International Journal of Human Research and Social Science Studies

ISSN(p): 3050-547X, ISSN(e): 3050-5488

Volume 02 Issue 12 December, 2025

DOI: https://doi.org/10.55677/ijhrsss/05-2025-Vol02I12

Page No : 995-1009

Lead with Payload: A Christian Stewardship Model for Digital-Era Resilience in Micro-Ministries

Jackson Saya[1], Kelvin Onongha[2], Paul Ataro[3]

[1,2,3] Adventist University of Africa

ABSTRACT: Faith-based micro-ministries often launch change efforts that outpace the digital foundations needed for daily execution. This study examines whether pairing a tangible digital base—governed data, simple automation, and dependable infrastructure—with disciplined leadership practice strengthens organisational resilience among Seventh-day Adventist self-supporting ministries in Kenya. We analysed cross-sectional survey data from 141 organisations using confirmatory factor analysis and structural equation modelling.

Measurement showed acceptable reliability and validity. Structurally, the digital base related positively to resilience, while leadership practice alone contributed little without that base; their convergence produced the strongest association. Robustness checks using alternative estimators and sensitivity analyses yielded consistent rankings of effects. We translate these findings into a sequenced, resource-sensitive operating plan tailored to micro/volunteer ministries and ministry-run enterprises. The results suggest that ministries improve situation awareness, elasticity, and reliability when they first establish a minimal digital payload and then bind it with focused portfolios, cyber hygiene, and adoption rituals. We outline practical implications for leaders, boards, and partners.

Corresponding Author:
Jackson Saya

KEYWORDS:
digital maturity; organisational resilience; faith-based nonprofits; micro-ministries; Kenya; structural equation modelling

INTRODUCTION

Problem Framing for Christian Leadership

Faith-based self-supporting ministries (SSMs) affiliated with the Seventh-day Adventist Church in Kenya operate under persistent constraints: irregular funding, volunteer-heavy staffing, uneven governance capacity, and variable digital access. Even as connectivity improves, gaps in devices, skills, and affordability disproportionately affect smaller nonprofits, and tightened regulatory expectations under Kenya's Data Protection Act have raised baseline requirements for stewardship and cyber hygiene. In this environment, disruption—epidemiological, economic, climatic, or regulatory—is a planning premise rather than an exception. The practical question is which digital investments and managerial routines actually strengthen organisational resilience (OR)—the capacity to anticipate, absorb, and adapt—rather than merely accumulating tools that add cost and complexity (GSMA, 2023, 2024; Kenya National Assembly, 2019).

The Leadership Illusion: Strategies and Committees Without a Payload.

Across faith-based micro-enterprises, leadership teams often begin with away-days, mission statements, and change committees—only to discover that implementation stalls because the informational core is thin: lacking canonical contact lists, duplicate records, manual workflows, and brittle infrastructure. Scholarship on digital transformation is clear that strategy alone does not move the needle; impact arises when managerial intent is tethered to governed digital assets and executable routines (Kane et al., 2015; Verhoef et al., 2021; Vial, 2019). In resilience terms, organisations absorb and adapt to shocks when they possess reliable information, repeatable routines, and slack/buffers—not when they merely declare priorities (Hillmann & Guenther, 2021; Lengnick-Hall et al., 2011). In complex, tightly coupled operating environments—exactly the setting of many ministries—failures propagate through invisible dependencies when data are dirty and processes are hand-built, which is why high-reliability practice (e.g., preoccupation with failure, discipline around checklists) must be married to a usable digital base (Weick & Sutcliffe, 2015). The illusion is seductive: leaders view "alignment workshops" as a sign of progress. However, without a digital payload—clean data, simple automation/analytics, and reliable infrastructure—alignment has little to align (Barney, 1991; Wade & Hulland, 2004). Section 6 operationalises these thresholds as stage gates in the 12-month plan.

Framing the Synergy: When DI × TMI Works—and When It Stalls

The SDMR logic rests on a simple claim: leadership amplifies a real digital base; it does not substitute for it. In practice, that means Digital Intensity (DI)—clean, governed data (DM), simple automation and analytics (AAI), and reliable, cost-steady infrastructure (GD)—must clear a threshold before Transformation Management Intensity (TMI) can pay off. Below that threshold, additional planning, committees, and rhetoric often add friction without creating resilience. Above it, leadership attention, role clarity, and learning rituals convert the payload into robust routines that hold during disruption.

This threshold view is consistent with the resource-based perspective, which posits that digital assets become useful when they are valuable, rare, inimitable, and organised (VRIO/VRIN). Thin, fragmented data or brittle workflows are not yet "resources" in that sense; governance can only amplify what is already capable of travelling across decisions (Barney, 1991; Wade & Hulland, 2004). It also accords with dynamic capabilities: sensing and seizing depend on what can be sensed and seized, which requires instrumentation, feedback, and repeatable processes. Leadership that reconfigures without a clear substrate risks generating noise (Eisenhardt & Martin, 2000; Teece, 2007; Verhoef et al., 2021; Vial, 2019).

There are also boundary conditions. In small ministries with volatile cash flow and limited staff time, adding new tools or policies can tip the system into overload—a complexity cost that cancels out intended gains. Resilience is an emergent property of tightly coupled sociotechnical routines: when coupling is incoherent or energy (time/attention) is insufficient, the organisation becomes brittle (Weick & Sutcliffe, 2015). The implication is not to slow transformation, but to sequence it: establish a minimal payload (governed contact lists, one or two automations that actually run, verified backups/uptime), then scale leadership rituals and portfolio choices. In short, do payload first, then governance.

For Christian leadership, this is more than technique. Servant leadership emphasises listening, foresight, stewardship, and community—virtues that map directly onto the operating choices that make DI and TMI work together. Stewardship frames data as a trust, not a trophy; processes as care for people, not paperwork; and reliability as a moral duty to the community one serves (Greenleaf, 1977; Spears, 2010; Banks & Ledbetter, 2004). Read this way, DI is care of decisions (accurate, timely, fair), while TMI is care of people and practices (clear roles, learning, accountability). Together, they form a theology of digital stewardship that seeks continuity of mission, not accumulation of gadgets.

The following sections translate these thresholds into a staged operating plan. Section 6 turns the threshold logic into quarter-by-quarter "stage gates" that leaders can use to time governance to payload maturity.

Ministry realities: reliance on volunteers, cash flow volatility, compliance, and uneven connectivity.

Self-supporting ministries and ministry-run businesses in Sub-Saharan Africa operate under structural constraints. Volunteer-heavy staffing and episodic funding make it challenging to sustain process discipline; staff turnover erodes tacit knowledge and undermines record-keeping; and connectivity, device access, and digital skills vary significantly across urban and rural contexts (GSMA, 2023; Verhoef et al., 2021). In Kenya, compliance expectations have tightened with the Data Protection Act (2019), which requires lawful, fair, and transparent processing; data minimisation; integrity and confidentiality; and demonstrable accountability—obligations that apply to nonprofits that collect personal data for outreach, education, or social services (Kenya National Assembly, 2019). These realities mean that "strategy-first" initiatives—new mission dashboards, restructured committees, or culture campaigns—frequently under-deliver if the ministry cannot see its work (no canonical datasets), act at speed (no low-code automation of high-friction workflows), or stay up during disruptions (no backup/UPS/cloud posture). The empirical resilience literature reiterates that continuity and adaptive capacity hinge on situation awareness (timely, accurate, decision-ready data), elasticity (ability to reconfigure workflows quickly), and reliability (infrastructure and routines that prevent minor faults from cascading) (McManus et al., 2008; Duchek, 2020; Hillmann & Guenther, 2021). Put simply, in ministry operations, resilience is defined as mission continuity—the ability to sustain worship, education, evangelism, media, or health services despite volatility (Vargo & Seville, 2011; Lee et al., 2013).

Faith and Systems Logic

For Christian leaders, stewardship extends to the care of information, processes, and people. Information care means knowing *what* data are held, *why* they are held, *who* is responsible, and *how* quality is maintained—governance that transforms data from liability into an asset (Barney, 1991; Wade & Hulland, 2004). Reliability implies attention to backups, role-based access, continuity drills, and energy-aware "green" choices that reduce downtime and cost volatility (Weick & Sutcliffe, 2015; Verhoef et al., 2021).

