Shared Infrastructure for Civil Society Sustainability

A Framework and Resource-Sharing Protocol for Civil Society Organisations

Shared Infrastructure for Civil Society Sustainability

A Framework and Resource-Sharing Protocol for Civil Society Organisations

EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org.

Research and writing
Arul Prakkash
Sinar Project

Editorial and layout
EngageMedia
Amry Al Mursalaat

Confidentiality note

All interviewees and their organisations are anonymised throughout this report and referred to by codes (INT-01 to INT-09). Names, exact organisational identities, sensitive security details and donor-sensitive information have been withheld to protect participants.

Table of Contents

Purpose of this study

EngageMedia commissioned this study to examine how sharing infrastructure can help civil society organisations (CSOs) become more resilient and survive in the long term. Organisations and movements are deeply rooted in the human rights struggle, driven by their commitment to and belief in the cause they champion. Being an activist or running a grassroots group or organisation today is incredibly tough. In Malaysia, most of these groups are run by a handful of core staff members who are highly reliant on fragile, project-based funding and operate under a legacy of systemic containment dating back to the Tun Dr Mahathir era and the 1987 *Operasi Lalang* arrests. Today, this historical pressure continues as authorities frequently weaponise restrictive laws, such as the Communications and Multimedia Act (CMA) and the Sedition Act. Teams constantly work under immense pressure, navigating state surveillance, arbitrary arrests, and strict funding restrictions while carrying the heavy responsibility of protecting the communities they serve. This constant stress makes it harder for groups to stay afloat and causes deep exhaustion for activists and organisations on the ground.

The finding of this report is that keeping our movements alive in this challenging time of regional and global conflict, shrinking civil society space, and funding cuts means that simply finding more resources, especially more money, won't be an adequate solution. Unpredictable funding, growing digital repression, and shifting geopolitical conditions are pushing human rights defenders to look beyond individual survival to collective approaches. True sustainability must be holistic: it affects the well-being of the individual just as much as the organisation's survival. By moving toward this model, human rights groups, digital rights advocates, and independent media can ensure they have the shared systems, services, tools, spaces, relationships, and governance

arrangements they need to survive, respond to threats, protect communities, reduce duplication, care for their people, and build long-term collective power. Ultimately, this research aims to show how sharing our resources reduces the burden on overworked teams, fosters real community care, and builds long-term collective power and sustainability.

Methodology

This research adopted a qualitative methodology to gather core insights. The study involved a thorough review of the research framework and interview guides; a thematic analysis of nine anonymised interviews (INT-01 to INT-09) conducted across six civil society organisations in Klang Valley, Malaysia; and a targeted desk review of existing shared infrastructure models. AI tools were used to help sort and organise the interview data and support the analysis and drafting. However, the researcher read all interviews and sources in full, and the findings, analysis, and conclusions are the researcher's own.

Data collection was conducted from April to June 2026. The participating groups represent six civil society organisations working on human rights, media freedom, digital rights, youth and democratic reform, and LGBTQI advocacy. Most are small to medium organisations (under 20 staff) operating in a Southeast Asian context where civic space is rated "obstructed" (CIVICUS Monitor, 2025). To protect the participants given this challenging environment, the findings were synthesised across the interviews rather than reported organisation by organisation.

Interviews

Nine semi-structured interviews (n=9) were conducted with staff in operational, financial, programme, knowledge-management and senior leadership roles. Interviews lasted roughly 45 to 90 minutes and followed a shared question guide covering daily work and operational pressures; tools, devices, connectivity, and storage; donor-imposed tools; capacity gaps; collaboration and existing sharing; shared-infrastructure needs and feasibility; and risk, digital security, and sustainability.

Several interviews were drawn from the same organisations (two pairs of interviews came from one organisation), which allowed both leadership and operational perspectives to be captured.

Although the participating organisations are themselves small to small-medium and based in the Klang Valley, their reach extends well beyond their size and location. Most work directly with grassroots and marginalised communities, including Indigenous Peoples (Orang Asli communities), refugees, and migrant workers, and maintain partnerships that reach beyond the Klang Valley, including collaboration with partners in East Malaysia. Several of these organisations also carry significant cross-sector experience and are connected to regional human rights, digital rights, and thematic networks that organise around their core advocacies across the region, as well as wider international networks. These connections and partnerships were deliberately considered in the selection, as they allow the findings to speak to realities beyond any single organisation. The sample below describes the organisations in general terms only.

