gisf

# Risk Appetite Statements: A guide for NGOs

## May 2026

## 1. Introduction

No organisation can achieve its objectives without taking risks, and defining a clear risk appetite establishes the parameters within which teams can operate confidently and effectively.

This guide explains what a Risk Appetite Statement (RAS) is, outlines its value, and provides practical guidance on how to develop one. While the focus is on security risk, the broader aim is to support the integration of SRM into broad organisation-wide risk management (Enterprise Risk Management - ERM), ensuring that all risks are considered holistically rather than in isolation. By leveraging the strengths of existing security risk practices, organisations can strengthen overall risk management frameworks to create a more coherent, aligned, and effective approach.

### Audience

This guidance can support security risk management (SRM) practitioners who want to ensure that security considerations are integrated into wider organisational risk management processes, rather than managed in isolation.

It also supports senior leadership and governing bodies by explaining the strategic value of a risk appetite statement, how it strengthens governance and accountability, and practical steps for developing and implementing one effectively.

Funded by the European Union

This guide is made possible with the support of the European Union.

# Table of Contents

## 2. What is Risk Appetite Statement?

A Risk Appetite Statement (RAS) is typically a documented consensus declaration made by an organisation's leadership (usually the board, as owners of the risk, in consultation with senior management) that defines the types and amount of risk the organisation is willing to take in pursuit of its strategic objectives. An RAS is rarely made public. Some organisations may choose not to formalise the document due to legal considerations. However, its key purpose is to align decision-making and risk management practices across the organisation and ensure that there is mutual understanding amongst the owners of the risk. Such a statement typically:

- Clarifies acceptable levels of risk (e.g., financial, reputational, operational).
- Guides decision-making when taking on new projects, partnerships, or funding sources, or when taking a major programmatic decision (e.g., to stay or go, etc)
- Demonstrates accountability to regulators, donors, and beneficiaries by showing that risks are being managed responsibly.

An RAS is deliberately high-level and does not try to account for every situation. It feeds into the systems and processes in place to ensure that risk owners manage the risks in their specific context within the overall risk appetite.

### Risk terminology: risk appetite, capacity, attitude, tolerance, and threshold

There are several terms similar to risk appetite which can be used interchangeably but have different meanings and interpretations. It is important to understand the differences between these terms. [1]

| Definition | Key Questions | Example |
|---|---|---|
| **Risk appetite** is about what an organisation wants to do and how it goes about it. It therefore becomes the board's responsibility to define this all-important part of the risk management system. | **Do we want to take the risk?** (Strategic choice within capacity) | "We have a low appetite for reputational risks." |
| **Risk attitude** is an organisation's cultural and behavioural approach to risk. It reflects the mindset of decision-makers (board, leadership, staff) toward uncertainty and opportunity. | **How do we feel about risk?** (Cultural or psychological stance). | "We have a cautious attitude to regulatory risks, as a result of past compliance issues, even though our capacity is high." |

[1] Whilst these terms are interlinked, for the purpose of this guide we are focusing on risk appetite. While it's possible, and even desirable, to define security tolerances and thresholds, doing so can be difficult because risk is contextual, subjective, and dynamic. This paper does not lay out the benefits (and challenges) of doing so, or seek to outline the practical approaches to make thresholds or tolerances workable.

| Definition | Key Questions | Example |
|---|---|---|
| **Risk capacity** is the objective ability of an organisation to take on risk, given its operational footprint and resources, and its risk management capabilities and expertise. It reflects the maximum level of risk the NGO could withstand without jeopardising its mission or survival. | **Can we take the risk?** (Objective limit based on resources) | "We have strong reserves and diversified funding, resulting in a higher capacity to take risks (e.g., trying an innovative project or working in a fragile state)." |
| **Risk tolerance** is the range of acceptable variation around the risk appetite before management action is needed. It is often expressed as a band or buffer (e.g., ±10per centfrom appetite) and gives flexibility, acknowledging that risks fluctuate in real life without triggering constant alarms | **How far can we take this risk?** (Accepted variance or deviation around risk appetite, usually with specific metrics). | "We are willing to tolerate up to 20 per cent of planned field activities being delayed per quarter, due to local unrest or environmental hazards." |
| **Risk threshold** is the specific point or limit at which a risk becomes unacceptable and requires escalation or intervention. | **At what exact point would we consider this risk unacceptable?** (Trigger for predefined action or escalation). | "Any potential incident with high-profile exposure (>7/10 on internal media impact scale) must undergo crisis communication protocol." |

**Resource – GISF glossary**

While risk appetite is about the pursuit of risk, risk tolerance is about what you can allow the organisation to deal with. Risk capacity is resource-driven, determined by factors like financial reserves, staff skills, systems, donor support, and legal obligations. It is also impacted by external factors such as regulatory frameworks, donor requirements, and contractual obligations. Unlike risk appetite (a choice), risk capacity is a constraint; if you exceed it, the NGO could fail or face serious consequences. See the following examples for further illustration of the terminology:

