International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 425-438
https://doi.org/10.70917/ijcisim-2026-2270
Article

Information Security Governance in Not-for-Profit Organisations: A Critical Review and Research Agenda

Samuel O. Fakunle1, Bright Onyedikachi Asonye2

[1,2]Rome Business School
Correspondence email1: yinkafakunle@gmail.com8

Abstract: Information Security Governance (ISG) — the system by which an organisation directs and controls its information security activities — has accumulated a substantial empirical base in corporate and public-sector settings but remains under-examined in not-for-profit organisations (NFPs). Not-for-profits are simultaneously high-value targets for cyber threat actors and structurally resource-constrained, with around one-third of UK charities reporting cyber incidents in 2024 and the proportion rising to two-thirds among charities with annual income above £500,000. This article presents a critical review of the published evidence on ISG in NFPs and articulates a structured research agenda for the field. The review makes three contributions. First, it maps the literature against the eight components of the ISO/IEC 27014:2020 ISG construct and exposes a systematic imbalance: operational and protective components (risk management, policy, organisation and roles, compliance) are reasonably well evidenced, while strategic and oversight components (board oversight, security strategy, performance measurement, stakeholder communication) remain under-researched. Second, it critically examines the portability of corporate-derived ISG constructs to the resource, accountability, and mission conditions of the non-profit sector. Third, it articulates a four-stream research agenda — conceptual, methodological, empirical, and theoretical — with specific research questions to advance NFP ISG research over the next three to five years. The review draws on Stakeholder Theory, the Resource-Based View, and Legitimacy Theory to frame both the critique and the agenda. The article argues that NFP ISG should be treated not as a weaker version of corporate ISG, but as a distinct governance problem shaped by mission accountability, resource scarcity, and beneficiary protection.

Keywords: Information security governance; cybersecurity; not-for-profit organisations; non-governmental organisations; charity sector; critical review; research agenda; stakeholder theory; resource-based view; legitimacy theory

1. Introduction

1.1. The cybersecurity threat landscape facing not-for-profit organisations

Not-for-profit organisations (NFPs) — registered charities, non-governmental organisations (NGOs), faith-based organisations, charitable foundations, non-profit higher education institutions, and social enterprises with a non-distribution constraint — are increasingly the focus of cyber threat actors. The United Kingdom's Cyber Security Breaches Survey 2024 reported that approximately one-third of UK charities identified a cyber breach or attack in the preceding twelve months, with the proportion rising to around two-thirds among charities with annual income above £500,000 (Department for Science, Innovation and Technology, 2024). NetHope's State of Humanitarian and Development Cybersecurity Report has documented a comparable pattern of escalating exposure across international NGOs (NetHope, 2024). High-profile incidents — including the 2022 compromise of the International Committee of the Red Cross, in which records relating to approximately 515,000 highly vulnerable individuals were exposed (International Committee of the Red Cross, 2022), and the 2023 Evide breach affecting more than 140 UK charities supporting survivors of abuse — illustrate that the consequences of cyber incidents in NFP contexts extend beyond financial loss to direct harm to mission delivery and beneficiaries (Marelli, 2022; Anfuso et al., 2026). Although UK charity data are among the most developed recurring sources, the governance

problem addressed in this review is international, particularly for humanitarian and development NGOs operating across jurisdictions.

NFPs face this landscape from a disadvantaged starting position. The sector is characterised by chronic resource constraints, reliance on volunteer governance, limited in-house cybersecurity expertise, and frequent dependence on outsourced or pro bono information technology support (CyberPeace Institute, 2024; Imboden et al., 2017; Misata, 2020). NFPs handle data of high interest to threat actors — donor financial information, beneficiary case files, advocacy correspondence, and humanitarian programme records — that creates both economic and political incentives for attack (Le Blond et al., 2018; Searle, 2018). Sector surveys repeatedly find that substantial proportions of NFPs operate without documented incident response plans, regular cybersecurity training, formal risk assessment processes, or board-level engagement with information security (Department for Science, Innovation and Technology, 2024; Ramljak, 2025).

1.2. Information Security Governance as an organisational discipline

Information Security Governance is defined by ISO/IEC 27014:2020 as "the system by which an organisation's information security activities are directed and controlled" (International Organisation for Standardisation, 2020). The construct encompasses eight components: board and executive oversight; information security strategy and its alignment with organisational strategy; information security policy framework; information security risk management; security organisation, roles, and accountability; compliance with applicable legal, regulatory, and contractual requirements; performance measurement and reporting; and stakeholder communication on information security matters. ISG is conceptually distinct from information security management. Where management concerns the operational implementation of controls and processes, governance concerns the oversight arrangements, decision rights, accountability structures, and strategic alignment that direct security activity (Von Solms & Von Solms, 2009; Schinagl & Shahim, 2020). In practice, ISG is operationalised through frameworks including ISO/IEC 27001, ISO/IEC 27014, COBIT 2019 (ISACA, 2019), and the NIST Cybersecurity Framework 2.0, whose February 2024 revision introduced a dedicated Govern function (National Institute of Standards and Technology, 2024).

ISG research in corporate settings has accumulated a substantial empirical base examining board oversight, the role of the Chief Information Security Officer, the relationship between ISG maturity and security outcomes, and the institutional and regulatory pressures shaping ISG adoption (Yaokumah, 2014; Carcary et al., 2016; Schinagl & Shahim, 2020; AlGhamdi et al., 2020; Da Veiga et al., 2020). Public-sector ISG research has likewise developed, including maturity-model work in critical infrastructure and central government contexts (Almuhammadi & Alsaleh, 2017; Maleh et al., 2021; Yusif & Hafeez-Baig, 2021). The translation of these constructs and findings to the NFP context, however, has been uneven and incomplete — a gap this review interrogates directly.

1.3. The research problem and rationale for a critical review

Three features of the existing NFP cybersecurity literature motivate a critical review at this stage. First, the empirical base is geographically and methodologically fragmented; studies appear across information systems, public administration, the voluntary sector, and cybersecurity outlets without an integrating synthesis (Ramljak, 2025). Second, the dominant construct in published NFP cybersecurity work has been incident exposure or technical control adoption rather than governance arrangements, leaving the strategic and oversight dimensions captured by ISG comparatively under-researched. This pattern mirrors a wider critique of nonprofit governance research, which has been faulted for over-reliance on cross-sectional, board-focused designs that miss the wider governance system (Cornforth, 2012). Third, and most consequentially, the construct portability problem is acute: ISG was developed in contexts that presume board-level oversight structures, dedicated security functions, and formal risk management processes that many small and mid-sized NFPs do not possess. Whether and how ISG concepts apply in NFP settings is itself an open empirical and conceptual question — and one that the existing literature has not directly addressed.

