Asian Journal of Social Science and Management Technology
ISSN: 2313-7410
Volume 8, Issue 3, May-June, 2026
Available at www.ajssmt.com

The Nexus of Security Risk Management and Business Continuity in Humanitarian Operations: How Integrated Approaches enable Operational Resilience in Insecure Environments

Michael Munyaradzi Makova (PhD)

2375 Bluffhill Westgate, Harare, Zimbabwe

Abstract:
Humanitarian operations are conducted in some highly insecure field environments with diverse security risks that simultaneously threaten staff safety and the continuity of critical programmes. Insecure and conflict affected field environments are associated with diverse security threats and risks, chronic volatility and instability, and recurrent operational disruptions that undermine the ability of humanitarian organisations to continuously sustain critical life-saving programmes. Within this operational landscape, Humanitarian Security Risk Management (HSRM) and Business Continuity Planning (BCP) have emerged as central to operational resilience. HSRM focuses on identifying, assessing, and mitigating security threats in order to enable safe, secure and effective humanitarian operations while BCP focuses on preserving critical functions during and after significant disruptive events. Together they create the conditions for operational resilience, where humanitarian organisations can absorb shocks without losing their ability to operate in insecure environments. This study examines the nexus between HSRM and BCP, contending that their integration is a necessary condition for achieving operational resilience in insecure humanitarian environments marked by conflict and instability. Drawing on existing literature, organisational frameworks, field reports, case studies and empirical insights from humanitarian practitioners, the study demonstrates how integrated HSRM and BCP approaches enhance preparedness, decision-making, and continuity of operations. The study underscores the importance of treating HSRM and BCP as interdependent components of a unified operational resilience architecture, essential for sustaining humanitarian action in insecure environments.

Key words: Business continuity, Operational resilience and Humanitarian security risk management.

---

1. Introduction

The humanitarian operational environment has become highly insecure with significant risks to staff safety and operations continuity particularly in conflict affected settings since the turn of the millennium [1]. Insecure humanitarian environments unfold within highly volatile and diverse landscapes shaped by armed conflict, political instability, and chronic insecurity. In many insecure environments such as Ukraine, Yemen, Gaza, Sudan, Somalia, Sudan, and the Democratic Republic of Congo, active hostilities, shifting frontlines, and fragmented territorial control have generated large-scale displacement and acute and widespread humanitarian needs [1]. Even in post-conflict contexts like Colombia, Ethiopia, South Sudan, Iraq, Syria, and Libya, residual violence, weak governance, and fragile peace agreements continue to disrupt humanitarian access complicating humanitarian

operations and planning [1]. These environments continue facing uncertainty, fluidity, and the constant potential for sudden escalation in violence. The risk landscape in insecure humanitarian environments is further compounded by acts of terrorism, violent extremism, and the proliferation of local armed groups, as seen in Iraq, northern Nigeria, Afghanistan, northern Mozambique, Mali, Niger, and Burkina Faso, where extremist actors deliberately target civilians, state institutions, and humanitarian personnel [1]. Groups such as the Islamic State of Iraq and Syria (ISIS)and affiliates, Al-Shabaab, Boko Haram, and Al-Qaeda, have been responsible for severe harm, loss of life, and systematic violations of international humanitarian law directly obstructing humanitarian access and disrupting life-saving operations in these countries [1].

The dynamics in insecure humanitarian environments create a layered, unpredictable threat environment that demands continuous monitoring, adaptive and context specific security risk management. To meaningfully continue operating in complex and insecure environments, Humanitarian Security Risk Management (HSRM) and Business Continuity Planning (BCP) have emerged as central to operational resilience. HSRM provides the analytical and procedural foundation for understanding threats in the environment, negotiating access, and ensuring staff safety, enabling humanitarian organisations to maintain presence in the most volatile settings [2]. BCP complements this by identifying critical functions, mapping operational needs, and establishing alternative modalities for programme delivery when normal operations are compromised [2]. Operational resilience provides the capacity for humanitarian organisations to absorb shocks, adapt rapidly, and continue delivering essential services even when safety and security conditions deteriorate [2]. Together, the three frameworks form the backbone of an organisation's ability to anticipate, absorb, and adapt to shocks while upholding duty of care to staff and humanitarian principles [2]. Their integration has become essential to build a unified system that ensures staff safety, continuity of services that sustain humanitarian presence and protecting affected populations in insecure environments where volatility is the norm rather than the exception. This enables humanitarian organisations to maintain life-saving services in crises situations and times of uncertainty.

The practical implementation of HSRM, BCP and operational resilience varies widely across humanitarian organisations, reflecting differences in mandate, institutional culture, resources, leadership priorities, and operational models [3,4]. Despite broad consensus that all three frameworks are essential for sustaining humanitarian action in insecure environments, they are often developed and executed as separate technical functions rather than as components of a unified system. By examining how HSRM, BCP and operational resilience interact, overlap, and influence decision-making, this study highlights the need for integrated approaches that enable humanitarian organisations to anticipate disruptions, protect staff, sustain essential services, and remain operationally present in insecure humanitarian settings.

The study demonstrates how an integrated HSRM–BCP-Operational resilience approach enables humanitarian organisations to anticipate disruptions, absorb shocks, adapt rapidly, and continue delivering assistance in conflict-affected environments where volatility is regular. In volatile environments where disruptions are inevitable, neither framework on its own is sufficient, it is their combined application that enables organisations to protect staff, sustain critical functions, and maintain humanitarian presence despite instability. The argument is that operational resilience depends on the integration of humanitarian security risk management and business continuity planning.

2. The Humanitarian Operational Environment: Nature of Risks and Disruptions

Humanitarian operations in insecure environments unfold within complex and highly volatile operational landscapes shaped by diverse forms of conflict, political instability, chronic insecurity and natural disasters. Many contexts are characterised by international or internal armed conflict, where fighting between states, or between governments and organised armed groups, generates large-scale displacement and acute humanitarian needs. Countries such as Ukraine, Yemen, Gaza, Sudan, Somalia, and the Democratic Republic of Congo are illustrative of environments where frontlines shift rapidly, civilian populations are repeatedly uprooted, and humanitarian

organizations must navigate complex fragmented territorial control [5]. Even in post-conflict settings such as Iraq, Colombia, Ethiopia, South Sudan, Syria, or Libya, persistent or residual violence, weak governance, and fragile peace agreements continue to disrupt humanitarian access and space, threaten staff safety and complicate humanitarian operational planning [5]. These environments are defined by uncertainty, fluidity, and the constant potential for sudden escalation.

The risk landscape is further shaped by terrorism, violent extremism, and the presence of non-state armed groups (NSAGs) and localised armed groups pursuing political, economic, or community-based agendas. In contexts such as Iraq, northern Nigeria, Afghanistan, northern Mozambique, Mali, Niger, and Burkina Faso, some extremist groups deliberately target civilians, state institutions, and humanitarian actors, creating unacceptable security risks that can shift within hours [5]. Local militias, vigilante groups, and community-based armed actors also exert influence, often controlling territory, imposing informal taxation, or interfering with aid delivery when their interests are not met [5]. In displacement settings, the presence of armed combatants or ex-combatants within refugee or internally displaced persons (IDP) camps can create parallel governance structures that undermine civilian administration and expose humanitarian staff and beneficiaries to intimidation or violence [5]. These dynamics create a layered and unpredictable threat environment that requires constant monitoring and adaptive security risk management strategies.

Operational disruptions are a routine feature of insecure humanitarian environments and can significantly impede humanitarian delivery. Access constraints arise from active hostilities, bureaucratic impediments, roadblocks, or the presence of improvised explosive devices, often forcing humanitarian organisations to suspend movements or rely on remote management [5]. Relocations, evacuations or hibernation measures may be triggered by sudden outbreaks of violence, political unrest, or targeted attacks on humanitarian personnel. Communications failures due to diverse reasons, whether due to infrastructure damage, government shutdowns, or cyberattacks can sever links between field teams and coordination hubs. Supply-chain interruptions, including fuel shortages, border closures, or looting of warehouses, further complicate the continuity of operations. High levels of criminality, including kidnapping, armed robbery, extortion, and gender-based violence, add another layer of risk that affects both humanitarian staff safety and the security of programme assets. Civil unrest, protests, or strikes whether by host communities, displaced populations, or national actors can further destabilise operations and heighten tensions around humanitarian assistance delivery.

These disruptive conditions have significant implications for staff safety, programme continuity, and operational resilience. Humanitarian programmes may be disrupted, scaled down, or temporarily suspended when security thresholds are breached, yet affected populations continue to rely on uninterrupted humanitarian assistance. The cumulative effect of these risks underscores the necessity of integrating HSRM, BCP, and operational resilience into a unified system. Such integration allows humanitarian organisations to anticipate disruptions, protect staff, maintain critical functions, and sustain humanitarian presence in insecure environments where volatility is the norm rather than the exception**.**

3. Conceptual Framework

This study is anchored in the intersection of humanitarian security risk management, business continuity, and operational resilience, recognising these three frameworks as mutually reinforcing components of effective humanitarian action in insecure environments. Together, they form a holistic approach in which threat mitigation, staff safety (duty of care), continuity of critical functions, and adaptive capacity in crisis situation, are not treated as separate technical areas but as interconnected processes that shape an organisation's ability to operate safely, effectively and dependably in volatile humanitarian environments. By analysing how the three intersect, reinforce one another, and shape humanitarian operational choices, the study demonstrates the necessity of integrated approaches that enable humanitarian organisations to anticipate disruptions, sustain staff safety, sustain critical services, and maintain continued operational presence in insecure environments.

The conceptual framework underpinning this study positions humanitarian security risk management (HSRM) as the foundational layer upon which all other organisational resilience mechanisms are built. HSRM provides the essential processes of situational analysis, threat assessment, security risk assessment, and implementation of mitigation and preventive measures. This also includes compliance with established security standards such as United Nations designated area security risk management measures, minimum operating security standards (MOSS) and non-governmental organizations (NGO) security frameworks and protocols and global humanitarian guidelines and norms [2]. These functions create the baseline conditions that allow humanitarian organisations to operate safely in insecure environments. In insecure and volatile humanitarian environments, without robust security risk management foundation, humanitarian operations are exposed to unacceptable levels of risk ranging from targeted violence to access denial that can rapidly undermine staff safety and programme continuity. In this regard, HSRM is more than a technical function that ensures staff safety and well-being but is also the structural bedrock of operational resilience [2].

At the next level is business continuity planning (BCP) functions as the adaptive mechanism within the conceptual framework. BCP equips humanitarian organisations with the tools and strategies needed to maintain or rapidly restore operations when disruptions occur [6]. This includes establishing alternate work sites, enabling remote programming, strengthening local partnerships, and building redundancy into logistics and communications systems. In conflict-affected settings, these measures allow organisations to continue delivering essential services even when staff must relocate or access routes are compromised. BCP therefore transforms HSRM's risk insights into tangible resilience measures, ensuring that humanitarian operations can absorb shocks and adapt to rapidly changing conditions [6]. In practice this means HSRM provides the situational awareness, while BCP operationalises that awareness into structured preparedness.