## Example 1: Operating in Conflict Zones

- **Capacity:** NGO could technically operate in three high-risk regions with its current staff/security resources.
- **Appetite:** Leadership chooses to limit this to two regions.
- **Tolerance:** A short-term overrun (e.g., temporary entry into a third region for disaster response) may be acceptable, but sustained engagement beyond two regions is outside tolerance and not allowed.
- **Threshold:** If engagement in the third region looks like it will exceed three months, board-level review and mitigation actions are required (e.g., temporary recruitment/surge capacity).

## Example 2: Foreign Funding Dependence

- **Capacity:** The NGO could technically survive with up to 80 per cent of its income from foreign donors, but anything higher would leave it extremely vulnerable if funding stopped.
- **Appetite:** The board decides it is comfortable with up to 50 per cent of total income from foreign donors, as a strategic choice to balance flexibility with stability.
- **Tolerance:** The NGO sets an acceptable variation of ±10 per cent around that appetite. If foreign funding reaches 60 per cent, this is still within tolerance - but requires closer monitoring.
- **Threshold:** If it goes beyond 60 per cent, it breaches tolerance, triggering a board-level review and mitigation actions (e.g., diversifying funding sources, tightening reserves).

It is important to note that an organisation's overall risk appetite statement will not automatically translate to all contexts. The board may wish to repeat the process for specific geographic locations, business units or objectives, informed by the overall RAS.

# 3. Why have a Risk Appetite Statement?

NGOs operate with legal, donor and compliance requirements that establish minimum standards for conduct and accountability. However, these external constraints do not determine how much operational, security, financial, or reputational risk an organisation is prepared to accept in pursuit of its mission.

A risk appetite statement fills this gap by defining the organisation's own boundaries for risk-taking, supporting more consistent decision-making, stronger governance, and clearer accountability around liability and duty of care.

It supports but does not replace decision-making with regards to specific risks. It allows boards to empower and delegate decision-making within the organisation, and increase the efficiency of decision-making. It can provide a common starting point from which to assess and approach risks.

A well-defined RAS therefore becomes a practical bridge between security risk management and broader organisational risk management - supporting better decision-making, stronger governance, and more coherent risk oversight.

## Benefits for NGOs

**1. Aligns strategy and risk**
A risk appetite statement ensures that the NGO's activities and initiatives remain within defined risk boundaries that support its mission and long-term strategy. This helps avoid unintended risk-taking and provides clarity during decision-making. Security teams can contribute by providing context-specific risk analysis, helping leadership understand what levels of risk are realistic and manageable in different operational environments.

**2. Strengthens risk management**
By clearly defining acceptable levels of risk, NGOs can better monitor and control exposure. Security professionals can enhance this by applying established SRM methodologies, such as threat analysis, risk assessments, and mitigation planning, to other categories of risk.

**3. Improves communication and accountability**
An RAS sets a clear tone from leadership and creates a shared understanding of risk across the organisation. Security teams, often already communicating risk to diverse audiences, can help translate complex risk concepts into practical guidance for staff and partners.

**4. Supports compliance and builds credibility**
A structured approach to risk demonstrates accountability to regulators and donors. Security functions contribute by ensuring that risk decisions, particularly in high-risk contexts, are documented, justified, and aligned with organisational thresholds.

**5. Supports financial and operational management**
NGOs often operate with limited resources. An RAS helps balance ambition with sustainability. Security teams can support this by identifying cost-effective risk mitigation measures and advising on when risks may be too high relative to available resources.

**6. Enhances organisational culture**
A clear risk appetite empowers staff to make informed decisions. Security professionals can reinforce this by promoting a proactive risk culture: encouraging critical thinking, awareness, and responsible risk-taking across all levels of the organisation.

## 4. When to establish a Risk Appetite Statement?

While it is possible to introduce a formal Risk Appetite Statement at any time, it may be more useful for an organisation to implement risk appetite when they are establishing, or have already established, strong governance practices around risk management. If the potential benefits of risk appetite are to be realised, the following prerequisites should ideally be in place. These prerequisites include:

- Having clear and well-defined strategic objectives;
- Senior management and staff being sufficiently aware of current risks as well as risk management concepts, and the processes and systems of the organisation;
- Having basic risk management governance and accountability structures in place;
- Having a process and repository for collecting and analysing risks and risk information across the organisation (including in field locations if applicable) enabling risk trade off decisions;
- Having the capacity to report on actual levels of risk through measurable indicators in a timely manner; and
- Having the capacity to act in response to reported risk information in a timely and effective manner. If an organisation attempts to implement risk appetite without these prerequisites in place, there is a danger that it will not realise the benefits, whilst still incurring costs, which may in turn lead to additional resistance. [2]

Not having these prerequisites may be an indication that risk management is not yet embedded within an organisation, which may make setting risk appetite more difficult, though not impossible.