A critical review is the appropriate genre for this state of affairs. Where a narrative review would summarise, and a systematic review would synthesise effect estimates, a critical review evaluates the literature against external standards — in this case, the corporate ISG canon and the conditions of the non-profit sector — and articulates a corrective agenda for the field (Grant & Booth, 2009). The contribution claimed here is therefore evaluative and agenda-setting rather than effect-summarising.

1.4. Theoretical positioning

This review is positioned at the intersection of three theoretical traditions. Stakeholder Theory (Freeman, 1984) provides the primary lens: NFPs are constituted by accountability relationships with multiple, often non-financial stakeholders — beneficiaries, donors, members, regulators, partners, and the wider public — whose interests in information protection and service continuity differ from those of shareholders in for-profit firms. ISG in NFPs can therefore be understood as a mechanism for balancing and discharging multiple accountabilities, with beneficiary stakeholders frequently bearing the direct harm of governance failure (Marelli, 2022). The Resource-Based View (Barney, 1991; Wernerfelt, 1984) supplies a complementary lens: NFPs operate under chronic resource constraints, and ISG capability development is itself a resource allocation problem competing with mission-delivery priorities. Legitimacy Theory (Suchman, 1995) provides a tertiary lens: ISG adoption in NFPs can be interpreted as a legitimacy-maintenance practice directed at donors, regulators, and beneficiaries — a means of demonstrating trustworthy stewardship of sensitive information and maintaining the social licence on which NFPs depend. These three lenses are used both to organise the critical assessment and to structure the research agenda.

1.5. Contribution and organising questions

This review makes three contributions to the literature. First, it maps the existing evidence base against the components of the ISO/IEC 27014:2020 ISG construct, exposing a systematic imbalance between operational-protective and strategic-governance content. Second, it critically interrogates the portability of corporate-derived ISG constructs to the resource and accountability conditions of the non-profit sector, identifying construct translation as a foundational limitation of the current literature. Third, it articulates a structured research agenda — conceptual, methodological, empirical, and theoretical — with specific research questions to advance the field over the next three to five years. Four organising questions guide the review: (i) what does the existing literature establish about ISG arrangements and practices in NFP settings; (ii) what contextual and organisational factors shape ISG in this sector; (iii) what outcomes have been linked to ISG in NFPs; and (iv) what gaps, limitations, and priorities for future research follow from a critical reading of the evidence base.

2. Approach to Literature Identification

This is a critical review rather than a systematic or scoping review, and the approach to literature identification is correspondingly descriptive rather than protocol-driven (Grant & Booth, 2009). Sources were identified through targeted searching of the published literature, including queries across major bibliographic databases (Scopus, Web of Science Core Collection, IEEE Xplore, EBSCO Business Source Complete) using concept terms for information security governance, cybersecurity, and not-for-profit organisations, supplemented by citation tracking from key recent contributions (notably Ramljak, 2025; Anfuso et al., 2026) and by targeted searches of recognised national cybersecurity agency and sector-body grey literature (UK National Cyber Security Centre; US Cybersecurity and Infrastructure Security Agency; ENISA; NetHope; CyberPeace Institute; Charity Commission for England and Wales; Scottish Government, 2020). Search terms combined variants of "information security governance," "cybersecurity governance," "cyber risk governance," "non-profit," "not-for-profit," "charity," "NGO," "humanitarian organisation," and "third sector."

Inclusion was guided by relevance to the four organising questions and by the substantive criterion that sources address information security governance — as distinct from purely technical security controls or attacker methodology — in not-for-profit settings as defined by a non-distribution constraint. Both peer-reviewed and high-quality grey literature were included. Sources published from 2010 onwards were prioritised to align with the maturation of breach-disclosure regimes and the publication of the first edition of ISO/IEC 27014 (2013). English-language sources only. As is appropriate for a critical review, the literature identified is the basis for the synthesis below; the review does not claim systematic completeness, and an explicit research agenda for systematic and scoping review work on narrower questions is articulated in Section 7.

Table 1 summarises the principal NFP-focused sources informing the review, with their type, context, and the ISG components and outcome dimensions each addresses. The table is intended to serve as a transparent reference map of the current evidence base; it is indicative rather than exhaustive, and the relative-coverage judgements it supports are illustrative (see Section 9).

Source	Type	Context / sub-sector	ISG focus	Outcome focus
Imboden et al. (2017)	Empirical survey	International NGOs / non-profits	Policy; organisation & roles; risk	Protection; process
Hassan et al. (2023)	Empirical survey (n=168)	NGOs, Saudi Arabia	Risk management; awareness	Protection; process
Yaokumah (2013, 2014)	Empirical study	Industry sectors, Ghana	Governance practices; maturity	Process; protection
Le Blond et al. (2018)	Case study	Large humanitarian NGO	Organisation & roles; risk	Protection; service delivery
Marelli (2022)	Case analysis	Humanitarian (ICRC)	Policy; stakeholder comms	Service delivery; beneficiary harm
Tshifhumulo & Mudafu (2025)	Empirical study	Religious organisations	Awareness; policy	Process
Misata (2020)	Practitioner research	US non-profits	Organisation & roles; strategy	Process; protection
Ramljak (2025)	Systematic review	Non-profit sector (general)	Cross-cutting (all components)	Protection; process
Anfuso et al. (2026)	Scoping review	Humanitarian operations	Stakeholder comms; strategy	Service delivery; process
DSIT (2024)	Recurring sector survey	UK charities	Board oversight; policy; risk; compliance	Protection; process
NetHope (2024)	Sector report	Humanitarian / development NGOs	Organisation & roles; policy	Protection; process
CyberPeace Institute (2024)	Threat intelligence	NGO sector	Risk; organisation & roles	Protection
Chartered Gov. Inst. (2025)	Sector commentary	Non-profit boards	Board oversight	Process

Table 1. Transparent reference map of principal NFP-focused sources informing the review (indicative, not exhaustive). ISG focus categorised against the eight ISO/IEC 27014:2020 components; outcome focus against the four dimensions used in Section 5. DSIT = Department for Science, Innovation and Technology.