Building on this foundation, the conceptual framework identifies the integration of HSRM and BCP as a critical bridge that connects risk awareness to organisational preparedness. Continuity planning draws directly from HSRM outputs, translating security risk assessments into practical operational safeguards [2]. Continuity frameworks such as BCP are the operational expressions of humanitarian security risk management. They translate security risk assessments into actionable protocols that ensure staff safety, protection of assets, and beneficiaries in volatile environments [2]. For example, threat analysis informs decisions on security measures to be implemented, site selection, safe-room design, relocation or evacuation triggers, and the viability of remote management. Similarly, HSRM insights shape supply-chain diversification, partner-led delivery models, and the identification of critical functions that must be preserved during crises. This integration ensures that continuity planning is grounded in real time risk analysis rather than abstract assumptions.

The combined effect of a strong HSRM foundation and an adaptive BCP mechanism is the emergence of operational resilience. This is the capacity of humanitarian organisations to sustain critical functions in volatile and conflict-affected environments. Operational resilience is reflected in the continuity of humanitarian assistance, the safety of staff, the preservation of donor confidence, and the maintenance of community trust [6]. It is not a static but an ongoing organisational capability that enables humanitarian organizations to navigate uncertainty, recover quickly from disruptions, and maintain principled humanitarian presence even under extreme pressure.

Finally, the conceptual framework incorporates a feedback loop that ensures continuous improvement. Operational experiences whether successful adaptations or failures feed back into both HSRM and BCP processes. Lessons learned from disruptions refine risk assessments, strengthen continuity strategies, and inform future planning cycles. This iterative loop transforms resilience from a one-time achievement into a dynamic organisational practice. By continuously integrating field learning into risk and continuity systems, humanitarian

organisations enhance their ability to anticipate emerging threats, adapt to evolving contexts, and sustain operations in some of the world's most insecure environments [6].

4. Developing Common Understanding: HSRM, BCP and Operational Resilience

To provide a clear theoretical foundation for this study and a common understanding, the key concepts of humanitarian security risk management, business continuity planning, and operational resilience are defined and examined. The gaps in implementation by humanitarian organizations and the need for integration are interrogated. This is essential for understanding how humanitarian organisations function in insecure environments and why effective integration of humanitarian security risk management, business continuity planning and operational resilience is critical for staff safety, sustaining safe humanitarian access, and ensuring uninterrupted delivery of humanitarian assistance.

4.1 Humanitarian Security Risk Management (HSRM)

Security Risk Management (SRM) refers to the systematic process of identifying, analysing, and mitigating threats that may affect an organisation's personnel, assets, reputation, and operations [7,8,9]. In humanitarian contexts, HSRM encompasses threat analysis, access strategies, mitigation measures, incident management, and crisis response mechanisms tailored to complex and often unpredictable environments [7,8,9]. Security risk management in humanitarian operations has substantially evolved since the early 2000s, driven by the sharp rise in complex emergencies and increasing deliberate attacks on aid workers in places like Afghanistan, Somalia, Sudan, South Sudan and Iraq [10,11]. After several high profile attacks against humanitarian personnel including the Baghdad bombing of August 2003, which killed at least 22 people including the UN Secretary General's Special Representative for Iraq and wounded more than 160 others, several global reviews were made on the safety and security of humanitarian personnel [12]. The UN subsequently passed Security Council Resolution 1502, which declared deliberate attacks against humanitarian organizations or peacekeepers, a war crime [13]. The United Nations Department for Safety and Security (UNDSS) was formally established in January 2005 to manage the safety and security of UN personnel, assets, and operations worldwide [10]. At the same time, NGOs and independent humanitarian organisations, such as ICRC significantly strengthened their own security risk management systems, recognising that safe access in volatile environments required structured, professionalised approaches to managing risks [10].

The contemporary advancement of humanitarian security management frameworks and the development and implementation of attendant security risk management strategies is therefore directly linked to the increased dangers in the humanitarian operational environment [10]. Many humanitarian organizations operating in insecure environments have institutionalized security risk management in order to continue operating in those environments. The evolution led to the development of formal security risk management strategies focused on identifying threats, analysing risks, and implementing context-appropriate mitigation measures [10]. Modern HSRM now centres on enabling operations rather than restricting them, balancing threat mitigation, duty of care, access, and continuity of programmes [10]. By systematically managing threats and defining acceptable risk levels, humanitarian organisations are able to protect personnel, maintain presence, and deliver assistance more reliably in insecure settings. The objective of humanitarian's security risk management is to allow humanitarian organizations to carry out their mandates to meet their stated objectives while managing security risks in the environment [8,9]. The thrust is that security risks should be systematically managed for humanitarian assistance to be delivered safely to communities in need.

Humanitarian security risk management is built on a set of several principles that enable humanitarian organisations to operate safely and predictably in volatile environments. The core principles are threat mitigation, duty of care, access and continuity of operations [14,15].Threat mitigation focuses on identifying, analysing, and reducing the risks in the operational environment[16]. Risks come from diverse threats posed by armed conflict, crime, political instability, civil unrest, natural hazards and others. Threat mitigation is achieved

through context-specific policies, procedures, and protective and acceptance measures that lower exposure without undermining humanitarian objectives[16]. Duty of care reinforces the organisation's legal and ethical responsibility to safeguard staff by ensuring that decisions, resources, and operational practices prioritise staff safety and wellbeing[16].

Complementing threat mitigation and duty of care, is humanitarian access and continuity of operations that ensure humanitarian action remains possible even when conditions deteriorate. Humanitarian access requires understanding the environment, engaging with stakeholders, and managing risks in ways that preserve acceptance and operational space[17,18]. Continuity of operations ensures that essential programmes can continue or are rapidly restored through contingency planning, redundancies, and adaptive ways of working[2]. Together, these principles create a coherent approach that protects humanitarian personnel, sustains presence, and enables reliable delivery of assistance in insecure humanitarian environments.

The effectiveness of humanitarian security risk management in volatile environments depends fundamentally on its integration with business continuity planning and broader operational resilience systems, because security risks and operational disruptions are deeply interconnected in insecure humanitarian settings. HSRM provides the threat analysis, access strategies, and protective measures that enable staff to operate safely, while BCP ensures that critical functions can continue or rapidly recover when insecurity, political shocks, or logistical breakdowns interrupt normal operations[2]. When these systems are aligned, security thresholds trigger continuity actions, continuity plans are grounded in real threat dynamics, and resilience measures are designed to sustain presence even when conditions deteriorate[2]. This integrated nexus allows humanitarian organisations to anticipate disruptions, adapt operations without compromising safety, and maintain essential services for affected populations despite the volatility that defines insecure humanitarian environments.

4.2 Business continuity planning (BCP)

BCP in humanitarian contexts refers to the structured process by which an organization ensures that critical life-saving and protection activities can continue despite insecurity, shocks, or operational disruptions[6,19,20]. BCP principles must adapt to the complex context, realities of conflict, displacement, diverse security threats, weak infrastructure, and volatile access. BCP is not about preserving business functions for profit, the classical BCP position. It is about preserving humanitarian impact, duty of care, and principled humanitarian operations when the environment becomes unstable[6,19,20]. Business Continuity Planning (BCP) focuses on ensuring that essential functions can continue or can be rapidly restored during and after a disruption. It includes continuity strategies, recovery procedures, resource prioritisation, and organisational resilience measures that allow operations to withstand shocks such as attacks, displacement of staff, infrastructure failures, or sudden access constraints[6,19,20].

The evolution of Business Continuity Planning (BCP) in humanitarian organisations is closely tied to the increasing volatility of humanitarian operations since the early 2000s. After major global shocks, such as the USA 9/11 attacks in 2001, Afghanistan(2001 and thereafter) conflicts, the Iraq attacks in 2003, the 2004 Indian Ocean tsunami, and the surge in complex emergencies such as Sudan -Darfur 2003 and Somalia 2005, humanitarian organizations recognised that continuity could no longer be assumed, it had to be deliberately planned[21]. Humanitarian organizations accepted that traditional contingency planning was insufficient for maintaining life-saving operations during prolonged insecurity and system-wide disruptions. Continuity planning became essential to ensure that life-saving activities such as food assistance, health services, and protection could continue even when normal systems were compromised. BCPs emerged as the operational safety net that reduces vulnerability, strengthens resilience, and protects both humanitarian personnel and affected communities[21].

As humanitarian operations became increasingly exposed to insecurity, political instability, and large-scale disasters, BCP frameworks were progressively adapted from the private sector into the UN system and the wider humanitarian community. This shift aimed to ensure that critical humanitarian functions could continue during crises such as relocations, evacuations, access constraints, and operational disruptions. The United Nations, major NGOs, and independent humanitarian organisations including IFRC, the Red Cross Movement, and MSF have since developed policy frameworks to institutionalise continuity and resilience in high-risk environments[2]. Within the UN system, the Organizational Resilience Management System (ORMS) (CEB/2014/HLCM/17) identifies business continuity management (BCM) as a core element, setting standards to ensure that UN agencies can sustain essential functions during emergencies[22]. Complementing this, the UN Security Policy Manual outlines security and operational resilience requirements to protect personnel and maintain operations in volatile contexts[23]. UN Agency-specific guidance such as UNHCR, WFP, UNICEF and WHO BCP guidelines provides structured approaches for maintaining critical operations during and after disruptive events[19,24].

Across the NGO sector, continuity and resilience practices are shaped by internal frameworks, inter-agency standards, global humanitarian frameworks and norms. Many NGOs develop their own business continuity plans (BCPs), crisis-management protocols, and security risk management systems. NGOs also align their preparedness and continuity measures with Inter-Agency Standing Committee (IASC) guidance, including the Humanitarian Programme Cycle (HPC), which emphasises risk management, preparedness, and operational continuity as prerequisites for effective response[2]. IASC Emergency Response Preparedness (ERP) guidance requires humanitarian organizations to plan for continuity of critical functions during shocks[2]. The Sphere Standards further reinforce these expectations by setting global minimum requirements for humanitarian action, including preparedness, risk reduction, and continuity of essential services in disaster and conflict settings[2]. Further, core Humanitarian Standard (CHS), emphasizes organisational preparedness, risk management, and adaptive capacity. Together, the frameworks, standards, guidance and norms have driven humanitarian sector-wide shift toward more systematic, integrated approaches to continuity and resilience, ensuring that humanitarian organisations can sustain life saving and protection activities even in the most volatile operational environments.

UN agencies and NGOs regularly activate BCPs when safety and security conditions deteriorate to unacceptable levels, requiring relocation, evacuation, or alternative work modalities; during major health emergencies such as Ebola or COVID-19; and in anticipation of severe weather events like cyclones, tsunamis, or earthquakes. Contemporary examples include Syria, Yemen, South Sudan, Sudan, Myanmar, Bangladesh, Afghanistan, Somalia, Libya, and the DRC, highly complex contexts where BCPs are routinely activated to ensure staff safety and maintenance of critical humanitarian operations amid persistent instability and weather events[2].

Business continuity planning in volatile humanitarian environments offers clear strengths but also faces significant constraints. Its primary advantage lies in providing a structured approach that helps humanitarian organisations identify critical functions, establish alternative delivery modalities, and maintain life-saving services even when insecurity disrupts normal operations[6,21]. Well-developed continuity plans reduce operational paralysis and support rapid adaptation ensuring that essential activities such as health services, water and sanitation, protection activities, or cash assistance continue despite relocations or evacuations, access restrictions, or supply-chain breakdowns[2]. However, BCP is often constrained by the unpredictability of conflict dynamics, limited communications infrastructure, and the difficulty of implementing redundant systems in resource-poor settings[2]. Plans may become unrealistic when they do not fully account for security constraints, rely too heavily on expatriate staff presence, or assume stable logistics and partner capacity[2]. In many contexts, sudden escalations of violence, bureaucratic impediments, or community displacement can outpace even the best continuity strategies.