[2] Source: HLCM Guidelines on Risk Appetite Statements

## Key situations for use:

| When | Why | Example |
|---|---|---|
| During strategic planning | Risk appetite defines the level of risk the organisation is willing to accept to achieve its mission. Aligning it with your strategic goals ensures decisions are consistent across programmes and operations. | Before launching a new field programme in a high-risk area, the NGO knows what level of security, financial, or reputational risk is acceptable. |
| When enhancing a risk management framework | A risk appetite statement is foundational to risk assessment, monitoring, and reporting. It sets the boundaries for risk tolerance and informs risk mitigation strategies. | Defining thresholds for staff safety, data security, and operational disruption becomes meaningful once you've stated what risks are acceptable. |
| Before expanding operations | Are there limits on collecting or sharing data? If your NGO is scaling up geographically or programmatically, a clear risk appetite helps avoid overexposure to financial, operational, or security risks. | Deciding whether to operate in a conflict zone or invest in new technology platforms depends on your appetite for these risks. |
| Before engaging (new) donors or partners | A clear risk appetite can reassure donors and partners that the NGO manages risks consciously and proactively. | Donors may require evidence that high-risk programmes have risk boundaries aligned with organisational values. |

## Differences for INGOs and NNGOs

While the purpose of a Risk Appetite Statement (RAS) is broadly the same for both international NGOs (INGOs) and national NGOs (NNGOs) - to define how much risk an organisation is willing to accept in pursuit of its objectives - the way this is articulated and applied can differ significantly due to their distinct contexts.

INGOs often operate across multiple countries, with complex governance structures, layered decision-making processes, and diverse stakeholder expectations, including donors, headquarters, and field offices. This typically results in a more formalised and standardised RAS, with clearly defined thresholds, escalation processes, and accountability mechanisms. Their broader operational reach and higher international visibility can also lead to a more conservative approach in certain areas, particularly reputational and compliance risks, while still accepting higher levels of programmatic or security risk in order to operate in high-need, high-risk environments.

In contrast, NNGOs are often more locally embedded, with flatter governance structures and more agile decision-making processes. Their risk appetite may be less formally documented but more adaptive in practice, reflecting a closer proximity to communities and a nuanced understanding of the local context. NNGOs may accept different types or levels of risk based on their acceptance within communities and their operational realities. However, they may also face constraints in terms of resources, systems, and formal risk management structures, which can influence how explicitly risk appetite is defined and communicated.

Security structures also play a role. INGOs are more likely to have dedicated security risk management functions that contribute systematically to the RAS, whereas in NNGOs, security responsibilities may be more decentralised or integrated into operational roles. This can affect the level of detail, consistency, and technical framing of security-related risk appetite.

As above, reputational exposure differs. INGOs often face global scrutiny and donor expectations, shaping a more cautious and compliance-driven articulation of risk appetite. NNGOs, while not immune to reputational risk, may experience it more locally, influencing how they prioritise and balance risks.

In practice, these differences mean that while both INGOs and NNGOs benefit from having an RAS, the content, level of detail, and implementation approach should be tailored to reflect their governance, capacities, and operational realities. A well-designed RAS is therefore not one-size-fits-all, but context-specific, grounded in the organisation's identity, risk culture, and the environments in which it operates.

## 5. Process for creating a Risk Appetite Statement

Creating an RAS is both an art (capturing the organisation's culture and strategy) and a structured process.

### Step 1: Understand Context

- Map the operational environment, organisational priorities, legal and regulatory obligations, and risk landscape to understand the scope within which the organisation operates.

**Security Role:** Security Focal Points can provide critical insights into threat environments, incident trends, and operational constraints. Their knowledge of security realities helps ensure the RAS reflects both internal vulnerabilities and external threats, grounding risk appetite in real-world operational conditions.

### Step 2: Engage Leadership

- Work with leadership to align the RAS with strategic objectives, organisational values, and decision-making priorities. If there is a Board, they typically set the overall tone: how much risk is acceptable in pursuit of objectives, whilst senior management supports translation into practical limits, policies, and tolerances.

**Security Role:** SFPs can advise leadership on security implications of strategic choices, helping translate complex threat information into actionable guidance. They can also highlight scenarios where security risk may influence operational risk decisions, ensuring leadership has a full picture when setting appetite thresholds.