Organisation type	Organisation size	No. of interviews
Human rights (general, documentation, advocacy)	Small–medium (1–20)	3
Media/film/freedom of expression	Small–medium (1-20)	3
Digital rights / civic tech	Small (1–10)	1
LGBTQI advocacy	Small (1–10)	2
TOTAL		**9**

Limitations

This is a qualitative study based on nine interviews and a targeted desk review. It does not include a quantitative survey, cost modelling, a technical security audit, a legal opinion, or a full mapping of all CSOs in the ecosystem. The participating organisations differ in size and digital maturity, offering a range of perspectives rather than a representative cross-section of the sector.

The sample also has clear boundaries. All participants are small to small-medium organisations connected to overlapping trusted networks and coalitions. Some types of groups are not represented at all, including larger organisations, those based outside the Klang Valley grassroots collectives, and groups working outside these networks. Because participants were selected through groups that already work together, the sample may lean toward organisations already inclined to collaborate and share, which is worth keeping in mind when reading findings on trust and willingness to share.

Because confidentiality and safety are central, some details have been intentionally generalised. Where evidence is missing, this report states the limitation rather than filling gaps with assumptions.

Executive Summary

Key findings

- **Operational pressure is a structural problem, not an organisational failure**. Small, overworked teams carry heavy administrative, compliance, security and reporting burdens. Almost no interviewed organisation has dedicated in-house IT, digital security, legal, or monitoring and evaluation capacity; these functions are absorbed ad hoc by whoever is most willing or technically capable, outsourced temporarily, or left unaddressed due to funding and project-cycle pressures. Finding trusted, affordable vendors is itself a cost and capacity problem (INT-01; INT-03; INT-04; INT-08).

- **Informal resource-sharing is strong but fragile**. Most organisations already share peer referrals, ad hoc legal and security advice, training materials, equipment loans (cameras, microphones, speakers, projectors, etc.), meeting space and campaign resources, but the practice is informal, trust-based and vulnerable. The goodwill inside established clusters is deep; its informality limits its reliability (INT-06; INT-08; INT-09).

- **Tool fragmentation is often imposed from the outside**. Organisations run on an overwhelming mix of cloud drives, chat apps, accounting systems, project tools, and personal devices, and much of this is not by choice. For instance, one organisation was required to drop its usual cloud suite and switch entirely to Microsoft's system for a specific partnership, leaving the team to struggle with unfamiliar logins and interfaces (INT-08). Another group had a donor-mandated secure messenger that separated their official communications channel from the apps the staff actually use day-to-day (INT-04). A third organisation was told to use a partner's monitoring tool despite its limited functionality (INT-03). The result of this fragmentation is predictable: files end up scattered across personal laptops, portable drives, and chat apps; accounts stay active long after staff leave; and institutional memory is lost when someone moves on (INT-03; INT-04). Ultimately, every imposed tool adds operational friction and a new security gap rather than building real capacity.

- **Governance, not trust, is the barrier to scaling up.** Trust within clusters is high, but goodwill alone cannot sustain shared infrastructure. The main barrier is the absence of clear governance: who controls a resource, who maintains it, who pays, how data separation is guaranteed, who bears liability, and what happens when an organisation leaves. Trust is also uneven across the wider sector (INT-04; INT-08; INT-03; INT-02).

- **Technical capacity and data risk are decisive barriers.** When one interviewee was asked directly to choose between trust, cost, governance and technical capacity, they pointed to technical capacity, citing the steep learning curve of complex software and a lack of technical interest, noting that staff "just want to focus on their core human rights work" and that even younger team members prefer simple

tools like Canva over heavier programs (INT-08). The same organisation said CSOs "do not have the tech literacy to maintain servers or open-source configurations on their own" and need a dedicated technical administrator to turn to for help (INT-08). Connectivity is a further limitation: even with good office internet, the signal drops in parts of the premises, disrupting calls despite repeated mesh-router upgrades, and online screenings depend on wired connections that public venues increasingly no longer provide (INT-08; INT-09). Data protection risks weigh heavily too. Interviewees wanted any shared system to be encrypted, "partitioned so organisations can only access their respective data," and "safe from physical raids," or hosted offshore where the state "cannot be blocked or wiped out" from accessing it (INT-08; INT-09).