The effectiveness of BCP in volatile humanitarian environments depends on its tight integration with HSRM because both systems address different dimensions of the same problem- sustaining operations amid persistent

and unpredictable threat environment. HSRM focuses on understanding the threat environment, protecting staff, and enabling safe access, while BCP ensures that critical functions can continue or rapidly recover when disruptions occur. When combined, they create a unified resilience framework that links security analysis to continuity strategies, aligns triggers for operational adaptation, and ensures that decision-making is grounded in both risk realities and programmatic priorities. This nexus allows humanitarian organisations to anticipate shocks, maintain essential services during crises, and preserve humanitarian presence even when insecurity, displacement, or operational disruptions escalate.

4.3 Operational resilience

Operational resilience in humanitarian settings is the organisation's ability to withstand shocks, adapt to rapidly changing conditions, and continue delivering life-saving assistance despite disruptions [4,6,25]. It reflects how well an organisation can anticipate risks, absorb the impact of crises such as armed conflict, terrorism, civil unrest, disasters, or epidemics, and maintain critical functions without collapsing [25,26,27]. In essence, operational resilience ensures that humanitarian presence, staff safety, and essential services remain reliable even in the most volatile environments. This particularly depends on the organisation's ability to anticipate shocks, absorb disruptions, and continue delivering essential services, such as health, food, water, shelter and protection despite insecurity, disasters, or system failures [25,26, 27].

Operational resilience in volatile humanitarian environments is only effective when it is fully integrated with HSRM and BCP, because resilience depends on both the ability to withstand shocks and the ability to operate safely within insecure settings [2]. HSRM provides the threat analysis, access strategies, and protective measures that enable staff to function amid insecurity, while BCP ensures that critical activities can continue or rapidly recover when disruptions occur [2]. Together they create the conditions for operational resilience, where organisations can absorb shocks without losing their ability to operate. By integrating these frameworks, humanitarian actors build a unified system that maintains safe access, continuity of services, and adaptive capacity even in the most insecure environments [28]. Significantly, when these frameworks are aligned, insecurity thresholds trigger continuity actions, continuity plans are then grounded in real-time risk dynamics, and resilience measures are designed to sustain presence even during all periods of volatility or instability[28].This nexus creates a coherent, adaptive framework that allows organisations to anticipate disruptions, protect staff, and maintain essential services for affected populations despite the volatility that defines humanitarian operations in insecure environments.

4.4 The Gap

A persistent gap in humanitarian operations is that HSRM, BCP and operational resilience are often developed and implemented as separate, parallel systems rather than as a single integrated framework. Research by ALNAP, GISF, Humanitarian Outcomes, and the UN Inter-Agency Standing Committee (IASC) shows that humanitarian organisations frequently maintain siloed approaches to risk management, continuity planning, and operational resilience due to differences in mandate, institutional culture, leadership priorities, and organisational structures [14,15,27,29,30]. This fragmentation weakens humanitarian organisations' ability to anticipate and manage disruptions in volatile environments, and limits coherence in decision-making compromising the ability of organisations to sustain operations during complex crises [14,15,27,29,30].

The consequence is that humanitarian organisations struggle to maintain presence when crises escalate, because the systems designed to ensure staff safety, sustain critical functions, and adapt operations are not aligned [3,14,15,30]. Without integration, security thresholds may trigger relocations or evacuations without corresponding continuity measures, or continuity plans may assume operational conditions that are no longer viable due to insecurity [3,6,15,30]. Operational resilience intended to ensure that essential services continue despite shocks cannot be achieved if security and continuity planning are disconnected. Integrating HSRM, BCP, and operational resilience into a unified system enables humanitarian organisations to link threat analysis to

continuity actions, align action triggers and decisions, and design adaptive strategies that preserve both staff safety and programme delivery [3,6,14,30].In volatile humanitarian settings, this integration is not optional, it is the foundation for ensuring staff safety, sustaining humanitarian presence and protecting affected populations amid persistent instability.

4.5 The call for integration:

The integration of humanitarian security risk management (HSRM), business continuity planning (BCP), and operational resilience is essential in insecure environments. Yet, as studies show, many humanitarian organisations continue to treat these frameworks as separate technical workstreams, operating independent of each other. This fragmentation creates structural blind spots leading to flawed judgments, unanticipated problems, or critical failures [3,6,14,15]. For example, security teams might focus on threat mitigation and duty of care while continuity planners concentrate on maintaining critical functions, and resilience efforts remain broad organisational aspirations rather than operationalised practices. When these disciplines operate in isolation, risk analysis does not fully inform continuity planning, continuity plans overlook the constraints imposed by insecurity, and resilience strategies remain conceptual rather than embedded in daily decision-making [3,6,14,15]. The result is a system that reacts to crises rather than anticipating and absorbing them.

Contemporary examples demonstrating the need for integration include Gaza and Southern Israel (2023–2025): Northeast Nigeria (2023–2024): Sudan (2023–2025): Ukraine (2022–2025): Mozambique-Cabo Delgado (2020–2025) [7,31,32,33,34,25,36]. Across these contexts, the evidence was clear, and the pattern was consistent that security risk management alone can protect staff but cannot sustain programmes and continuity planning alone can preserve critical functions but fails when field security realities are ignored [6,7,28,37]. Operational resilience emerges only when the two are integrated into a single decision-making system. The contemporary evidence is thus clear that humanitarian organisations that integrate HSRM, BCP, and resilience frameworks maintain presence longer, recover faster, and deliver assistance more dependably in insecure environments [6,7,28,37].

A unified approach that brings HSRM, BCP, and operational resilience into a single system enables humanitarian organisations to anticipate disruptions more effectively and respond with greater coherence and sustainability. Research by ALNAP, GISF, Humanitarian Outcomes, and the IASC shows that fragmented approach to HSRM, BCP and operational resilience weakens humanitarian organisations' ability to anticipate and manage disruptions in volatile environments [15,27,29,30]. When risk analysis directly informs continuity strategies, continuity plans become realistic and implementable under difficult and diverse field conditions. When continuity priorities shape security decision-making, staff safety measures are aligned with programme criticality rather than applied uniformly [6,7,28,37]. And when both are embedded within a broader resilience framework, organisations develop the adaptive capacity needed to maintain presence in insecure settings [6,7,28,37]. This integrated approach transforms resilience from an abstract concept into a practical capability allowing humanitarian organisations to absorb shocks, adapt rapidly, and continue delivering essential assistance even as insecurity intensifies and humanitarian needs rise.

5. Humanitarian Security Risk Management, BCP and Operational Resilience in Practice

Humanitarian security risk management (HSRM), business continuity planning (BCP), and operational resilience converge most visibly in the day-to-day realities of humanitarian action in volatile and unpredictable environments.

5.1 Humanitarian Security Risk Management

HSRM in practice provides the immediate mechanisms through which organisations understand and navigate threats and risks, negotiate access, and protect their staff. HSRM begins with systematic, continuous threat and risk analysis, which forms the foundation for all operational decision-making in insecure environments

[7,38,39,40]. This process involves a range of activities which include assessing security threats, armed-actor dynamics, criminality, political instability, community tensions, and environmental hazards to determine how these factors may affect staff safety, organization assets, and humanitarian programme delivery[7,38,39,40]. For humanitarian organisations operating in insecure contexts such as Ukraine, Syria, South Sudan, Sudan, Yemen, Afghanistan, the Central African Republic, eastern Democratic Republic of Congo, northern Nigeria, Mali, Niger, and Libya, embedding rigorous risk analysis into daily operations is not optional but very essential for maintaining staff safety fulfilling duty of care to staff and safe access to conduct humanitarian operations[7,10,16]. In these diverse settings, threats evolve rapidly, frontlines shift unpredictably, and access can be lost within hours, making real-time risk assessment a critical operational imperative and competency rather than a periodic administrative exercise.

A core component of HSRM in practice for humanitarian organizations operating in insecure environments is the routine conduct of threats assessment, security risk assessments, context assessments, conflict-sensitivity analyses, and stakeholder mapping to understand the intentions and capabilities of armed actors, criminal networks, and political authorities[7,10,11,30].To be effective, this analytical process must be systematically integrated into organisational security strategies, informing programme design, contingency planning, and crisis response[7,10,11,30].These security processes are underpinned by policy and security management frameworks. For example, the UN security management system (UNSMS) follows the UN Security Risk Management (SRM) approach to manage security risks [41,42]. The UN Security Risk Management (SRM) approach evaluates the operational context in which UN activities take place, identifying the specific threats that may affect personnel, assets, and programmes in order to determine corresponding risk levels[16,41,42]. These security assessments form the basis for security management decisions aimed at reducing risks to acceptable thresholds. In line with this approach, the UN system is required to develop and implement security policies, procedures, and context-specific measures that are directly informed by security risk assessments (SRAs) allowing for a coherent and evidence-based framework for managing security in diverse and often volatile environments[16,41,42].

NGO humanitarian organizations have security policies and frameworks that ensure staff safety and continuity of operations in the most unstable environments. NGO humanitarian organizations and independent organizations such as, International Committee of the Red Cross (ICRC) have specific security risk management frameworks that are tailored based on their mandate, risk tolerance, and operational footprint[37,38]. International NGOs like Save the Children, OXFAM, CARE, World Vision, Building Resources Across Communities (BRAC), Plan International, Mercy Corps, International Rescue Committee (IRC), among many others have security management policies and frameworks that emphasize staff safety and continuity of operations[37,38]. These international NGOs are very active in high risk environments such as Ukraine, Syria, South Sudan, Sudan, Yemen, Afghanistan, the Central African Republic, eastern Democratic Republic of Congo, northern Nigeria, Mali, Niger, and Libya. Non-Governmental organizations(NGOs) also follow Global Interagency Security Forum (GISF) guidelines which provide practical tools for NGOs to develop security risk management strategies that are context sensitive and field-adaptable[43,44]. Resources include templates and toolkits for setting up safety, security, contingency plans and risk management SOPs in humanitarian contexts[44,45]. The GISF Security to Go Toolkit offers modular SOP and Contingency templates for rapid-onset emergencies in insecure environments [45,46].

Another core component of HSRM in practice is the implementation of security protective measures and operational protocols that enable staff to work safely despite persistent insecurity. These security measures translate security risk assessments into concrete operational systems that reduce staff exposure to threats while preserving humanitarian access and continuity of operations. For example, security protective measures may include implementation of movement controls and journey management systems such as route-risk assessments, movement tracking, and mandatory check-ins to ensure travel occurs only on assessed and

approved roads and at safe times[37,38]. Compound facilities are reinforced through perimeter walls and fencing, access-control systems, safe rooms, guarding system, and blast protection to reduce vulnerability to intrusion or attack. Staff preparedness is strengthened through context-specific regular security briefings, training, such as hostile environment awareness training (HEAT) and scenario-based exercises that equip staff to navigate difficult situations such as checkpoints, civil unrest, ambushes, or improvised explosive devices (IED) threats[7,10,37,38]. Robust and redundant communications systems, including satellite phones, VHF radios, GPS trackers, and emergency call trees, ensure field staff and team members remain connected even when networks fail or are deliberately shut down, a routine in some insecure environments[10,16,37,38].