**Tool:** Annex 6.1 Questions for the Board
**Resource:** GISF's Bold Steps, Quiet Impact: Pathways to Influencing and Engaging Executive Leadership in Security Risk Management

### Step 3: Define Risk Categories

- Identify and categorise the key risks the organisation faces, including financial, operational, reputational, compliance, and security risks. Typical categories could include:
  - Strategic risk (e.g., entering new markets)
  - Financial risk (e.g., credit, liquidity, market risk)
  - Operational risk (e.g., systems failures, fraud, cyber)
  - Security Risk
  - Compliance/legal risk (e.g., regulatory breaches, sanctions)
  - Reputational risk

**Security Role:** SFPs can lead on defining and refining security risk categories, ensuring they are comprehensive (e.g., threats to staff, assets, information, and operations) and aligned with existing SRM frameworks. They can also support identifying interconnections between security risks and other categories, enabling a holistic approach.

**Tool:** Annex 6.3 Risk Appetite Statement (Template), section 5 on risk categories.

## Step 4: Set Qualitative Statements and Metrics

- Describe the level of risk the organisation is willing to accept in each category, using both qualitative statements and quantitative thresholds where possible. Develop clear, practical statements which guide decisions, such as:
  - "The organisation has low appetite for risks that could result in serious harm or death to staff."
  - "The organisation has moderate appetite for operating in volatile environments where mitigation measures significantly reduce likelihood."
  - "The organisation has no appetite for operating where staff detention is highly likely and mitigation options are minimal."

If possible, translate qualitative appetite into measurable boundaries, for example:

- Operational risk: "No single IT outage may exceed 2 hours without escalation to the board."

**Security Role:** SFPs can contribute by translating security assessments into clear statements about acceptable and unacceptable risk levels. They can provide metrics such as incident frequency tolerances, acceptable exposure levels, or operational limits in high-risk contexts, helping quantify risk appetite where feasible.

## Step 5: Document and Communicate

- Create a clear, accessible RAS document and ensure it is communicated to all relevant staff and stakeholders.

**Security Role:** SFPs can help ensure that security-related risk appetite is clearly documented, illustrated with practical examples, and communicated to field teams. They can also provide guidance on how staff should apply security thresholds in operational decision-making, reinforcing consistency across the organisation.

## Step 6: Monitor and Review

- Continuously track risks, evaluate incidents, and periodically review the RAS to ensure it remains relevant and effective.

**Security Role:** SFPs can play a leading role in monitoring emerging threats, reviewing security incidents, and assessing whether existing risk appetite levels are still appropriate. Their ongoing analysis informs updates to the RAS, ensuring the organisation can adapt to changing environments and maintain an aligned approach to all risks.

## Critical sucess factors for RAS

Five critical success factors have been identified [3] which will increase the likelihood of risk appetite statements being operationalised effectively. The questions below are intended to help organisations respond to those success factors.

1. **Grounded with governing bodies and senior management buy-in.** Who will ultimately be accountable for risk appetite and how will senior management (and eventually the governing body) be involved in reviewing the organisation's risk maturity and risk appetite? How will risk appetite be cascaded down to business units?
2. **Clear and measurable** (to the extent possible) in defining the levels and type of risk an organisation is willing to assume in pursuit of its strategic objectives. How will the organisation ensure that risk appetite will be forward-looking and aligned with the organisation's strategic goals? How will risk trade-offs influence the levels of various risks that are connected various strategic goals.
3. **Flexible and adaptable** enough to address changing operational and strategic conditions (both internal and external) while informing decision making. How will risk appetite be tailored to the organisation? How will risk appetite take into account differing views at a strategic, tactical and operational level?
4. **Integrated and aligned** with the wider control framework, ERM framework, decision making processes and organisational culture. How will risk appetite guide decision making, facilitate measurable actions and support monitoring? How will risk appetite be developed in the context of the control framework and culture of the organisation?
5. **Sustained once established** with clear ownership and constant communication, reporting and action. How will risk appetite be communicated transparently within the organisation, and what key information will be shared with relevant stakeholders (both internal and external, as appropriate)? What processes will business units follow for communicating when risk appetite is nearing a breach or is breached and requesting technical assistance to respond?

[3] United Nations System Chief Executives Board for Coordination (CEB), High-Level Committee on Management (HLCM), Guidelines on Risk Appetite Statements (CEB/2019/HLCM/26, 16 October 2019).

## Overcoming challenges in creating a risk appetite statement: a guide for SFPs

Creating a Risk Appetite Statement (RAS) can be complex, especially in NGOs with diverse operational contexts. Below are common challenges and practical ways Security Focal Points (SFPs) can address them to ensure the RAS is meaningful, operationally relevant, and fully integrated into organisational risk management.

### Balancing top-down and bottom-up approaches

**Challenge:** A purely top-down approach risks disconnection from operational realities, while a purely bottom-up approach risks inconsistency and misalignment across the organisation.