3. The Information Security Governance Construct in NFP Settings

3.1. Mapping the literature against the ISO/IEC 27014 components

The ISO/IEC 27014:2020 construct identifies eight components of ISG (International Organisation for Standardisation, 2020). Mapping the NFP-focused literature against these components reveals a marked unevenness in coverage, captured in Figure 1. The figure presents an illustrative summary of the author's reading of the evidence base rather than a measured frequency count (see Section 9).

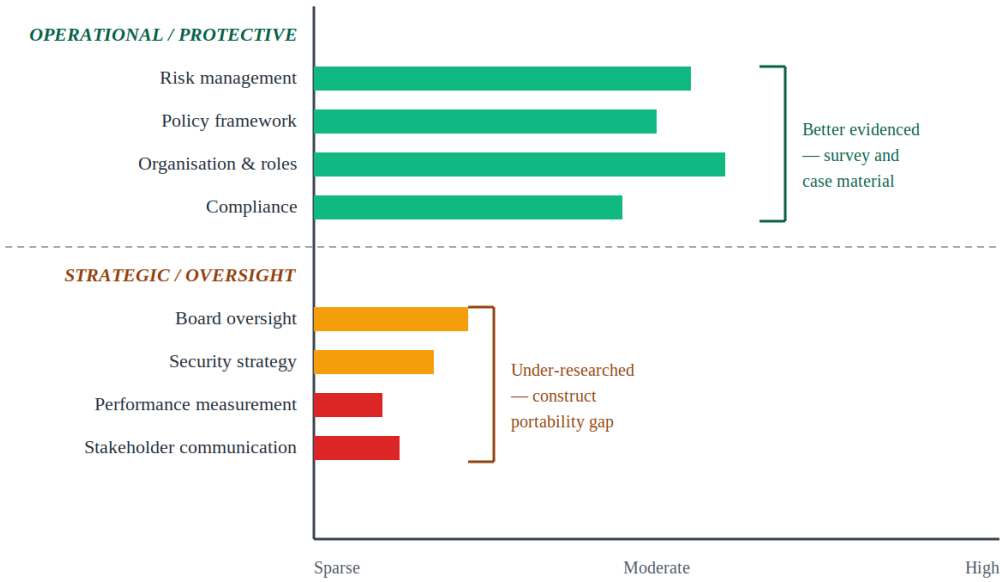

Figure 1. Engagement of the NFP-focused literature with the eight components of the ISO/IEC 27014:2020 Information Security Governance construct. Bars indicate relative density of empirical coverage identified during literature review (illustrative: high/moderate/low/sparse).

Board and executive oversight. Empirical evidence on board-level engagement is dominated by recurring sector surveys rather than peer-reviewed analytic work. The UK Cyber Security Breaches Survey reports that approximately 30 per cent of UK charities have a board member or trustee with explicit cybersecurity responsibility, a figure stable across recent years and substantially below comparable figures for businesses (Department for Science, Innovation and Technology, 2024). Sector commentary increasingly characterises cybersecurity as a trustee governance responsibility (Chartered Governance Institute, 2025). However, rigorous empirical study of how NFP boards actually engage — frequency of discussion, quality of risk dialogue, use of metrics — appears largely absent from the peer-reviewed literature identified.

Security strategy. Sources directly examining the formulation and alignment of information security strategy in NFP settings are sparse. Earlier NGO-focused surveys reported that around 80 per cent operated without a formal cybersecurity policy (Imboden et al., 2017); the figure appears to have improved, but, on the available evidence, remains below corporate benchmarks. Conceptual contributions propose adapted strategy frameworks (Horne et al., 2015), but empirical work testing strategy implementation in NFP contexts is limited.

Policy framework. Policy adoption is the most-studied governance component, primarily through sector surveys. Documented incident response policies, acceptable use policies, and data protection policies are present in a minority of NFPs, with proportions rising with size and sub-sector regulatory pressure (Department for Science, Innovation and Technology, 2024; NetHope, 2024). Within humanitarian NGOs, policy work is more developed: the International Red Cross and Red Crescent Movement adopted formal resolutions on humanitarian data protection following the 2022 ICRC breach (International Committee of the Red Cross, 2022).

Risk management. Risk management practice in NFPs is characterised by informality and reliance on external advice. UK charity sector studies indicate low rates of documented cyber risk assessment and limited trustee-level engagement with risk registers (Department for Science, Innovation and Technology, 2024). A Saudi Arabian survey of 168 NGOs identified a persistent gap between information security risk assessment standards and practical capability, attributed to resource and expertise constraints (Hassan et al., 2023).

Organisation and roles. Recent synthesis identifies dedicated information technology or security staff — rather than organisational size alone — as the strongest predictor of essential safeguard adoption, such as multi-factor authentication and structured access controls in non-profits (Ramljak, 2025). NFPs without dedicated security

roles typically depend on volunteer technical support, pro bono partnerships, or outsourced managed-service providers (CyberPeace Institute, 2024; Misata, 2020; NetHope, 2024).

Compliance. Compliance content focuses on general data protection obligations (GDPR; sector regulators such as the Charity Commission for England and Wales) rather than sector-specific cybersecurity statutes. UK Charity Commission CC3 and CC10 guidance explicitly expects trustees to identify, assess, and manage cyber risk proportionate to size and activities, although compliance is uneven. Certification regimes such as Cyber Essentials are increasingly cited as accessible baselines (UK National Cyber Security Centre, 2024).

Performance measurement. Performance measurement of ISG in NFPs is, on the basis of the literature identified, virtually unexamined in peer-reviewed empirical work. Where measurement appears, it tends to focus on technical metrics (incident counts, patching cadence) rather than governance indicators (board attention, policy maturity, audit findings). The apparent absence of validated NFP-adapted ISG maturity instruments is one of the most consequential gaps in the field.

Stakeholder communication. Stakeholder communication is an emerging concern. The 2026 humanitarian cybersecurity scoping review identifies "a complete absence of knowledge on crisis communication strategies" as one of the most striking gaps in the humanitarian sub-literature (Anfuso et al., 2026) — a finding that may extend across NFP sub-sectors.