These security protective measures are complemented by protocols that guide staff behaviour and conduct and organisational decision-making during heightened risk. For example, incident-driven procedures for hibernation, relocation, or evacuation provide clear actions to be followed when violence escalates or staff are directly threatened and the risk has to be managed[10,16,37,38]. Staff are also trained in checkpoint conduct and armed-actors engagement to de-escalate encounters and minimise risk in militarized or contested environments. Other security protective measures such as compound access and visitor-management systems, identity verification and controlled entry prevent infiltration, theft, or targeted harm[7,10,37,38]. Together, these security protective measures form the operational backbone of HSRM in practice, enabling humanitarian organisations to maintain presence and deliver assistance in volatile environments.

HSRM in practice also involves continuous engagement with communities, authorities, and diverse armed actors to maintain acceptance and negotiate humanitarian access. Acceptance-based strategies such as sustained engagement with community leaders, informal power brokers, and local authorities help reduce tensions and build trust, lowering the likelihood of interference or targeted attacks[10,15,16]. Many humanitarian organizations, particularly NGOs, rely heavily on acceptance-based strategies, investing in community liaison officers, local staff networks, and transparent communication to reduce the likelihood of targeted attacks[14,15,16,29]. In eastern DRC, for instance, humanitarian access negotiations became increasingly complex in 2024–2025 due to escalating conflict, shifting armed-group control, and severe movement restrictions[53,54,55]. Negotiations focussed on securing safe passage along key road corridors, reopening blocked routes, and maintaining operational presence amid intensified insecurity. Humanitarian organisations worked closely with community leaders and local staff to negotiate safe access to displacement sites, reducing reliance on armed escorts[53,54,55]. In Afghanistan, organisations such as the International Committee of the Red Cross (ICRC) and several NGOs have historically negotiated access with multiple armed groups by emphasising neutrality, impartiality, and the humanitarian imperative[15,29,56]. Similarly, in South Sudan, community engagement has been essential for securing safe passage for mobile health teams operating in areas controlled by shifting alliances of armed actors[57, 58,59].

HSRM in practice in both UN system and NGOs generally follows similar approaches but may differ in implementation due to a variety of factors which include mandate, resources available, culture and risk appetite. UN agencies typically operate under the UN Security Management System (UNSMS), to manage security risks. The UN Security Risk Management (SRM) approach begins with a structured assessment of the operational environment, identifying the diverse spectrum of threats that may affect UN activities and determining the corresponding risk levels[23].This analysis provides the foundation for all security decision-making, enabling context and area specific security measures to be implemented, that reduce risks to levels deemed acceptable for safe and effective UN programme delivery[16,23,37].The security risk management measures implemented are generally classified in categories of security management procedures, physical security, equipment and supplies, training, medical, telecommunications, vehicles, residential security, and structured incident-reporting systems [16,37,38]. These security risk management measures are a typical expression of HSRM in practice as they provide among others, security protective frameworks in UN operations. For example, compound physical security measures such as high walls and presence of armed guards at UN compounds are protection security

risk management measures. Significantly, the implementation of context and area specific security risk management measures within the UN system enables UN agencies to fulfill their diverse mandates while at the same time ensuring staff safety and continuity of operations within acceptable risk thresholds[16,37,38].

NGOs, while generally more flexible than UN agencies, also often adopt security protective frameworks tailored to their operational footprint, organisational culture, and acceptance strategies. Many NGOs rely heavily on community engagement and local networks to build acceptance and reduce the likelihood of targeted attacks[16,37,38]. However, NGOs operating in insecure contexts routinely adopt layered protective strategies that include secure compounds, guarding systems, movement tracking, communications redundancy, and context-specific travel protocols[10,16,37,38]. For example, in northeast Nigeria, NGOs use armed-group mapping, daily movement clearance procedures, and vehicle tracking systems to reduce the risk of ambushes and kidnappings along insecure roads[29,32,33]. In Yemen, organisations rely on hardened offices, safe rooms, and satellite communications to maintain staff safety during airstrikes or sudden escalations[47,48,49,50]. Protective frameworks in contexts such as Somalia and Yemen, include the use of armed escorts for road movements. Similarly, in South Sudan, UN and NGOs implement curfews, radio check-ins, and phased hibernation–relocation–evacuation (HRE) procedures that allow teams to shelter in place or withdraw safely when fighting intensifies[51,52]. These protective measures are not static, they are continuously adapted to reflect changes in threat patterns, community dynamics, and operational needs. The reality on the ground is that NGOs blend protective measures, operational protocols, and community-based acceptance strategies to maintain presence and deliver assistance in some of the world's most volatile environments[10,14,15].

The UN and NGOs approaches demonstrate that HSRM is not merely a technical function but a relational practice that depends on, contextual understanding, trust-building and the ability to navigate complex security, political and social landscapes. When effectively implemented, HSRM enables humanitarian organisations to remain operational in insecure settings while upholding duty of care and humanitarian principles[7,10,16]. Good humanitarian security risk management strategies must significantly address the security threats in the operating environment with the objective of reducing the impact and likelihood of undesirable events or incidents that may affect humanitarian personnel[7,10,16].

5.2 Business Continuity Planning

Business Continuity Planning (BCP) in insecure humanitarian settings is fundamentally about sustaining life-saving operations when security or hazards conditions deteriorate. Humanitarian organizations have activated BCPs in many insecure humanitarian operations when the security situation deteriorated to unacceptable levels requiring relocation or evacuation of staff or other extraordinary temporary work modalities. BCP has also been activated due to health pandemic (e.g., significant community transmission considered a serious risk to staff and communities (e.g., Ebola and COVID 19) and expected excessive weather conditions e.g., cyclone, tsunami and flooding[2]. Business continuity plans (BCPs) and other operational continuity strategies have been activated by UN agencies and NGOs in insecure environments in several countries. In contexts like Syria, Yemen, South Sudan, Gaza, Ukraine, Northen Nigeria, Sudan, Myanmar, Afghanistan, Somalia, Libya, Eastern DRC, and Bangladesh among many others, UN agencies and NGOs frequently activate BCPs to safeguard personnel and maintain critical operations[2].

BCP in practice begins with the ability to maintain critical life- saving operations during disruptions, through for example, remote-management models or local implementing partner led delivery. When insecurity prevents international staff and others from accessing field locations as seen during the 2023 conflict in Sudan or repeated insurgent attacks in northeast Nigeria, national field teams and local partners assumed expanded responsibilities, supported by remote technical oversight[29,32,33,60 61 62]. These arrangements were not improvised, they were pre-planned continuity measures that ensured essential services such as health, nutrition, and protection continued even when physical access was compromised. In Gaza and Afghanistan local partner-based

programming has been central to sustaining humanitarian assistance during periods of intense volatility demonstrating how continuity planning enabled humanitarian organisations to remain operational despite severe constraints in the environment [63,64,65,66,67].

Another core element of BCP in practice is ensuring staff safety while sustaining programmes. This typically involves several structured processes that include, security risk assessments, scenario planning and activation of triggers that guide organizational field operational posture in crisis situations. Humanitarian organisations develop diverse phased response models depending on risk tolerance, ranging from full operations, alternate work sites, to remote management or hibernation, relocation and evacuation [3,15]. This is in most cases based on predefined thresholds linked to security incidents, political developments, or environmental hazards. Some of the decisions may follow a collective approach by humanitarian organizations. In South Sudan, for instance, continuity plans enabled humanitarian organizations to maintain essential nutrition and health services during periods of intense fighting by activating "skeleton team" models supported by local staff and community volunteers [57,68]. In Yemen, continuity strategies have included rerouting supply chains through alternative ports, decentralising procurement to field offices, and using digital cash transfers when physical distributions became unsafe[69,70]. Similarly, in Ukraine, humanitarian organizations activated relocation plans during the early months of the 2022 invasion, moving staff from high-risk areas while maintaining programme oversight from safer hubs in central and western Ukraine [71,72,73,74]. In eastern DRC, humanitarian organizations have repeatedly relocated staff from North Kivu, South Kivu and Uturi provinces during rebels attacks, relying on pre-identified safe sites and relocation and evacuation routes[53,54]. These measures are supported by robust and redundant communication systems which include satellite phones and radios, VHF radios, tracking systems and digital check-ins that allow organisations to maintain command and control even during communications blackouts, as seen in Yemen and Sudan[75,76]. These examples show that staff safety and programme continuity are mutually reinforcing pillars of BCP in practice.

BCP in practice also requires building redundancy into essential systems, ensuring that critical functions continue even when critical infrastructure collapses and access routes are blocked. In Gaza, where electricity and telecommunications are frequently disrupted, humanitarian organisations rely on backup generators, solar power, and satellite communications to maintain operational continuity [31,63,64,65]. In Ukraine, redundant power sources and distributed warehousing have been essential for sustaining humanitarian operations and others during regular and targeted missile attacks induced blackouts[35,73,77]. Supply-chain redundancy is equally vital. In Yemen, humanitarian organizations regularly diversify supply routes to mitigate port closures and access constraints[77,78,79,80]. The continuity strategies have included rerouting supply chains through alternative ports and routes, decentralising procurement to field offices, and using digital cash transfers when physical distributions became unsafe[77,78,79,80]. In South Sudan, pre-positioning supplies before the rainy season ensured uninterrupted assistance when roads become impassable[68,81]. These redundancies convert operational vulnerability into adaptive capacity, turning potential disruption into operational flexibility, demonstrating BCP in practice

BCP in practice also involves prioritising essential functions and reallocating resources to ensure that the most critical humanitarian activities continue during periods of volatility. In northern Nigeria, humanitarian organisations routinely prioritise life-saving health and nutrition services when insecurity soars and movement restrictions widen and tighten, temporarily causing the pausing of less critical activities [29,82]. After the Taliban takeover in Afghanistan in August 2021, several humanitarian organizations including UN agencies conducted rapid programme-criticality analyses to determine which humanitarian services and activities could continue under new restrictions and which required adaptation[83,84]. BCP in practice means resource reallocation is an imperative in emergency situations. For example, during the 2023 conflict in Sudan, some humanitarian organizations redirected funding and logistics capacity toward emergency response while scaling back

longer-term development programming [85,86]. These flexible decisions, guided by continuity plans, ensured that humanitarian organisations remained focused on their core mandate even under extreme pressure.

The above examples of BCP in practice from diverse insecure humanitarian contexts illustrate how BCP operationalises adaptability, ensuring that humanitarian organisations can continue delivering assistance even when the operating environment deteriorates rapidly. The examples also illustrate that BCP is not a static document but a dynamic operational system. It enables humanitarian organisations to absorb shocks, adapt to rapidly changing conditions, and sustain critical services in some of the world's most insecure environments. The success at individual humanitarian organization depend on many other factors including the extent to which BCP in institutionalized.

5.3 Operational Resilience

Operational resilience emerges when organisations can absorb shocks, adapt to disruptions, and continue delivering essential services despite repeated crises[2,28,87,88]. It is not a standalone function but the cumulative outcome of effective HSRM and BCP working in tandem[2,28]. An example comes from the response to cyclone Idai in Mozambique in 2019, where humanitarian organisations had to rapidly reconfigure operations after widespread flooding destroyed infrastructure and cut off access to many affected communities[89,90]. Humanitarian organizations that had pre-existing continuity plans and decentralised decision-making structures were able to mobilise local staff, re-establish supply routes, and resume life-saving activities within days, demonstrating operational resilience through rapid adaptation[90].

