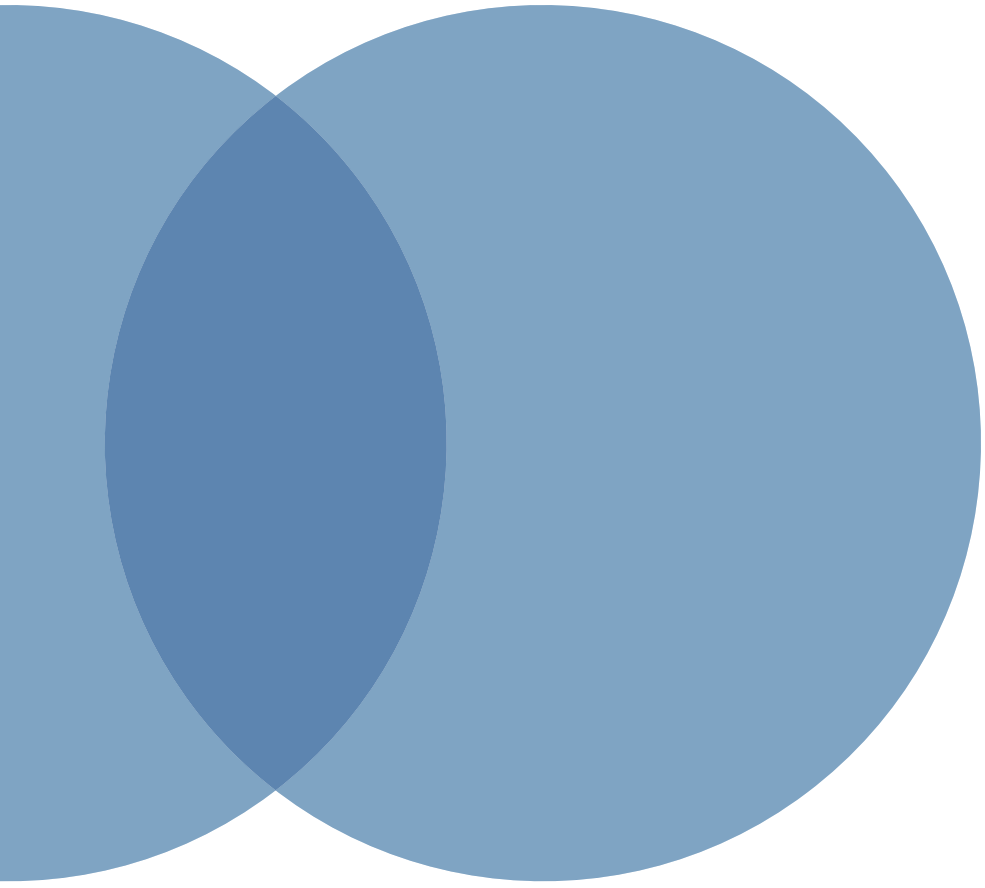
gisf

Bold Steps, Quiet Impact

Pathways to Influencing and Engaging Executive Leadership in Security Risk Management



Global Interagency Security Forum (GISF)

About the Global Interagency Security Forum (GISF)

The Global Interagency Security Forum (GISF) is a member-led NGO forum that works to strengthen the safety and security of aid workers globally. GISF drives collaboration among key stakeholders, strengthens security risk management capabilities, influences global policy, and equips NGOs with the specialised resources, evidence, and tools to effectively manage security risks. With its membership of over 140 NGOs, GISF bridges the gap between operational realities and high-level policy discussions, ensuring aid workers can deliver life-saving assistance in even the most challenging environment.

About the authors

Dr Sean Denson is a humanitarian security leader with over 30 years of experience in security, crisis, and risk management across public service and the aid sector. His career spans frontline operations to senior leadership, where he has shaped institutional SRM practices and supported executive teams in embedding risk thinking across complex organisations. He currently serves as Senior Advisor, Enterprise Risk at World Vision International, where he works with global leadership on strengthening governance and strategic risk oversight. Sean holds a Doctorate in Security Risk Management from the University of Portsmouth, where his research examined the effectiveness and limitations of SRM in the aid sector. His work focuses on advancing the professionalisation of SRM and rethinking how organisations engage with risk at strategic levels.

Marieke van Weerden has built her career in the health, safety, and security (HSS) sector, steadily advancing through progressively senior roles into her current senior leadership position. Marieke has an academic background in non-Western history and human rights complemented with post-graduate programmes at IE Business School, University of Pennsylvania, and Harvard. A committed leader in HSS, Marieke has held impactful volunteer roles, notably serving on the International NGO Safety and Security Association (INSSA) Board of Directors, Overseas Security Advisory Council (OSAC), United Nations Saving Lives Together Oversight Committee, and Deputy Chair of the GISF Steering Group. She is passionate about revolutionising the integration of physical and mental safety, advancing a community widely known for its innovation, resilience, and agility, and empowering executives to be the leaders we need when it matters most.

About this article

Effective engagement of executive leadership is essential for establishing and sustaining SRM as a strategic priority in aid organisations. However, as outlined in State of Practice: The Evolution of SRM Practice in the Humanitarian Space (GISF & Humanitarian Outcomes, 2024), practitioners face systemic barriers, ranging from cultural resistance to competing priorities and limited resources. These challenges are compounded by the dynamic risk environments in which humanitarian aid organisations operate, demanding innovative and context-specific approaches to leadership, collaboration, and SRM practice (GISF, 2024a).

This study draws upon quantitative data from a survey of GISF members and qualitative insights from the "Engaging Executive Leadership" focus groups conducted during GISF workshops in Washington, D.C. (10 September 2024) and Edinburgh (11 September 2024). By examining the factors influencing leadership engagement, the study underscores the critical role of leveraging data, enhancing competencies, and strategically utilising crises as catalysts for strengthening leadership support.

Acknowledgements

The authors would like to thank the GISF membership for the thoughtful discussions on their experiences, successes, and challenges. A special thank you to the CEOs of Catholic Relief Services (CRS), Save the Children US, and Lifes2good Foundation for their openness and willingness to engage. We also acknowledge the support of GISF, and in particular to Dimitri Kotsiras and Jon Novakovic, for their contributions to make this report possible.

Suggested citation

Global Interagency Security Forum (GISF). (2025). *Bold Steps, Quiet Impact: Practical Pathways to Engaging and Influencing Executive Leadership in Security Risk Management.*

Executive Leadership

Refers to the most senior leaders within the organisation, including members of the C-suite (e.g., Chief Executive Officer, Chief Operating Officer, Chief Financial Officer) and other top-tier executives responsible for strategic decision-making, up to and inclusive of board members.

Contents

Introduction 6

Methodology 6

1. From the margins to the mainstream: The evolution of SRM in the NGO sector 8

Military legacy 8

Expanding scope 9

Uneven integration 10

2. To lead is to influence and to influence is to lead: From tactical operator to strategic influencer 12

Move beyond the security function 12

Cultivate trust 13

Harness the power of data 14

Blend communication styles 15

Secure allies and champions 16

3. Never waste a good crisis: Mobilising leadership engagement 18

Leverage crises as catalysts of change 18

Build leadership literacy in SRM 19

Broaden your ecosystem 20

Know your executive 21

Don't be a security leader, be a leader 23

From CEOs to the future generation of CEOs 25

Conclusion 26

References 27

Contributors 28

Acronyms

ECHO	European Civil Protection and Humanitarian Aid Operations
ERM	Enterprise Risk Management
GISF	Global Interagency Security Forum
HSS	Health, Safety, and Security
IFRC	International Federation of the Red Cross and Red Crescent Societies
IRM	Institute of Risk Management
KPI	Key Performance Indicator
NGO	Non-Governmental Organisation
ODI	Overseas Development Institute
OSAC	Overseas Security Advisory Council
PHAP	Professionals in Humanitarian Assistance and Protection
SRM	Security Risk Management

Introduction

NGO security professionals operate in an increasingly complex and dynamic environment, where their ability to influence and engage executive leadership can determine the effectiveness of security risk management (SRM) within an organisation. Despite the widespread recognition of SRM's importance, and the potentially catastrophic consequences of error or failure, SRM professionals often struggle to secure a seat at the executive table. Most, if not all, of the skills and experience needed to navigate effectively at the executive level are present in the SRM sector, though these skills often go unrecognised. This research article explores strategies for overcoming leadership engagement barriers and positioning SRM as a strategic function critical to organisational success.

The article is structured into three key parts:

Part 1: Examines the underlying historic and contemporary challenges SRM professionals have faced in engaging executive leadership, exploring the evolution of their influence over decision-making.

Part 2: Investigates how SRM professionals can cultivate influence within complex organisational structures, with a focus on leveraging trust and effectively utilising strategic information.