**Practical tips for SFPs**

- Gather operational insights from field teams and translate them into high-level guidance for leadership.
- Use structured security risk assessments, incident trends, and scenario planning to bridge the gap.

**Outcome:** The RAS reflects both organisational strategy and operational realities, enhancing credibility and usability.

### Linking RAS to resilience, business continuity, and crisis management

**Challenge:** Without integration, the RAS can remain theoretical and disconnected from critical frameworks such as business continuity, crisis management, or operational resilience.

**Practical tips for SFPs**

- Map the RAS against existing security, resilience, and contingency frameworks.
- Highlight how risk thresholds affect operational decisions during emergencies (e.g., evacuation triggers, hibernation procedures, or programme suspension).

**Outcome:** Risk appetite becomes actionable and embedded in organisational preparedness and response structures.

## Engaging country teams

**Challenge:** Local teams often perceive the RAS process as extractive, providing data for headquarters with little tangible benefit for their operations.

### Practical tips for SFPs

- Position the RAS as a tool that improves local decision-making and operational safety.
- Share practical examples: travel risk guidelines, community engagement protocols, or allocation of security resources.

**Outcome:** Teams see direct benefits, improving input quality and local buy-in.

## Securing senior leadership buy-in

**Challenge:** Without visible leadership commitment, the RAS risks being ignored or inconsistently applied. Leadership may see the process as a compliance exercise rather than a strategic tool.

### Practical tips for SFPs

- Link security risk appetite to organisational priorities: staff safety, operational continuity, donor confidence, and reputation protection.
- Present evidence of security risk management successes - incidents avoided or mitigated - to illustrate tangible value.

**Outcome:** Leadership commits to and champions the RAS, ensuring alignment across all functions.

## Managing complexity and interdependence

**Challenge:** NGOs manage multiple interrelated risks (financial, operational, reputational, security). Aligning these so the RAS reflects a holistic view is complex.

### Practical tips for SFPs

- Highlight interconnections between security risks and other risk categories.
- Use visual tools like heatmaps, dependency charts, or scenario matrices to demonstrate cascading impacts and thresholds, and how risks interplay (e.g., physical security breaches resulting in digital risks).

**Outcome:** The RAS supports coordinated, organisation-wide risk management and better-informed decision-making.

## Maintaining relevance through monitoring and review

**Challenge:** Risk environments are dynamic. Without ongoing monitoring, the RAS can quickly become outdated, reducing its usefulness.

### Practical tips for SFPs

- Schedule periodic reviews with leadership and country teams to ensure thresholds remain realistic and actionable.
- Treat the RAS as a living document, updated regularly based on security incidents, emerging threats, and operational lessons.

**Outcome:** The RAS stays relevant, practical, and aligned with both organisational objectives and field realities.

# 6. Annex

## 6.1 Questions for the Board

To initiate the development of a Risk Appetite Statement (RAS), engaging the board (or senior leadership) with the right questions is critical. The aim is to draw out their implicit views on risk, translate these into clear parameters, and ensure alignment with organisational values and strategy. SFPs can play a key role by shaping and informing this discussion, particularly on how security risks influence overall risk tolerance.

Below are some core questions for the Board, followed by security-specific questions to deepen the conversation. You may inherently feel that you know the answers to these, but it is important that the Board and senior management are given the opportunity to engage on each of these.

**1. Strategic Risk and Mission**

- What level of risk are we willing to accept to achieve our mission, particularly in high-need or high-risk environments?
- What are the strategic objectives of the organisation? Are they clear? What is explicit and what is implicit in those objectives?
- What steps has the board taken to ensure oversight over the management of the risks?

**2. Boundaries and Red Lines**

- What types of risk are we not willing to accept under any circumstances (e.g., legal, ethical, safeguarding)?
- Where are our "no-go" thresholds?

**3. Trade-offs and Decision-Making**

- How do we balance competing risks (e.g., program delivery vs. staff safety, speed vs. due diligence)?
- What level of uncertainty are we comfortable with when making decisions?

**4. Reputational Risk**

- How much reputational risk are we willing to tolerate in pursuit of our objectives?
- How would we respond to negative public or donor scrutiny arising from operating in high-risk contexts?

**5. Financial and Operational Risk**

- What level of financial exposure or loss is acceptable?
- How much disruption to operations can we tolerate before taking action?

**6. Governance and Oversight**

- What level of risk requires Board visibility or approval?
- Where should decision-making authority sit across the organisation?

## Security-Specific Questions (Where SFPs can add value)

**1. Staff Safety and Duty of Care**

- What level of risk to staff safety is acceptable in delivering programmes?
- Are there clear thresholds (e.g., incident severity, threat levels) where operations must be paused or adapted?

**2. Operating in High-Risk Environments**

- Under what conditions are we willing to operate in insecure or conflict-affected areas?
- What security conditions would trigger withdrawal, relocation, or remote management?