The humanitarian response in northeast Nigeria is another example where humanitarian organisations continue facing a combination of armed conflict, terrorism, displacement and high criminality. Over the past decade, humanitarian organizations have repeatedly had to relocate staff from towns such as Bama, Dikwa, and Monguno due to attacks by non-state armed groups[32,33,91,92]. Yet operations have continued through remote management, strengthened local partnerships, and pre-positioned supplies that allow programmes to resume quickly once access is restored[32,33,91,92]. This resilience is rooted in the integration of security analysis, continuity planning, and flexible operational postures that can withstand sudden shocks. Similarly, in Yemen, humanitarian organizations have maintained essential health and nutrition services despite airstrikes, fuel shortages, access constraints and bureaucratic impediments by decentralising authority to field offices, diversifying supply routes, and investing in local staff capacity[49,78,93,94]. These examples demonstrate that operational resilience is achieved when humanitarian organisations embed adaptability into their structures, enabling them to sustain humanitarian presence in environments where volatility is constant. This function is achieved together with effective security risk management and continuity planning.

Operational resilience also emerges when organisations are able to absorb shocks, adapt, and continue delivering assistance despite repeated disruptions. It is demonstrated through the ability to reorganise rapidly, reallocate resources, and maintain critical services even as the context deteriorates. In Yemen, for example, humanitarian organizations had to repeatedly adjust to airstrikes, fuel shortages, bureaucratic impediments, access constraints and shifting frontlines[49,78,93,94]. Their resilience is reflected in the capacity to reroute supply chains through alternative ports, decentralise decision-making to field offices, and maintaining remote management systems when access was denied. This adaptive capability is not a standalone function, rather it is the cumulative outcome of effective security risk management and continuity planning working in concert.

When humanitarian security risk management (HSRM), business continuity planning (BCP), and operational resilience are aligned, organisations are significantly better able to maintain presence and deliver impact in some of the world's most insecure environments. Integrated practice ensures that security risk assessments directly inform continuity strategies, continuity plans remain realistic within prevailing security constraints, and resilience becomes embedded in daily operations rather than activated only during crises [28,40, 95,96]. For example, in

northern Mozambique, Cabo Delgado, humanitarian organisations that synchronised security risk management and BCP were able to sustain essential protection and shelter activities during sudden insurgent advances by activating pre-agreed triggers, shifting to partner-led delivery, and relocating staff without halting critical services[97,98,99].

These examples from diverse insecure contexts illustrate that effective humanitarian action in insecure settings depends not on any single discipline, but on the coordinated application of all three- security risk management, continuity planning, and operational resilience functioning as an integrated system.

5.4 The Criticality of Integration

Integrating humanitarian security risk management, business continuity planning (BCP), and operational resilience is essential in insecure humanitarian environments because these systems address different parts of the same problem. The problem is how to keep life-saving operations running despite persistent threats to staff safety. Security risk management helps humanitarian organisations understand and mitigate threats and risks to staff and assets, while BCP ensures that critical functions can continue during disruptions such as attacks, displacement, or access constraints. Operational resilience ties these together by enabling humanitarian organisations to absorb shocks, adapt quickly, and recover without compromising assistance to affected populations. In volatile contexts like Syria, Yemen, South Sudan, Gaza, Ukraine, Northen Nigeria, Sudan, Myanmar, Afghanistan, Somalia, Libya, eastern DRC, Bangladesh and Northen Mozambique (Cabo Delgado) integration is particularly critical. In these contexts, armed attacks, displacement, and access volatility can halt operations overnight. An integrated approach prevents siloed decision-making, aligns security posture with programmatic priorities, and ensures that humanitarian staff and operations are safe, predictable, and sustainable even under extreme pressure[7,11,100,101]. Contemporary examples in insecure environments demonstrating the criticality for integrating humanitarian security risk management, business continuity planning (BCP), and operational resilience include:

- **Northeast Nigeria (2023–2024):** Humanitarian organizations managed to maintain presence despite ongoing insurgency in Northeast Nigeria. In Borno State, humanitarian actors faced chronic threats from non-state armed groups, road ambushes, and internally displaced camps infiltrations. Humanitarian organisations that aligned HSRM (security risk assessments, movement tracking, community acceptance, redundant communication systems, armed-group analysis) with BCP (skeleton-team models, remote management, alternative supply routes) demonstrated stronger operational resilience. When towns such as Dikwa or Monguno were temporarily overrun. Integrated systems allowed humanitarian organizations to relocate staff safely while sustaining critical health, nutrition and protection services through local partners and pre-positioned stocks[29,32,33,91, 92].
- **Sudan(2023–2025):** Responding to sudden state collapse and extensive urban warfare was extremely complex. The outbreak of conflict in April 2023 forced mass evacuations from Khartoum and Darfur. Humanitarian organizations with integrated HSRM–BCP systems were able to shift operations to Port Sudan, decentralise decision-making, and maintain cash-based assistance and health services through remote modalities. Those without integrated systems experienced prolonged operational shutdowns, loss of assets, and major gaps in programme continuity[61,102,103,104].
- **Ukraine(2022–2025):** Multi-hazard resilience in a high-intensity conflict has been shown the importance of integration. Humanitarian organisations in Ukraine have had to manage missile strikes, cyberattacks, power outages, and shifting frontlines. Integrated approaches allowed humanitarian organizations to combine security risk assessments (air-raid patterns, access negotiations, digital-threat monitoring) with continuity strategies (backup power systems, redundant communications, distributed warehousing). This enabled uninterrupted delivery of winterisation supplies and medical support even during nationwide infrastructure failures sustaining resilience[105,106].
- **Mozambique-Cabo Delgado (2020–2025):** Adaptive operations amid active non state armed groups insurgency sustained humanitarian organizations in Cabo Delgado. Humanitarian organisations that integrated

security analysis (insurgent movements, community acceptance, safe-route mapping) with continuity planning (mobile teams, partner-led delivery, relocation triggers) were able to maintain protection and shelter programmes during sudden attacks in Palma, Mocímboa da Praia, and Macomia. Integrated systems allowed humanitarian organizations to relocate staff without halting essential services, demonstrating the practical value of aligning HSRM BCP and operational resilience in a highly fluid conflict environment[36, 97,98,107].

- **Gaza and Southern Israel (2023–2025):** Humanitarian organisations operating in Gaza have had to regularly manage extreme volatility, mass displacement, and repeated communications blackouts. Humanitarian organisations that integrated security analysis (e.g., airstrike patterns, sustained access negotiations, deconfliction mechanisms) with continuity planning (e.g., remote operations, partner-led delivery, pre-positioned supplies) were able to maintain essential health and food assistance even during periods of intense bombardment. The 2025 Good Practice Review 8 highlights Gaza as a case where security risk management, digital-risk mitigation, and continuity strategies had to be fused to keep operations running under unprecedented constraints[7,31,108,109].

6. The Nexus Between HSRM, BCP and Operational Resilience

6.1 Conceptual Overlaps: The three share foundations in managing uncertainty. That is, managing what you do not know by recognising the limits of available information and data, anticipating a range of conceivable scenarios, and building flexible systems that allow humanitarian organisations to adapt as reality unravels. Humanitarian security risk management (HSRM), business continuity planning (BCP), and operational resilience are built on a shared foundation of anticipating, analysing, and preparing for disruptions. All three disciplines rely on systematic threats and risks identification and mitigation, scenario planning, and contingency development to navigate volatile environments and situations[11,23,100,101]. In humanitarian operations, this means continuously assessing threats such as armed-group activities, political instability, criminality, and infrastructure collapse and come up with strategies to continue operating in the volatile environment. For example, in eastern DRC, humanitarian organisations track diverse militia movements, road ambush patterns, and community tensions to inform both security posture and continuity strategies sustaining operational resilience[29,110,111]. Similarly, in northern Nigeria, some humanitarian organizations use incident trend analysis and scenario planning to anticipate Boko Haram or Islamic State West Africa Province (ISWAP) attacks, enabling them to adjust access routes, staffing levels, and programme modalities[29,112,113,114]. These shared analytical processes from complex security environments demonstrate that HSRM, BCP, and operational resilience are inherently interconnected, each seeking to ensure staff safety, reduce uncertainty, protect critical assets and maintain operational continuity.

Crisis decision-making frameworks further reinforce the overlaps between HSRM, BCP, and operational resilience. Crisis management tools such as hibernation, relocation, and evacuation (HRE) protocols are used across HSRM and BCP to guide rapid operational choices under pressure. In Ukraine, for instance, individuals, humanitarian organisations and others rely on air-raid monitoring systems and missile-strike patterns to determine when to suspend movement or activate remote-working protocols[115,116]. In Sudan, escalating urban warfare in Khartoum and other towns in April 2023 and thereafter forced humanitarian organizations to activate relocation and evacuation plans while simultaneously shifting to remote management and partner-led delivery[117,118]. These examples illustrate that HSRM and BCP share not only analytical foundations but also decision-making mechanisms that enable organisations to respond coherently to sudden shocks. Operational resilience emerges when these shared foundations are aligned and applied consistently across the organisation.

6.2 Complementarities: Despite their shared foundations, HSRM and BCP perform distinct but complementary functions that together enable operational resilience. HSRM protects staff, premises, and access, ensuring staff can operate safely and humanitarian space is preserved. BCP protects critical functions, ensuring that essential services such as food, health, nutrition, cash assistance, and supply-chain operations continue even when insecurity disrupts normal operations. Together, they create operational resilience, where humanitarian organisations can anticipate shocks, absorb their impact, and maintain delivery even in volatile environments

and situations. For example, in Yemen, humanitarian security and field teams monitor airstrikes, front-line shifts, and bureaucratic impediments, while BCP teams design alternative delivery modalities such as remote management, partner-led programming, and decentralised supply chains[49,80,93,94]. HSRM also provides the triggers that activate continuity plans, such as when rising insecurity necessitates staff relocation or suspension of field movements[49,80,93,94]. Operational resilience emerges when both HSRM and BCP systems are integrated, operational and continuously updated.

Conversely, BCP ensures that humanitarian operations can continue during significant security incidents, reinforcing the protective function of HSRM. In South Sudan, for example, skeleton-team models and pre-positioned supplies allowed essential food, health and nutrition services to continue during repeated widespread fighting in Upper Nile - Bentiu and Malakal towns [57,58,68]. In Afghanistan, NGOs have used continuity strategies such as remote case management, digital cash transfers, and local-partner delivery to sustain operations during periods of heightened Taliban restrictions or urban insecurity post August 2021[83,84]. These examples show that HSRM and BCP are mutually reinforcing. HSRM enables safe access, while BCP ensures that critical functions remain operational even when access is compromised. Together, they form the operational backbone of resilience in insecure environments.

6.3 Points of Friction: Despite their natural alignment, HSRM and BCP often operate in silos due to organisational structures, professional cultures, and misaligned planning cycles[7,28,38]. Organisational and cultural barriers can also be sources of friction**.** For example, field security teams may prioritise risk avoidance and duty of care, while programme and continuity teams may emphasise service delivery and operational imperatives. This divergence can create tension, particularly when security recommendations appear to conflict with programme objectives. In Sudan, for example, some security teams from diverse humanitarian organizations recommended immediate relocation from Khartoum during the April 2023 conflict outbreak, while management and some programme teams argued for maintaining presence to avoid service gaps for displaced populations [85,103,104,118]. Similar tensions had emerged in Afghanistan in 2021 where some humanitarian security teams pushed for movement restrictions during periods of heightened threat, while programme teams sought to continue field activities to meet urgent humanitarian needs[119,120,121].These organizational differences can lead to fragmented decision making and inconsistent application of risk thresholds or acceptable risk.