Inclusion requires low-bandwidth options, simple language, and privacy-by-design features that widen participation and build trust, as mandated by the Data Protection Act (Kenya National Assembly, 2019; GSMA, 2023). Dynamic capabilities theory frames this as sensing, seizing, and reconfiguring: leaders curate high-quality signals (sensing), convert them into quick and safe actions (seizing), and refit routines and structures as context changes (reconfiguring) (Teece, 2007; Eisenhardt & Martin, 2000). The study's evidence underscores the same logic: TMI amplifies only when tethered to DI; governance and change rituals (DBS/DR/HCD) create value when the informational and operational substrate exists to carry them (Kane et al., 2015; Vial, 2019; Hillmann & Guenther, 2021).

Within Christian leadership traditions, stewarding information and routines is part of neighbour-love and accountability. Servant

leadership emphasises enabling others to flourish through trustworthy systems (Greenleaf, 1977; Spears, 2010). Transformational stewardship frames digital care as co-labour with God's mission—aligning resources to calling with prudence and transparency (Banks & Ledbetter, 2004). These commitments translate operationally into governed data, safety by design, and inclusion for the least connected—practices that anchor the doctrine advanced here.

MATERIALS AND METHODS

This study surveyed SDA self-supporting ministries (SSMs) in Kenya at the organisational level (one senior informant per ministry). Because SSMs are hard to list formally, ministries were identified through denominational networks and respondent-driven sampling (seeds, controlled waves) to reach a broader field (Heckathorn, 2002; Salganik & Heckathorn, 2004). The digital-maturity items—Digital Intensity (data governance/quality; simple automation & analytics; reliability/green rationalization) and Transformation Management Intensity (mission-linked digital portfolio; readiness/cyber hygiene; human-centric adoption)—were contextualized for faith-based nonprofits through expert review and cognitive pretesting with SSM leaders; only minor wording localizations were made, preserving construct meaning (Beaton et al., 2000; International Test Commission, 2018; Tourangeau, Rips, & Rasinski, 2000). To limit common-method bias, we employed procedural remedies (assured anonymity, varied anchors, and proximal separation) and post-hoc checks. A single-factor solution did not dominate, and the results were not consistent with a marker-artefact (Podsakoff et al., 2003). We estimated a hierarchical CFA and then SEM with robust MLR and bootstrapped CIs for direct/indirect effects; WLSMV with polychoric correlations served as a sensitivity estimator for Likert indicators (Hu & Bentler, 1999; Flora & Curran, 2004; Li, 2016).

Detailed fit indices, estimator choices, and small-sample corrections appear in Appendix B, along with a brief note on invariance screening by organisation size/type and the outcome of early–late wave nonresponse checks (Kline, 2016; Satorra & Bentler, 1994; Bollen & Stine, 1992).

See table 1 for full indices, robustness notes.

RESULTS

What Model 2 revealed—why the TMI → OR direct path is attenuated.

The single-stream leadership specification (Model 2) tested whether Transformation Management Intensity (TMI)—the bundle of digital business strategy (DBS), digital readiness (DR), and human-centric digitisation (HCD)—by itself predicts organisational Resilience (OR). The result was a small, statistically non-significant direct effect, indicating that leadership activity untethered from a substantive digital base does not reliably translate into continuity, recovery, or adaptive capacity. This attenuation is consistent with three literatures. First, alignment/contingency: Managerial intent yields performance only when it aligns with the organisation's technological and environmental context; absent a functioning information substrate, alignment workshops and committees have little to align (Henderson & Venkatraman, 1993; Coltman, Tallon, Sharma, & Queiroz, 2015). Second, dynamic capabilities — sensing, seizing, and reconfiguring — presuppose signal quality and executable routines; a leadership process without actionable data and automatable workflows cannot sustain reconfiguration under turbulence (Teece, 2007; Eisenhardt & Martin, 2000).

Third, resilience scholarship suggests that adaptive capacity emerges from reliable information, routinised coordination, and slack/buffers; exhortation alone cannot substitute for these operational antecedents (McManus, Seville, Vargo, & Brunsdon, 2008; Hillmann & Guenther, 2021). In short, TMI under-delivers when the digital base is thin—a ministry can articulate strategy, change rituals, and still struggle to detect issues early, move work quickly, or stay up during shocks if the informational and infrastructural core is weak (Kane, Palmer, Phillips, Kiron, & Buckley, 2015; Vial, 2019).

Table 1 — Global fit indices (CFA and SEM)

Model	CFI	TLI	RMSEA	SRMR
Measurement model (CFA; DI/TMI/OR; 2nd-order)	0.936	0.922	0.058	0.061
Structural Model 1 (DI → OR)	0.931	0.918	0.060	0.064
Structural Model 2 (TMI → OR)	0.915	0.898	0.067	0.070
Structural Model 3 (DML → OR)	0.948	0.937	0.054	0.056

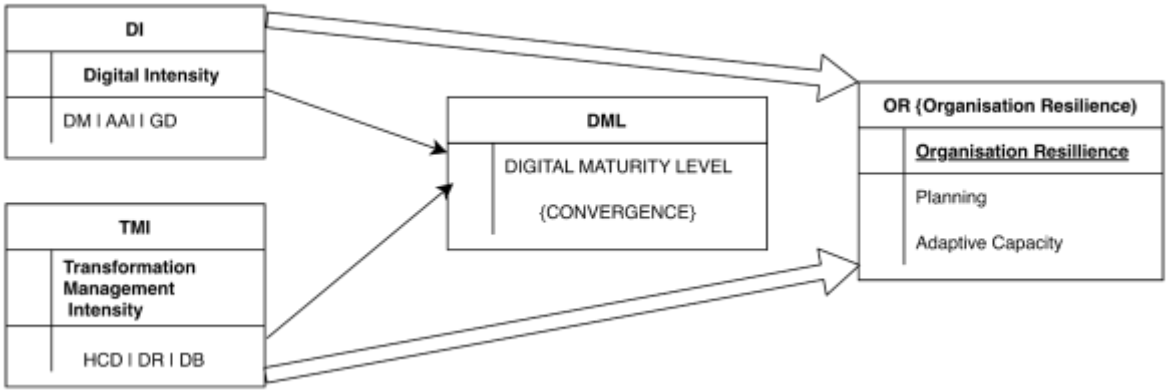
Notes. CFI/TLI ≥ .90 and SRMR ≤ .08 indicate acceptable fit; RMSEA ≤ .08 indicates reasonable error of approximation.

DISCUSSION

What Model 3 clarified—convergence outperforms single streams.

The convergence specification (Model 3) modelled Digital Maturity Level (DML) as a higher-order factor that binds DI and TMI. This model delivered the most significant and most stable association with OR, and the ordering of effects was DML > DI > TMI. Substantively, ministries that pair governed data, simple automation, and reliable "green" infrastructure (DI) with strategy focus, readiness baselines, and human-centric adoption (TMI) report stronger planning discipline and greater adaptive capacity. This pattern aligns with RBV: governed digital assets and routines behave like VRIN resources—valuable, hard to imitate quickly, and non-substitutable when embedded in processes—especially in resource-constrained contexts (Barney, 1991; Wade & Hulland, 2004). It also extends dynamic capabilities by showing that orchestration (the "binding" represented by DML) is not a soft overlay but a capability in its own right, converting technical potential into resilient performance (Teece, 2007; Verhoef et al., 2021). From a complexity/systems view, resilience appears as an emergent property of coherent coupling: when information flows, operational routines, and buffers are synchronised, minor faults do not cascade and organisations recover faster (Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021). The evidence, therefore, cautions against strategy-first approaches and favours payload-then-practice sequencing: build enough DI to cross a threshold, then apply TMI to amplify and institutionalise use (Kane et al., 2015; Vial, 2019). At the same time, leadership should expect thresholds and diminishing returns: as complexity outpaces adaptive capacity, digitalisation can saturate or even erode resilience—underscoring the importance of staging and fit.

Figure. Evidence map contrasting Model 2 and Model 3.



Evidence map contrasting Model 2 and Model 3. Thicker arrows denote stronger associations. Model 2 shows an attenuated TMI → OR path; Model 3 shows the strongest DML → OR pathway with DI and TMI converging.

