Holland Quaestor

ASSOCIATION OF QUALITY
CORPORATE SERVICES PROVIDERS

Practical Guidance: SIRA Framework & Methodology for Trust Offices

Integer

Onafhankelijk

Betrouwbaar

Duurzaam

Professioneel

Content

1 Purpose

This guidance provides next to the **Holland Quaestor SIRA Framework & Methodology** for trust offices a practical framework for assessing and scoring risks based on their **likelihood** (the probability that a risk event will occur) and **impact** (the severity of the consequences if the event occurs). The added **Matrix** will help to prioritize risks and allocate resources effectively to mitigate them. This guidance should not be seen as a mandatory number to be followed one-on-one but provides insight into what the SIRA analysis process could look like in reality.

2 Likelihood Scale

The likelihood scale measures how probable it is that a risk or event will occur. Assigning a score to likelihood helps in assessing the probability based on historical data, expert judgment, or other indicators.

Scale Definitions:

Likelihood Level	Definition	Score
Rare	The event is highly unlikely, and there is no precedent or minimal possibility of occurrence. Example timespan: Within 5 years	1
Unlikely	The event could occur but is improbable. It has happened rarely in the past. Example timespan: 2-5 years	2
Possible	The event might occur occasionally but is not frequent. Example timespan: 1 year - 2 years	3
Likely	The event is expected to occur with regularity based on past patterns or current indicators. Example Timespan: 3 months – 1 year	4
Almost Certain	The event is highly likely to occur and could happen frequently or in the near future. Example timespan: within 3 months	5

3 Impact Scale

The impact scale measures the severity of the consequences if a risk event occurs. The scale is designed to cover a wide range of impacts, from minor to catastrophic.

Scale Definitions:

Impact Level	Definition	Score
Insignificant	Little or no impact. No significant consequences for operations, finance*, reputation, or regulatory compliance	1
Minor	Some impact on operations or finance but manageable. Minor legal, regulatory, or reputational consequences.	2
Moderate	Noticeable disruption to business, financial losses, or reputational damage. May involve regulatory intervention or moderate legal consequences.	3

Impact Level	Definition	Score
Major	Significant financial loss, severe reputational damage, or operational disruption. Likely to attract regulatory scrutiny or legal consequences.	4
Catastrophic	Major disruption to business operations, severe financial impact, or irreparable reputational damage. High likelihood of legal action or regulatory sanctions.	5

It is customary to use a financial impact scale based on EBITDA/Revenue% or quantitative thresholds depending on size of the trust-office.

4 Likelihood and Impact Matrix

The matrix is a combination of the likelihood and impact scores to give a **risk rating**. This rating guides the prioritization of risks and helps determine the level of management attention required.

Risk Rating Matrix:

Likelihood/ Impact	Impact: Insignificant (1)	Impact: Minor (2)	Impact: Moderate (3)	Impact: Major (4)	Impact: Catastrophic (5)
Likelihood: Rare (1)	1 (Low)	2 (Low)	3 (Low)	4 (Moderate)	5 (Moderate)
Likelihood: Unlikely (2)	2 (Low)	4 (Moderate)	6 (Moderate)	8 (High)	10 (High)
Likelihood: Possible (3)	3 (Low)	6 (Moderate)	9 (High)	12 (High)	15 (Very High)
Likelihood: Likely (4)	4 (Moderate)	8 (High)	12 (High)	16 (Very High)	20 (Very High)
Likelihood: Almost Certain (5)	5 (Moderate)	10 (High)	15 (Very High)	20 (Very High)	25 (Very High)

5 Risk Treatment Guidance

Once a risk rating is determined using the matrix, the urgency and scope of mitigating actions should be proportionate to the assessed risk level.:

Risk Rating	Action Required
1-3: Low	Monitor periodically. Risks in this category are minor and do not require immediate action.
4-7: Moderate	Develop a risk mitigation plan. Regularly monitor these risks, ensuring controls are in place and functioning.

Risk Rating	Action Required
8-12: High	Immediate attention required. Mitigate risks by strengthening controls, procedures, or oversight.
13-25: Very High	Immediate and robust action is required. These risks pose a significant threat and need urgent mitigation efforts.