- **Digital security needs are urgent but uneven**. Stronger organisations enforce the use of password managers and virtual private networks (VPNs), run annual training, and hold risk assessments before public events (INT-08; INT-09; INT-03). Some also use hardware security keys and separate email access by role and data sensitivity (INT-02; INT-03). Yet, even these groups describe critical gaps. One organisation admitted its security policies are entirely verbal and not written (INT-09), another noted that training rarely sticks in a small team (INT-08), and a third explained that security rests on one person making manual changes, a process that is highly labour-intensive and prone to error (INT-07).

  The threats facing these groups are concrete and shared. Organisations reported a compromised website, which was eventually mitigated by hosting servers outside the country (INT-03). They also face frequent brute-force login attempts, social engineering, and doxxing, including a severe escalation involving arrests that forced immediate credential changes and the temporary use of burner devices (INT-07). Other

reported incidents include platform failures, sudden data loss, account lockouts, and a total unpreparedness for physical raids due to a severe lack of backups (INT-02). Furthermore, groups deal with office raids, event-time surveillance, and raw-data drives kept unencrypted in a locked desk drawer (INT-08). Because these exact threats recur across the sector, a collective response would raise the safety floor for everyone. Specific details have been generalised to protect participants.

- **The project "cliff edge" is widespread**. Access to tools, services, and qualified staff tends to disappear the moment a project or grant ends. One organisation had funding to hire an external agency to run a campaign, but that funding line was cut after shifts in overseas politics; the campaign stalled before staff could absorb the work back in-house with their own limited capacity (INT-08). For another, a shortage of funds directly cripples operations: essential monitoring software cannot be purchased, and specific initiatives, including legislative-reform work, are forced to stop entirely (INT-02). Recent global aid cuts have deepened this pattern across the sector (OHCHR, 2025).

- **Care and continuity are at risk**. Well-being and overreliance on a few key people are real sustainability threats. A director described sleeplessness driven by the sheer volume of daily tasks, such as scheduling, logistics, and coordination (INT-09). A coordinator described difficulty with sustained attention and constant task-switching, leading to an organisation "living in the breach" where security rests entirely on one person's vigilance (INT-07). Overload also appears structurally: when stretched, staff fall back on small tasks rather than deeper work and feel unproductive as a result (INT-03). In contrast, small teams say their limited capacity forces them to rely on mutual support to keep going (INT-02).

- **The most viable path forward is modular and phased**. The interviews show strong interest in shared infrastructure but also clear concerns about data risk, privacy, technical capacity, and governance. This means that a single shared platform introduced all at once is unlikely to earn trust immediately. A step-by-step approach is more realistic. One organisation identified technical capacity as the primary barrier to implementation, rather than cost or governance alone. The same interview identified three core pillars for infrastructure sharing: shared hosting, legal support, and pooled funding, provided that governance arrangements are clear and robust (INT-03). This phased approach is already reflected in current practice. One organisation said it would use a shared subscription only if its data were kept private and separate from other organisations' data (INT-08). Another viewed reliance on a single shared server as high risk and maintained backup options because of concerns about data leaks, doxxing, and exposure of sensitive information (INT-07). For this reason, shared infrastructure should begin with lower-risk, higher-trust forms of sharing, such as knowledge resources, joint training, digital audits, and pooled services. It can then move into small tool pilots among trusted peers before expanding into shared hosting or shared data systems once access controls, data separation, accountability mechanisms, clear and documented operating procedures, and clear rules for joining, leaving, data export, access removal, and shutdown are in place. (INT-02; INT-03; INT-07; INT-08).

Summary of recommendations

The detailed recommendations are in Section 8. In short, this report does not recommend building one large shared platform first. The strongest and safest path is phased: start with low-risk sharing, move to pooled services and shared tools, and only later develop sensitive infrastructure such as secure hosting, backup, documentation systems, pooled funds, or fiscal hosting, once trust, governance, technical capacity, and funding are in place.

A practical starting package, achievable within six months and with little or no additional funding, could begin with a monthly peer-learning circle and a shared knowledge folder containing templates, compliance notes, and security checklists. Alongside this, a trusted roster of referrals for lawyers, accountants, security responders, and trainers provides organisations with someone to turn to in a crisis. Simple written rules for existing sharing, such as equipment sign-out and cost-splitting, make current practice safer. At the same time, a basic digital-security refresher leaves each organisation with at least one written procedure. Mapping where files, accounts, and backups live then shows the most exposed points so they can be addressed first.