Mechanisms—how DI components and TMI routines produce resilience.

DM → situation awareness (clean data = foresight).

Data Management (DM)—including ownership, quality rules, canonical lists, and auditability—improves situation awareness, the cornerstone of crisis readiness and adaptive control. Ministries with decision-ready data detect anomalies earlier, target outreach more precisely, and coordinate volunteers with fewer hand-offs. This pathway aligns with resilience research, which identifies early detection and shared information as precursors to robust planning and improvisation (McManus et al., 2008; Lee, Vargo, & Seville, 2013; Duchek, 2020). In RBV terms, high-quality, governed data are foundational digital assets; they are sticky, path-dependent, and difficult for peers to replicate quickly, making them resilience-relevant beyond short-term efficiency (Barney, 1991; Wade & Hulland, 2004).

AAI → elasticity (cycle times shrink; error traps).

Automation & Intelligence (AAI) shortens cycle times and traps routine errors at source (e.g., validations, deduplication, workflow triggers). Under volatility, the ability to pivot workflows quickly without introducing defects is a form of operational elasticity that supports both continuity and adaptation (Eisenhardt & Martin, 2000; Teece, 2007). The digital-transformation literature consistently reports that even low-code automations yield outsized returns in small organisations by releasing scarce human attention for non-routine work and institutionalising good practice (Kane et al., 2015; Verhoef et al., 2021). AAI therefore acts as the execution engine that turns awareness into timely action—central to the observed DI → OR effect.

GD → reliability/legitimacy (uptime, cost stability).

Green Digitisation (GD)—favouring the cloud over ageing hardware, disciplined backups, power protection/UPS, and basic monitoring—raises uptime and stabilises costs (e.g., reduced hardware failures, a smoother energy profile). In resilience terms, this is a buffering mechanism that prevents small shocks (power dips, device loss) from escalating into extended outages (Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021). In nonprofit settings, reliability also carries legitimacy benefits: consistent service

builds trust with congregations, donors, and partners, which sustains resources during times of shock (Vargo & Seville, 2011; Verhoef et al., 2021). GD thus supplies the infrastructural bedrock on which DM and AAI can operate predictably.

DBS/DR/HCD bind DI into routine use.

The managerial stream—**DBS, DR, HCD**—**amplifies** the payload by enforcing focus, safety, and adoption. DBS keeps scarce effort focused on a few mission-linked use cases; DR institutionalises cyber hygiene (MFA, backups, role-based access) and continuity drills so that new capabilities do not introduce fragility; HCD turns tools into habits through micro-learning, visible champions, and weekly 30-minute governance rituals. Alignment theory anticipates this: fit arises when structures and behaviours match strategic intent and context (Henderson & Venkatraman, 1993; Coltman et al., 2015). The study's attenuation of TMI's direct path and the superiority of DML are precisely what would be expected if TMI's value is conditional—an amplifier rather than a substitute—for DI (Kane et al., 2015; Vial, 2019). In complexity terms, DBS/DR/HCD are the couplers that synchronise signals (from DM), moves (through AAI), and buffers (via GD) so that resilience emerges from the system rather than from any single excellence (Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021).

Synthesis

Taken together, the evidence suggests that leadership is most effective when it has a tangible focus: a minimal payload of clean data, straightforward automation, and dependable infrastructure. Once that threshold is met, TMI's routines bind and magnify those assets into planning discipline and adaptive capacity. Hence, the observed ordering—DML > DI > TMI—and the managerial corollary for faith-based microenterprises: build the payload first, then couple it with practice (Kane et al., 2015; Verhoef et al., 2021; Vial, 2019; McManus et al., 2008; Hillmann & Guenther, 2021).

What SDMR Adds for Christian Leaders

- **Complementarity**: Digital payload + transformation routines yield the strongest resilience signal.
- **Threshold**: A minimum viable digital base is needed before leadership rituals pay off.
- **Staging**: Sequence payload → governance, not the reverse; keep two–three bets per quarter.
- **Pastoral stewardship**: Treat adoption as technical **and** pastoral—govern data, include the least connected, and practice continuity.

The Leadership Model: TMI as Amplifier of DI

Threshold logic: leadership pays off after a minimal digital base exists.

The study's pattern—DML > DI > TMI—implies a threshold: until a ministry achieves a minimal digital payload, leadership intensity has little to amplify. This threshold is practical, not mystical. It consists of three conditions. First, decision-ready data exists because ownership is assigned, canonical lists are defined, and quality rules are enforced. Second, at least one low-code automation runs end-to-end on a high-friction workflow, reducing handoffs and trapping routine errors at source. Third, reliability basics are in place: working backups, role-based access, and power/cloud safeguards. Below this threshold, strategy workshops, change campaigns, and governance committees can only stir aspiration. They cannot produce resilience because there is nothing operational to align, routinise, or scale (Henderson & Venkatraman, 1993; Kane, Palmer, Phillips, Kiron, & Buckley, 2015; Vial, 2019).

This logic is consistent with the Resource-Based View and the concept of dynamic capabilities. RBV argues that advantage flows from governed, hard-to-imitate assets embedded in processes—precisely what clean datasets, instrumented workflows, and reliable infrastructures become inside small organisations (Barney, 1991; Wade & Hulland, 2004).

Dynamic capabilities theory adds that sensing and seizing require signal quality and executable routines; leadership cannot reconfigure what does not yet exist in usable form (Eisenhardt & Martin, 2000; Teece, 2007). Resilience research follows a similar sequence: early detection, coordinated response, and buffers precede adaptive renewal; exhortation alone does not deliver situation awareness or elasticity (McManus, Seville, Vargo, & Brunsdon, 2008; Hillmann & Guenther, 2021; Weick & Sutcliffe, 2015). In faith-based microenterprises and ministry-run businesses—settings characterised by high volunteer turnover, limited cash reserves, and uneven connectivity—the threshold is even more pronounced, as every routine must carry a disproportionate burden (GSMA, 2023; Verhoef et al., 2021).

Staging principle: sequence payload → governance, not the reverse.

The correct sequence follows a simple rule: build the payload first, then bind it with governance. Reversing the order—starting with policy frameworks, culture campaigns, and performance dashboards—creates the appearance of movement without traction. The payload phase focuses on three moves. The first step is Data Management: appoint a data steward, enumerate the core objects (people, partners, donations, programs, and assets), consolidate them into canonical lists, define quality checks at capture, and publish a one-page data map. The second is Automation & Intelligence: select one workflow with tangible friction (intake, volunteer rostering, outreach, procurement) and implement a low-code automation to eliminate rework and reduce cycle time. The third is Green Digitisation: stabilise reliability with tested backups, minimal monitoring, basic power protection, or a cloud shift, and simple cost controls. These moves deliver the minimum viable DI.

Only then does Transformation Management Intensity earn its keep. With a payload in place, Digital Business Strategy can prioritise a narrow portfolio of use cases that ride on the newly governed data and automated steps; Digital Readiness can institutionalise

cyber hygiene and continuity routines so that added complexity does not erode reliability; Human-Centric Digitisation can convert tools into habits through micro-learning, champions, and lightweight rituals. Alignment theory predicts this order: performance effects emerge when structures fit both strategy and the available technological base (Henderson & Venkatraman, 1993; Coltman, Tallon, Sharma, & Queiroz, 2015). Complexity perspectives add a caution: introducing governance without payload increases coupling without capacity, making systems more brittle. Sequencing the payload → governance reduces brittleness by allowing information flows, operational routines, and buffers to mature together (Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021). The empirical result—Model 3 outperforming Model 2—demonstrates the practical payoff of this order (Kane et al., 2015; Vial, 2019).

Roles and rituals: how to make TMI amplify DI.

Digital Business Strategy (DBS): quarter-by-quarter portfolio choices tied to mission metrics.