Part 3: Highlights best practices from SRM leadership in leveraging critical events to create and expand engagement and understanding, outlining key steps for incorporating SRM into high-level strategic planning.

Through these discussions, this report aims to provide SRM professionals with practical insights and approaches to enhance their influence and engagement with executive leadership.

Methodology

This study employs a mixed-methods approach to explore leadership engagement in aid sector SRM, combining quantitative survey data and qualitative insights from focus group discussions for practical, actionable findings tailored to SRM practitioners.

Electronic Survey Instrument

An online survey was distributed to GISF member security focal points, who represent over 130 non-governmental organisations (NGOs) of varying size, mission, and operating model. The survey was also distributed to a wider group of NGO security practitioners to allow for the inclusion of broader sector perspectives. The survey explored topics such as SRM's positioning within organisations, leadership attitudes toward risk, and barriers to effective engagement.

The survey design featured:

- Likert-scale questions, asking respondents to rate their level of agreement on a scale (typically ranging from "not likely" to "very likely"), used to measure opinions and attitudes on leadership engagement and SRM influence.
- Open-ended questions capturing participant narratives on SRM challenges and successes.
- Comparative analysis balanced across small, medium, and large NGOs to identify organisational trends.

In total, the survey received 98 responses: 24 per cent work for 'small' organisations, 44 per cent for 'medium' organisations, and 32 per cent for 'large' organisations (Figure 1).

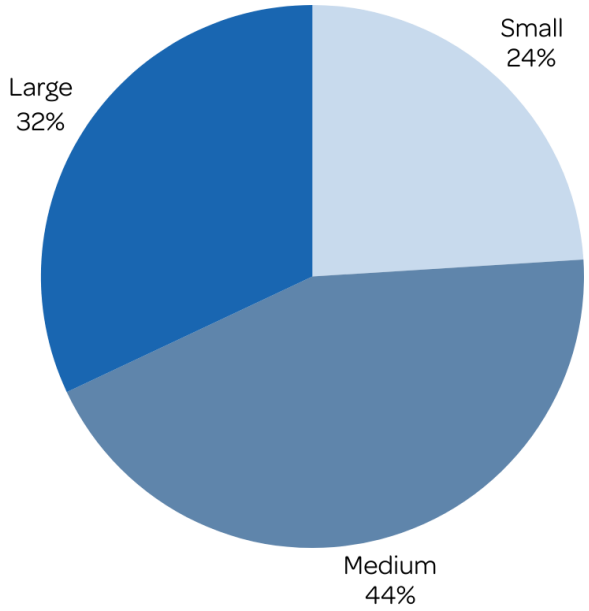


Figure 1: Survey Respondents by Organisation Size

Focus groups contributions

Qualitative data was gathered during focus groups and plenary sessions at GISF Forums in Washington, D.C. on 10 September 2024, and Edinburgh on 11 September 2024. These Forums brought together security professionals from GISF member organisations alongside external experts from across the humanitarian aid, development, and advocacy sectors to explore critical questions related to senior leadership engagement in SRM. The majority of participants were linked to international NGOs. Key topics included:

- Engaging senior leadership effectively
- Balancing risk and strategic objectives
- Strengthening SRM influence within organisations
- Competencies for leadership engagement
- Expanding SRM's role across the sector

These sessions facilitated an exchange of ideas on the topic, resulting in a wealth of practitioner-driven insights and practical examples that form a strong qualitative foundation for this study.

Key Informant Interviews

To complement the survey and focus group findings, seven key informant interviews were conducted with senior security practitioners and organisational leaders (see Contributors for details). These interviews provided deeper insights into the contextual factors influencing leadership engagement, offering valuable case-specific examples that support the study's broader conclusions. Those interviewed were SRM practitioners of different nationalities and backgrounds, from a mix of international and local NGOs.

From the margins to the mainstream: The evolution of SRM in the NGO sector

Over the past two decades, SRM in the NGO sector has undergone a significant transformation, evolving from a marginal support function with operational roots into a critical and strategic function that supports organisational leadership and decision-making (GISF & Humanitarian Outcomes, 2024). However, the path to this more fundamental role has been neither linear nor universal. Drawing on historical context and current insights, this section charts SRM's ongoing shift from a peripheral to a central role within humanitarian organisations.

Military legacy

For many years, NGO security operated in an informal space, driven more by personal networks and rapid responses than by clear policies or shared standards. The archetype of the 'humanitarian cowboy', a term used to refer to aid workers who rushed into active conflict and humanitarian disasters, persisted long after aid agencies began to professionalise. Only after vulnerabilities were exposed by high-profile incidents, legal action, and increased donor scrutiny did NGOs begin to codify their approach.

The humanitarian sector saw the emergence of the SRM function in the mid-1990s, at a time when aid agencies were operating in increasingly conflict-affected and fragile states. As reports of mounting threats to aid workers grew, organisations enlisted former military and police veterans to professionalise their security functions and establish formal standards. In practice, former veterans made up a significant proportion of SRM practitioners in the early years of humanitarian security (Neuman & Weissman 2016).

The early SRM adopters instigated the first wave of professionalisation of SRM in the aid sector, which is also where the challenges lay. In essence, the emphasis on rigorously structured security procedures contrasts with both the variable nature of humanitarian work and its underpinning principles. Although many aid organisations maintain formal hierarchies with centralised leadership and executive oversight, their operational ethos tends to prioritise decentralised coordination, stakeholder consultation, community trust, and negotiated access (Donini, 2012; Egeland, Harmer, & Stoddard, 2011).

These specialists' early leadership in the NGO security space led to widespread adoption of terminology reflecting their military roots. Despite the diversification of the SRM workforce in recent years, a military-influenced mindset persists in the language, tools, and risk frameworks

that continue to shape organisational approaches to security.[1] Correspondingly, early foundational publications such as ODI's *Operational Security Management in Violent Environments* (Van Brabant, 2000) prioritise similarly technical procedural guidance including detailed checklists, protocols, and matrices as benchmarks of effective SRM. The early SRM specialists set up security coordination platforms, developed centralised operational manuals and incident databases, and designed tailored training programmes to equip aid workers in increasingly high-risk environments. This professionalisation predominantly took place in the technical and tactical sphere, rather than at the strategic level.

Expanding scope

Where the establishment of core SRM structures on a semi-militarised approach represents the first wave of maturity, the sector's expanding scope can be viewed as the second. SRM professionals increasingly work in exceptionally complex and volatile operational environments, where they contend with shifting threat landscapes, diverse stakeholder expectations, and the imperative to manage risks while upholding humanitarian principles (Stoddard, Harmer & Haver, 2006). In these contexts, cultural differences are widespread, and SRM professionals must work with varying social norms, languages, and power structures while respecting local customs and sensitivities. This often requires strategies that go beyond traditional security methods, relying instead on adaptability and a strong understanding of cultural nuances (Fast, 2014). These skills have become crucial for fostering acceptance, a key security strategy in humanitarian settings, where the ability to build trust with local stakeholders can be the difference between access and exclusion (Fast et al., 2013).

Reflecting this complexity, the sector's SRM talent pool has diversified significantly. Where the field was once dominated by ex-military and police, today's practitioners include an increasing number of programme managers, logisticians, and private sector specialists, each bringing distinct

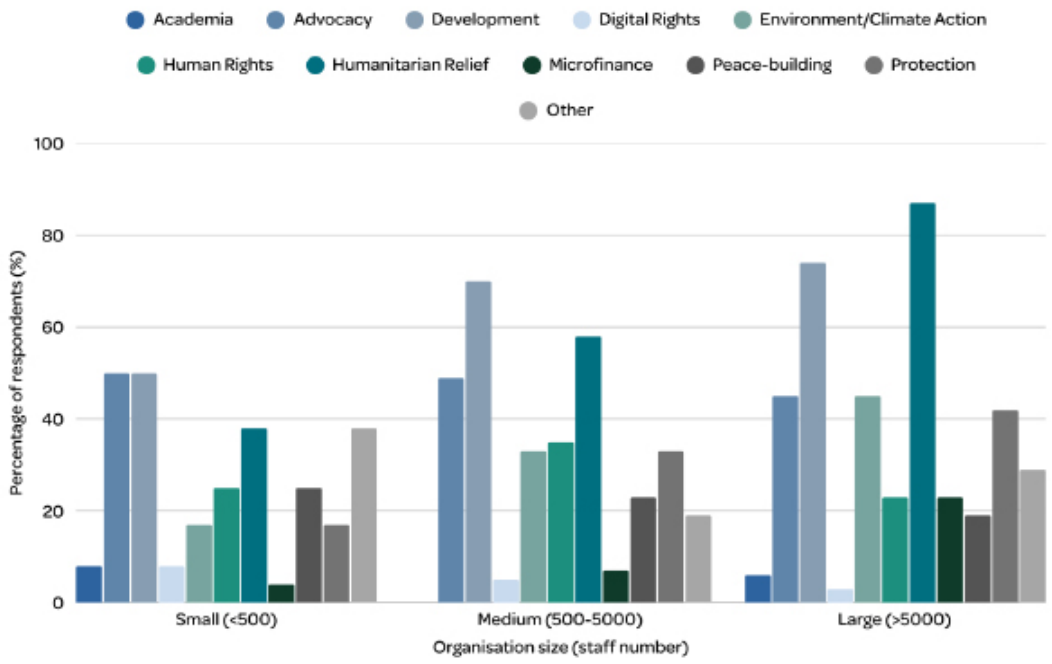


Figure 2: Sectors Engaged in by Respondents by Organisation Size

1 Examples are references to 'violent environments' in SRM guidance and branding core security training as 'hostile environment' training as well as the use of jargon such as 'Standard Operating Procedures (SOPs)', 'medevac' (medical evacuation), 'sitrep' (situation report), and acronyms used around weapons such as ERW (explosive remnants of war), UXO (unexploded ordnance), and UAVs (unmanned aerial vehicle).