**3. Incident Tolerance and Response**

- What types and frequency of security incidents are considered acceptable, if any?
- At what point do repeated incidents indicate that risk levels exceed our appetite?

**4. Risk Mitigation vs. Access**

- How do we balance security measures (e.g., restrictions, escorts, remote management) with maintaining humanitarian access and acceptance?
- When do mitigation measures become too restrictive for effective programme delivery?

**5. Acceptance of Residual Risk**

- After all reasonable mitigation measures are in place, how much residual security risk are we willing to accept?
- Who is accountable for accepting this residual risk?

**6. Information and Decision Thresholds**

- What level of security information or analysis does the Board expect before making decisions on high-risk operations?
- How should security risks be escalated and communicated to leadership?

## 6.2 Possible risk appetite scales

Organisations can use a range of different scales to categorise and assess their risk appetite, depending on their context, maturity, and operational needs. There is no one-size-fits-all approach—each option comes with its own strengths and limitations. The following examples outline some common approaches, highlighting their pros and cons, and how they can be applied in practice, including from a security risk management perspective.

### 1. Qualitative Scale (5-point model – most common)

A clear, narrative-based scale that works well for NGOs where risks are often non-financial.

**Pros:**

- Simple and easy to understand across all levels of the organisation
- Flexible and adaptable to different contexts and risk types
- Useful for initiating discussions with leadership

**Cons:**

- Can be vague and open to interpretation (what "high" means may differ between teams)
- Difficult to apply consistently across countries or functions
- Limited usefulness for setting clear thresholds or triggers

**Security Angle:**

- Works well in early-stage SRM or where risk management maturity is low
- However, security decisions (e.g., whether to suspend operations) often require more precision—so qualitative scales alone may not provide enough clarity for field teams
- SFPs should supplement with examples or scenarios to reduce ambiguity

**Examples:**

| | |
|---|---|
| **No Appetite (Zero Tolerance):** Will not accept under any circumstances. | Example: Fraud, corruption, safeguarding violations, regulatory breaches. |
| **Low Appetite:** Very cautious, only minimal risk-taking acceptable. | Example: Minor reputational risks in advocacy campaigns. |
| **Moderate Appetite:** Willing to accept some risk in pursuit of objectives, provided strong controls exist. | Example: Expanding into a new country with known operational challenges. |
| **High Appetite:** Open to taking significant risks where there are high potential benefits to mission delivery | Example: Piloting innovative service delivery models. |
| **Very High Appetite:** Will actively pursue risky opportunities with transformational potential | Example: Partnering with new, untested organisations in crisis zones. |

## 2. Quantitative Scales (e.g. numeric thresholds, % limits, incident frequency)

**Pros:**

- Provides clear, objective thresholds for decision-making
- Enables consistency and comparability across the organisation
- Supports monitoring, reporting, and accountability

**Cons:**

- Can be difficult to define meaningful metrics, especially for complex or unpredictable risks
- May create a false sense of precision
- Requires reliable data, which may not always be available

**Security Angle:**

- Useful for setting measurable thresholds (e.g., number of incidents, acceptable exposure levels, response times)
- However, security risks are often context-specific and dynamic, making strict quantification challenging
- SFPs should use quantitative measures selectively, combined with qualitative judgement

**Examples:**

| | |
|---|---|
| Incident Thresholds | The organisation will tolerate up to X number of security incidents per quarter in a given location, provided none exceed [defined severity level]. |
| Financial Exposure | The organisation will accept potential financial losses of up to X% of annual budget in pursuit of programme objectives. |
| Operational Disruption | Programmes may tolerate disruption of up to X days per quarter due to external risks before escalation is required. |
| Staff Exposure Limits | No more than X% of staff should be exposed to high or very high-risk environments at any given time without senior approval. |
| Response Time Metrics | All critical incidents must be responded to within X hours, with escalation to senior management within X timeframe. |
| Compliance Thresholds | The organisation has zero tolerance for legal or regulatory breaches; 100% compliance is required at all times. |

## 3. Customised scale by risk category

An NGO might adopt different appetites depending on risk type.

**Pros:**

- Reflects the reality that organisations tolerate different levels of risk across categories (e.g., low tolerance for safeguarding risk, higher for programmatic risk)
- Enables more tailored and meaningful risk appetite statements
- Supports holistic risk management across functions

**Cons:**

- More complex to design and communicate
- Risk of fragmentation if not aligned across the organisation
- Requires strong coordination to ensure consistency

**Security Angle:**

- Particularly valuable for SRM, as it allows organisations to clearly articulate their tolerance for security risk relative to other risks (e.g., financial, reputational)
- Helps clarify trade-offs (e.g., accepting higher security risk to maintain access vs. protecting staff at all costs)
- SFPs can play a key role in defining realistic security risk thresholds and ensuring alignment with operational practices

**Examples:**

| | |
|---|---|
| Financial risk | Low appetite (must protect donor funds, avoid deficits). |
| Compliance/Safeguarding Risk | Zero tolerance. |
| Operational/Delivery Risk | Moderate appetite (NGOs often work in fragile, unpredictable contexts). |
| Reputational Risk | Low to moderate (NGOs rely on donor trust). |
| Strategic/Innovation Risk | Moderate to high (open to trying new models to reach underserved populations). |

## 4. Traffic Light System (Simple, visual)

Useful for boards/trustees who want a quick grasp of tolerance.

