAP (Integriteits Risico Analyse Proces) is considered the main base for this overview and could be considered as the organizational overview. The IRAP is a mandatory structured, annually reviewed report that captures key elements of the organisation's operations, including services offered, jurisdictions involved, types of clients served, and any inherent vulnerabilities. A Dutch trust office needs to report the IRAP to the DNB via its portal annually. However, for internal purposes it is good prepare the IRAP overview more frequently (quarterly or monthly)

It is recommended to summarize the key findings of the IRAP and check if the numbers correspond with the risk appetite tolerance. The results should be discussed with the management which would result in further action points in case required. By integrating the SIRA with the IRAP, the trust office ensures that its risk assessment remains institution-specific, up to date, and proportionate to its risk exposure.

This approach aligns with expectations under the Wtt 2018 and the DNB's SIRA Good Practices, and supports both risk-based compliance and internal governance. A clear organisational overview enables the trust office to identify and assess integrity risks effectively and to determine where control measures are necessary.

4 Analysis and risk categorization

Analysing the organisational overview via scenarios and categorize it into the different integrity risks are the next steps in the process. Here are some examples of how these insights can be translated into a specific SIRA scenario**:**

- **Geographic presence in high-risk jurisdictions:**
  If the organizational overview reveals operations or significant client bases in high-risk jurisdictions (e.g., countries identified with higher levels of money laundering, financial crime or corruption), this could lead to a SIRA scenario focused on "Cross-Border transactions with high-risk jurisdictions." The risk score for this scenario might be elevated due to the increased likelihood and impact of exposure to financial crime, regulatory scrutiny, reputational damage.

DNB emphasizes assessing the effectiveness of controls specifically related to high-risk jurisdictions, including transaction monitoring mechanisms and staff training tailored to these geographies

- **Client base with high proportion of Politically Exposed Persons (PEPs):**
  An organizational overview showing a high percentage of PEPs among clients would inform a SIRA scenario like “Services to high-risk client profiles (PEPs).” The presence of PEPs generally increases the inherent risk of Bribery and Corruption leading to a higher score based on both the likelihood and probability and its potential impact (reputational and financial risks), given the potential risks associated with PEPs.
- The DNB highlights the importance of granular risk assessments for PEPs, including detailed screening and ongoing monitoring mechanisms. By adopting these practices, trust offices can enhance their ability to mitigate risks effectively
- **Introduction of digital products or services:**
  If the organization has recently launched digital services, such as online account management or onboarding, this innovation could inform a SIRA scenario focused on “Increased exposure to cybersecurity and fraud risks.” The risk score might be higher due to the increased vulnerability to cyber threats and fraud, considering the likelihood of attacks on digital platforms and the impact of potential financial and reputational losses.

Drafting the SIRA matrix and the risk scenarios

The SIRA matrix is a structured tool used to visualize and assess integrity risks by mapping the likelihood of occurrence against the potential impact on the trust office. This two-dimensional grid enables trust offices to categorize risks as low, medium, high, or extreme, thereby supporting prioritization of mitigation efforts. Each identified risk scenario is plotted in the matrix based on a qualitative or quantitative assessment, ensuring a consistent and transparent evaluation of threats to integrity. The matrix serves as a central element in the Systematic Integrity Risk Assessment (SIRA) process, facilitating informed decision-making and demonstrating risk awareness to regulators

A scenario is a detailed description of how a specific risk could manifest, including the sequence of actions, decisions, or events, designed to assess and address vulnerabilities and threats within a trust office. Based on a scenario, the likelihood and impact of this scenario are rated. This scenario is used to identify, assess, and analyse how such a risk could impact the institution’s operations, reputation, and compliance with regulatory requirements. It serves as a tool to evaluate the institution's existing controls and risk appetite, helping to develop strategies to mitigate or manage the identified risks effectively.

When drafting a scenario for SIRA, the primary goal is to ensure that it effectively identifies and communicates institution-specific risks. A good scenario provides a concrete description of how a specific risk might materialize, translating abstract risks into actionable insights.

Through workshops with various departments of the organization information can be retrieved which is specifically relevant to create a valid and practical scenario. This involves creating scenarios tailored to the unique characteristics of the trust office, enabling clear recognition and assessment of potential vulnerabilities.