competencies and perspectives (Neuman & Weissman, 2016). This diversification has broadened the sector's capacity to respond to different risks, but it has also introduced challenges. Bridging diverse operational cultures and backgrounds requires deliberate efforts to foster shared understanding and recalibrate expectations around authority, negotiation, and local agency (Donini, 2012; Schneiker, 2018).

Adding to this complexity is the reality that SRM professionals often operate within multi-mandated organisations, where each sector brings its own distinct priorities, risk profiles, and operational requirements. Survey respondents work within organisations that generally work across more than four sectors,[2] reflecting the expansive and multifaceted scope of their work.

Large international NGOs, for example, demonstrate the broadest reach, with 38.7 per cent reporting engagement with more than four sectors and one reporting working across nine sectors, including in advocacy, international development, and humanitarian relief. This diverse operating landscape requires security professionals to tailor risk management strategies that respond to sector-specific challenges, all the while maintaining a cohesive organisational approach, adding layers of complexity to their role.

Figure 2 above shows the breadth of sectors survey respondents' organisations work in, and how this varies across small, medium, and large NGOs.

In recent years, there has been growing recognition of the need to move beyond the narrower, technical, and tactical conception of SRM. The sector has increasingly embraced a more holistic and strategic approach, one that positions SRM not merely as a set of operational tools, but as a cross-cutting discipline that supports resilience, accountability, and effective programme delivery. The *Security Risk Management Strategy and Policy Development Guide* (GISF, 2024b) underscores this shift, calling for SRM to be integrated within broader risk governance frameworks and leadership structures. As this evolution gains traction, it raises important questions about how SRM professionals can enable executive leaders to engage more deliberately with security, not just in moments of crisis, but as part of everyday decision-making and organisational learning.

Uneven integration

While the integration of SRM in organisational structures has come a long way over the past few decades, this transition has been uneven and remains a work in progress. Where the NGO sector has professionalised as a whole, maturity between aid organisations and their SRM functions still varies widely. The uneven integration of SRM is visible in two interlinked ways.

The first is the positioning of the SRM function in the organisational hierarchy. Security professionals frequently find themselves reporting to different departments or being shuffled between them in a 'ping-pong' effect that stymies long-term institutional learning and makes it difficult to build executive leadership literacy in security over time.[3] The inconsistent positioning of SRM within organisational hierarchies often makes SRM the 'ugly duckling' of humanitarian organisations, valued in times of crisis but rarely integrated as core departments like Programmes, HR, or Finance. Traditional line management structures, from head of office to country director, regional director, and CEO, leave little room for SRM professionals to advance or influence strategic direction without formal authority. Instead, SRM professionals often operate in advisory roles outside these hierarchies and influence vicariously through other senior leaders.

The second way relates not to *where* SRM is placed in the organisational hierarchy, but *at*

2 Respondent-level analysis of the GISF Engaging Senior Leadership Survey (n=98) indicates that 38.7 per cent of large INGOs (>5,000 staff), 27.9 per cent of medium INGOs (500–5,000 staff), and 20.8 per cent of small INGOs (<500 staff) reported engagement in more than four sectors.

3 Executive security literacy refers to the understanding senior leaders have of core SRM principles, roles, and value, enabling them to ask the right questions, interpret risk information effectively, and support security decision-making proactively.

which level. Survey data suggests that the influence of security on leadership decisions rises in importance in organisations where security professionals report directly to executive teams. This proximity increases the likelihood of SRM being integrated into enterprise risk management (ERM) and strategic discussions. Some organisations now boast of robust SRM structures with dedicated staff, clear policies, and direct reporting lines into executive leadership.

Other organisations continue to restrict security to mid-level roles or embed it within other functions like HR or Finance, without clear authority or progression paths (see Figure 3 below for a comparison of security positioning between small, medium, and large NGOs). Those within or reporting directly to the executive leadership team report a substantially higher level of influence with executives, with over 80 per cent this group rating their level of influence as high. Of those with reporting lines further removed from leadership, less than half feel that they have influence. In summary, the closer the SRM leader is to the executive level, the more influential they are.

This lack of structural integration presents two key challenges. First, SRM often lacks a standardised career progression pathway or recognised executive equivalent, unlike HR or Finance, which have well-defined trajectories leading to C-suite roles. Second, the absence of a consistent reporting line means that there is little to no permanent executive leadership literacy in how SRM is used and adds value. Low security literacy at the executive level means that SRM practitioners must work harder to earn influence rather than wield it by mandate. This significantly reduces the likelihood of sustained, informed leadership engagement across the sector.

While underlying historical and organisational challenges may have impeded SRM's integration, these same experiences and subsequent growing maturity have led to the structural opportunities to bridge the gap.

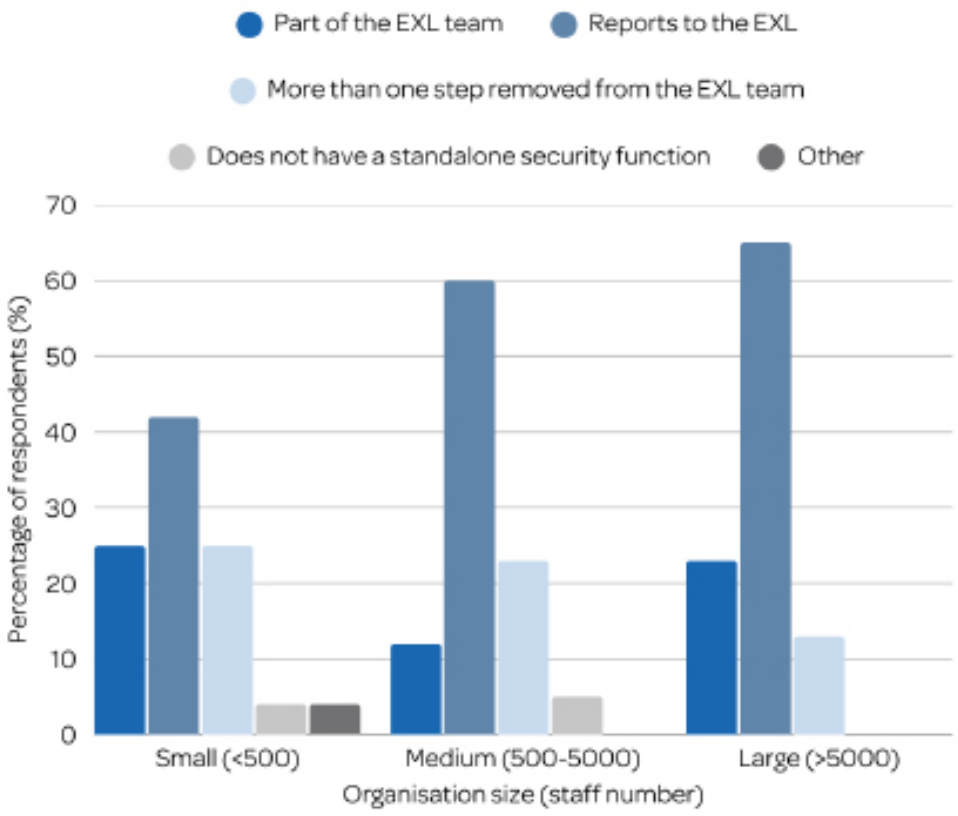


Figure 3: Security Positioning in Organisation in Relation to the Executive Leadership Team

To lead is to influence and to influence is to lead: From tactical operator to strategic influencer

SRM professionals in the humanitarian sector are progressively shifting from operational enforcers to strategic influencers within their organisations, sometimes playing a critical role in shaping organisational resilience, risk governance, and executive decision-making. Regardless of whether the SRM function has an advisory or directive mandate, no leader can lead without influence. This section explores practical strategies to lead through influencing in humanitarian settings defined by decentralised decision-making, competing priorities, and cultural diversity.