Misaligned planning cycles and inconsistent leadership ownership further exacerbate these frictions. HSRM processes such as security risk assessments and incident monitoring are updated frequently, often daily or weekly, while BCP reviews may occur annually or semi-annually. This mismatch can result in continuity plans that do not reflect current security realities. Leadership engagement is also sometimes uneven. Some organisations invest heavily in HSRM while under-resourcing BCP, or vice versa. In northern Mozambique, for example, some humanitarian organisations had strong security risk management systems in place during the Cabo Delgado insurgency but lacked robust continuity plans, resulting in prolonged programme suspensions after attacks in Mocímboa da Praia and Palma in 2020 and 2021 respectively [122,123,124]. These structural and cultural barriers weaken the overall system, reducing organisational agility and undermining the potential for integrated resilience.

6.4 Why Integration Matters: Integrating HSRM and BCP is essential for achieving operational resilience. Operational resilience is the ability to absorb shocks, adapt, and continue delivering assistance. When these systems operate together, humanitarian organisations make faster, more informed decisions because security analysis and continuity priorities are aligned. This reduces operational downtime and ensures that essential services remain available even during crises. In Ukraine, humanitarian organizations with integrated HSRM–BCP systems maintained operations during missile strikes and nationwide power outages by combining security assessments with continuity measures such as redundant communications, distributed warehousing, and

decentralised decision-making[72,106].Integration also improves staff safety, ensuring that protective measures are calibrated to programme criticality rather than applied uniformly or reactively.

Integrated systems also enhance organisational learning and adaptability. When HSRM and BCP teams collaborate, they can jointly identify vulnerabilities, test contingency plans, and refine operational models based on real-time feedback. In Syria, for example, humanitarian organisations that integrated security risk management and continuity planning were able to maintain cross-border operations despite shifting frontlines and bureaucratic restrictions by using scenario-based planning and flexible supply-chain models[125,126]. In South Sudan, integrated approaches enabled humanitarian organizations to rapidly reconfigure operations during flooding and conflict, reducing service interruptions and improving response times[57,72,127]. Ultimately, integration strengthens organisational resilience by ensuring that decisions are coherent, timely, and grounded in a holistic understanding of risk and operational priorities.

6.5 Operational Resilience in Practice: Evidence from contemporary crises shows the practical value of integrating HSRM and BCP. This is most evident in contexts where volatility is constant, and disruptions are frequent. In Gaza and Ukraine, humanitarian organisations that combined real-time security analysis with continuity strategies such as partner-led delivery, pre-positioned supplies, and remote coordination were able to sustain essential services despite bombardment, communications blackouts, and access restrictions[72,105,106,108]. These integrated approaches allowed humanitarian organizations to maintain life-saving health, WASH, and food assistance even during periods of intense escalation. In Mozambique's Cabo Delgado province, humanitarian organizations that aligned HSRM and BCP were able to relocate staff during non-state armed groups attacks without halting protection, food, health and shelter programmes, demonstrating how integrated systems enable rapid adaptation to sudden shocks[36,97,98,107].

Similarly, in northeast Nigeria, integrated HSRM–BCP approaches enabled humanitarian organisations to continue nutrition and health services through remote management when towns such as Dikwa or Monguno were temporarily overrun by armed groups. Pre-positioned supplies, local-partner networks, and decentralised decision-making allowed programmes to resume quickly once access was restored [29,32,33,91,92]. In Yemen, integrated systems helped humanitarian organisations maintain operations during fuel shortages, airstrikes, and bureaucratic impediments by diversifying supply routes and empowering field offices[49,78,93,94]. These examples demonstrate that operational resilience is not a theoretical construct but a practical outcome of aligning HSRM, BCP, and adaptive decision-making into a single, coherent system capable of sustaining humanitarian presence in the world's most insecure environments**.**

6.6 Structured Feedback: Operational experiences in insecure humanitarian environments consistently demonstrate the critical importance of HSRM and BCP frameworks that incorporate structured feedback loops. In practice, every disruption whether a security incident, access denial, communications blackout, or sudden political shift generates lessons that reshape future security risk assessments and continuity strategies. For example, after the rapid Taliban takeover in Afghanistan in August 2021, humanitarian organizations revised their relocation and evacuation triggers, remote-management protocols, and partner-engagement strategies based on what worked and what failed during the initial shock[66,67,83,84]. Similarly, in Ukraine, repeated missile strikes, and power outages from February 2022 forced humanitarian organizations to refine their redundancy measures, invest in distributed warehousing, and strengthen staff relocation plans[72,106]. These experiences show that resilience is not achieved through static plans but through iterative learning that continuously sharpens organisational preparedness.

This feedback loop is equally evident in contexts such as Gaza, northeast Nigeria, and Cabo Delgado, where recurring insecurity requires constant adaptation. In Gaza, lessons from previous escalations informed improved pre-positioning strategies and more robust communication redundancies during the 2023–2025 bombardments[7,31,108,109]. In northeast Nigeria, humanitarian organisations have repeatedly adjusted their

remote-management models and partner-vetting processes after towns were temporarily overrun by armed groups. In Mozambique- Cabo Delgado, humanitarian organizations refined their relocation procedures and community-acceptance strategies following insurgent attacks in Palma and Mocímboa da Praia[36,97,98,107]. These examples illustrate how operational learning feeds directly back into both HSRM and BCP systems, transforming resilience from a one-time achievement into a dynamic organisational practice. By institutionalising these feedback loops, humanitarian organisations strengthen their ability to anticipate emerging threats, adapt to evolving contexts, and sustain critical operations in some of the world's most volatile environments.

7. Implications for Humanitarian Organisations

7.1 Leadership and Governance Requirements: The integration of HSRM, BCP, and operational resilience demands strong, consistent leadership commitment. Senior management must champion a unified risk-management approach, ensuring that security, programme, and continuity functions are not treated as parallel systems but as interdependent components of organisational survival. For example, as noted in volatile contexts such as Sudan, Yemen and Gaza, organisations that maintained operational presence did so because leadership empowered field teams with delegated authority, rapid decision-making protocols, and clear escalation pathways. Governance structures must therefore institutionalise cross departmental coordination, embed risk-informed decision-making at all levels, and ensure that operational resilience is treated as a strategic priority rather than a technical add-on[105].

7.2 Policy and Procedural Alignment: Humanitarian organisations must strengthen and harmonise their security policies to ensure that HSRM and BCP frameworks reinforce rather than contradict each other. This includes aligning security risk assessments with business continuity plans, synchronising planning cycles, and ensuring that operational procedures reflect real-time threat environments. As observed in Yemen and northeast Nigeria, organisations that integrated security triggers into continuity protocols were able to shift seamlessly from in-person delivery to remote management when insecurity escalated. Policy alignment also requires updating standard operating procedures (SOPs) to reflect contemporary risks such as cyberattacks, communications blackouts, access denials and bureaucratic impediments, which increasingly shape humanitarian operating environment [38].

7.3 Training and Capacity Development: Effective integration requires investment in staff competencies across all levels. Security teams need training in continuity planning and programme criticality analysis, while programme and operations staff must understand security risk management principles. Joint simulation exercises such as relocation and evacuation drills, remote-management scenarios, or supply-chain disruption simulations help build shared understanding and reduce siloed thinking. As observed in Ukraine, humanitarian organisations that conducted joint crisis simulations before major escalations were better able to maintain operations during missile strikes and power outages. Capacity development must also extend to national staff and local partners, who often sustain operations when international staff are relocated or evacuated.

7.4 Information Sharing and Coordination: Integrated resilience depends on timely, accurate information flows across departments and between humanitarian organisations. Humanitarian organizations must strengthen internal coordination mechanisms such as joint analysis teams, cross-functional crisis teams, and shared incident-reporting platforms to ensure that security insights inform continuity decisions and vice versa. Externally, improved coordination with the diverse humanitarian clusters, access working groups, and UN and NGO security forums enhances situational awareness and reduces duplication. In contexts like eastern DRC, it was observed that humanitarian organisations that participated actively in inter-agency security coordination were better able to anticipate access constraints and adjust continuity plans accordingly. Information sharing is therefore both an operational necessity and a collective responsibility.

7.5 Resource Allocation and Preparedness Investments: Building operational resilience requires sustained investment in preparedness, redundancy, and adaptive systems. This includes funding for secure communications, backup power systems, pre-positioned supplies, alternative delivery modalities, and decentralised operational hubs. As observed in Gaza and northern Mozambique, Cabo Delgado, humanitarian organisations that had invested in pre-positioned stocks and partner-led delivery were able to maintain essential

services despite severe access restrictions. Similarly, in South Sudan, humanitarian organizations with flexible funding and contingency budgets were able to activate skeleton-team models and sustain critical health and nutrition services during conflict surges. Donors also play a critical role. Their flexible, multi-year funding enables organisations to invest in resilience rather than reacting to crises episodically.

8. Recommendations

1) Develop Integrated HSRM–BCP Frameworks: Humanitarian organisations should design and adopt unified frameworks that explicitly link Humanitarian Security Risk Management (HSRM) with Business Continuity Planning (BCP). This requires embedding continuity considerations into security risk assessments, aligning triggers for crisis situations such as hibernation, relocation or evacuation with programme criticality analysis, and ensuring that both systems use shared terminology and decision-making thresholds[2,19,37,128]. Integrated frameworks should be mandated across all country operations, particularly in insecure contexts such as Sudan, Gaza, Somalia, Yemen, eastern DRC and northeast Nigeria.

2) Institutionalise Joint Planning Cycles: HSRM and BCP processes must be synchronised through joint bi-annual planning, shared scenario exercises, and coordinated crisis-management structures. Humanitarian organisations should establish cross-functional planning teams that bring together security, programme, logistics, and senior leadership to ensure that continuity plans reflect real-time threat environments. Regular simulation exercises, such as evacuation drills, cyber-disruption scenarios, or access denial simulations should be institutionalised to test and refine integrated plans[2,19,37].

3) Strengthen Field-Level Decision-Making Autonomy: To ensure rapid and context appropriate responses, humanitarian organisations should decentralise decision making authority to field teams, supported by clear escalation pathways and pre-approved contingency thresholds[19,37,128]. In volatile environments like eastern DRC, Yemen, northern Nigeria or Cabo Delgado, empowering field managers to activate continuity measures or adjust operational posture without lengthy headquarters approval significantly reduced downtime and enhanced staff safety. Delegated authority frameworks should be formalised and regularly reviewed.

4) Invest in Continuity-Critical Infrastructure: Humanitarian organisations must allocate dedicated resources to preparedness and resilience infrastructure. This includes redundant communications systems, backup power solutions, secure data storage, pre-positioned supplies, alternative logistics routes, and decentralised operational hubs[19,37,38]. Investments should also target digital resilience such as cybersecurity measures and remote-work capabilities. This is particularly important given the increasing prevalence of cyber threats in conflict settings like Ukraine. Donors should be encouraged to provide flexible, multi-year funding to support these resilience-building measures.