3.2. The strategic-operational imbalance

Figure 1 makes visible a pattern that is otherwise dispersed across the literature: empirical engagement with ISG in NFPs concentrates on operational and protective components and appears to thin markedly when the construct moves into the strategic and oversight dimensions that distinguish governance from management. This imbalance is unlikely to be a coincidence of the researcher's interest. It plausibly reflects three deeper features of the NFP cybersecurity literature.

First, the literature has been driven principally by incident exposure and remediation. The empirical questions that get asked are protection-oriented: how many NFPs have been attacked, what controls do they have, and what training do staff receive? These are operational management questions. The strategic governance questions — how boards exercise oversight, how strategy is set, how performance is measured — require different data sources (board minutes, executive interviews, governance documents) that have rarely been accessed in published work — a limitation echoed in broader critiques of nonprofit governance research that has tended to over-rely on positivist cross-sectional designs (Cornforth, 2012).

Second, the practitioner and policy literature that surrounds the academic work is similarly operational. National cybersecurity agency guidance for NFPs — including the UK National Cyber Security Centre's Small Charity Guide (UK National Cyber Security Centre, 2024) — focuses on control implementation rather than governance architecture, and academic researchers have, to a substantial extent, followed the policy lead. Where governance has been addressed in sector-level outputs, it has tended to be by sector bodies and governance institutes (Chartered Governance Institute, 2025) rather than by academic researchers.

Third, and most fundamentally, the strategic components of ISG presuppose organisational structures — formally appointed boards exercising fiduciary oversight, executive functions with delegated authority for information security, performance measurement systems generating governance-relevant data — that many NFPs do not have in the forms presupposed by corporate ISG frameworks. The strategic-operational imbalance is therefore partly a reflection of construct mismatch: researchers have studied what NFPs have rather than what corporate ISG frameworks would have them have.

3.3. Construct portability: corporate-derived ISG in a non-profit context

The construct portability problem is the central conceptual issue facing NFP ISG research and merits substantive treatment. ISG was developed in corporate governance contexts and presumes a set of organisational features that are not uniformly present in the non-profit sector. The corporate ISG construct presupposes: a board of directors with formal fiduciary responsibility for organisational risk, exercising oversight over a salaried executive team that includes or reports to a Chief Information Security Officer or equivalent; a documented information security strategy aligned with an organisational strategy that has commercial or competitive content (Horne et al., 2015); a risk management function with formal risk appetite statements and risk-register processes; a compliance function responsive to sector-specific regulatory regimes; performance measurement systems generating board-level

dashboards; and stakeholder communication addressed primarily to shareholders, regulators, and customers (International Organisation for Standardisation, 2020; ISACA, 2019; Schinagl & Shahim, 2020).

The non-profit sector departs from each of these presuppositions in characteristic ways. Trustee boards are typically composed of volunteers serving for fixed terms, often with limited cybersecurity background and with multiple board commitments that constrain available attention (Chartered Governance Institute, 2025). Executive teams are smaller and frequently lack dedicated information security roles; the Chief Executive often holds direct or de facto responsibility for cybersecurity matters that would, in a comparably sized for-profit firm, be delegated. Organisational strategy is mission-driven rather than commercial, which alters the alignment problem: information security strategy must align with mission delivery and beneficiary protection, not with revenue generation or market positioning. Risk appetite frameworks adapted from corporate practice often translate poorly because the underlying risk taxonomy — financial loss, regulatory penalty, brand damage — does not capture the mission-specific risks that matter most (beneficiary harm, programme disruption, donor trust erosion, advocacy effectiveness). Compliance regimes are general (data protection, charity regulation) rather than sector-specific cybersecurity statutes equivalent to HIPAA or PCI-DSS. Performance measurement infrastructures are typically underdeveloped, with information security competing against many other reporting demands on small administrative teams. Furthermore, stakeholder communication is addressed to beneficiaries, donors, regulators, and members — a different set, with different informational expectations, than the shareholders and customers presupposed by corporate frameworks.

Three implications follow from this construct mismatch. First, the empirical literature in NFP cybersecurity has been answering operational questions in part because the strategic and oversight constructs do not have well-defined NFP-context referents to study. Researchers can count whether NFPs have antivirus software more easily than they can measure whether NFP boards exercise good cybersecurity oversight, because the operational concept maps directly onto observable reality, while the governance concept requires both adaptation and instrument development. Second, the gap is unlikely to be closed simply by accumulating more empirical studies of the kind already being conducted; the field plausibly needs theoretical and conceptual work to develop NFP-adapted ISG constructs before further large-scale empirical work can produce coherent cumulative findings (AlGhamdi et al., 2020). Third, the construct portability problem creates a methodological trap: applying corporate ISG instruments to NFPs without adaptation risks systematically producing findings of low NFP "maturity" that conflate genuine deficiency with construct mismatch.

Some of the resources for resolving this problem already exist outside the NFP-specific literature. Public-sector ISG research has confronted analogous adaptation challenges and produced sector-specific maturity models (Almuhammadi & Alsaleh, 2017; Maleh et al., 2021; Yusif & Hafeez-Baig, 2021). Critical-infrastructure work has reframed ISG as "information protection governance" to capture multi-stakeholder protection concerns (Carcary et al., 2016). Information security culture research has developed instruments that capture organisationally specific governance climate independent of formal structure (Da Veiga & Eloff, 2010; Da Veiga et al., 2020). The NFP literature has yet to draw systematically on these adjacent literatures to develop its own adapted construct. This is, on the evidence reviewed here, the most consequential single opportunity for the field over the next three to five years.

4. Contextual and Organisational Factors

Resource and budget constraints emerge as the dominant theme across virtually every empirical source identified. Sector surveys and case studies repeatedly document difficulty in funding dedicated cybersecurity roles, maintaining licensed security tooling, and releasing staff time for training (Imboden et al., 2017; Misata, 2020; NetHope, 2024; Ramljak, 2025). Pro bono and volunteer partnerships substitute partially for paid capability but introduce continuity and accountability complications (CyberPeace Institute, 2024).