Move beyond the security function

In many NGOs, SRM leaders and departments have consistently expanded their scope of operations, be it through proactive engagement or by being tasked to do so. This expansion requires SRM leaders to foster cross-functional engagement to develop a deeper understanding of the organisation as a whole, moving beyond their traditional focus on security operations to embrace a broader strategic perspective in which they can anticipate and contribute to other executive and non-executive departmental priorities and needs.

SRM leaders' ability to navigate ambiguity, build cross-functional relationships, and promote collaborative decision-making can serve as a critical lever in influencing leadership (Neuman & Weissman, 2016). Focus group participants note that when SRM professionals positioned security as a strategic enabler rather than a siloed function, leadership engagement increased significantly. Milicent Waithagu, Global Safety and SRM Lead at Save The Children, observes that "[i]t gives us visibility of other people's identified risks. It gives other people visibility on our risks, but also the fact that we have to come together to speak about risk means that we're all looking at risk holistically. It is no longer isolated in our silos of departmental risks."

In many organisations there is a growing recognition that SRM extends beyond solely security risk reduction, beyond what is typically considered 'traditional' SRM. Effective SRM professionals must be able to 'wear multiple hats' and a majority of focus group participants highlight how their roles have changed in this way, requiring a more strategic mindset to navigate complex

Example: The International Federation of the Red Cross and Red Crescent Societies (IFRC) has adopted a cross-functional approach by involving its security, communications, and advocacy teams in the recruitment of a digital security officer. This shift ensured that security considerations were embedded within broader organisational functions, aligning risk management with advocacy and operational needs.

Source: GISF & Humanitarian Outcomes, 2024.

environments effectively. Janti Soeripto, CEO at Save The Children US, concludes that "[t]he shift from compliance-focused security to integrated risk management has made [Save the Children's Security Function] more relevant."

Maksym Skrypal, Head of Safety and Security Unit at ICF Caritas Ukraine (CUA), shared another example of gaining influence by extending the scope of SRM. His security risk assessment tool and methodology were adopted across other risk areas in the organisation, including financial and reputational risk. Skrypal asserts that when SRM leads the way, it can encourage other functions to adapt and align with its tools, creating greater synchronisation across departments. This not only makes it easier for SRM leaders and executive leaders to work across functions but also positions SRM as a strategic driver within the organisation. By actively supporting other departments in adapting the tool for their own workstream, Skrypal demonstrated how SRM can be embedded as an enterprise function that is integrated into the broader organisational mission rather than operating as a separate or isolated function.

Cultivate trust

Research by Harvard Business Review demonstrates that trust forms the foundation of any successful professional relationship (Frei & Moriss, 2021). This is particularly true in SRM's engagement with executive leadership in the humanitarian sector. As the *State of Practice* report highlights, trust is gradually built through consistent engagement and by demonstrating clear, measurable value to leadership, especially during periods of heightened organisational sensitivity (GISF & Humanitarian Outcomes, 2024).

Focus group participants in Edinburgh emphasise this point. Consistency, transparency, and relevance are essential to earning leadership's confidence, and trust is strongest when SRM professionals cultivate personal relationships with executives and position themselves as reliable problem-solvers during crises. Participants assert that trust is built on evidence, open communication, and reminding leaders of their responsibility while supporting them through complex decision-making. This trust allows SRM professionals to be seen as indispensable advisors during high-risk situations.

> **Example:** An SRM leader spent her first three months meeting with every team across the organisation. To ensure all voices were heard, she followed up with an anonymous survey, allowing those who may not have felt comfortable sharing their thoughts directly to provide feedback on what was working and what wasn't. This gave her both a good sense of the needs and challenges as well as the opportunity to establish rapport and build trust with key stakeholders.

Deliberate early engagement can lay the groundwork for trust. Crucially, strong relationships must be in place *before* a crisis hits. Daniel Goleman (1998) notes that "the time to build trust is before the storm," and Egeland, Harmer, and Stoddard (2011) similarly emphasise that security managers who are trusted before a crisis are far more likely to influence operational decisions when it matters most. Focus group discussions with SRM leaders conclude that from their experience, having pre-existing connections between SRM professionals and executive leaders helps them to consistently manage crises more effectively.

The awareness that SRM leaders have close ties with country level leaders and amplifies trust at the executive level. Sean Callahan, CEO and President of Catholic Relief Services, echoes this insight that a "thoughtful approach, where people at the local level have participated, knowing the on-the-ground reality and having systems in place before a situation escalates" is key to effective security management.

Sourig Aboutali, *Directeur Département Assistance Humanitaire* at ADKOUL in Niger notes that

the trust that international partners and donors place in the SRM analysis and knowledge of his organisation is a unique selling point of his NGO. As he explains: *"Ça fait de nous un acteur incontournable dans les zones à risques. C'est devenu un atout pour nous dans la question de mobilisation des ressources et de la confiance avec les autres acteurs"* ("This makes us a key player in high-risk areas. It has become an asset for us in terms of mobilising resources and building trust with other stakeholders").

This ability to build donor relationships through SRM emerged across several interviews with local aid workers as a potential advantage in securing funding. Even though many of the local NGOs interviewed do not have the funds for dedicated SRM staff, they still see SRM as an important tool for building their organisational and financial resilience.

One key tactic to build trust is to meet directly with leadership, rather than relying on emails or indirect communication. Maurice McQuillan, CEO of Lifes2good Foundation and a former SRM lead for a large NGO, emphasises this: "What I felt was really important was to get in front of them and get in front of them personally, not [over] an e-mail." However, he acknowledges the challenge of doing so, particularly in organisations where security is still an emerging function. Skrypal agrees with McQuillan's advice, distinguishing between direct communication and direct presence. He notes that trust cannot be built on emails alone; face-to-face meetings are essential, as is travelling to field locations and working alongside staff to build credibility with leadership.

Each successful interaction reinforces leadership's confidence, creating a cumulative trust building effect. This foundation of trust is reinforced through regular, structured communication. Participants note this can be achieved through concise updates during senior management meetings, or monthly updates focusing on key countries that provide actionable insights. All interactions can reinforce the importance of security analysis while maintaining leadership's attention.

Through these communications, the SRM function demonstrates situational awareness and control, often anticipating developments before leadership is aware of them. One SRM professional shares that they always communicate about developments that have the potential to garner international media attention. Hearing the news from their SRM leader before seeing it in the news increases the executives' trust in the function. This cumulative trust can then be wielded most effectively in combination with additional influencing tools.

Harness the power of data

Effective communication is a cornerstone of leadership engagement, and well-presented data can be a complementary and powerful lever in this process. Valuable data markers include among others: incident statistics and trends, financial impact, cost savings, Key Performance Indicators (KPIs), enterprise risk indicators, and programme results.

Stoddard's *Necessary Risks* (2020) reinforces the power of data-driven communication in earning leadership trust and influencing decision-making, particularly in high-stakes situations. Focus group discussions share the importance of tailoring data to leadership priorities. For example, showing how incident trends align with cost savings or operational resilience makes SRM interventions more relevant to executive agendas. Examples from the sector can be placed into three categories:

- Single critical incident driven, e.g., showing the difference between a pre-emptive security evacuation through commercial airlines versus a security company's arranged charter flight.
- Multiple-incident driven, e.g., the costs of pre-deployment medical clearance compared to the decrease in medical evacuation costs.
- Cross-departmentally driven, e.g., road safety initiatives leading to cost savings in fleet repairs, insurance premiums, medical expenses, legal fees, etc.

> **Anytime you can tie it back to a financial marker or budget a line that shows a clear win for the agency, you do so.**

Translating risk into terms that align with organisational performance, such as financial impact, was seen as particularly effective. As Emily Timmreck, Director of Health Operations at Catholic Relief Services, observes: "Anytime you can tie it back to a financial marker or a budget line that shows a clear win for the agency, you do so, that's such a strong argument and selling point."

Focus groups consistently identify dashboards as particularly effective to harness data and convey risk to leadership. These visual platforms provide a clear overview of security trends and mitigation efforts, transforming complex data into concise, actionable insights. In addition to single-function dashboards, participants agree that risk hubs (cross-functional data platforms that embed security into broader enterprise management structures) are helpful. They ensure data completeness and help leaders monitor risks across multiple departments effectively, reinforcing transparency and strategic oversight. Examples of commonly used cross-departmental data points are ERM and global risk and compliance dashboards. Waithagu emphasises the value of aligning risk dashboards with organisational KPIs in her security leadership role and how this approach can strengthen SRM professionals' internal advocacy efforts and increase influence.