DBS translates vision into narrow, timed bets that ride atop the existing payload. Leaders commit to two or three use cases per quarter, not a dozen. Each use case is linked to a mission-relevant metric—for a media ministry, verified contactability and time-to-publish; for a health outreach, appointment adherence and referral turnaround; for a school, fee reconciliation and parent engagement. The portfolio is reviewed monthly and pruned quarterly. DBS thereby constrains distraction, concentrates scarce talent, and channels DI into visible outcomes (Kane et al., 2015; Verhoef et al., 2021). In RBV terms, DBS selects where to deploy the organisation's few VRIN-like digital assets to achieve maximum resilience. In dynamic-capability terms, DBS is the seizing routine that turns improved signals into focused action (Eisenhardt & Martin, 2000; Teece, 2007).

Digital Readiness (DR): a baseline of cyber hygiene and continuity drills.

DR reduces keystone vulnerabilities so that new digital capacity does not exacerbate fragility. Four non-negotiables define the baseline—first, multi-factor authentication for admin and finance roles. Second, test backups with at least one offline or logically isolated copy. Third, role-based access that respects the principle of least privilege and removes access upon exit. Fourth, continuity drills twice a year: a restore test and a failover or manual-mode test. These are light, scripted exercises that surface weak links and train muscle memory. In Kenya, adherence to the Data Protection Act (2019) principles—lawfulness, purpose limitation, data minimisation, integrity and confidentiality—should be woven into DR practice and policy templates (Kenya National Assembly, 2019). DR complements Green Digitisation by ensuring that reliability is not only engineered but practised. From a resilience lens, DR expands buffers and prevents minor faults from cascading, thereby strengthening continuity during shocks (Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021).

Human-Centric Digitisation (HCD): micro-learning, champions, and 30–60–90 adoption check-ins.

HCD converts tools into habits. Three routines anchor this. First, micro-learning: 10–15 minute modules aligned to the quarter's use cases, delivered weekly or bi-weekly, with a one-page quick-reference. Second, visible champions: named practitioners in each unit who demo real workflows, not slides; they troubleshoot, model practice, and feed back
improvement needs. Third, 30–60–90 check-ins: Short adoption reviews are conducted at the end of weeks 4, 8, and 12, assessing usage, errors, rework, and satisfaction. Leaders ask four questions: Are the right people using the tool? Are errors declining at source? Is cycle time down? What got in the way? HCD thus aligns incentives, narratives, and peer modelling with the payload. Literature on transformation highlights that adoption rituals and visible wins, rather than generic training alone, are essential for sustaining behavioural change—especially in small, volunteer-reliant settings (Kane et al., 2015; Verhoef et al., 2021; Vial, 2019). In dynamic-capability terms, HCD is a reconfiguring routine that embeds new micro-behaviours and keeps them adaptive (Eisenhardt & Martin, 2000; Teece, 2007).

Bringing the pieces together: coupling as the source of resilience.

When DBS prioritises a few payload-ready use cases, DR hardens them with hygiene and drills, and HCD embeds them through learning and check-ins, TMI amplifies DI. The result is coherent coupling: clean data improve situation awareness; small automations compress cycle time and trap errors; reliability buffers prevent cascades; governance focuses attention; adoption rituals keep usage real. That coupling is what the Model 3 effect captures as DML. The implication for Christian leadership is concrete. First, cross the DI threshold quickly by making three visible moves: name a data steward and publish a one-page data map, automate one end-to-end workflow, and verify backups and access controls. Second, apply TMI to those moves: one-page DBS with two quarterly bets, DR baseline with two drills per year, HCD cadence with champions and 30–60–90 reviews. Third, measure five simple KPIs: record completeness and time-to-insight (situation awareness); cycle time and %
automation-first (elasticity); uptime and mean time to recovery (reliability); active users and micro-learning completion (adoption); and drill cadence and corrective actions closed (continuity). The doctrine is modest, frugal, and repeatable—and it aligns with the evidence that convergence, rather than accumulation, best explains resilience in resource-constrained ministry settings (Kane et al., 2015; Verhoef et al., 2021; Vial, 2019; McManus et al., 2008; Hillmann & Guenther, 2021).

Stewardship, Inclusion, and Ethics in Practice

Faith and Systems Logic: A Theology of Digital Stewardship

In Christian leadership, stewardship is not a metaphor—it is an operating doctrine. Data are not merely records; they are a trust that protects the people served. Processes are not bureaucratic hurdles; they are acts of care that make service reliable. This framing aligns with servant leadership—encompassing listening, foresight, persuasion, commitment to growth, and building community—traits that directly translate into DI and TMI routines (Greenleaf, 1977; Spears, 2010). Stewardship literature in Christian leadership further emphasises wise, transparent, mission-aligned use of resources (Banks & Ledbetter, 2004). Read through this lens, DI becomes care of decisions—clean data, simple automation, dependable infrastructure—while TMI becomes care of people and practices—clear roles, micro-learning, ethical governance. The purpose is mission continuity, not novelty.

Scripture anchors:

- Nehemiah 3–7: The work advances when the payload (walls built section by section) is matched with governance (gates, watches, records). This pairing models DI (visible progress, registries) bound to TMI (guardrails, routines).
- Acts 6:1–7: Appointing deacons adds process capacity so mission focus is preserved.
  Leadership stages governance after the payload (gospel growth) demands it—a template for sequencing DI → TMI.
- Proverbs 11:14; Romans 12:6–8: Counsel, diverse gifts, and sober judgment frame data-informed decisions as communal stewardship, not technocracy.

Spiritual Resources as Moderators of Resilience

Resilience in faith communities is also spiritually resourced—through calling, hope, and communal trust. Contemporary overviews of spirituality and resilience note that spiritual meaning-making strengthens persistence, coherence, and recovery during disruption (Spirituality and resilience, 2022). For micro-ministries, such resources do not replace DI/TMI; they moderate how well DI/TMI convert into durable routines. Practically, leaders can name and cultivate these resources by beginning board meetings with a brief narrative of calling linked to one operational KPI, ending weekly stand-ups with gratitude tied to a real process improvement, and inviting testimony on how the care of data (e.g., accurate contact lists) tangibly serves people. This is theological alignment, not ornament—an integrative practice that binds technical change to shared identity and hope.

Taken together, scripture-anchored stewardship and spiritual resources provide the moral energy that sustains DI and TMI routines when budgets are thin and time is scarce. They also guard against the leadership illusion—committees without payload—by insisting that worshipful intent show up in governed data, simple automation, and reliable service. The next section's 12-month plan turns these convictions into roles, rituals, and KPIs that leaders can execute in ordinary weeks.

The 12-Month Operating Plan

This plan sequences payload → governance so leadership effort amplifies a real digital base. It moves in four 90-day sprints, each with concrete deliverables, lightweight rituals, and a compact KPI set that tracks situation awareness, elasticity, reliability, adoption, and continuity. The cadence is grounded in evidence that convergence (DML) outperforms single-stream maturity and that routines must couple governed data, simple automation, and green/reliable infrastructure with strategy focus, cyber hygiene, and human-centric adoption (Kane, Palmer, Phillips, Kiron, & Buckley, 2015; Verhoef et al., 2021; Vial, 2019; Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021).

Quarter 1 (Foundations): Establish the minimum viable DI.

DM (six-week data inventory). Appoint a **data steward** and publish a one-page data map: core entities (people, partners, programs, assets), systems of record, and hand-offs.

Consolidate canonical lists (e.g., contacts, volunteers, donors) and set three quality rules at capture (e.g., phone format, duplicate check, consent flag). Document ownership and update rhythm. Clean, decision-ready data raises situation awareness, the precursor to timely coordination under stress (McManus, Seville, Vargo, & Brunsdon, 2008; Lee, Vargo, & Seville, 2013).

AAI (one low-code automation). Select the **highest-friction workflow** (intake, rostering, outreach, or procurement). Implement a low-code flow that de-duplicates records, enforces validations, timestamps steps, and triggers handoffs. Even modest automation compresses cycle time and identifies routine errors at their source, freeing scarce human attention for non-routine work (Kane et al., 2015; Verhoef et al., 2021).

GD (basic reliability). Test backups and document a simple restore procedure. Introduce surge protection/UPS where power is unstable. Shift fragile file storage to a low-cost cloud tier. Set up basic uptime pings. Reliability buffers prevent minor faults from cascading, a known driver of resilience in tightly coupled systems (Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021).