Sub-sector. NFPs operating in health- and education-adjacent functions appear to adopt encryption, incident handling procedures, and formalised training earlier than comparable charities in other functions, owing to data protection obligations arising from the data they handle (Ramljak, 2025). Humanitarian NGOs face threat-actor profiles — including state-aligned and politically motivated actors — that are atypical of community-based charities and drive distinctive governance responses (Le Blond et al., 2018; Marelli, 2022; Searle, 2018). Emerging evidence suggests that some faith-based organisations may face distinctive governance tensions, including openness-oriented cultures, lower security awareness, and legacy infrastructure (Tshifhumulo & Mudafu, 2025).

Organisational size. Cyber incident rates and governance maturity both appear to rise with organisational size in the UK charity sector, with the proportion of charities reporting incidents rising from approximately one-third

overall to around two-thirds among those with annual income above £500,000 (Department for Science, Innovation and Technology, 2024). Size is, however, a coarser predictor of ISG maturity than dedicated staffing: the available synthesis suggests small charities with even a single dedicated security role can outperform substantially larger charities without one (Ramljak, 2025).

Board composition and capability. Volunteer trustee governance — with trustees often having limited technical background and multiple competing commitments — interacts with the absence of dedicated security staff to limit board-level engagement with cybersecurity oversight (Chartered Governance Institute, 2025; Cornforth, 2012).

Vendor and supply-chain dependencies. NFP reliance on outsourced IT support and on third-party data hosting creates supply-chain exposure that has been the proximate cause of significant incidents, including the 2023 Evide breach affecting more than 140 UK charities and the 2022 ICRC breach traced to a Swiss third-party contractor (Marelli, 2022).

Geographic and jurisdictional setting. The literature concentrates on jurisdictions with active national cybersecurity agencies and well-resourced charity regulators — the United Kingdom (Department for Science, Innovation and Technology, 2024; Scottish Government, 2020), the United States, and Switzerland (the latter driven by ICRC-related research). Coverage of NFPs in lower- and middle-income jurisdictions is uneven, with notable exceptions in Ghana (Yaokumah, 2013, 2014) and Saudi Arabia (Hassan et al., 2023). African, South Asian, Latin American, and Pacific NFP contexts are sparsely represented.

5. Evidence on Outcomes

Protection outcomes are the most-evidenced. The UK Cyber Security Breaches Survey provides recurring sector-level data on incident incidence (Department for Science, Innovation and Technology, 2024). Surveys of international NGOs and Saudi Arabian NGOs document low baseline rates of essential protective controls (Imboden et al., 2017; Hassan et al., 2023). The relationship between specific ISG arrangements and protection outcomes appears less rigorously established than in the corporate ISG literature; the available evidence is largely associative rather than causal (AlGhamdi et al., 2020).

Compliance outcomes are addressed primarily through descriptions of expected regulator behaviour and sector guidance rather than outcome-focused empirical study. Compliance with sector-regulator cybersecurity expectations (such as the UK Charity Commission's trustee guidance) is uneven, and systematic studies linking ISG arrangements to compliance attainment appear absent from the literature identified.

Service-delivery outcomes are evidenced predominantly through qualitative case material rather than quantitative analysis. The 2022 ICRC incident provides the strongest single illustration: the breach forced the shutdown of the Restoring Family Links service for several weeks, with reunification work continuing in a heavily degraded form, including reversion to manual processes (International Committee of the Red Cross, 2022; Marelli, 2022). The 2023 Evide breach disrupted services provided to survivors of abuse across more than 140 UK charities. Such cases establish that cyber incidents can directly damage NFP service delivery, but systematic evidence on the relationship between proactive ISG arrangements and service-delivery resilience is sparse.

Process outcomes (training adoption, awareness levels, policy adoption, ISG maturity) are the most variably reported. Sector surveys provide aggregate data on training and policy adoption rates (Department for Science, Innovation and Technology, 2024; NetHope, 2024). Validated NFP-adapted maturity instruments are not in routine use, and what counts as "mature" ISG in an NFP context remains undefined.

6. Critical Assessment of the Existing Literature

6.1. Methodological limitations

Cross-sectional surveys and qualitative case studies dominate the empirical NFP cybersecurity literature. Longitudinal, comparative, and quasi-experimental designs that could establish whether and how ISG investments produce protection, compliance, or service-delivery outcomes appear essentially absent from the literature identified. Sample sizes are often small. The recurring sector surveys conducted by national bodies are valuable for sector-level trend monitoring but are not designed to support causal inference about ISG–outcome relationships (AlGhamdi et al., 2020). The over-representation of self-report survey data, with its known social desirability and respondent expertise problems, further limits the strength of the existing evidence base. These limitations parallel longstanding critiques of nonprofit governance research more broadly (Cornforth, 2012).

6.2. Conceptual limitations

As argued in Section 3.3, the central conceptual limitation of the field is the largely unchallenged application of corporate-derived ISG constructs to NFP contexts. The empirical findings of low "maturity" or weak "governance" that recur in the literature should be read with care. In many cases, they may reflect a mismatch between the construct being measured and the organisational reality being assessed. The field has not yet produced a systematic conceptual reframing of ISG for NFP contexts, although adjacent literatures provide resources (Carcary et al., 2016; Da Veiga et al., 2020).

6.3. Geographic and sub-sector blind spots

Empirical work concentrates on higher-income jurisdictions. Faith-based organisations, member-based associations, foundations, and social enterprises are sparsely represented relative to their prevalence in the sector. Non-profit higher education institutions appear largely in adjacent higher-education information security literatures rather than in NFP-specific work. This geographic and sub-sector concentration limits the external validity of cross-cutting claims about "NFP cybersecurity" and obscures variation that may be theoretically and practically important.

7. A Research Agenda for NFP Information Security Governance

The critique above implies a structured research agenda spanning four mutually reinforcing streams: conceptual, methodological, empirical, and theoretical. Figure 2 sets out the proposed agenda and the indicative time horizons over which each stream should be advanced; Table 2 specifies illustrative research questions for each stream.