**Pros:**

- Highly visual and intuitive - easy for quick decision-making
- Effective for communication, especially in fast-moving environments
- Aligns well with operational tools (e.g., dashboards, situation reports)

**Cons:**

- Oversimplifies complex risks
- May obscure important nuances or changes in risk levels
- Can create false confidence if not backed by clear criteria

**Security Angle:**

- Commonly used in security (e.g., threat levels, movement restrictions) and familiar to field teams
- Useful for linking risk appetite to operational decisions (e.g., "Red = no movement")
- SFPs must ensure clear definitions sit behind each colour to avoid inconsistent application across locations

**Examples:**

- Red (No tolerance): Never acceptable.
- Amber (Cautious): Limited risks allowed, tightly controlled.
- Green (Open): Risks actively pursued if they advance mission.

## 5. Mission-Impact Scale (NGO-specific)

Frames risk appetite in terms of impact on beneficiaries, which may resonate well with values-driven, non-profit organisations.

**Pros:**

- Strongly aligned with NGO values and purpose, making it intuitive for leadership and staff
- Frames risk appetite in terms of impact on beneficiaries, rather than abstract risk levels
- Encourages strategic thinking about when taking greater risks may be justified to achieve higher impact
- Can be particularly effective for engaging non-technical stakeholders and Boards
- Cons:
- Can be subjective and harder to translate into clear operational thresholds
- Risk of being interpreted differently across teams or contexts
- May underplay operational, compliance, or security constraints if not balanced with other frameworks
- Requires careful definition to avoid overly aspirational or vague language

**Security Angle:**

- Highly relevant for security decision-making in NGOs, where trade-offs between access and safety are common
- Helps frame discussions such as: when is it acceptable to take on higher security risk to reach vulnerable populations?
- Supports SFPs in linking security risk decisions directly to programme impact, strengthening their strategic influence
- However, SFPs must ensure that "mission-transforming" ambitions do not override critical duty of care obligations—clear red lines and minimum security standards are still essential
- Works best when combined with more concrete scales (e.g., traffic light or qualitative thresholds) to guide field-level decisions

**Examples:**

| | |
|---|---|
| Mission-Protecting Risks (Zero tolerance) | Anything that undermines core mission, values, or safety (e.g., child safeguarding, fraud). |
| Mission-Enabling Risks (Moderate tolerance) | Risks that may cause short-term setbacks but enable long-term sustainability (e.g., investing in new fundraising channels). |
| Mission-Transforming Risks (High tolerance) | Bold risks that could significantly expand reach or impact, even if uncertain (e.g., innovative digital platforms, partnerships in fragile contexts). |

No single scale may be sufficient on its own. In practice, the most effective RAS approaches combine multiple methods. From a security perspective, the goal is to ensure that whichever approach is used, it:

- Reflects real operational constraints and threat environments
- Provides clear, actionable guidance to field teams
- Supports consistent decision-making under pressure

## 6.3 Risk appetite statement (Template)

### 1. Introduction & Purpose

- Keep this short and clear - set the tone for the document.
- Emphasise decision-making, not just compliance.
- Link explicitly to mission and strategy.

**SFP Role:** Ensure security risk is recognised as a core enabler of operations, not just a constraint.

> e.g., This Risk Appetite Statement sets out the amount and type of risk [Organisation Name] is willing to accept in pursuit of its strategic objectives. It provides a framework for decision-making, risk management, and accountability across the organisation, ensuring alignment between strategy, risk-taking, and stakeholder expectations.

### 2. Scope

- Clarify whether the RAS applies globally or varies by country/context.
- Ensure all relevant risk categories are included.
- Avoid creating a "headquarters-only" document.

**SFP Role:** Confirm that security risks across different contexts (e.g., field vs HQ) are reflected.

> e.g., This statement applies to all functions, programmes, and operations of [Organisation Name], across all locations. It covers all major categories of risk, including strategic, operational, financial, compliance, reputational, and security risks.