DBS/DR/HCD (governance starter). Leadership **commits** to two Q1 use cases that ride on the new data and automation. Open a one-page risk register (top five vulnerabilities; owner; mitigation). Hold a 30-minute weekly stand-up (data steward, ops lead, one ministry lead) with a three-question script: What changed in the data? What failed in the workflow? What is the next fix? Launch one micro-learning module (10–15 minutes) to introduce the new workflow. These rituals focus effort and begin to routinise adoption (Vial, 2019).

Quarter 2 (Elasticity): turn awareness into speed and safe execution.

AAI (extend to two workflows). Add two automations adjacent to Q1 (e.g., follow-up scheduling; receipting). Build a basic dashboard that displays timeliness, error flags, and bottlenecks; leaders review it every week. This makes elasticity visible and coachable (Eisenhardt & Martin, 2000; Teece, 2007).

DR (enforce minimum cyber hygiene). Enable **multi-factor authentication** (at least for admin/finance roles); implement role-based access; conduct continuity drill #1 (tabletop plus one real restore). Kenya's Data Protection Act principles—lawfulness, purpose limitation, minimisation, integrity/confidentiality—should be embedded in policies and forms during this quarter (Kenya National Assembly, 2019).

HCD (adoption rituals). Run **peer demos** during regular staff meetings so champions can show real tasks, not just slides. Publicly recognise champions (simple certificates; testimony moments). Repeat microlearning for new flows and hold 30–60–90-day check-ins on adoption (use, errors, rework—not just satisfaction). Adoption rituals convert tools into habits (Kane et al., 2015; Verhoef et al., 2021).

DBS (portfolio discipline). Review Q1 commitments; keep at most three active bets; kill or pause distractors. Portfolio pruning concentrates scarce capacity—a prerequisite for durable gains in small organisations (Vial, 2019).

Quarter 3 (Scale & Reliability): harden what now works; cut waste.

GD (green/cloud rationalisation). Retire ageing devices/servers that create hidden failures; shift to cloud services where cost and reliability dominate; enable basic log monitoring (alert on failed logins, backup errors). Reliability and legitimacy rise with consistent service, which sustains donor and community trust during shocks (Vargo & Seville, 2011; Hillmann & Guenther, 2021).

DR (continuity drill #2 & policy refresh). Run a failover or manual-mode drill for one week's operations (e.g., WhatsApp-first backup for field work, paper fallback for cash receipts) and close corrective actions within 30 days. Refresh privacy notices, retention schedules, and consent flows; embed **privacy-by-design** in forms.

DBS (focus on two "resilience KPIs"). Narrow Q4 aims to two key KPIs that matter for mission continuity in your domain (e.g., time-to-contact for media outreach, appointment adherence for healthcare, and fee reconciliation for schools). This aligns effort to measurable resilience outcomes (Kane et al., 2015).

HCD (institutional learning). Convert the best peer demos into 3–to 5-minute clips and publish a one-page playbook for each workflow. Micro-learning libraries sustain capability despite volunteer churn and skill gaps (GSMA, 2023).

Quarter 4 (Institutionalise): lock governance and handover to steady state.

Governance (embed cadence). Establish a quarterly data review (quality trends, ownership changes); formalise an annual continuity test (restore + manual mode); and document succession for digital roles (who covers the data steward and automation admin). Publish a board reporting cadence (two-page dashboard each quarter).

DBS (annual portfolio roll-over). Close the year with a portfolio harvest: what worked, what to retire, and two bets for the following year. Link each to the two resilience KPIs.

DR/HCD (institutional metrics). Fix three DR non-conformities identified in the year (e.g., offboarding lag, stale backups, shadow IT) and maintain the 30–60–90 adoption rhythm for any new tool. Leadership continuity of attention is a key determinant of sustained transformation (Kane et al., 2015; Verhoef et al., 2021).

Two archetype tracks (woven across all quarters).

Micro/volunteer ministry (≤5 staff). Keep governance ultra-light: one page per artefact (data map, risk register, playbooks), one automation in Q1 and at most one new per quarter, and utilise shared services wherever possible (email, storage, forms, messaging). Choose tools with offline modes and low-bandwidth support to accommodate connectivity realities (GSMA, 2023). Emphasise champions over formal training; rotate roles to guard against single-point dependence.

Ministry-run business. Deploy a stronger DR stack early: fine-grained access controls, basic audit trails, and vendor SLAs; add a cost-to-serve dashboard (e.g., cost per order/contact/visit) to inform green/cloud choices; formalise change management for any workflow touching payments or personal data. This track treats reliability and compliance as part of market legitimacy (Weick & Sutcliffe, 2015; Kenya National Assembly, 2019).

KPI set (a few, memorable) with target bands you can tune.

Situation awareness. (i) **% records complete** on canonical lists (target: +20–30 pp from baseline in 90 days); (ii) **time-to-insight** for a standard decision (e.g., "How many active contacts by region?" target: <24 hours by Q2). Situation awareness underpins early detection and coordinated response (McManus et al., 2008; Lee et al., 2013).

Elasticity. (i) **Cycle time** for the core automated workflow (target: −30–50% by Q2); (ii) **% automation-first runs** where the standardised flow is used end-to-end (target: >70% by Q3). Elastic routines support rapid reconfiguration (Eisenhardt & Martin, 2000; Teece, 2007).

Reliability. (i) **% uptime** of key systems (target: >99% after Q3 cloud/UPS moves); (ii) **mean time to recover** from a routine incident (target: <4 hours by Q4) plus **verified backup restores** quarterly. Reliability prevents minor faults from cascading (Weick & Sutcliffe, 2015).

Adoption. (i) **% staff completing micro-learning** per quarter (target: >85%); (ii) **weekly active users** of the key tool (target: trend up and stabilise after Q2). Adoption rituals sustain behaviour change (Kane et al., 2015; Verhoef et al., 2021).

Continuity. (i) **Drill cadence** completed (two per year, with findings logged); (ii) **corrective actions closed** within 30 days (target: 100% closure). Continuity practice converts plans into readiness (Hillmann & Guenther, 2021; Weick & Sutcliffe, 2015).

Operational notes and guardrails.

1. **Time-boxing beats ambition.** Limit changes to two or three bets per quarter; prune ruthlessly at monthly reviews (Vial, 2019).
2. **Privacy-by-design.** Minimise the collection of personal data, record consent, and publish a plain-language privacy notice; this approach is both an ethical stewardship and a legal compliance requirement (Kenya National Assembly, 2019).
3. **Green choices as reliability.** Prefer cloud over ageing hardware; consolidate vendors; monitor basic energy and bandwidth costs. This stabilises uptime and budgets—key to nonprofit legitimacy (Vargo & Seville, 2011; Verhoef et al., 2021).
4. **Measure the few that matter.** Use the KPI set to steer, not to perform for optics. The aim is **mission continuity**, not dashboards for their own sake (Hillmann & Guenther, 2021).

By the end of twelve months, ministries following this plan will have crossed the DI threshold (clean data + two to four automations + basic reliability), bound it with TMI (focused bets, cyber hygiene, adoption rituals), and institutionalised a cadence that can survive leadership turnover and funding volatility. This is the ground on which organisational resilience—planning discipline plus adaptive capacity—emerges in resource-constrained, faith-based settings (Kane et al., 2015; Verhoef et al., 2021; Vial, 2019; Weick & Sutcliffe, 2015).

Lessons for Boards, Pastors, and CEOs

For Boards: approve the 12-month plan, assign data ownership, and govern by five KPIs. Board stewardship begins with authorising a sequenced 12-month plan that builds a minimum viable digital payload—clean canonical data, one or two low-code automations, and reliability basics—before layering transformation routines. This is the least risky way to create the conditions under which leadership intensity amplifies rather than substitutes for digital capacity (Kane, Palmer, Phillips, Kiron, & Buckley, 2015; Vial, 2019). Each board should name a data steward (a role, not just a person), approve a one-page data map (including what data, where it is located, who owns it, and how quality is maintained), and require quarterly confirmation that ownership and quality rules are intact. Oversight should focus on five material KPIs rather than vanity metrics: *(1) situation awareness*—% records complete and time-to-insight for a standard decision; *(2) elasticity*—cycle time of one core workflow and % automation-first runs; *(3) reliability*—% uptime and mean time to recover with verified backup restores; *(4) adoption*—% staff completing micro-learning and weekly active users of the key tool; and *(5) continuity*—drill cadence and corrective actions closed. These indicators align with resilience research emphasising shared information, routinised coordination, and buffers (McManus, Seville, Vargo, & Brunsdon, 2008; Hillmann & Guenther, 2021; Weick & Sutcliffe, 2015). Boards should also ensure that Kenya's Data Protection Act principles—lawfulness, minimisation, and integrity/confidentiality—are reflected in policy and practice, treating privacy-by-design as part of their fiduciary duty (Kenya National Assembly, 2019).