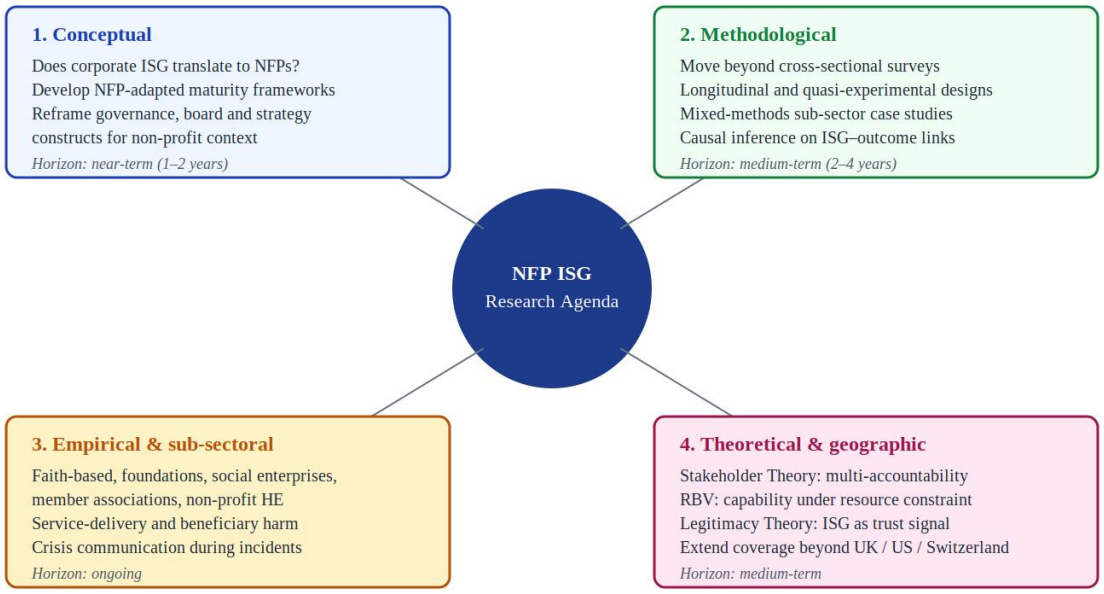

Figure 2. A research agenda for Information Security Governance in not-for-profit organisations, organised in four mutually reinforcing streams with indicative time horizons.

Stream	Illustrative research questions	Horizon
Conceptual	What would an NFP-adapted ISG maturity model look like across small, medium, and large charities? How should the eight ISO/IEC 27014 components be redefined for volunteer-governed, mission-driven organisations? What risk taxonomy captures mission-specific risks (beneficiary harm, programme disruption, donor trust)?	Near-term (1–2 yrs)

Stream	Illustrative research questions	Horizon
Methodological	Does appointing a cyber-responsible trustee improve incident response maturity over time? Do NFPs achieving Cyber Essentials certification show measurably different incident outcomes than comparable non-certified NFPs? How can governance-document review, interviews, and outcome tracking be combined to validate NFP-adapted constructs?	Medium-term (2–4 yrs)
Empirical & sub-sectoral	How do cyber incidents affect beneficiary trust and service continuity in humanitarian NGOs? How do ISG arrangements differ across faith-based organisations, foundations, social enterprises, and member associations? What crisis-communication practices do NFPs adopt during and after incidents?	Ongoing
Theoretical & geographic	Can ISG capability be treated as a legitimacy resource in donor-funded organisations? How should Stakeholder Theory be extended where beneficiaries bear the direct harm of governance failure? Do findings from UK, US, and Swiss-humanitarian settings hold in African, South Asian, and Latin American NFP contexts?	Medium-term

Table 2. Research agenda for NFP Information Security Governance: four streams, illustrative research questions, and indicative time horizons. The research questions are offered as a starting framework for the field rather than an exhaustive specification.

7.1. Conceptual priorities

The most consequential priority is conceptual reframing. The field plausibly requires NFP-adapted constructs and frameworks before further large-scale empirical work can produce coherent cumulative findings. Three lines of conceptual work are needed in the near term. First, as the lead question in Table 2 indicates, the development of an empirically grounded NFP-adapted ISG maturity model that addresses the structural features of the non-profit sector: volunteer boards, dedicated-staffing variability, mission alignment in place of commercial alignment, and beneficiary-protection risk taxonomies in place of financial-loss taxonomies. Adjacent maturity-model work in critical infrastructure (Maleh et al., 2021), public organisations (Almuhammadi & Alsaleh, 2017), conceptual models for cybersecurity governance (Yusif & Hafeez-Baig, 2021), and capability frameworks (Carcary et al., 2016) provides a methodological template. Second, a reconceptualisation of the eight ISO/IEC 27014 components specifying what each looks like in an NFP context: what "board oversight" means with a volunteer trustee board; what "security strategy" alignment means in a mission-driven organisation (Horne et al., 2015); what "stakeholder communication" means when beneficiaries are the principal affected stakeholder. Third, a reframing of risk appetite for NFPs that captures mission-specific risks rather than transposing the financial-loss and regulatory-penalty taxonomy from corporate ISG practice.

7.2. Methodological priorities

The empirical NFP cybersecurity literature is dominated by methodologies that cannot answer the questions the field most needs to answer. Three methodological priorities follow. First, the field needs longitudinal designs that track ISG arrangements and outcomes in the same organisations over multi-year periods; cross-sectional survey snapshots cannot establish whether governance changes produce outcome changes, yet that is precisely what the policy- and practice-relevant questions require (Cornforth, 2012). Second, quasi-experimental and natural-experiment designs — comparing NFPs that adopt particular governance arrangements (such as appointing a cyber-responsible trustee or achieving Cyber Essentials certification) with comparable NFPs that do not — could provide credible causal evidence on the value of ISG investment. Third, mixed-methods sub-sector case studies that combine governance-document review, trustee and executive interviews, and outcome tracking are needed to develop and validate the NFP-adapted constructs called for in Section 7.1. Future systematic and scoping reviews on narrower questions should follow established reporting guidance such as PRISMA-ScR (Tricco et al., 2018).

7.3. Empirical and sub-sectoral priorities

Several empirical priorities follow directly from the gaps identified in Section 6. First, faith-based organisations, foundations, social enterprises, member-based associations, and non-profit higher education institutions all require substantive sub-sector-specific empirical work. The pattern reported in religious organisations — prioritising openness over security, with consequent governance gaps (Tshifhumulo & Mudafu, 2025) — suggests sub-sectors may differ in ways that aggregate cross-sector findings obscure. Second, service-delivery and beneficiary-harm outcomes require dedicated empirical attention; the question of how cyber incidents affect beneficiary trust and service continuity in humanitarian NGOs (Table 2) is of direct mission relevance, yet the existing literature establishes that such harms can be severe while providing little quantitative evidence on the conditions under which they occur or the governance arrangements that mitigate them. Third, crisis communication during and after cyber incidents in NFPs is essentially un-researched (Anfuso et al., 2026); this gap is immediately addressable through case-study work and through a targeted survey of NFPs that have experienced incidents. Fourth, the relationship between specific governance arrangements (cyber-responsible trustees, certification adoption, formal policy frameworks) and downstream outcomes (incident frequency, recovery time, donor retention) is essentially unexamined and is the empirical question of greatest direct practical relevance.