An integrative approach to data driven communication provides SRM leaders with an amplified voice where executives hear the same messaging from different cross-functional experts.

Blend communication styles

Data-driven messaging is only one aspect of clear, targeted communication for SRM professionals seeking to influence leadership. Dave Kerpen (2016) stresses that "successful leadership engagement relies on listening, storytelling, and building relationships based on authenticity and transparency". Correspondingly, Stoddard (2020) and Joseph Grenny (2013) argue that a mixed skillset of effective storytelling and evidence-based proposals contributes to 'developing street credibility', combining field experience, executive insight, and robust networks to influence organisational decision-making. To gain traction, SRM professionals must present risk in ways that align with leadership priorities and decision-making styles. While some leaders value data-driven presentations, others engage more effectively with stories and case studies that emotively illustrate security's positive impact on staff safety and programme continuity.

SRM professionals who successfully engage executive leadership do so through a combination of consistency, alignment with organisational goals, and the ability to communicate security's strategic value. Kerry Patterson (2013) asserts that "Leadership is ultimately about influencing people to align their behaviour with key objectives, fostering an environment where change is embraced for meaningful outcomes." This insight underscores the need for SRM professionals to cultivate not only technical expertise but also relational intelligence,[4] which can be utilised to identify which key objective or change in environment is best suited to secure executive and board level buy-in.

Executive leaders are more likely to prioritise security when risks are framed in business terms they understand, such as financial impact, operational continuity, and strategic outcomes. Yet, the emotional component of influencing should not be underestimated. Soeripto recalls a pivotal board meeting where the organisation's Global Safety & Security Director led a risk appetite session: "We put him in front of the board, and you should have seen their faces. The

4 Relational intelligence refers to the ability to understand, navigate, and manage interpersonal relationships effectively in a given context. It encompasses skills such as emotional intelligence, social awareness, active listening, adaptability, and the capacity to build trust and influence others.

scenarios he shared with the board were all based on real incidents at the organisation, and the strategic topic combined with the realisation that this was all real, gave our board a very clear and realistic overview of what's at stake." Focus group discussions reinforce this perspective, with several SRM professionals highlighting the need to demonstrate business acumen, align security with organisational priorities, and translate risk management into language that resonates with leadership.

Practitioners caution against alarmism. The most effective messaging is measured and relatable, helping leadership see security as integral to their priorities. Focus group participants note that showcasing positive examples added weight to their arguments and supported their internal advocacy efforts.

Example: Leveraging data, organisational value, and positive change

During the COVID-19 pandemic, an NGO made the high-profile decision to mandate vaccinations for all staff entering offices, field sites, project locations, or engaging in organisation-sponsored travel. At the time, few peer organisations had implemented similar policies, opting instead for encouragement rather than requirement.

The SRM department saw the vaccination mandate as a key lever in their operational COVID-19 response to continue programming while mitigating risk to as low as practicable. The successful influencing of executives to support this decision was largely attributed to a dual approach, grounding the mandate in objective data and scientific evidence while also appealing to the organisation's values, particularly the need to protect the most vulnerable. This balanced strategy resonated with different segments of leadership, gaining their trust and securing executive buy-in.

As a result, vaccination rates surged to nearly 98 per cent, leading to a noticeable decline in COVID-19 cases among staff and reducing disruptions to programming.

The impact was significant: beyond the immediate health benefits, this decision strengthened the organisation's overall risk management capacity and also elevated the SRM department's standing within the organisation. By demonstrating technical expertise and strategic decision-making, it gained credibility with executive leadership. This trust extended beyond the pandemic response, positioning them as a valued advisor on future organisational risks and policies.

For SRM professionals, relational intelligence is particularly important when working with executive leadership, cross-functional teams, and operational staff. It enables them to frame security concerns in ways that resonates with leaders across departments.

Secure allies and champions

Advancing SRM across an organisation can feel like pushing a stalled car uphill. Building a network of allies and champions, both internally and across the wider sector, makes this task not only easier but far more effective. These supporters help drive momentum, amplify messages, and ensure that SRM gains traction at all levels of the organisation.

When discussing effective approaches to assess existing and potential SRM allies and champions, focus groups propose actor mapping as a powerful method to identify key stakeholders who can advocate for SRM priorities within decision-making processes. Some of these will be natural allies such as the leaders for safeguarding and humanitarian response, and some will be strategic allies, such as the advocacy executive or the head of communications. Actor mapping and similar exercises also help spot any changes in alliances between different stakeholders and identify opportunities for new champions.

> **I don't have to market it. People are marketing it for us.**

Focus group participants describe two ways to leverage these supporters. The first is through a targeted and deliberate approach, engaging allies with a particular support or advocacy request. The second involves organic advocacy, capitalising on spontaneous praise when it arises, even if it falls outside of a carefully managed narrative. Both approaches are equally powerful and are most effective when used together.

Investing in SRM champions is recognised as an important influencing element by focus group participants. However, there is a difference between having a few champions and creating a critical mass. The latter is necessary to create a culture of security. Champions can help convince others to conform to socially acceptable behaviour. Importantly, this category of supporter does not necessarily need absolute power. Many of these are the 'hustlers and shakers' who hold relative power that is just as, if not more, effective in creating engagement. When key champions adapt behaviour and raise awareness, others are likely to follow this social proof until the tipping point for critical mass has been reached.

Example: When an SRM leader started their new position, they undertook a stakeholder mapping exercise. The exercise was a physical exercise on paper as SRM professionals are used to doing as part of their context analysis. This exercise was focused on the internal stakeholders, their level of power, their engagement with the security function, and their potential to become and remain allies. This mapping helped the SRM professional understand the power dynamics, opportunities, and challenges. By leveraging the insight from the exercise, they were able to take a more deliberate and targeted approach in neutralising potential blockers, gaining allies and building up their champions.

CEO Callahan underscores this dynamic when reflecting on his field visits: "I meet with regional directors and people in the field and ask them how they feel about our approach to safeguarding and our approach to health, safety, and security [...]. I am very impressed with the feedback I receive, and the security measures taken, I feel that when I go out into the field." Melanie Murphy, Director of Physical Security at Human Rights Watch, also experienced the power of social proof. Murphy describes how her organisation's in-house personal security training gained momentum without needing a formal communications push: "I don't have to market it. People are marketing it for us." This organic advocacy helps SRM initiatives to scale more easily and sends a powerful message to leaders that the SRM function is delivering value and meeting the needs of staff on the ground.

When identifying allies, participants noted that SRM leaders should ensure these champions are positioned at all levels within the organisation. Callahan's example shows that just having supporters at the executive level is not enough. Tara Arthur, Owner and Co-Founder of the Collective Security Group, also highlights the value of identifying rising leaders within the organisation, particularly those with the potential to become future senior executives. Building relationships with these individuals early ensures that, as they move into leadership roles, a trusted SRM ally is already in place, helping to embed security considerations at the highest levels. And finally, Skrypal asserts that even your most senior leader can be your powerful ally: "Where I could not reach the hearts of some of our leaders, she [the Caritas Ukraine CEO] helps me to reach them." The more people speak up, the stronger the voice.

Never waste a good crisis: Mobilising leadership engagement

Crises can serve as unique opportunities for SRM professionals to influence leadership, not as situations to exploit, but as critical junctures to gain traction on improvements and institute meaningful change. This section unpacks how SRM professionals can mobilise leadership engagement by recognising how pivotal events within and outside of the organisation and the sector present opportunities for growth, making use of good practice from the SRM sector. It navigates the benefits of educating executive leaders, as well as exploring how to advance from serving an executive leader to becoming one.

Leverage crises as catalysts for change

During crises, vulnerabilities within organisations often become starkly apparent, compelling leaders to confront risks and reassess priorities. This heightened focus can pave the way for substantive discussions about security's strategic importance, offering SRM professionals an opportunity to demonstrate value and advocate for lasting reforms. As Murphy reflects, crises provide opportunities to showcase the effectiveness of existing systems: "When leadership sees that decisions made under pressure were based on solid analysis and foresight, it builds trust and strengthens the case for SRM as a strategic enabler."

Focus group participants highlight that crises frequently place security at the forefront of executive discussions, especially when SRM professionals provide clear, actionable recommendations. For example, incident reviews were noted to drive leadership action, leading to increased resources in security, allocation of funds for training, and recruitment for key roles. One participant recommends having a 'low bar' for executive engagement in critical incident management. They observe that frequently engaging their executives in incident management response situations, either involving or informing them, not only improved their familiarity with SRM processes but also strengthened their ability to respond strategically under pressure. These efforts illustrate how crises can foster both immediate responsiveness and longer-term investment in security measures.