The organization overview (and IRAP) provides the data to come to a structured approach for developing scenarios. A scenario must offer a detailed account of the sequence of actions, decisions, or events through how a risk could materialize. This includes identifying not only the triggers or causes of the risk but also the resulting impact on the trust office’s operations, compliance, or

reputation. Each described event or action should be explicit and observable, so it is clear when and how the scenario is unfolding in real-world circumstances.

The clarity and specificity of these scenarios are crucial for ensuring their effectiveness. By describing actions and events in a way that does not require specialized background knowledge to interpret, trust offices can enhance the usability of their scenarios. This ensures that risk management professionals and auditors alike can identify and verify the occurrence of the described events or actions, allowing for prompt and effective responses to mitigate risks as they arise.

5 Assessment and risk measures

The SIRA enables trust offices to identify control gaps and determine if certain risks have a higher likelihood of materializing. When this occurs, a plan of action shall be defined, and adjustments should be made e.g. to policies, processes, and employee knowledge and awareness.

During the integrity risk assessment, a trust office should evaluate whether existing policies and procedures already address certain integrity risks, even if not explicitly stated. Many trust offices have built up controls over time, but employees may not always be aware of how these relate to current risk exposures. To strengthen risk awareness, it is recommended to involve first-line staff in the assessment process. Ask them to work together with Compliance to identify any changes in the client or service profile that could affect the integrity risk level.

For example, if there is an increase in clients from high-risk countries, reassess whether the client acceptance policy and procedures are still appropriate. The trust office should update these where needed to ensure sufficient controls are in place and include references to the SIRA and its outcomes in the policy and procedure manuals to show alignment. The full SIRA documentation and governance should be kept separate from procedural handbooks. This ensures the SIRA remains a standalone, risk-based tool that supports continuous improvement.

Example: Steps taken for the "Money Laundering" component

1. **Risk Identification**: During a working group session involving first and second-line employees, the analysis showed a high inherent risk of money laundering via clients with structures involving a trust.
2. **Control Effectiveness Assessment**: Reviewing the design and performance of controls (e.g., audit and compliance reports), it was found that structure overviews in client files were often incomplete.
3. **Net Risk Assessment**: Due to gaps in control measures, the net risk level remained unacceptably high.
4. **Additional Measures**: Management, on Compliance's recommendation, established additional control measures with set timelines to mitigate the risk.
5. **Procedural Amendments**: Client acceptance and review procedures were adjusted, with added guidance and training for employees on structure verification.
6. **Updating Records**: The adjustments were reflected in client files, with a focus on structure overviews and risk substantiation.
7. **Monitoring and Evaluation**: In the next review cycle, the trust office will assess whether the amended measures have effectively lowered the net risk to an acceptable level

Action planning and Risk Appetite

To ensure that SIRA results are actionable, they should be considered to in policies, controls, and training. Action plans designate responsible parties, set timelines, and link SIRA findings to policies and staff training. Ongoing collaboration between first and second-line teams is critical for implementing these controls. Furthermore, a monitoring program aligned with SIRA helps maintain effective risk management.

As part of this ongoing process, the risk appetite should be reviewed regularly in conjunction with SIRA. This ensures that any shifts in risk levels or organizational priorities are reflected in both the risk appetite and the integrity risk analysis, maintaining alignment with business objectives and regulatory requirements. It is recommended that the main control measures of scenarios with high-risk scores in the SIRA are reflected in the compliance monitoring program to ensure that integrity risks are within the risk appetite of the organisation.

6 Monitoring and Updating

The SIRA is a dynamic and ongoing process that requires continuous monitoring and updates as new risks emerge or existing risks evolve. In line with regulatory expectations, the SIRA must be formally reviewed and updated at least once per year. The review cycle should be clearly documented in the organization's internal policies. Depending on the nature, size, and risk profile of the organization, more frequent updates may be necessary to ensure the SIRA remains current and effective.

Triggers for SIRA Review

Changes in regulations, significant compliance findings, business model updates, or client portfolio profile changes can prompt a review. As stated above, the IRAP data is a good moment to review the client portfolio and check if there are major changes or areas which needs to be addressed better. Since SIRA development is a collaborative effort, all departments contribute to the creation, review, and updates.