7.4. Theoretical and geographic priorities

The theoretical agenda follows the three lenses identified in Section 1.4. Stakeholder Theory in NFP contexts requires extension to address the distinctive feature that beneficiary stakeholders frequently bear the direct harm of governance failure — a feature that mainstream stakeholder theorising, developed in corporate contexts, does not directly address. Resource-Based View applications to NFP ISG require empirical work testing whether ISG capability functions as a strategically valuable resource in mission-delivery terms, and what conditions support its accumulation. Legitimacy Theory applications are essentially undeveloped in the NFP cybersecurity literature and represent a substantial open opportunity: as the lead theoretical question in Table 2 frames it, ISG capability can be theorised as a legitimacy resource in donor-funded organisations, with empirical implications for how breaches damage organisational legitimacy and how proactive governance investments may produce legitimacy returns. The geographic agenda is straightforward: empirical work is needed in African, South Asian, Latin American, Pacific, and Middle Eastern NFP contexts to test the portability of findings derived from UK, US, and Swiss-humanitarian-NGO settings (Yaokumah, 2014; Hassan et al., 2023).

8. Theoretical and Practical Implications

8.1. Theoretical contributions

The review suggests that NFP ISG cannot usefully be theorised as a simple translation of corporate ISG. Each of the three theoretical lenses adopted here generates distinct implications. Stakeholder Theory illuminates the multi-accountability structure that distinguishes NFP ISG from corporate practice and identifies beneficiaries as a category of stakeholder whose direct vulnerability to governance failure has no clear analogue in for-profit settings. The Resource-Based View illuminates ISG capability as a resource developed under chronic constraint, with implications for how the field should conceptualise capability development trajectories. Legitimacy Theory illuminates ISG as a legitimacy practice with implications for how breaches damage organisational standing and how proactive investments may generate legitimacy returns. The combined theoretical contribution is the proposition that NFP ISG should be understood as a multi-stakeholder, resource-constrained, legitimacy-relevant practice — rather than as a thin or delayed version of corporate ISG.

8.2. Implications for trustee boards and executive leadership

For trustee boards, the evidence supports treating cybersecurity as a board-level governance responsibility rather than an operational IT matter, with at least one trustee carrying explicit cyber responsibility and with cyber risk integrated into the charity's risk register and reviewed at least annually (Chartered Governance Institute, 2025; Department for Science, Innovation and Technology, 2024). For executive leadership, the centrality of dedicated security capability — even at modest scale — is supported across multiple empirical sources; where dedicated staffing is infeasible, structured partnerships with sector cybersecurity bodies such as NetHope, the CyberPeace Institute, or national cyber agencies offer a partial substitute (Misata, 2020; NetHope, 2024; CyberPeace Institute, 2024). For operational managers, evidence-supported priorities include documented incident response planning, regular awareness training, multi-factor authentication, structured access management, and explicit attention to

vendor and supply-chain risk. These recommendations should be read as consistent with the current evidence base rather than as causally validated prescriptions; the limitations in Sections 6 and 9 apply.

8.3. Implications for policymakers and sector bodies

National cybersecurity agencies have an important role in supporting NFP cybersecurity through accessible, sector-adapted guidance and free or low-cost protective services (UK National Cyber Security Centre, 2024). Charity regulators have a parallel role in articulating clear ISG expectations of trustees. Sector bodies, including NetHope, the CyberPeace Institute, and the Global Cyber Alliance, are providing capacity-building infrastructure at an international scale. Funders and donors have potential leverage to shape ISG adoption through grant conditions and capacity-building investment; this leverage is not yet systematically deployed and represents a near-term opportunity for sector-wide ISG improvement.

9. Limitations

This is a critical review, not a systematic or scoping review, and the limitations are correspondingly different in character. The review does not claim to be exhaustive in its coverage of the published literature; sources were identified through targeted searching guided by the four organising questions and the substantive criterion of ISG relevance, and additional sources may exist that would refine the analysis. The review is restricted to English-language sources, which excludes potentially relevant scholarship in other languages — notably Spanish, French, Mandarin, and Arabic — where NFP cybersecurity research is developing. The boundary between ISG and adjacent constructs (information security management, data protection governance, IT governance) is not always clean in the literature, and inclusion decisions, while transparent, are inevitably interpretive. Importantly, the source map in Table 1 and the relative-coverage judgements summarised in Figure 1 are illustrative syntheses of the author's reading of the literature rather than measured frequency analyses; they are intended to orient the field and should not be cited as quantitative measures. A formal scoping review applying reproducible search and screening procedures would be required to confirm or refine them. Several claims in Sections 3 to 6 are necessarily qualified — "appears," "on the evidence reviewed here," "plausibly" — precisely because the underlying evidence base is thin; readers should treat these as provisional readings rather than settled findings. Finally, the research agenda articulated in Section 7, including the specific research questions in Table 2, reflects the author's judgement on priorities and is offered as a proposal for the field rather than as a definitive prescription.

10. Conclusion

Information Security Governance in not-for-profit organisations is an emergent research field facing a foundational construct portability problem. The existing literature, though growing rapidly, appears to engage unevenly with the components of the ISO/IEC 27014:2020 ISG construct — operationally rich, strategically thin — and has done so in part because the strategic and oversight components of the corporate-derived ISG framework do not have well-defined NFP-context referents. This review has mapped the imbalance, critically interrogated its origins, and articulated a four-stream research agenda — conceptual, methodological, empirical, and theoretical — with specific research questions to advance the field over the next three to five years. The central claim is that the priority for the field is not more empirical work of the kind already being conducted, but rather conceptual and methodological work that produces NFP-adapted constructs and the instruments to study them. Above all, the review argues that NFP ISG should be treated not as a weaker version of corporate ISG, but as a distinct governance problem shaped by mission accountability, resource scarcity, and beneficiary protection. Pursued seriously, this agenda would convert NFP ISG from an emerging area of episodic research into a coherent field capable of supporting the trustees, executives, regulators, and funders who must collectively raise cybersecurity capability across a sector under accelerating threat.