Similarly, focus group participants specifically highlight that donor scrutiny following high-profile incidents can act as a powerful catalyst for reform, prompting leadership to prioritise SRM improvements. In one example discussed, a serious security incident resulted in donor-mandated changes to the organisation's risk management framework, including new protocols, targeted training, and greater cross-departmental engagement. Similarly, post-crisis reviews have been shown to solidify SRM's value by linking lessons learned to actionable improvements.

In the absence of a crisis, deeper leadership engagement with SRM can also be facilitated through simulations and debriefs, which help bridge the gap between operational realities and strategic decision-making. Focus groups highlight that involving executives in crisis simulations and security trainings is especially effective to humanise the risks and demonstrate real-world implications of operational decisions, such as the cascading effects of delayed evacuations or inadequate risk assessments.

Build leadership literacy in SRM

If an organisation consistently works in high-risk or complex contexts, the opportunity to catalyse engagement via crises is not confined to singular events but instead likely to become an integral part of the operational mindset. An organisation's risk appetite, as defined by its board and executives, and the nature of its work are key factors shaping how crises influence leadership thinking and decision-making. By translating risk appetite (taking risk) and risk tolerance (controlling risk) into strategic action, SRM professionals can build up the SRM literacy (security knowledge and understanding) of their executives. Hamel and Välikangas (2003) state that sustainable progress requires more than short-term gains, it depends on an organisation's ability to anticipate risks and build adaptive capacity over time.

The Professionals in Humanitarian Assistance and Protection (PHAP) association argues that a high-risk appetite is often essential for humanitarian organisations to act decisively in volatile and dangerous contexts to address critical needs.[5] As Figure 4 illustrates, organisations engaged in humanitarian work indeed demonstrate the highest levels of risk tolerance, with over 50 per cent exhibiting a high or very high risk appetite. This contrasts with the advocacy and development sectors at just over 40 per cent, which may reflect the less immediate life-or-death stakes in their operations.

Rather than aiming to eliminate risk, SRM seeks to enable access through risk mitigation. As noted in the Humanitarian Access SCORE Report (Stoddard et al., 2020), many aid agencies now explicitly frame risk acceptance as a strategic enabler of access, balancing programmatic need against organisational tolerance. Focus group discussions stress the use and importance of risk appetite statements. This notion is echoed in broader risk management research. The Institute of Risk Management (IRM) recommends that organisations clearly define and communicate their risk appetite as part of a broader enterprise risk management, ensuring it supports their strategic objectives and operational realities.[6] Soeripto underscores that, "Trust in [SRM] expertise is what I am looking for. We're making those decisions, and the culture change and way of managing

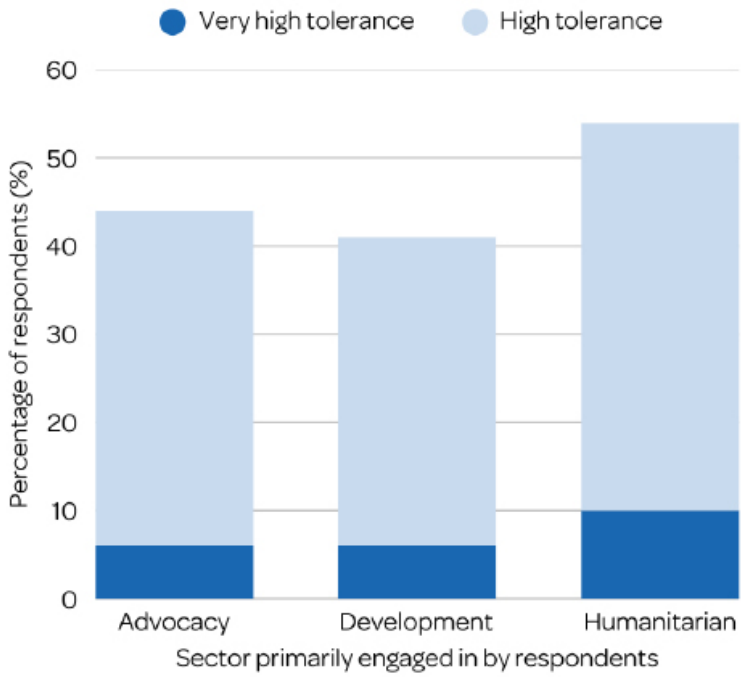


Figure 4: Sector Engaged by Risk Appetite

5 See https://phap.org.

6 Institute for Risk Management. "Risk appetite and tolerance". IRM: https://www.theirm.org/what-we-say/thought-leadership/risk-appetite-and-tolerance/

security is part and parcel of approving programmes. I have to know that it is a well calculated risk, and if you have those systems well embedded in countries now, then you can take more risk."

Following the 2015 Médecins Sans Frontières Kunduz hospital airstrike, for example, rapid investment in security infrastructure and protocols was followed by longer-term ambiguity about structural SRM integration (Bouchet-Saulnier & Whittall, 2019). Similar patterns observed during and after major crises in Afghanistan, South Sudan, and West Africa were highlighted by participants during focus group discussions. These examples show that caution is warranted. In the aftermath of a crisis, leadership may rapidly increase investment in security, but not always sustainably. Security professionals, who have long struggled to secure buy-in from leadership for additional resources, may find themselves advocating for restraint even in high-risk settings or during and after crises to avoid a reactive overcorrection. This risk aligns with organisational leadership theories on oscillation, where responses to crises often alternate between underinvestment and overcompensation, creating instability.

In these contextual engagements, SRM professionals are well-positioned to educate leadership toward measured, sustainable progress balancing urgent operational demands with longer-term resilience, whilst preventing the kinds of overreach that can create lasting setbacks and erode organisational trust.

Broaden your ecosystem

The crises and other pivotal events that an SRM practitioner can use to advocate for security are not limited to those within their own organisation. The legal case brought to court (and won) by Steve Dennis against Norwegian Refugee Council in 2015 had a ripple effect across the NGO security sector as the first case on SRM brought against an NGO that was not dismissed or settled out of court.[7] Many used the case example to address duty of care with their executive leadership and bring about change. SRM professionals do not operate in a vacuum. A broader ecosystem of external stakeholders, including donors, partners, SRM networks, legal decision makers, and the media can play a pivotal role in shaping SRM practices and strengthen leadership engagement. These stakeholders often provide the broad visibility and external pressure needed to prioritise SRM within organisational structures.

Donors increasingly require robust SRM frameworks as part of funding agreements, making them powerful allies in advocating for leadership engagement. Focus group participants highlight that compliance with donor-driven SRM standards often leads to tangible organisational improvements, such as stronger risk assessment procedures and enhanced security protocols. For example, the European Commission's Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) includes explicit SRM obligations in its partnership framework, requiring humanitarian organisations to conduct risk assessments, implement appropriate safety measures, and uphold a clear duty of care to staff (European Commission, 2021). Several practitioners urge involving donors early in programme design to strengthen this dynamic. Proposals that feature detailed risk analyses and security mitigation strategies are more likely to secure funding, with donors increasingly valuing proactive risk management. This approach ensures not only that SRM considerations are embedded in programme designs from the outset, but it also signals to leadership that robust SRM frameworks are both strategically and financially necessary.

The supportive ecosystem expands beyond the NGO sphere. For instance, court cases in the airline sector have helped SRM leaders and their organisations further define their legal duty of

7 See, Kemp, E. & Merkelbach, M. (2016). Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications. European Interagency Security Forum (EISF).

care towards travellers and staff deployed overseas during non-work hours.[8] Participants also point to the role that media can play in grabbing leadership's attention. Public scrutiny of security failures can serve as a catalyst for change. An example of media impact is the murder of the UnitedHealthcare CEO in 2025, which led many SRM professionals across the sector to review their executive protection measures with their CEOs. These cases with high-level media attention provide openings for executive engagement just as valuable as internal incidents.

Lastly, the value of engaging peers across the sector (in the aid sector as well as the wider SRM sector, including public and private/corporate SRM) is a way to raise the visibility of SRM, including through coalitions, working groups, and sector forums such as those held by GISF. Gathering comparative data through both formal and informal benchmarking surveys is an often-used tool to influence decision-making, focus groups disclose. Questions shared in informal NGO security social media platforms for example are: "How many Security Directors sit on the Executive Team/C-Suite?" and "I want to convince my organisation to adopt an AI policy. Who already has a policy in place?" Formal benchmarks and assessments can lend additional weight to SRM positions through their regard and standing, such as those provided by Overseas Security Advisory Council (OSAC), ASIS International, Security Executive Council, and GISF's SRM Self-Assessment tool.