From there, the report identifies shared services as the strongest medium-term opportunity, since the clearest need is not only for more tools but also for people to maintain them. Pooling digital security responders, technical administrators, legal and compliance advisers, and documentation support reduces pressure on small teams and prevents organisational risk from resting on one exhausted person. Throughout, smaller and higher-risk organisations should be protected, and maintenance should be funded from the start rather than treated as an afterthought. The aim is for shared infrastructure to be collectively owned and governed across the civil society network in Malaysia, with coordination among trusted peers rather than concentrated in any single organisation.

1. Introduction and Context

1.1 Background

Civil society organisations are operating in a difficult and uncertain environment. Funding is becoming less predictable, civic space is under pressure, digital threats are growing, and organisations are expected to deliver complex human rights, advocacy, media, documentation, and community support work while also meeting heavy reporting and compliance requirements. Desk research confirms that these pressures are not isolated: CIVICUS reports serious restrictions on civic space in many contexts, an OECD analysis points to declining official development assistance, and Freedom House reports ongoing global pressure on internet freedom and on encrypted or anti-censorship tools.

The interviews show how these macro-level pressures become daily operational strain. Staff described accounting software that does not match donor reporting formats, cloud storage that fills up, personal phones used for work, project information lost in chat apps, staff turnover creating knowledge gaps, and digital security tasks falling to whoever is most technically confident. These are not signs of weak commitment. They are signs that essential infrastructure is being carried by individuals rather than sustainable systems.

For human rights defenders, digital rights group, media organisations, community-based groups, and movement actors, infrastructure is not neutral. It shapes whether sensitive documentation is preserved safely, whether communities can access support, whether campaign materials remain available, whether staff can respond to incidents, and whether small organisations can continue after a grant ends.

1.2 Why shared infrastructure – and why now

Shared infrastructure means pooling the resources, services, tools, spaces, relationships, and governance arrangements that civil society organisations need but cannot always afford, maintain, or safely manage on their own. It encompasses shared knowledge resources, secure communications tools, hosting, open-source technologies, pooled software subscriptions, shared databases, secure backup systems, specialist retainers for digital security, legal support, communications, administration, monitoring and evaluation, fiscal hosting, pooled funding, meeting spaces, coordination bodies, and peer support systems.

The case for shared infrastructure is strongest when organisations face similar pressures but are forced to solve them separately. The interviews show common needs across IT support, digital security, accounting and compliance, communications, monitoring and evaluation, knowledge management, data protection, storage, backup, and subscriptions. They also show that many organisations already share informally through coalitions, trusted personal relationships, equipment loans, referrals, joint campaigns, and peer support. The opportunity is not to build from nothing, but to make these existing practices more intentional, safer, fairer, and more sustainable.

This matters now for three reasons. First, funding uncertainty has made duplication harder to justify. When every organisation pays separately for the same underused tools, hires short-term consultants for similar needs, or absorbs security and compliance risks alone, scarce resources are stretched even further. Second, many threats facing civil society are collective. A website attack, device seizure, data leak, account compromise, or legal pressure on one organisation often reflects a wider pattern across the sector.

Collective defence is therefore more effective than an isolated response. Third, the relationships needed for sharing already exist in parts of the ecosystem. Several interviewees described active clusters, shared equipment, joint campaigns, shared content, and trusted informal support systems. These are foundations that can be strengthened.

Shared infrastructure is especially urgent because short-term project funding often pays for activities but not long-term maintenance. A tool may be purchased for one grant, a consultant hired for one project, or a platform built for one campaign. When the project ends, organisations may lose access, technical support, staff time, or the ability to keep systems updated. Shared infrastructure can reduce duplication and distribute maintenance costs, but only if trust, governance, data protection, access control, and long-term responsibility are built into the design from the start.

2. Findings: Needs and Challenges

2.1 Operational context of interviewed organisations

The interviewed organisations work across human rights, legal reform, civic education, freedom of expression, media documentation, digital rights, civic technology, community advocacy, and social filmmaking. Most operate with very small teams, several running on five or fewer staff. Yet, they carry expectations from donors, communities, partners, boards, and regulators that would stretch a far larger organisation. This is easy to underestimate from the outside. “Small” here does not mean a modest team with a light workload, but rather a handful of people holding an entire organisation together on project-based funding.