5) Build Organisational Cultures That Value Resilience: Achieving integrated resilience requires cultural change, not just technical adjustments. Humanitarian organisations should promote a culture where risk-informed decision-making, adaptive planning, and cross-departmental collaboration are recognised as core competencies[37,38, 129]. This includes embedding resilience principles into induction training, leadership development programmes, and performance management systems. Documented adaptive successes, such as effective remote management in Yemen or rapid re-establishment of services in South Sudan helps reinforce the value of resilience oriented behaviours.

6. Enhance Information Sharing and Coordination: Internal and external information-sharing mechanisms must be strengthened to support integrated decision-making. Humanitarian organisations should establish joint analysis teams , shared incident-reporting platforms, and cross-functional crisis teams to ensure that security insights inform continuity decisions in real time. Externally, active participation in diverse working groups (e.g., access,) NGO security forums, and cluster coordination mechanisms enhances situational awareness and collective preparedness [37,38 128].

7. Prioritise Training and Capacity Development: Humanitarian organisations should invest in cross training of security, programme, and operations staff to build shared understanding of HSRM, BCP, and resilience principles. Joint training modules, scenario-based exercises, and mentorship programmes help break down silos

and strengthen institutional coherence[37,38,129]. Capacity development must also extend to national staff and local partners, who often sustain operations when international staff are relocated or evacuated.

9. Summary of Findings

The findings of this study demonstrate that Humanitarian Security Risk Management (HSRM), Business Continuity Planning (BCP), and operational resilience are deeply interconnected systems, each contributing essential but distinct functions that enable humanitarian organisations to operate effectively in insecure environments. Across diverse contexts such as Gaza, Ukraine, Sudan, Yemen, northeast Nigeria, and Mozambique -Cabo Delgado, evidence shows that all three disciplines share foundational practices, including risk identification, scenario planning, contingency development, and crisis decision making. These shared analytical processes form a common understanding for managing uncertainty and provide the basis for coherent organisational responses to rapidly evolving threats.

The study also finds that HSRM and BCP offer complementary strengths and when aligned reinforce one another. HSRM protects people, premises, and access, while BCP safeguards critical functions and ensures continuity of essential services during disruptions. HSRM informs the triggers that activate continuity plans, and BCP ensures that operations can continue even when security incidents occur. The research also identifies persistent points of friction, including organisational silos, divergent professional cultures, misaligned planning cycles, and inconsistent leadership ownership. These barriers often result in fragmented decision-making, delayed responses, and reduced organisational agility during crises.

The study concludes that integrating HSRM and BCP is essential for achieving operational resilience. Humanitarian organisations that align these systems demonstrate faster decision-making, reduced operational downtime, improved staff safety, and stronger continuity of life-saving services. Contemporary case studies from remote management in northeast Nigeria to adaptive operations in Gaza and decentralised programming in Ukraine show that operational resilience is not an abstract concept but a practical outcome of coordinated risk management and continuity planning. The evidence underscores that in volatile humanitarian environments, resilience emerges only when HSRM and BCP function as a unified, mutually reinforcing system embedded across organisational structures and decision-making processes.

10. Conclusion

This study has demonstrated that the integration of Humanitarian Security Risk Management (HSRM) and Business Continuity Planning (BCP) is not optional but essential for humanitarian organisations operating in conflict-affected and insecure environments. The evidence from contemporary crises ranging from Gaza and Ukraine to Sudan, Yemen, eastern DRC and northeast Nigeria shows that fragmented or siloed approaches are no longer adequate for navigating the scale, speed, and complexity of disruptions that humanitarian organizations now face. Instead, humanitarian organisations require unified planning architectures that align security analysis, continuity strategies, and adaptive operational models into a single, coherent system capable of sustaining presence under extreme volatility.

The findings reinforce that HSRM and BCP are interdependent components of operational resilience. HSRM protects people and access, while BCP safeguards critical functions and ensures that life-saving services continue during crises. When integrated, these systems enable faster decision-making, reduce operational downtime, and enhance staff safety. This ultimately strengthens the organisation’s ability to deliver principled humanitarian assistance in insecure settings. Ahead, humanitarian organisations must invest in leadership ownership, policy alignment, cross-functional training, and preparedness resources to institutionalise this integration. Future research should further explore how digital risks, localisation, and climate-related shocks further shape the

HSRM–BCP–resilience nexus, ensuring that humanitarian systems remain adaptive and fit for purpose in an increasingly unpredictable world.

11. References

1. Michael Munyaradzi Makova (PhD), Risky Business: 21st Century and Changing Dynamics of Insecurity in Humanitarian Operations. *Asian. Jour. Social. Scie. Mgmt. Tech*. 2024; 6(1): 227- 252.
2. Michael Munyaradzi Makova (PhD), Developing Effective Field Contingency Plans for Staff Safety and Security in High Risk Humanitarian Operations, *Asian. Jour. Social. Scie. Mgmt. Tech*. 2025; 7(5): 24-53.
3. Inter-Agency Standing Committee. (2021). *Operational guidance on humanitarian security risk management*. IASC.
4. Metcalfe-Hough, V., Poole, L., Bailey, S., & Belanger, J. (2020). *The humanitarian "system": A critical review*. Overseas Development Institute.
5. Michael Munyaradzi Makova (PhD), The Complex Dynamics of Aid Beneficiaries Security in Insecure Humanitarian Environments: A 21st Century Imperative and Challenge for Humanitarian Organizations, *Asian. Jour. Social. Scie. Mgmt. Tech*. 2025; 7(2): 01-28.
6. Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. *International Journal of Disaster Risk Science, 14*, 713–721.
7. Humanitarian Practice Network (2025). Humanitarian Security Risk Management- Good Practice Review 8. 3rd edition. HPN.
8. Bickley, S.(2017).*Security risk management: A basic guide for smaller NGOs.* EISF. https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/.
9. GISF (2024). *Security risk management (SRM) strategy and policy development: A cross-functional guide* https://gisf.ngo/resource/srm-strategy-and-policy-guide/.
10. Michael Munyaradzi Makova(PhD), Security Management and Risk Management Strategies in Humanitarian Field Environments: A Conceptual Analytical Approach. *Asian. Jour. Social. Scie. Mgmt. Tech*. 2023; 5(6): 25-47.
11. Egeland, J., Harmer, A., & Stoddard, A. (2011). *To stay and deliver: Good practice for humanitarians in complex security environments*. Policy Development and Studies Branch (PDSB), OCHA.
12. Foulkes, I. (2013, August 18). How Baghdad attack put UN aid missions at risk. https://www.bbc.com/news/world-europe-23717105
13. Fast, L. A. (2010). Mind the gap: Documenting and explaining violence against aid workers. *European Journal of International Relations*, 16(3), 365–389. https://doi.org/ 10.1177/135406610935004
14. ALNAP. (2022). *The State of the Humanitarian System 2022*. ALNAP/ODI.
15. Global Interagency Security Forum. (2020). *Security to go: A risk management toolkit for humanitarian aid agencies*. GISF.
16. Michael Munyaradzi Makova (PhD), "Security Risk Management Strategies in High-Risk Environments", Asian. Jour. Social. Scie. Mgmt. Tech.2023; 5(4): 45-66.
17. Harmer, A., Stoddard, A., and Sarazen, A. (2018). *Humanitarian access in armed conflict: A need for new principles?* UK Department for International Development.
18. Stoddard, A., Harvey, P., Czwarno, M., and Breckenridge, M.-J. (2020). *Humanitarian access SCORE report: Northeast Nigeria. Survey on the coverage, operational reach, and effectiveness of humanitarian aid.* Humanitarian Outcomes.
19. UNHCR. (2022). *Business continuity planning*. In *UNHCR Emergency Handbook*. UNHCR.
20. World Health Organization. (2019). *WHO guidance for business continuity planning*. WHO.
21. Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History, 52*(6), 978–1002.
22. United Nations. (updated 2021). Policy on the Organizational Resilience Management System (CEB /2014/ hlcm /17). https://docs.un.org/en/JIU/REP/2021/6

23. United Nations Security Management System. Security Policy Manual. (updated April 2024) UN. mhttps://unsms.un.org/security-policy-manual.
24. World Health Organization. (2021). *Business continuity planning for health emergencies*. WHO.
25. Talisuna, A., Saikat, S., Seifeldin, R., *et al*. (2025). Operationalising health in the humanitarian–development–peace nexus in Africa: A framework for building resilience. *BMJ Global Health.*
26. World Health Organization.(2020). *Operational framework for building climate-resilient health systems*. WHO.
27. United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030.* UNDRR
28. Åslund, R. (2019). *Organizational resilience and the humanitarian sector: Exploring organizational resilience in policy and practice within the United Nations*. Master's thesis, Umeå University, Sweden.
29. Humanitarian Outcomes. (2023). *Aid Worker Security Report 2023: Violence against aid workers*. Humanitarian Outcomes.
30. Humanitarian Outcomes & Global Interagency Security Forum. (2024). *State of practice: The evolution of security risk management in the humanitarian space*.
31. OCHA. (2024). *Gaza Strip: Humanitarian access and operational constraints.* United Nations Office for the Coordination of Humanitarian Affairs.
32. UNOCHA. (2023). *Humanitarian needs overview: Northeast Nigeria.* United Nations Office for the Coordination of Humanitarian Affairs
33. Médecins Sans Frontières. (2023). *Northeast Nigeria: Adapting operations amid insecurity.* MSF Operational Updates
34. ACAPS. (2024). *Sudan: Humanitarian access overview.* ACAPS. https://www.acaps.org
35. OCHA. (2023). *Ukraine humanitarian response: Operational updates.* United Nations Office for the Coordination of Humanitarian Affairs. https://www.unocha.org
36. UNHCR. (2023). *Mozambique: Cabo Delgado situation update.* UNHCR
37. Michael Munyaradzi Makova (PhD), Developing an Operational Framework for Security Relocations and Evacuations in High Risk Humanitarian Environments, *Asian. Jour. Social. Scie. Mgmt. Tech*. 2026; 8(2): 13-35.
38. Michael Munyaradzi Makova (PhD), Developing Effective Field Standard Operating Procedures (SOPs) for Staff Safety and Security in High risk Humanitarian Operations: A Contextual and Operational Framework, *Asian. Jour. Social. Scie. Mgmt. Tech*. 2025; 7(6): 283-304
39. Humanitarian Outcomes. (2025). *The humanitarian security risk management system*. https://humanitarianoutcomes.org/sites/default/files/2025-06/Chapter%203.1.pdf
40. Humanitarian Practice Network (2010). Good practice review, (revised). Operational Security Management in Violent Environments. Humanitarian Policy Group, ODI.
41. United Nations Security Risk Management Manual. Updated November 2025, New York: United Nations
42. UNSMS-Security Policy manual (updated Feb 2025). New York: United Nations
43. Global Interagency Security Forum (GISF). (2018). *Security risk management: A guide for humanitarian organizations*. GISF.
44. Global Interagency Security Forum. (2018). *Standard operating procedures (SOPs): Policy, procedure and practice for security risk management*. GISF.
45. Global Interagency Security Forum. (2022). *Security to Go: A risk management toolkit for humanitarian aid agencies* (3rd ed.). https://gisf.ngo/toolkit/security-to-go/
46. Global Interagency Security Forum. (2022). *NGO Security Collaboration Guide*. GISF https://www.gisf.ngo/wpcontent/uploads/2022/09/NGO-Security-Collaboration-Guide.pdf
47. Centre for Humanitarian Leadership. (2023). *Operational resilience in protracted crises: Lessons from Yemen and South Sudan.* CHL Publications.
48. Inter-Agency Standing Committee (IASC). (2022, July 13). *Inter-agency humanitarian evaluation of the Yemen crisis*. IASC.