### 3. Guiding Principles

- Keep principles concise (6–8 is usually sufficient).
- Ensure they reflect organisational values, not just technical risk language.
- Use them to guide behaviour and decision-making—not just as statements of intent.
- Align with existing organisational principles (e.g., humanitarian principles, safeguarding commitments).
- Avoid duplication with other policies, but ensure coherence.

e.g., The following principles guide how [Organisation Name] understands, assesses, and manages risk in pursuit of its objectives:

- Mission-Driven: Risk-taking is aligned with and supports the organisation's mission and the needs of affected populations.
- Do No Harm: The organisation prioritises the safety, dignity, and well-being of staff, partners, and communities.
- Informed Decision-Making: Risks are identified, analysed, and assessed using the best available information.
- Proportionality: Risk mitigation measures are proportionate to the level and type of risk faced.
- Zero tolerance: applies to breaches of laws, regulations, and ethical standards.
- Accountability: Risk decisions are transparent, documented, and taken at the appropriate level of authority.
- Consistency: Risk appetite is applied consistently across the organisation, while allowing for contextual adaptation.
- Adaptability: Risk management approaches are responsive to changing environments and emerging threats.
- Integration: Risk management is embedded across all functions and linked to broader organisational frameworks (e.g., strategy, operations, security, and compliance).

## 4. Overall Risk Appetite

- Capture the organisation's overall philosophy toward risk.
- Reflect leadership views gathered during consultations.
- Keep language high-level and values-driven.

**SFP Role:** Help frame how security risk enables access and delivery, while reinforcing duty of care.

e.g., [Organisation Name] has a moderate appetite for risk in areas that support sustainable growth and innovation, but a low appetite for risks that could threaten regulatory compliance, financial integrity, or reputation.

## 5. Risk Categories

- Define appetite for each category (e.g., low, moderate, high, or mission-based).
- Add short, clear statements explaining what this means in practice.
- Include thresholds where possible (quantitative or qualitative triggers).
- Ensure consistency across categories (e.g., avoid contradictions).
- **SFP Role:** Lead or heavily contribute to the security row
- Ensure statements reflect real operational conditions
- Provide thresholds (e.g., incident levels, access constraints, evacuation triggers)
- Highlight linkages between security and other risks (e.g., reputational or operational)

*(Use following table only if adopting this type of risk categorisation)*

| Risk Category | Risk Appetite Level | Statement | Key Thresholds / Indicators |
|---|---|---|---|
| Strategic | | | |
| Operational | | | |
| Financial | | | |
| Compliance | | | |
| Reputational | | | |
| **Security** | | | |

## 6. Risk tolerances & limits

- Clearly distinguish between risk appetite (overall intent) and risk tolerance/limits (operational boundaries).
- Define what "within," "approaching," and "exceeding" limits look like in practice, using a mix of qualitative and quantitative indicators where possible.
- Ensure limits are realistic, measurable, and actionable.
- Align thresholds with existing systems (e.g., risk matrices, security levels, escalation protocols).
- Be explicit about what actions are triggered when limits are reached or exceeded.

> e.g., Risk tolerances are established around each risk category and cascaded into operational risk limits to ensure consistency between strategy, governance, and day-to-day decision-making.

## 7. Governance & Oversight

- Define who can accept which level of risk (delegation of authority).
- Be explicit about escalation triggers.
- Link to existing decision-making processes.

**SFP Role:** Define security-specific escalation triggers (e.g., serious incidents, deteriorating context)

- Ensure clarity on who can accept residual security risk at field vs HQ level (if applicable)

e.g.,

- Board / Senior Leadership: Approve and oversee the RAS
- Management: Ensure alignment of decisions with risk appetite
- Risk Management Function: Monitors, reports, and escalates breaches of risk appetite.
- Security Focal Points: Provide analysis, guidance, and monitoring on security risks
- All Staff: Operate within defined risk appetite
- Risks within defined appetite may be accepted at the appropriate management level
- Risks exceeding appetite must be escalated to [senior management/Board]
- Clear escalation thresholds must be defined and applied consistently

## 8. Monitoring & Reporting

- Define how the RAS will stay "live" and relevant.
- Link to reporting cycles and governance structures.
- Include triggers for review (e.g., major incidents, context shifts).

e.g., Key Risk Indicators (KRIs) will be tracked against thresholds. Breaches of appetite or tolerance must be escalated immediately to senior management and the Board. Risk appetite will be reviewed annually, or sooner if business conditions change.

## 9. Approval

- State formal approval process and reinforce accountability at the highest level.

e.g., This Risk Appetite Statement is reviewed annually by the Risk Committee and approved by the Board of Directors on [Date].


**The Global Interagency Security Forum (GISF)** is a member-led network committed to strengthening the safety and security of aid workers worldwide.

Through collaboration, research, and advocacy, GISF brings over 150 NGOs together to drive sector-wide advancements in security risk management and promote practical, effective solutions to keep aid workers safe.


www.gisf.ngo