Benchmarks can be helpful to demonstrate where and when the SRM leader's organisation is falling below the standards of its peers. They can also be used to showcase where an organisation is ahead of the curve, strengthening the organisation's reputation and enhancing executives' credibility.

Know your executive

In the previous section we discussed the importance of *how* SRM leaders communicate with executives. Equally important is having a thorough understanding of *who* you engage with. When asked how an SRM leader's executive (their direct line manager) perceives them, one focus group participant answers, "The board praises [my line manager] because they are impressed with the organisation's approach to security. I make [the CEO and his executive team] look good. The board is pleased with him, which makes him pleased with me. [The executive team] see me as a partner in their engagement with the board."

When questioned on how to develop the understanding of what a board wants to hear, focus group participants explain that they gather this information through trial and error. Present the different styles of information as discussed in the previous section, *listen* to their comments and questions, but also *look* at their reactions and *adapt*. Securing these types of partnerships within the executive team and the board can help push new initiatives forward.

Executive buy-in has two important components. First, by showing up and being there for executives through their difficult decisions, SRM leaders demonstrate their value to their executive leadership. Second, SRM leaders help executives project credibility to both their board and staff.

---

8 In 2021, a Hong Kong court ruled in favour of a former employee or Bellawings Jet Limited, who claimed wages for standby duty on rest days. These were days that the employee did not work but could also not do as they pleased (similarly, in Australia in 2025, Corporate Air Charter lost a court case brought by a pilot claiming that her standby time is counted as "hours of work" as she was under 'a number of directions' from her employer. The same can be argued for international travellers, who have to abide by security measures while travelling on official organisational business even after hours.

Hong Kong case: Lewis Silkin, Hong Kong court finds that pilot's standby time did not constitute rest days (17 Dec 2021), available at: https://www.lewissilkin.com/en-hk/insights/2021/12/17/hong-kong-court-finds-that-pilots-standby-time-did-not-constitute-as-rest-days.

Australia case: Norton White, The Full Federal Court orders standby duty to be paid as work and included in average work hours (2025), available at: https://www.nortonwhite.com/publications/the-full-federal-court-orders-standby-duty-to-be-paid-as-work-and-included-in-average-work-hours.

By showing genuine care, SRM leaders signal that the organisation itself cares. Callahan outlines what he sees as two key components of impactive security leadership:

Executive impact

Leadership relies on trusted systems that provide clear, context-specific information to inform decision-making. SRM professionals play a critical role by ensuring leadership has access to accurate, timely insights on the ground, enabling programmatic and operational decisions that are well-informed and responsive to emerging risks.

Organisational impact

Security management is not just about mitigating risk; it is about building trust and demonstrating organisational integrity. By prioritising staff well-being and engaging proactively with teams in crisis settings, SRM fosters a culture of care and collaboration, reinforcing confidence in the executive leadership at all levels.

Even when building executive leadership's literacy in risk appetite and other SRM areas, different executives have different experiences and perceptions of SRM risks. Arthur emphasises the importance of understanding these dynamics, "Who are the executive leaders who have *actual* security knowledge? Who are the executive leaders who *feel* that they have security knowledge, but actually don't? Tailor your messaging, but also who you're targeting." In most cases, success is not just determined by the message, it is conditional on knowing your audience.

Some leaders' perception of their SRM understanding does not match reality. This can be particularly challenging for early-career professionals. However, Murphy argues that pushing back against poor security guidance is critical. In these pivotal moments, the risk of losing executive support depends on how their decisions are challenged. In Murphy's words, "An important point in engaging any sort of leadership is around the balance of not only supporting them to make the right decisions, but how you support them when they've made the wrong decision." Advice arising from the focus group participants is to take time to explain your position, to feed information piece-meal to prevent information overload, and most importantly, to let executives form the answer themselves instead of telling them. This approach may, in some cases, result in the SRM professional not receiving recognition for certain improvements; however, the end result will be increased engagement through deliberate influence.

Successfully engaging with executive leadership also means knowing when to engage and, perhaps even more crucial, when not to engage. Murphy notes, "I really try to stay off executive people's radars unless it's really needed because I want them to know that if I reach out, it's something that's really, really important and they have to pay attention." Focus group advice on knowing your executive and their priorities outlined four key actions: Read the room, Reframe, Rebalance and Rationalise.

The Four Rs of Executive Engagement

Read the Room: Even if the request is warranted, is this the right time? Rethink your ask of executives based on their priorities and concerns. Asking for additional budget just as they have lost a large grant or have spent a considerable amount on another initiative may negatively impact their view of you and your SRM function.

Reframe: Is your ask in line with their current priority or concern? Determine how to reframe your request to enhance what they are focussing on instead of detracting attention from their priority. For example, when they are investing heavily in partner safeguarding, explain how your request advances that initiative as well as provide further benefits to the organisation.

Rebalance: When you ask for more, how can you visualise that this means less of something else? When submitting a request, demonstrate how additional costs are counteracted

by savings or efficiencies. Successful managing up includes offsetting a new cost with a corresponding saving elsewhere. For example, when requesting for an additional position, show that this offsets the use of an external vendor for those same services.

Rationalise: What rationale does the executive use to justify change? Understand what reasoning your executive uses when approving requests and proposals. Adapt justification that has proven successful in the past and/or by other departments. In a faith-based organisation with a high moral duty of care, instead of citing legal duty of care, staff care and human dignity could be more effective.

By handling issues quietly and efficiently, SRM professionals can ensure that when they do step forward, their insights carry weight and urgency. They make their executives *look* good, they make their executives *feel* good because of the trust they inspire, and ultimately, they are in a unique position to *lead* alongside their executives.

Don't be a security leader, be a leader

The main reason for SRM in NGOs is to help these organisations fulfil their mission. The organisation comes first; it needs to survive and thrive. And to help the organisation do that, the SRM professional must do what needs to be done, inside and even outside of their SRM function.

One SRM leader summarises this in a focus group discussion: "When it is all hands-on deck, be that extra pair of hands. Do not wait until you are asked, think of where you can support and be proactive, even if it is outside of SRM." McQuillan agrees that SRM professionals should practice adaptive leadership. For him, the essence is "knowing when you need to step in more, when someone needs more support, and when they just need you as a sounding board or second opinion to make sure that they're doing the right thing. Being adaptable in your support to leadership at all levels, would be a very good trade. Recognising where are these people in their journey? How much support do they need? How much support are they open to as well? And then finding [...] where to place your own value add and also how much value that adds to you, not just in upping the bench line, but also when translating that to influence with senior leadership."

Example from the sector: Losing a battle, but winning a war

At the start of the Ukraine war in 2022, an NGO wanted to send a regional staff member into Ukraine for analysis and reporting. As the regional staff member was Russian, the SRM lead for the organisation advised against this, citing risk of harm of the staff member and reputational risks around perceived bias. The SRM leader made sure the advice was put in writing and documented everywhere. The matter was escalated all the way up to the most senior executive. That executive appreciated the thought and work that had gone into the security advice, but decided to move ahead with sending the Russian staff regardless. This quickly led to some of the risks the SRM leader had warned against manifesting and escalated to a withdrawal of the Russian staff member from Ukraine. The SRM leader commissioned an external after-action review conducted by a professional experienced in handling sensitive incidents, ensuring an accurate yet constructive evaluation. By maintaining professionalism through the formal review and strengthening relationships through informal discussions, the SRM leader positioned themselves as a trusted partner. They didn't point out the 'I told you so' moment, letting a balanced external review speak for itself. While their initial advice was overlooked in this incident, the organisation adopted the SRM leader's recommendations in subsequent situations—showing that sometimes, losing a battle can ultimately win the war.

What came out strongly from conversations with local NGO executive and security leaders is their unwavering focus on inclusion of their local partners. Skrypal's and Aboutali's perspective on engagement and leadership is that in almost every aspect of SRM, they rate their successful influencing not just by their level of engagement with their agency's leadership, but with their wider network of local actors and partners. Aboutali states that this has strengthened their credibility with both their board and local authorities, and it has made them a source of inspiration for international partners.

When risky organisational problems arise, emotions can run high, and the stakes feel greater. A calm approach can help de-escalate tension and keep everyone focused on finding solutions. As SRM leaders are often used to dealing with multiple critical incidents at the same time, they are well placed to support executives through any crisis. One example from an SRM professional includes stepping in as mediator between the programmes department and the procurement department in a dispute about an online driver safety training. Even though the reason for the disagreement (the cost allocation decision for countries) was outside of the SRM leader's scope, their executive asked them to resolve it. By agreeing to mediate and presenting a solution acceptable to all parties, the SRM leader resolved a conflict that was a headache for their executive and increased their trust not only with that executive, but also with both departments involved in the disagreement.