49. United Nations Office for the Coordination of Humanitarian Affairs. (2024). *Yemen: Humanitarian needs overview*. OCHA.
50. OCHA. (2020). *Yemen humanitarian response plan: Operational challenges and staff safety*. OCHA.
51. OCHA. (2020). *South Sudan: Humanitarian access and operational environment report*. United Nations Office for the Coordination of Humanitarian Affairs
52. UNICEF. (2021). *Evaluation of the UNICEF response to the South Sudan humanitarian crisis (2016–2019)*. United Nations Children's Fund.
53. United Nations Office for the Coordination of Humanitarian Affairs. (2025). *Democratic Republic of the Congo: Humanitarian access and operational environment update*. OCHA.
54. Humanitarian Outcomes. (2024). *Aid Worker Security Report 2024: Trends in violence and access constraints*. Humanitarian Outcomes.
55. ACAPS. (2024). *Humanitarian access overview: Democratic Republic of Congo*. ACAPS.
56. International Committee of the Red Cross. (2018). *The ICRC's approach to ensuring safe access in armed conflict and other situations of violence*. ICRC.
57. United Nations Office for the Coordination of Humanitarian Affairs. (2024). *South Sudan: Humanitarian access overview*. OCHA
58. United Nations Office for the Coordination of Humanitarian Affairs. (2025). *South Sudan: Humanitarian access and operational environment report*. OCHA
59. ACAPS. (2025). *South Sudan: Drivers of access constraints*. ACAPS.
60. ACAPS. (2023). *Sudan: Humanitarian access overview*. ACAPS.
61. United Nations Office for the Coordination of Humanitarian Affairs. (2023). *Sudan: Humanitarian response update*. OCHA.
62. Norwegian Refugee Council. (2022). *Remote programming in northeast Nigeria: Lessons learned*. NRC.
63. World Health Organization. (2024). *Health cluster operational update: Gaza*. WHO.
64. United Nations Office for the Coordination of Humanitarian Affairs. (2024). *Occupied Palestinian Territory: Humanitarian needs and response update*. OCHA
65. World Health Organization. (2024). *Health response in Gaza: Operational update*. WHO.
66. International Committee of the Red Cross. (2022). *ICRC in Afghanistan: Operational update*. ICRC.
67. United Nations Development Programme. (2022). *Afghanistan: Local service delivery under extreme constraints*. UNDP.
68. REACH Initiative. (2024). *South Sudan: Hard-to-reach areas assessment*. REACH.
69. World Food Programme. (2023). *Yemen: Supply chain update*. WFP.
70. World Health Organization. (2024). *Yemen health cluster operational update*. WHO.
71. Barbelet, V. (2025). *Humanitarian evacuations: Practice, guidance, research gaps and lessons*. Overseas Development Institute (ODI).
72. Global Interagency Security Forum, & Humanitarian Outcomes. (2024). *Lessons learned across contexts: Relocations and evacuations*. Global Interagency Security Forum.
73. United Nations Office for the Coordination of Humanitarian Affairs. (2022). *Ukraine: Humanitarian impact situation report*. OCHA.
74. International Committee of the Red Cross. (2022). *ICRC operational update: Ukraine*. ICRC.
75. Norwegian Refugee Council. (2023). *Operational communications in high-risk environments*. NRC.
76. International Committee of the Red Cross. (2023). *Maintaining communication in conflict settings*. ICRC.
77. World Food Programme. (2023). *Ukraine: Logistics cluster operational update*. WFP.
78. ACAPS. (2024). *Yemen: Humanitarian access overview*. ACAPS.
79. World Food Programme. (2023). *Yemen: Supply chain update*. WFP.
80. OCHA. (2022). *Yemen: Humanitarian response plan 2022*. United Nations Office for the Coordination of Humanitarian Affairs
81. United Nations Office for the Coordination of Humanitarian Affairs. (2024). *South Sudan: Humanitarian access overview*. OCHA.

82. ACAPS. (2020). *Nigeria: Humanitarian access overview*. ACAPS.
83. United Nations Development Programme. (2022). *Afghanistan: Local service delivery under extreme constraints.* UNDP.
84. ACAPS. (2021, August 23). *Afghanistan: Humanitarian impact and trends analysis*. ACAPS.
85. United Nations Office for the Coordination of Humanitarian Affairs. (2024). *Sudan: Humanitarian response update*. OCHA.
86. Norwegian Refugee Council. (2023). *Sudan: Operational adaptation under conflict*. NRC.
87. Razzetti, E. A. (2021). *Contingency planning: Stuff happens, including pandemics—Don't just wait for it!* Defense Acquisition Magazine.
https://www.dau.edu/library/damag/january-february2021/contingency-planning.
88. Choularton, R. (2007). *Contingency planning and humanitarian action: A review of practice*. Humanitarian Practice Network, Network Paper No. 59.
89. IFRC. (2019). Cyclone Idai: Red Cross responds to devastating floods in Southern Africa. https://media.ifrc.org/medialibrary/2019/03/19/cyclone-idai-red-cross-responds-devastating-floods-southern-africa/.
90. Inter-Agency Humanitarian Evaluation Steering Group. (2020). *Inter-agency humanitarian evaluation of the response to Cyclone Idai in Mozambique*. IASC.
91. OCHA. (2021). *Nigeria: Humanitarian needs overview 2021.* United Nations Office for the Coordination of Humanitarian Affairs.
92. INSO. (2020–2023). *Nigeria: Safety and access reports.* International NGO Safety Organisation.
93. OCHA. (2023). *Yemen: Humanitarian response plan 2023*. United Nations Office for the Coordination of Humanitarian Affairs.
94. ACAPS. (2021). *Yemen: Operational constraints and access challenges*. ACAPS.
95. United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA). (2021). *Operational guidance for humanitarian response in complex emergencies.* UN OCHA
96. Stoddard, A., Czwarno, M., & Haver, K. (2019). *NGO security policy: Trends and challenges*. Humanitarian Outcomes.
97. OCHA. (2024). *Mozambique: Cabo Delgado humanitarian situation update – May 2024*. United Nations Office for the Coordination of Humanitarian Affairs.
98. OCHA. (2023). *Mozambique: Cabo Delgado humanitarian response overview*. United Nations Office for the Coordination of Humanitarian Affairs
99. ACAPS. (2021). *Mozambique: Cabo Delgado crisis—Humanitarian access and operational constraints*. ACAPS. https://www.acaps.org
100. CHS Alliance. (2020). *Managing risks in humanitarian operations: A CHS guidance note*. CHS Alliance.
101. Jackson, A and Zyck, S.A. (2016). *Presence and Proximity: To stay and deliver, 5 years on*. Independent study commissioned by OCHA, the Norwegian Refugee Council (NRC) and the Jindal School of International Affairs (JSIA), NY: OCHA.
102. Score (Dec 2023). Humanitarian Access SCORE Report: Sudan Survey on the Coverage, Operational Reach, and Effectiveness of Humanitarian Aid. SCORE
103. OCHA. (2023). *Sudan crisis: Humanitarian access and staff safety*. OCHA Flash Update. OCHA.
104. International Crisis Group. (2023). *Sudan's conflict and humanitarian evacuation challenges*. International Crisis Group Report.
105. Barbelet, V. (2025). *Humanitarian evacuations: Practice, guidance, research gaps and lessons*. Overseas Development Institute (ODI).
106. International Crisis Group. (2022). *The humanitarian response to the war in Ukraine: Challenges for NGOs and UN agencies*. International Crisis Group.
107. ACAPS. (2021). *Mozambique: Cabo Delgado crisis—Humanitarian access and operational constraints*. ACAPS.
108. OCHA. (2024). *Humanitarian access snapshot – Gaza Strip, September 2024*. OCHA.

109. United Nations Relief and Works Agency. (2025). *Situation Report #153 on the humanitarian crisis in the Gaza Strip and West Bank*. UNRWA.
110. INSO. (2023). *Democratic Republic of Congo: Quarterly safety and access review*. International NGO Safety Organisation
111. OCHA. (2023). *Democratic Republic of the Congo: Humanitarian needs overview 2023*. United Nations Office for the Coordination of Humanitarian Affairs
112. INSO. (2024). *Nigeria: Humanitarian access and security analysis*. International NGO Safety Organisation
113. OCHA. (2024). *Nigeria: Humanitarian access snapshot – Northeast*. United Nations Office for the Coordination of Humanitarian Affairs.
114. IOM. (2024). *DTM Nigeria: Northeast mobility and access report*. International Organization for Migration.
115. Multi-Hazard Threats, Remote Work Protocols, and Continuity State Service of Special Communications and Information Protection of Ukraine. (2025). *War and cyber: Three years of struggle and lessons for global security*. SSSCIP.
116. Bakalinskyi, O., & McDonough, M. (2025). *Ukraine's wartime experience provides blueprint for infrastructure protection*. Atlantic Council.
117. UNHCR. (2023). *Sudan emergency: Supplementary appeal*. UNHCR
118. OCHA.(2023). Sudan: *Humanitarian update*. OCHA
119. United Nations. (2022). *Report of the Secretary-General on the situation in Afghanistan and its implications for international peace and security*. United Nations Security Council.
120. United Nations Department of Safety and Security. (2022). *UNDSS Afghanistan crisis review: August 2021 evacuation and operational lessons*. United Nations.
121. Global Interagency Security Forum. (2022). *NGO security management in Afghanistan: Lessons from the 2021 transition*. Global Interagency Security Forum.
122. Humanitarian Outcomes. (2021). *Cabo Delgado: The Palma attack and implications for humanitarian operations*. Humanitarian Outcomes.
123. ACAPS. (2021). *Cabo Delgado: Impact of the Palma attack on humanitarian operations*. ACAPS.
124. ACAPS. (2020). *Cabo Delgado: Conflict and displacement update following the Mocímboa da Praia attack*. ACAPS.
125. OCHA. (2021). *Syrian Arab Republic: Humanitarian needs overview 2021*. United Nations Office for the Coordination of Humanitarian Affairs.
126. OCHA. (2020). *Syrian Arab Republic: Cross-border operations update*. United Nations Office for the Coordination of Humanitarian Affairs
127. OCHA. (2022). *South Sudan: Humanitarian needs overview 2022*. United Nations Office for the Coordination of Humanitarian Affairs.
128. Abuor, J. (2026). *Humanitarian access, integration with SRM and its challenges in INGO security*. LinkedIn Article.
129. Bhusiri, N., Julagasigorn, P., Varadejsatitwong, P., & Banomyong, R. (2022). *Resilient supplier relationship management framework for humanitarian organisations*. ResearchGate.

INFO

Corresponding Author: Michael Munyaradzi Makova, 2375 Bluffhill Westgate, Harare, Zimbabwe.

How to cite/reference this article: Michael Munyaradzi Makova, The Nexus of Security Risk Management and Business Continuity in Humanitarian Operations: How Integrated Approaches enable Operational Resilience in Insecure Environments, *Asian. Jour. Social. Scie. Mgmt. Tech*. 2026; 8(3): 96-121.