6 Examples of Likelihood and Impact Assessment

- **Scenario 1: Sanctions Evasion Using Dual-Use Goods**
    - **Likelihood**: Possible (3) – Dual-use goods have been identified as a common vector for sanctions evasion globally.
    - **Impact**: Major (4) – If sanctions are evaded, it could lead to significant legal and financial consequences, including regulatory fines.
    - **Risk Score**: 12 (Very High)
    - **Example Time and Action Plan:** Within 3 months, conduct a full review of all clients and transactions involving dual-use goods, enhance screening procedures to include end-use and end-user declarations, and provide targeted sanctions compliance training to relevant staff.
- **Scenario 2: Complex Ownership Structures in Sanctioned Countries**
    - **Likelihood**: Likely (4) – Complex structures are increasingly used to hide beneficial ownership and circumvent sanctions.
    - **Impact**: Catastrophic (5) – Severe legal consequences, including blacklisting and criminal charges, are possible.
    - **Risk Score**: 20 (Very High)
    - **Example Time and Action Plan:** Within 1 month, implement enhanced due diligence measures for all clients with ties to high-risk jurisdictions, including mandatory ownership structure mapping, senior management escalation, and external legal review for new onboarding requests

7 Tips for Using the Likelihood and Impact Scale Matrix

- **Use objective data where possible**: Base likelihood and impact assessments on historical data, alert and incident recordings, industry trends, or regulatory guidance.
- **Engage multiple stakeholders**: Involve management, legal, compliance, and operational teams to ensure all relevant risks are considered. For example, a dedicated team from various disciplines is established that will provide input from diverse expertise and perspectives.
- **Reassess periodically**: Regularly update your risk matrix, especially when significant events occur or new information becomes available. At least annually review if information is still accurate.

- **Document everything**: Ensure that each risk assessment and its rationale are documented for future audits or reviews e.g. by keeping notes of meetings, versions of the SIRA and reporting to the board.

8 Departments and Key Stakeholders Involved

- **Risk management department**: Coordinates the SIRA process and consolidates findings, provide SIRA and risk trainings.
- **Compliance department**: Provides regulatory insights, assesses control effectiveness and ensures alignment with legal requirements and perform trainings; also insights from the compliance monitoring are provided.
- **Legal department**: Assesses potential legal implications of identified risks for the trust office as well as specific client related risks from service provision to those clients.
- **Operations department**: Identifies operational risks and monitors internal controls.
- **IT department**: Assesses risks related to cybersecurity, data privacy, and IT infrastructure.
- **Finance department:** Provides financial data and insights for the trust office.
- **Financial Account Management**:: Provides information on financial integrity and potential risks from transaction monitoring for specific clients.
- **Internal audit department**: Verifies the effectiveness of risk management processes and internal controls.
- **Senior management (including if relevant CEO/CFO/COO)**: Reviews final SIRA reports and ensures that action plans are implemented.
- **Board of directors**: Is responsible and will need to approve the actions outcome of the SIRA. Provides oversight and approves high-level risk mitigation strategies.

9 Key Steps in the SIRA Process

Step 0: Define risk appetite

- **Senior management,** in consultation with Compliance and Risk Management, defines the organization's overall risk appetite and tolerance levels. This sets the boundaries for acceptable risk-taking and provides a reference point for the SIRA process.
- **Risk Appetite:** The risk appetite should be documented and aligned with regulatory expectations (e.g., WTT, WWFT, DNB SIRA guidance) and internal governance frameworks
- **Risk appetite statements** should cover integrity, compliance, operational, financial crime, and reputational risks, and indicate when escalation to the Board is required.

Departments involved: Senior management, Board, Compliance, Risk Management.

Step 1: Define scope and frequency

- **Risk Management/ Compliance** coordinates with all departments to define the scope of the SIRA. This includes identifying key risk areas such as compliance, financial crime, cybersecurity, and operational risks.

- **Frequency**: At least an annual SIRA review is recommended, with potential for more frequent (partial) reviews in high-risk areas. Trigger events like incidents may impact risk scenario analyses and could result in frequenter SIRA reviews (event-driven SIRA cycle).

Departments involved: Risk Management, Compliance, IT, Operations, Finance, Legal, senior management.

Step 2: Risk identification

- Each department identifies specific risks within their areas of responsibility. These risks could range from regulatory compliance breaches and alerts, operational disruptions, cybersecurity threats, or financial misreporting.
- Risks are categorized into key risk domains such as compliance risk, money laundering, terrorism financing, financial crime risk, operational risk, cybersecurity risk, and reputational risk. It is recommended to use DNB guidance SIRA typologies to avoid risk areas missed. Additionally, it is optional to include privacy related risks as well because of the integrity nature of those risks.

Departments involved: All.

Step 3: Risk assessment

- Assess the likelihood and impact of each identified risk using a **Likelihood** and **Impact Scale Matrix**.
- Departments assign likelihood and impact scores to their identified risks based on historical data, industry trends, and current operational conditions.