Declarations

Funding. No funding received, all was self-funded by the author.

Conflicts of interest. None

CRediT author contribution statement. Samuel O. Fakunle: Conceptualization, Methodology, Investigation, Formal analysis, Writing — original draft, Writing — review and editing. Bright Onyedikachi Asonye: Investigation, Validation, Writing — review and editing.

Data availability. This article is a critical review and uses only publicly available published sources. No new data were generated.

Ethical approval. Not applicable.

References

1. AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030. https://doi.org/10.1016/j.cose.2020.102030
2. Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for the NIST cybersecurity framework. Computer Science & Information Technology, 7(3), 51–62.
3. Anfuso, C., Bartolucci, A., Del-Real, C., & Kuipers, S. (2026). Cybersecurity threats, challenges, and strategies in humanitarian operations: A scoping review. International Journal of Disaster Risk Reduction. Advance online publication. https://doi.org/10.1016/j.ijdrr.2026.106082
4. Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108
5. Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. IT Professional, 18(2), 22–30. https://doi.org/10.1109/MITP.2016.27
6. Chartered Governance Institute UK and Ireland. (2025). Why cybersecurity is the new governance frontier for non-profits. CGI UK and Ireland. https://www.cgi.org.uk/resources/blogs/2025/why-cybersecurity-is-the-new-governance-frontier-for-non-profits/
7. Cornforth, C. (2012). Nonprofit governance research: Limitations of the focus on boards and suggestions for new directions. Nonprofit and Voluntary Sector Quarterly, 41(6), 1117–1136. https://doi.org/10.1177/0899764011427959
8. CyberPeace Institute. (2024, September 17). Cyber threat intelligence reports: August 2024, NGO Sector. https://cyberpeaceinstitute.org/news/cyber-threat-intelligence-report-august-2024/
9. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture — Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713
10. Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
11. Department for Science, Innovation and Technology. (2024). Cyber Security Breaches Survey 2024. UK Government. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024
12. Freeman, R. E. (1984). Strategic management: A stakeholder approach. Pitman.
13. Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. Health Information and Libraries Journal, 26(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x
14. Hassan, M., Saeedi, K., Almagwashi, H., & Alarifi, S. (2023). Information security risk awareness survey of a non-governmental organization in Saudi Arabia. In A. Visvizi, O. Troisi, & M. Grimaldi (Eds.), *Research and Innovation Forum 2022* (pp. 39–71). Springer. https://doi.org/10.1007/978-3-031-19560-0_4
15. Horne, C. A., Ahmad, A., & Maynard, S. B. (2015). Information security strategy in organisations: Review, discussion and future research directions. Australasian Conference on Information Systems.
16. Imboden, T. R., Phillips-Wren, G., & Schroeder, M. (2017). Cybersecurity in non-profit and non-governmental organisations: Results of a self-report web-based cybersecurity survey. Issues in Information Systems, 18(4), 169–178.
17. International Committee of the Red Cross. (2022, January 19). Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people. ICRC. https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people
18. International Organisation for Standardisation. (2020). ISO/IEC 27014:2020 — Information security, cybersecurity and privacy protection: Governance of information security. ISO.
19. ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA.
20. Le Blond, S., Cuevas, A., Troncoso-Pastoriza, J. R., Jovanovic, P., Ford, B., & Hubaux, J.-P. (2018). On enforcing the digital immunity of a large humanitarian organisation. Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), 424–440. https://doi.org/10.1109/SP.2018.00019
21. Maleh, Y., Sahid, A., Belaissaoui, M., & Sahid, K. (2021). A maturity framework for cybersecurity governance in organisations. EDPACS, 63(6), 1–22. https://doi.org/10.1080/07366981.2020.1815354
22. Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organisations. International Review of the Red Cross, 104(919), 1267–1284. Cambridge University Press.
23. Misata, K. (2020, November 4). Results from the field: Cybersecurity in nonprofits and why it matters (Security seminar presentation). Centre for Education and Research in Information Assurance and Security (CERIAS), Purdue University. https://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/0vk0ibok5k0cfta3d52f3pooaf

24. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
25. NetHope. (2024). 2024 state of humanitarian and development cybersecurity report. NetHope. https://nethope.org/
26. Ramljak, D. (2025). Enhancing cybersecurity readiness in non-profit organisations through collaborative research and innovation — A systematic literature review. Computers, 14(12), 539. https://doi.org/10.3390/computers14120539
27. Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": Towards digital security governance. Information & Computer Security, 28(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033
28. Scottish Government. (2020). Cyber resilience and the third sector: Risks, challenges and opportunities — Research report. Scottish Government.
29. Searle, M. S. (2018). Is the use of cyber-based technology in humanitarian operations leading to the reduction of humanitarian independence? Centre for Non-Traditional Security Studies Working Paper.
30. Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, 20(3), 571–610. https://doi.org/10.5465/amr.1995.9508080331
31. Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. Annals of Internal Medicine, 169(7), 467–473. https://doi.org/10.7326/M18-0850
32. Tshifhumulo, R., & Mudafu, T. (2025). Cybersecurity awareness and practices in religious organisations. International Journal of Business Ecosystem & Strategy, 7(4), 197–210.
33. UK National Cyber Security Centre. (2024). Small charity guide. National Cyber Security Centre. https://www.ncsc.gov.uk/
34. Von Solms, S. H., & Von Solms, R. (2009). Information security governance. Springer. https://doi.org/10.1007/978-0-387-79984-1
35. Wernerfelt, B. (1984). A resource-based view of the firm. Strategic Management Journal, 5(2), 171–180. https://doi.org/10.1002/smj.4250050207
36. Yaokumah, W. (2013). Evaluating the effectiveness of information security governance practices in developing nations: A case of Ghana. International Journal of IT/Business Alignment and Governance, 4(1), 27–43. https://doi.org/10.4018/jitbag.2013010103
37. Yaokumah, W. (2014). Information security governance implementation within Ghanaian industry sectors: An empirical study. Information Management & Computer Security, 22(3), 235–250. https://doi.org/10.1108/IMCS-06-2013-0044
38. Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. Journal of Applied Security Research, 16(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995