In the focus groups, participants expressed mixed opinions about strategic engagement beyond the SRM function, with many expressing the desire to stay out of organisational 'politics'. Understanding and engaging in organisational and relationship management is key to influencing. The importance of influencing and engaging outside of just the SRM sphere lies in the multi-dimensional role of leadership. Most executive roles are multi-faceted too, and these leaders have held many different roles leading up to where they sit now. Even if there might often not be a natural next step for an SRM professional into the executive team within their organisation, they can build their skills, expand their role, and grow personally and professionally. And then SRM leaders are not only ready to strengthen their executive relationships, but also ready to operate at that executive level themselves.

From CEOs to the future generation of CEOs

In his career path from SRM professional to CEO, McQuillan is one of the few. As SRM matures in the NGO sector, so too does the SRM professional. Their increased influence and engagement at the highest executive and board level can transform them from an advisor into an equal partner.

Six key lessons from CEOs for SRM practitioners

Throughout this report, experienced SRM professionals have shared best practices for engaging leadership. Equally important, however, are the insights from executives themselves. As a final takeaway, CEOs share their six key tips on how SRM professionals can engage effectively at the highest governance levels:

Keep it simple and concrete
Executives need clarity, not complexity. Use straightforward language, concrete examples, and avoid overwhelming them with excessive detail. They may not fully grasp the nuances of security in every context, so ensure SRM messaging is accessible and actionable.

Set clear boundaries
Honest, grounded conversations are essential. No sugarcoating, but also no fearmongering. If a security risk requires a 'No', it must be firm and final. While leadership may test limits, SRM professionals must have the confidence and authority to define and uphold essential boundaries.

Engage and stay engaged
Building executive buy-in isn't a one-time effort. Regular, face-to-face engagement ensures leaders remain actively involved in security decisions rather than defaulting to blind trust in security experts. The goal is sustained dialogue, not just occasional input on isolated issues.

Lead by example
Executives are staff members too, and they must follow the same security protocols as everyone else. When leaders model good security practices and demonstrate trust in local staff, it sets the tone for the entire organisation. Persuade them to lead by example, no exceptions.

Be present and prepared
During crises or moments of uncertainty, always 'show up' both physically and strategically. Executives rely on SRM leaders to provide timely, accurate information to support critical decisions. Trust in security guidance is built through consistency, expertise, and responsiveness.

Welcome the outsider perspective

Always have an outside eye on SRM's work. We all do our best and we are all flawed. Make sure to have outsider contributions from peers and partners to help the organisation's SRM approach improve and grow.

By embracing these principles, SRM professionals can enhance their influence, foster executive trust, and ensure security remains a strategic priority within their organisations.

Conclusion

Influencing and engaging executive leadership in SRM is a complex but essential task for ensuring organisational resilience and operational effectiveness. This report has outlined the structural challenges security professionals face, best practices for influencing, and the possible trajectory of SRM leadership.

The future of SRM leadership will be defined not just by technical expertise but by the ability to navigate organisational complexities, build relationships, and align security with overarching humanitarian objectives. As NGOs face increasingly complex and resource-constrained operational landscapes, SRM professionals must embrace their evolving role as strategic leaders. As Arthur highlights, "Security professionals are not just for security. They make some of the best leaders I've ever encountered in my whole career." Yet, this potential is often overlooked. To fully integrate SRM into leadership structures, there must be a recognition that many of these professionals are well-qualified to step into executive roles. Arthur adds, "We don't always give space to the fact that a lot of these amazing professionals in our sector are qualified to be the executive leaders."

> **"I think leading the way sometimes is a scary thing and it is a risk, but it positions you for success."**

The shift from operational tacticians to strategic influencers requires a blend of technical expertise, relational intelligence, and the ability to position security risk management as a driver of organisational resilience. As Timmreck admits, "I think leading the way sometimes is a scary thing and it is a risk, but it positions you for success."

NGO security leaders must embrace this risk, become better influencers, and thereby establish themselves as essential partners in shaping the future of humanitarian operations and beyond.

References

Bouchet-Saulnier, F. and Whittall, J. (2018). 'An environment conducive to mistakes? Lessons learnt from the attack on the Médecins Sans Frontières hospital in Kunduz, Afghanistan', International Review of the Red Cross, 100(907–909), pp. 337–372. doi:10.1017/S1816383118000619.

Donini, A. (2012). The golden fleece: Manipulation and independence in humanitarian action. Sterling, VA: Kumarian Press.

Egeland, J., Harmer, A., & Stoddard, A. (2011). To stay and deliver: Good practice for humanitarians in complex security environments. New York: United Nations Office for the Coordination of Humanitarian Affairs (OCHA).

European Commission. (2021). General Conditions applicable to humanitarian aid actions financed by the European Union. Brussels: European Civil Protection and Humanitarian Aid Operations (ECHO).

Fast, L., Curry, D., & O'Neill, M. (2013). Measuring acceptance: A toolkit for humanitarian assistance and development actors. Save the Children and CDA Collaborative Learning Projects. Available at: Acceptance Research [Accessed 14 April 2025].

Fast, L. (2014). Aid in danger: The perils and promise of humanitarianism. Philadelphia: University of Pennsylvania Press.

Frei, F. & Moriss, A. (2020). Begin with Trust. Cambridge: Harvard Business Review. Available at: HBR [Accessed 1 July 2025].

Global Interagency Security Forum (GISF) & Humanitarian Outcomes. (2024). State of Practice: The Evolution of SRM Practice in the Humanitarian Space. GISF.

GISF. (2024a). Good Practices, Lessons Learned, and the Unique Challenges Affecting SRM in Urban Humanitarian Responses. GISF.

GISF. (2024b). Security risk management strategy and policy development guide. London: GISF.

Goleman, D. (1998). Working with emotional intelligence. London: Bloomsbury Publishing.

Grenny, J., Patterson, K., Maxfield, D., McMillan, R., & Switzler, A. (2013). Influencer: The New Science of Leading Change. 2nd edn. New York: McGraw-Hill Education.

Hamel, G. & Välikangas, L. (2003). The quest for resilience. Harvard Business Review, 81(9), pp. 52–63.

Institute of Risk Management (IRM). (2018). Risk Appetite and Tolerance Guidance. Available at: IRM [Accessed 1 July 2025].

International Organization for Standardization (ISO). (2018). ISO 31000:2018 - Risk Management: Guidelines.

Kerpen, D. (2016). The Art of People: The 11 Simple People Skills That Will Get You Everything You Want. Penguin.

Neuman, M. & Weissman, F. (2016). Saving Lives and Staying Alive: The Professionalisation of Humanitarian Security. C. Hurst & Co. Ltd.

Professional Development Program (PHAP). (2020). Understanding Risk Appetite in Humanitarian Operations. Available at: PHAP [Accessed 16 January 2025].

Schneiker, A. (2018). Risk-Aware or Risk-Averse? Challenges in Implementing Security Risk Management within Humanitarian NGOs. Risk, Hazards & Crisis in Public Policy, 9(2), pp. 107–131.

Stoddard, A. (2020). Necessary Risks: Professional Humanitarianism and Violence Against Aid Workers. University of Pennsylvania Press.

Stoddard, A., Harmer, A., & Haver, K. (2006). Providing Aid in Insecure Environments: Trends in Policy and Operations. Overseas Development Institute.

Stoddard, A., Harvey, P., Breckenridge, M.-J., & Czwarno, M. (2020). Humanitarian Access SCORE Report: 2020 Global Synthesis – Survey on the Coverage, Operational Reach, and Effectiveness of Humanitarian Aid. Humanitarian Outcomes.

Van Brabant, K. (2000). Operational Security Risk Management in Violent Environments. Overseas Development Institute.

Contributors

Sourig Aboutali, *Directeur Département Assistance Humanitaire,* ADKOUL

Tara Arthur, *Owner and Co-Founder*, Collective Security Group

Sean Callahan, *Chief Executive Officer and President*, Catholic Relief Services

Maurice McQuillan, *Chief Executive Officer*, Lifes2good Foundation

Melanie Murphy, *Director of Physical Security*, Human Rights Watch

Maksym Skrypal, *Head of Safety and Security Unit*, ICF Caritas Ukraine (CUA)

Janti Soeripto, *Chief Executive Officer*, Save the Children US

Emily Timmreck, *Director of Health Operations,* Catholic Relief Services

Millicent Waithagu, *Global Safety and Security Risk Management Lead*, Save the Children

Global Interagency Security Forum

GISF Research and Programmes
T: +44 (0)20 7274 5032
E: research@gisf.ngo

www.gisf.ngo