Departments involved: All, led by Risk Management.

Step 4: Consolidation of risk data

- **Risk Management** consolidates the risk data from all departments, combining likelihood and impact assessments into an overall risk profile for the organization.
- **Compliance** ensures that all identified risks align with regulatory requirements and are updated to reflect any changes in law or regulation.

Departments involved: Risk Management, Compliance.

Step 5: Risk Mitigation planning

- For each identified risk, departments (and their appointed risk owner) suggest mitigation strategies. This includes measures, controls, policies, procedures, and technologies to minimize or eliminate the risks. Controls are coordinated with stakeholders like control owners (designated responsible persons providing the update on the actions) to ensure they are practical and effective in practice.
- **Operations** / first line and **IT** ensure that practical, real-time controls are in place, such as automated monitoring systems for sanctions screening.
- **Finance** reviews financial controls to ensure there are checks and balances to prevent financial crimes like money laundering.
- **Senior Management:** To ensure alignment and support it is recommended to include a senior management member early in the process and provide required information.

Departments involved: All, led by Operations, IT, and Finance.

Step 6: Management review and approval

- **Senior Management** reviews the consolidated SIRA report and risk mitigation strategies.
- Any significant risks that require high-level attention are escalated to the **Board of Directors** for review.

Departments involved: Senior Management, Board of Directors.

Step 7: Action plan implementation

- After approval, departments implement the risk mitigation strategies. This may involve updating policies, procedures, internal controls, improving reporting mechanisms, or deploying new technology.

Departments Involved: All, led by Operations, IT, Finance, and Compliance.

Step 8: Monitoring and reporting

- **Risk Management** and if relevant **Internal Audit** monitor the effectiveness of the design and operations of the risk controls, ensuring they are being followed and are mitigating the identified risks. Risk Management also provides the key risk indicator information to monitor risk exposure.
- **Compliance** and if applicable **Internal Audit** report back to management with updates on risk status, control effectiveness, any new risks identified, deviation on risk tolerance and determine a risk response to accept/mitigate/avoid/transfer the residual risk.

Departments involved: Risk Management, Internal Audit, Compliance.

Step 9: Periodic reviews and adjustments

- As part of the SIRA review cycle, risks and controls are revisited periodically to ensure relevance and effectiveness.
- New risks are added to the SIRA, and existing risks are reevaluated based on updated information and trigger events.
- Risk can also be retired or set at in-active if deemed not relevant anymore due to changes in organization, client portfolio or external developments (risk based approach). The review should aim to have a set of risk (scenarios) that are relevant and specific to the nature and size of the Trust Office and its client portfolio

Departments involved: All.

10 Practical Considerations

- **Technology integration**: Implement software tools to track risks, assessments, and mitigation actions across departments. This can streamline the SIRA process and ensure accessibility and transparency.
- **Accessibility**: Ensure that the SIRA should always be easily accessible and available for all relevant employees.
- **Clear communication channels**: Ensure continuous communication between departments to keep the process collaborative and up-to-date.
- **Documentation**: Maintain detailed documentation at every step of the SIRA process for audit trails and regulatory review.

- **Training and awareness**: Provide ongoing training for employees on how to identify risks and their role in the SIRA process. As well as training on how to implement the SIRA in their day-to-day job.
- **Workshops:** Use workshops to discuss risks, impacts and scenarios with different relevant groups in the organization who are dealing with the sort of risks.

11 Creation of Scenarios

The example SIRA scenarios provided are general topics within the trust sector and must be tailored to reflect entity specific situations. This involves linking the scenarios to relevant sources of indicators, such as incidents, IRAP data, audit findings. Additionally, each scenario should address a practical situation and illustrate how it could materialize as an integrity risk for the entity or the financial sector as a whole. Below are a few examples demonstrating how to refine and develop a scenario into a more specific and concrete one.

Examples on *evolving* SIRA Scenario Matrix:

Bribery and Corruption – Third-party logistics provider

a. SIRA Matrix short scenario: A third-party logistics provider of a client entity has bribed customs officials to expedite the clearance of goods.
b. Final SIRA scenario:
Risk: Bribery
Category: Client activities
Scenario: The adverse media screening resulted in a hit on a third-party logistics provider used by your Client Entity. It has bribed customs officials in a high-risk foreign jurisdiction to expedite the clearance of goods. Even though the client was unaware of these payments, the association with this provider creates indirect exposure. Authorities may investigate due diligence practices, and stakeholders could question commitment to ethical business conduct, leading to regulatory penalties and reputational damage.
c. Indicators:
• Adverse media hit linked to bribery or corruption.
• Client operating in or using suppliers from high-risk jurisdictions.
• Lack of visibility over third-party relationships or sub-contractors.
d. Control Measures:
• Implement third-party screening for suppliers and contractors of clients (Transaction Monitoring).
• Check if the supplier is in line with the client's compliance and anti-bribery policies.
• Escalate high-risk third-party relationships to senior management or the compliance committee.