For Pastors and CEOs: model micro-learning, protect focus, and schedule continuity drills.

Senior leaders set the tone for human-centric digitisation (HCD). Modelling micro-learning—short, frequent practice tied to real workflows—signals that adoption is not optional and that learning is continuous. Protecting focus means saying no to tool sprawl and concentrating effort on two or three quarterly bets that ride atop the existing payload; diffusion across many pilots erodes scarce capacity and undermines visible wins (Kane et al., 2015; Verhoef et al., 2021). Leaders should institutionalise continuity drills twice a year: a restore test and a failover or manual-mode exercise, followed by the rapid closure of corrective actions. These rituals reduce brittleness, surface hidden couplings, and build the muscle memory that high-reliability organisations rely on under pressure (Weick & Sutcliffe, 2015). From a capabilities perspective, this is classic sensing–seizing–reconfiguring: leveraging better signals from governed data, executing tasks quickly and safely through simple automation, and periodically reconfiguring processes that have become cemented through practice (Eisenhardt & Martin, 2000; Teece, 2007). The leadership contribution is not inspirational rhetoric but attention discipline—shielding the plan from distraction, and ensuring that portfolio choices, cyber hygiene, and adoption rituals remain synchronised.

For Operations Leads: keep the weekly ritual and publish a one-page dashboard. Operational leaders convert intent into repeatable routines. The anchor is a 30-minute weekly stand-up attended by the data steward, one ministry lead, and the automation owner. The script is simple: *What changed in the data? What failed in the workflow? What is the next fix?* This cadence enacts the principle that improvement is continuous and small; it prevents issues from ageing into incidents and keeps DI and TMI coherently coupled (Vial, 2019). A single-page dashboard should be updated before the meeting, reporting just the five KPIs with short narratives on anomalies and actions taken. As automations extend to adjacent workflows, operations leads should guard against over-engineering; low-code patterns, tested backups, role-based access, and basic log monitoring usually deliver the best resilience-per-shilling in small organisations (Verhoef et al., 2021; Weick & Sutcliffe, 2015). Where ministries run revenue-linked services, add a simple cost-to-serve panel (e.g., cost per contact/order/visit) to inform green/cloud rationalisation and vendor SLAs.

Finally, codify the best peer demos into 3–5 minute clips and a one-page playbook per workflow—an inclusion move that counteracts volunteer churn and uneven digital skills, expanding reliable participation (GSMA, 2023; Hillmann & Guenther, 2021).

Bottom line

Boards authorise and measure what matters; pastors and CEOs guard focus and practice; operations leads institutionalise the weekly ritual and make results visible. When these roles stay in sync, TMI amplifies DI, and resilience emerges from coherent coupling rather than isolated excellence (Kane et al., 2015; Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021).

Boundary Conditions, Thresholds & Transferability

Transferability: Where This Travels—and Where It Doesn't

The operating doctrine here—lead with payload; bind it with governance—transfers best to micro and small ministries with volunteer reliance, modest budgets, and episodic workloads (e.g., media, education, health outreach, community services). In such contexts, the DI threshold (managed data, one to two automations that actually run, basic reliability) creates the foundation upon which TMI (clear roles, microlearning, cyber hygiene, simple portfolio choices) can amplify outcomes. These conditions are not uniquely Adventist; they recur across small Christian nonprofits and church-adjacent social enterprises where staff time is thin and energy must be stewarded.

The framework is also adaptable for mid-sized faith organisations and ministry-run businesses—provided leaders establish governance that aligns with the real payload and avoid tool sprawl. Where cash flow is steadier and staff roles are clearer, the threshold can be crossed faster; the same sequence holds. In large NGOs (e.g., denominational agencies,
faith-based implementers), the logic scales through shared services (data platforms, identity/access management), lightweight standards, and board-level KPI oversight that keeps attention on reliability, inclusion, and continuity rather than vanity metrics (Banks & Ledbetter, 2004; Weick & Sutcliffe, 2015).

There are contexts where the model should be applied with caution. First, ministries operating in highly fragmented digital environments (characterised by unstable connectivity and insecure storage) may need to prioritise foundational reliability (such as paper trails, offline backups, and human redundancies) before attempting automation. Second, cultures with very high autonomy or low process tolerance can experience governance drag, characterised by committees without a clear purpose or direction. In such settings, leaders should scale adoption rituals and microlearning only after one or two visible automations have succeeded. Third, when external compliance burdens are heavy (e.g., strict data protection coupled with low tech literacy), leaders should treat data stewardship as a discipleship practice—emphasising small wins, explicit consent, and a narrow purpose—before advancing analytics.

How to test beyond the Kenyan SDA field. The SDMR routines are exportable by analogy: begin with a DI threshold diagnostic, run a 12-month plan with two automations, one reliability safeguard, and basic cyber hygiene, and track five KPIs (awareness, elasticity, reliability, adoption, and continuity). For replication pilots, we recommend (a) one
non-Adventist evangelical network with similar volunteer structures, and (b) one large Christian NGO unit for a shared-services test. Success is evidenced by shorter cycle times, cleaner contact data, and verified recovery drills, not by tool counts.

Bottom line. The doctrine generalises where energy is scarce and the mission is steady. It travels on sequence and stewardship, not brand-name tools. Where conditions deviate, leaders can still apply the spirit of the model—stage the payload, then bind it—while right-sizing the rituals and KPIs for their setting (Banks & Ledbetter, 2004; Weick & Sutcliffe, 2015).

LIMITATIONS AND FUTURE WORK

The evidence advances a leadership doctrine for faith-based micro-enterprises but carries essential limitations. First, in the study, Causality is not claimed. Paths are interpreted as *consistent with theory* rather than as causal effects because the design is cross-sectional; unmeasured third variables and reciprocal dynamics may remain (Shadish, Cook, & Campbell, 2002). Single-informant and common-method risk also apply: organisational constructs were reported by one key respondent per ministry, raising concerns about shared-source inflation despite procedural remedies (assured anonymity, varied anchors, proximal separation) and post hoc diagnostics typical for SEM studies (Podsakoff,
MacKenzie, Lee, & Podsakoff, 2003; Kline, 2016). Sample size and selection create further bounds. With $n = 141$ and several latent constructs, model parsimony was emphasised to maintain parameter-to-sample ratios, with the result that, while fit and reliability were acceptable, minor effects could be underpowered (Kline, 2016; Hair, Black, Babin, & Anderson, 2019). Recruitment used respondent-driven sampling to penetrate a hard-to-reach population; although sensitivity checks (seed/wave covariates, clustered SEs) stabilised inference, hidden network structures could limit representativeness beyond similar ministry networks (Heckathorn, 2002; Salganik & Heckathorn, 2004). Finally, context specificity matters: the legal and infrastructural environment (e.g., Kenya's Data Protection Act; connectivity variability) shapes feasible moves and vendor choices, cautioning against uncritical generalisation.

Future work should be practice-ready and cumulative in nature. First, longitudinal and quasi-experimental designs are necessary to test directionality. E.g., interrupted time-series analyses around staged DI deployments, stepped-wedge designs across ministry cohorts, or

panel SEM to examine lagged DI→DML→OR pathways (Shadish et al., 2002; Kline, 2016). Second, move beyond self-reporting by incorporating objective resilience outcomes, such as verified uptime, mean time to recovery, cycle-time telemetry from automated workflows, consent/retention audit logs, and drill completion with corrective-action closure. Third, undertake cross-denominational and cross-country pilots to test transferability under different governance and regulatory regimes, with explicit measurement invariance checks for DI/TMI/OR scales (Hair et al., 2019). Fourth, embed a mixed-methods process tracing approach—utilising leader diaries, observation of weekly rituals, and qualitative incident reviews—to explain *how* HCD routines convert payloads into durable habits. Finally, examine moderators salient to faith-based nonprofits—funding model, volunteer intensity, and ecosystem partnerships—to map where leadership amplification is strongest and where additional buffering (e.g., shared services) is necessary.