Examples of Triggers:

- **Regulatory change:**
  New anti-money laundering regulations requiring specific enhanced client due diligence may necessitate adjustments in the SIRA. These changes often prompt a review to ensure compliance with updated legal and regulatory standards.

- **Compliance findings:**
  Discoveries of significant amount or significant in risk impact of unusual transaction patterns during a compliance audit could indicate gaps in existing transaction monitoring processes. This may require a reassessment of the identified risk and corresponding control measures for transaction monitoring.

- **Business model updates:**
  Expanding into new geographical markets, especially those categorized as high-risk jurisdictions, can significantly alter the trust office's risk profile. This expansion may require an updated SIRA to address newly emerging risks.

- **Incidents and remarkable events:**
  Significant events, such as data breaches, client fraud, or operational disruptions, highlight vulnerabilities within the trust office's processes or controls. These events serve as critical triggers for re-evaluating the SIRA and implementing enhanced risk management measures.

- **New products:**
  The introduction of innovative products, can create new risk factors by exposing the trust office to increased vulnerabilities, such as fraud, misuse, or regulatory scrutiny. A thorough analysis of their potential implications is essential to ensure compliance and safeguard against unforeseen challenges.

- **New technology:**
  The adoption of new technologies, such as artificial intelligence, blockchain, or advanced data analytics, introduces both opportunities and risks, particularly in areas like cybersecurity, data privacy, and operational integrity. Conducting comprehensive risk assessments is critical to evaluate their impact and implement effective controls to mitigate potential vulnerabilities.

Testing and compliance monitoring plan

To ensure the effectiveness of control measures, a compliance monitoring plan should be implemented for testing. This plan should include periodic reviews of key processes, sample testing of client files, and validation of transaction monitoring systems. It is critical to evaluate the adherence of the trust office's practices to internal policies and regulatory requirements.

Additionally, findings from testing should be documented and periodically reported to management, along with recommended corrective actions to address identified gaps or deficiencies. By integrating testing and monitoring into regular operations or into the **compliance monitoring plan**, trust offices can strengthen compliance frameworks and demonstrate a proactive approach to risk management.

7 New DNB Guidance

DNB has released a consultation version of the updated SIRA Good Practices on November 19, 2024, which will replace the 2015 guidelines and also released DNB Good Practices WTT2018 which references the SIRA.

DNB SIRA Good Practices (old version)

From this consultation version the approach of the SIRA cycle remains the same with Risk Identification, Risk Analysis, Risk Control and Risk Monitoring. The new document emphasizes that the provided good practices are indicative, allowing institutions the flexibility to choose different approaches, provided they comply with laws and regulations.

The updated guidelines place greater emphasis on data and the organisational overview to better define the risks and implement effective controls. Institution-specific is understood to mean:

- Appropriate to the risks of the institution
- Appropriate to the profile of the institution
- Appropriate to the client portfolio

Additionally, the new document highlights the value of data analysis in preparing a SIRA, encouraging institutions to incorporate data-driven insights into their risk assessments. These revisions aim to enhance the practical application of SIRA, promoting a more dynamic and tailored approach to integrity risk management.

New Considerations from DNB SIRA Good Practices

To further enhance the SIRA process, organisations should refer to the **De Nederlandsche Bank (DNB) Good Practices**, which outline comprehensive guidelines and examples for implementing effective SIRA practices. These insights can be integrated into the organisational overview to better address emerging risks:

- **Focus on Continuous Risk Assessment**

The DNB Good Practices highlight the importance of continuous and dynamic risk assessment rather than relying on static models. By regularly updating the organisational overview with real-time data and industry developments, organisations can identify and address emerging risks promptly, ensuring the SIRA remains relevant and effective. The yearly IRAP data can be used as the basis to address the focus areas.

- **Integration of ESG (Environmental, Social, and Governance) Risks**

Organisations should also incorporate ESG risks into their SIRA scenarios, as outlined in the DNB guidance. For instance, exposure to industries with poor environmental practices or social governance concerns might lead to scenarios such as “Increased Reputational Risks from ESG Non-Compliance.” This enhances the risk identification process by aligning it with broader regulatory and societal expectations.

- **Emphasis on Proportionality and Customisation**

The guidance stresses proportionality in SIRA implementation, urging organisations to tailor their assessments based on size, complexity, and operational scope. For example, a smaller trust office might focus more narrowly on specific high-risk areas.