Bribery and Corruption – Lavish gifts and political contributions

a. SIRA Matrix short scenario: Client Entity provides lavish gifts to potential partners, risking bribery allegations.
b. SIRA scenario: From the internal incident register the following was noted. A real estate development client entity is found to have made multiple donations to a local mayoral candidate's campaign through shell companies, significantly exceeding legal contribution limits. Shortly after the candidate wins the election, the client is granted expedited approval for a controversial zoning change critical to one of their projects. The donations were concealed in campaign finance reports as coming from unrelated entities. Investigators discover that the company processed the client's fund transfers, raising questions about the adequacy of the due diligence and transaction monitoring processes in identifying and reporting potential illegal political contributions.
c. Indicators:
• Client makes large or frequent donations to political entities.
• Use of shell companies or non-transparent ownership structures.
• Sudden regulatory approvals linked to prior payments.
d. Control Measures:
• Define clear thresholds and reporting obligations for gifts and hospitality in client contracts.
• Include questions on gifting policies in the integrity risk assessment and client due diligence.
• Conduct event-driven file reviews to identify red flags in expenses and payments and to assess whether the client or client entity still fits the risk appetite.
• Notify MLRO to see if further reporting to the authorities is required.

Cybercrime – Phishing and data breach

a. SIRA Matrix short scenario: Phishing emails lead employees to reveal sensitive and confidential data of clients.
b. SIRA scenario: From the cyber security incident register: A member of the legal account management team receives a phishing email disguised as a legitimate communication from the Dutch Tax Authority (Belastingdienst), asking for confirmation of login credentials to access a tax-related form. The employee, believing it to be legitimate, enters sensitive information, including access credentials to the trust office's client database. This compromise leads to unauthorized access to several client profiles, potentially exposing confidential financial and personal data.
c. Indicators:
• Employees report suspicious emails or links.
• Login attempts from unusual IP addresses or locations.
• Unexpected access to client files or data movement detected.
d. Control Measures:
• Implement multi-factor authentication for all internal systems.
• Conduct regular phishing awareness training and simulated phishing campaigns.
• Install email filtering and anti-phishing software to block malicious emails.
• Restrict access to sensitive systems based on role and least privilege principle.
• Establish an incident response protocol with immediate credential revocation and client notification procedures.

External Fraud – Fake identification documents

a. SIRA Matrix short scenario: Fraudsters use false identities to open accounts.
b. SIRA scenario: Engagement parties/Clients submitted falsified identification documents, such as forged passports and utility bills, to open trust accounts under the guise of legitimate clients. The documents were sophisticated enough to evade standard verification procedures, and the accounts

are used for the illicit transfer of funds. The trust office's initial verification process fails to detect the fraudulent nature of the documents, risking the facilitation of money laundering activities.

c. Indicators:

• Poor quality or inconsistencies in ID documents or utility bills.
• Clients unwilling to provide originals or additional verification.
• Suspicious urgency or pressure during onboarding.

d. Control Measures:

• Implement advanced document verification tools for onboarding.
• Use biometric verification or video identification for remote clients.
• Require secondary verification for high-risk jurisdictions or suspicious profiles.
• Perform random quality assurance checks on KYC documentation.
• Update staff training on spotting forged documents and identity fraud indicators.

Internal Fraud – Employee falsifies records

a. SIRA Matrix short scenario: Employees engage in fraudulent activities, such as falsifying documents.

b. SIRA scenario: A senior officer within the trust office falsifies client transaction records and reports to cover up financial mismanagement. The employee creates fake documents to alter transaction histories and manipulate the outcome of audits, effectively embezzling client funds and obscuring the traces of fraudulent activity. This results in financial losses and exposes the trust office to regulatory scrutiny.

c. Indicators:

• Unexplained changes in transaction logs or records.
• Employee resistance to oversight or audit activities.
• Inconsistent data between systems or unusual reconciliation outcomes.

d. Control Measures:

• Implement strict segregation of duties for transaction processing and reporting.
• Enable audit logging and alerting for changes made in client records or financial data.
• Conduct periodic internal audits and independent reconciliation checks.
• Enforce dual-authorization requirements for critical financial actions.
• Introduce an anonymous whistleblower hotline and response protocol.