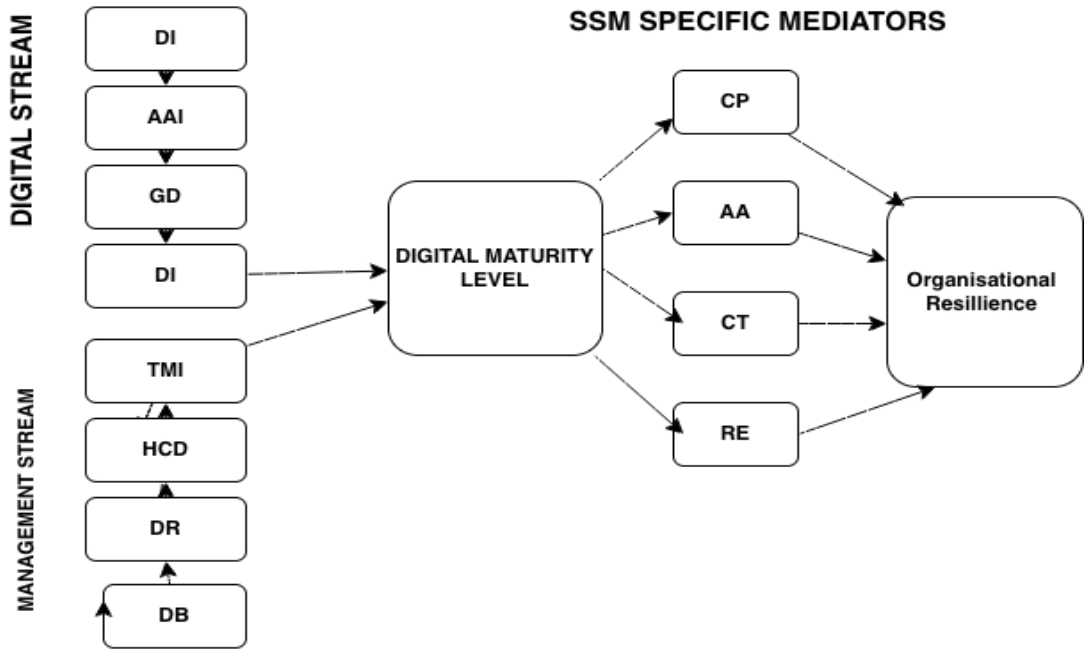
CONCLUSION: Lead with Payload

The central lesson is straightforward: leadership amplifies a real digital base; it does not substitute for it. Across Kenyan SDA self-supporting ministries, the strongest association with resilience emerged when digital intensity—encompassing governed data, simple automations, and reliable "green" infrastructure—was combined with transformation disciplines—focused portfolios, cyber hygiene, and human-centric adoption. That convergence (DML) outperformed either stream alone, clarifying why strategy retreats and culture campaigns under-deliver when the informational and operational substrate is thin. Resilience in these settings depends on situation awareness, elasticity, and reliability; those qualities arise from coherent coupling, not isolated excellence.

The call to action is pragmatic and time-boxed: adopt a frugal, sequenced playbook that is executable within 12 months. In the first quarter, establish the minimum viable payload by assigning data ownership, creating canonical lists with quality rules, automating one

high-friction workflow, and hardening basic reliability (backups, MFA, UPS/cloud). In the second, extend automation to adjacent steps, enforce cyber hygiene, and run the first continuity drill. In the third, rationalise toward the cloud, monitor logs, and prune distractions to focus on two resilience KPIs. In the fourth, institutionalise cadence: quarterly data reviews, annual continuity tests, clear role succession, and board reporting. Track five simple KPIs—situation awareness, elasticity, reliability, adoption, and continuity—to steer the work and make gains visible. Executed in this order, transformation management becomes the amplifier it is theoretically meant to be, converting a modest digital payload into durable organisational resilience and, ultimately, mission continuity under volatile conditions.

The Proposed SDMR Framework For Digital Maturity And Organisational Resilience In SSMs



Note. DML-Digital maturity level; TMI-transformation management intensity; DBS-digital business strategy; DR-digital readiness; HCD-human-centric digitization; DI-digital intensity; DM-data management; AAI-automation and intelligence; GD-green digitization; OR-organizational resilience; AC-adaptive capacity; P-planning; RE-Resource elasticity; CT-Community Trust; AA-Adaptive Agility; CP-Continuity Planning

Note. The arrows illustrate hypothesised relationships from digital and management capabilities through DML to resilience mediators—continuity, agility, trust, and resource elasticity—culminating in Organisational Resilience.

REFERENCES

1. American Association for Public Opinion Research. (2023). Standard definitions: Final dispositions of case codes and outcome rates for surveys (10th ed.). AAPOR. https://aapor.org
2. Banks, R., & Ledbetter, B. M. (2004). Reviewing leadership: A Christian evaluation of current approaches. Baker Academic.
3. Barney, J. B. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120.
4. Beaton, D. E., Bombardier, C., Guillemin, F., & Ferraz, M. B. (2000). Guidelines for the process of cross-cultural adaptation of self-report measures. Spine, 25(24), 3186–3191.
5. Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. MIS Quarterly, 36(4), 811–840.
6. Bollen, K. A., & Stine, R. (1992). Bootstrapping goodness-of-fit measures in structural equation models. Sociological Methods & Research, 21(2), 205–229.
7. Brown, T. A. (2015). Confirmatory factor analysis for applied research (2nd ed.). Guilford Press.
8. Coltman, T., Tallon, P. P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. Journal of Information Technology, 30(2), 91–100.
9. Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys: The tailored design method (4th ed.). Wiley.
10. Duchek, S. (2020). Organisational resilience: A capability-based conceptualisation. Business Research, 13, 215–246.
11. Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? Strategic Management Journal, 21(10–11), 1105–1121.
12. Flora, D. B., & Curran, P. J. (2004). An empirical evaluation of alternative methods of estimation for confirmatory factor analysis with ordinal data. Psychological Methods, 9(4), 466–491.
13. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50.
14. GSMA. (2023). The State of Mobile Internet Connectivity 2023. GSMA Association.
15. Greenleaf, R. K. (1977). Servant leadership: A journey into the nature of legitimate power and greatness. Paulist Press.
16. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage.
17. Heckathorn, D. D. (2002). Respondent-driven sampling II: Deriving valid population estimates from chain-referral samples of hidden populations. Social Problems, 49(1), 11–34.
18. Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging IT for transforming organisations. IBM Systems Journal, 32(1), 4–16.
19. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modelling. Journal of the Academy of Marketing Science, 43(1), 115–135.
20. Hillmann, J., & Guenther, E. (2021). Organisational resilience: A valuable construct for management research? International Journal of Management Reviews, 23(1), 7–44.
21. Hu, L.-T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modelling, 6(1), 1–55.
22. Iacobucci, D. (2010). Structural equations modelling: Fit indices, sample size, and advanced topics. Journal of Consumer Psychology, 20(1), 90–98.
23. International Test Commission. (2018). The ITC guidelines for translating and adapting tests (2nd ed.). https://www.intestcom.org
24. Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. MIT Sloan Management Review and Deloitte.
25. Kenya National Assembly. (2019). The Data Protection Act, No. 24 of 2019. Government Printer.
26. Kline, R. B. (2016). Principles and practice of structural equation modelling (4th ed.). Guilford Press.
27. Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organisations' resilience. Natural Hazards Review, 14(1), 29–41.
28. Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organisational resilience through strategic human resource management. Human Resource Management Review, 21(3), 243–255.
29. Li, C.-H. (2016). Confirmatory factor analysis with ordinal data: Comparing robust maximum likelihood and diagonally weighted least squares. Behaviour Research Methods, 48(3), 936–949.
30. Little, T. D., Rhemtulla, M., Gibson, K., & Schoemann, A. M. (2013). Why the items versus parcels controversy need not be one. Psychological Methods, 18(3), 285–300.
31. MacKinnon, D. P. (2008). Introduction to statistical mediation analysis. Lawrence Erlbaum.
32. McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). A facilitated process for improving organisational resilience

(Resilient Organisations Research Report 2008/01). Resilient Organisations.
33. Office of the Data Protection Commissioner (ODPC). (2024). Official guidance portal for data controllers and processors. https://www.odpc.go.ke
34. Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioural research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903.
35. Rindskopf, D., & Rose, T. (1988). Some Theories and Applications of Confirmatory Second-Order Factor Analysis. Multivariate Behavioural Research, 23(1), 51–67.
36. Salganik, M. J., & Heckathorn, D. D. (2004). Sampling and Estimation in Hidden Populations Using Respondent-Driven Sampling Sociological Methodology, 34(1), 193–240.
37. Satorra, A., & Bentler, P. M. (1994). Corrections to test statistics and standard errors in covariance structure analysis. In A. von Eye & C. Clogg (Eds.), Latent variable analysis: Applications for developmental research (pp. 399–419). Sage.
38. Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). Experimental and quasi-experimental designs for generalised causal inference. Houghton Mifflin.
39. Spears, L. C. (2010). Character and servant leadership: Ten characteristics of effective, caring leaders. The Journal of Virtues and Leadership, 1(1), 25–30.
40. Spirituality and resilience. (2022). Oxford Medicine Online. Oxford University Press. [https://doi.org/10.1093/med/9780198861478.003.0025](https://doi.org/10.1093/med/978019 8861478.003.0025)
41. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319–1350.
42. Tourangeau, R., Rips, L. J., & Rasinski, K. (2000). The psychology of survey response. Cambridge University Press.
43. Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889–901.
44. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144.
45. Vargo, J., & Seville, E. (2011). Crisis strategic planning for SMEs: Finding the silver lining (Resilient Organisations Research Report 2011/01). Resilient Organisations.
46. Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. MIS Quarterly, 28(1), 107–142.
47. Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). Wiley.
48. Wong, P. T. P., & Page, D. (2003). Servant leadership: An opponent-process model and the revised Servant Leadership Profile. Servant Leadership Research Roundtable, Regent University.
49. [http://www.drpaulwong.com/wp-content/uploads/2013/09/Wong-Servant-Leadership-An-Opponent-Process-Model.pdf](http://www.drpaulwong.com/wp-content/uploads/2013/09/Wong- Servant-Leadership-An-Opponent-Process-Model.pdf)

Appendix

Appendix A: Decision matrix: Standard Starting Profiles

Starting Profile	Highest-Leverage (First 90 Days)	Scale & Harden (6–12 months)	SDMR Levers Emphasised	Simple KPIs
Low maturity; ad-hoc spreadsheets	Name stewards; single sources of truth; MFA & weekly backups	Standardise forms; automate bottlenecks; basic dashboards	DM, DR → AAI	Restore test pass rate; workflow cycle time; % decisions with curated data
Data-rich but low adoption	Micro-learning launch; peer champions; prune tools	Opt-out defaults; monthly utilisation; dashboards in reviews	HCD, DBS	Active users/tool; post-training utilization lift; % meetings with dashboards

Tool sprawl; duplicated systems	Portfolio review; freeze new tools; cloud suite consolidation	Integration backbone; shared IDs; scheduled syncs	DBS, AAI/DM	Tool utilization; data latency (hrs); apps retired
Volunteer-reliant micro-ministry	Governance charter; automate reminders/attendance; password manager & MFA	UPS for stations, drills, and mobile-first forms	DM, AAI, DR, GD	Uptime (%); automation success (%); energy cost/beneficiary
SSM (shop/farm/training)	Clean masters; daily reconciliation; automate invoicing/re-order	Dashboard; redundancy (dual connectivity, mirrored backups)	DM, AAI, GD, DR	Days sales outstanding; stockout rate; downtime (min/month)
Connectivity/power instability	Consolidate cloud suite; offline capture; UPS where needed	Device lifecycle; solar/backup; monitor energy/beneficiary	GD, DM	Uptime (%); offline data capture sync; energy cost/beneficiary
High DI, weak TMI	Publish DBS priorities; micro-learning; basic cyber program	Roadmap with guardrails; after-action reviews; quarterly restore tests	DBS, HCD, DR	Training completion; incident response time; % initiatives tied to DBS
High TMI, thin DI	Data inventory; single truth sources; automate the bottleneck	End-to-end automation; minimal integration	DM, AAI	Cycle time (target process); data completeness; integration failures

Accompanying Note: Template Covenants for Board Approval Data Covenant (1 page)

Purpose. This ministry collects only the information needed to care for people and deliver programs well.

What we collect. Contact details, preferred language, program participation, and only the sensitive data strictly required for service delivery.

How we protect it. Access is granted by role, with strong passwords and multi-factor authentication for administrators. Encrypted storage is used where available, and access is reviewed quarterly to ensure compliance with applicable regulations.

Consent and control. Consent is requested in clear language. Individuals can change preferences or withdraw at any time.

Retention. Data are kept only as long as necessary and then safely deleted. **Accountability.** A named data steward reviews quality and privacy practices each quarter and reports to leadership. (Aligned to Kenya's Data Protection Act, 2019.)

Continuity Covenant (1 page)

Purpose. This ministry prepares for disruption so worship, education, service, and care can continue.

Backups and recovery. Backups are tested quarterly; a simple restore guide is documented and rehearsed.

Manual-mode and failover. Twice a year, the ministry practices operating without a core system (e.g., manual rosters, paper receipts) and records the corrective actions taken.

Roles. Named alternates cover critical digital responsibilities (data steward, finance system admin, communications lead).

Review. A concise after-action is shared with the board/pastorate, and actions are closed within 30 days.

These covenants set ethical, feasible, and verifiable expectations. They integrate compliance with Kenya's data-protection principles, advance inclusion through simplicity, and enact green reliability choices that reduce brittleness—all of which align with the leadership doctrine advanced by the evidence: lead with payload, couple with practice, and measure what sustains mission (Kenya National Assembly, 2019; GSMA, 2023; Weick & Sutcliffe, 2015; Hillmann & Guenther, 2021; Verhoef et al., 2021).

Appendix B: Methods Note B1. Sampling & Identification

- Frame: SDA-affiliated SSMs operating legally in Kenya; unit = organisation.

- Access: denominational networks + **respondent-driven sampling** (initial seeds; capped referrals per wave; duplicate checks). (Heckathorn, 2002; Salganik & Heckathorn, 2004)
- Ethics: AUA ISERC approval **AUA/ISERC/14/10/2024**; consent captured online/phone.

B2. Instrument Adaptation & CMB Checks

- Adaptation: expert review → cognitive pretest (think-aloud/probing) → **minor lexical localisation only**; no content changes to constructs. (Beaton et al., 2000; ITC, 2018; Tourangeau et al., 2000)
- CMB: procedural remedies + **single-factor**/marker diagnostics; no dominant common-method factor detected. (Podsakoff et al., 2003)

B3. Estimation & Fit Reporting

- Estimators: **MLR** (primary) with **FIML** for missingness; **WLSMV** (polychorics) as sensitivity. (Flora & Curran, 2004; Li, 2016)
- Fit indices (CFA then SEM): **CFI, TLI, RMSEA (90% CI), SRMR** reported together and judged as a **pattern** rather than by a single cutoff. (Hu & Bentler, 1999; Kline, 2016)
- Small-sample/robustness: Satorra–Bentler corrections; **bootstrap 5,000** for direct/indirect effects. (Satorra & Bentler, 1994; Bollen & Stine, 1992)
- Sensitivities: re-estimate with WLSMV; add seed/wave covariates and cluster-robust SEs; results **do not alter** the rank-ordering of paths (DML > DI > TMI).
- Invariance screen (brief): multi-group checks by **size** and **ministry type** were exploratory; no material instability in the core loadings/paths at the pragmatic thresholds used; complete invariance testing is flagged for future work.

B4. Data Protection & Compliance (1–2 sentences)

- The Kenya **Data Protection Act (2019)** and ODPC guidance are observed, with the following key principles: lawful basis (consent), data minimisation, access & erasure rights, encryption, and role-based access. (Kenya National Assembly, 2019; ODPC, 2024)