Crucially, the reach of these organisations extends well beyond their headcount. Many anchor or sit within active coalitions and must coordinate far more partners than they employ staff. One freedom-of-expression cluster links around 11 partner organisations in close, day-to-day collaboration, and some organisations coordinate wider networks of partners. Sinar Project, for example, works with roughly 20 partners, and some organisations interviewed had networks of 40 or more. A team of five may therefore be the coordination point for dozens of other groups, managing communications, scheduling meetings, coordinating shared campaigns, handling documentation, and coordinating joint responses across them. The operational and relational load scales with network size, not team size, and this gap between headcount and responsibility is at the heart of the burden.

The day-to-day picture is one of heavy operational load. Finance and administration staff spend time converting data between accounting systems and donor reporting formats. Programme staff manage events, community support, legal or advocacy work, and monitoring. Media organisations manage large volumes of video and archive material. Digital rights and civic technology groups manage platforms and documentation while also facing dependence on a small number of technical people. Across the sample, operational sustainability depends on informal workarounds, personal knowledge, trusted relationships, and staff willingness to stretch beyond formal job descriptions.

2.2 Capacity gaps: what CSOs are missing

2.2.1 Technical and IT capacity

Finding: Most organisations lack dedicated, routine IT capacity. Technical support is often handled by a staff member who happens to be more confident with technology, by an external consultant, or by a vendor only when something breaks.

Interview evidence shows repeated reliance on ad hoc support. INT-01 described no internal IT department and reliance on an internet service provider or external consultants for specific problems. INT-03 described self-managed IT workarounds, a customised ERP system that creates friction, and outsourced website support. INT-04 described the loss of a former IT role that had handled laptop audits and security tools. INT-08 described technical equipment, hard drives, and data management falling to the most technically inclined staff member. INT-05 described technical capacity concentrated in a small number of people.

Variation: Organisations with greater digital maturity are not free of capacity problems; rather, their risks become more complex. A civic technology organisation may have servers, VMs, coding tools, and documentation workflows, but still face key-person dependency and limited dedicated support. Smaller non-technical organisations face more basic problems such as device maintenance, troubleshooting, cloud storage, and software updates.

Why it matters for shared infrastructure: Shared IT support, pooled technical resources, shared help desks, and shared documentation can reduce dependence on individual staff members. However, shared technical support must be designed with clear prioritisation rules, confidentiality safeguards, and escalation pathways, especially for higher-risk organisations.

2.2.2 Digital security capacity

Finding: Digital security awareness exists, but capacity is uneven and often reactive. Some organisations have policies, onboarding training, password managers, hardware keys, VPNs, risk assessments, or access to external trainers. Others have only partial policies, one-off workshops, informal practices, or no dedicated security owner.

INT-02 described digital security as a major source of frustration, including platform failures, data loss, website access problems, lost login access, and weak backup arrangements. INT-03 reported a previous website compromise and described several security measures already in place, including security policies, staff onboarding training, annual security training, and server hosting outside the organisation's primary operating context. INT-04 described phishing attempts, unauthorised login attempts, risks on partner websites, and security tools that were no longer

reviewed regularly. INT-06 and INT-07 described operating in high-risk environments where public visibility brings digital targeting, login attacks, doxxing concerns, and strict limits on what data can be shared. INT-09 described risk assessments, password and VPN training, and quick access to digital rights expertise through a trusted coalition. INT-01 and INT-05 further show that some organisations rely on basic policies, ad hoc external consultants, or one-off workshops rather than sustained internal security capacity.

Variation: Groups with more mature security cultures still need external expertise and regular maintenance. Groups in higher-risk advocacy contexts are cautious about shared systems because a single breach could harm vulnerable people or expose sensitive documentation. Media and documentation organisations face a different security challenge: how to back up, access, and protect large files without exposing sensitive content or making cloud storage costs unmanageable.

Why it matters for shared infrastructure: Digital security support can be shared, but sensitive data and systems should not be placed in one shared space without strong safeguards. Shared incident response, training, risk assessment, secure backup standards, and tool hardening are feasible. A single shared repository for sensitive data is much riskier unless data separation, encryption, access control, jurisdictional analysis, breach response, and clear rules for joining, leaving, data export, access removal, and shutdown are in place.

2.2.3 Legal, compliance, and administrative capacity

Finding: Legal, compliance, finance, and administrative functions are major sustainability pressures. Several organisations rely on a small number of staff, volunteers, external accountants, lawyers, or

informal peer advice to manage donor reporting, local compliance, tax or registration issues, legal risk, and day-to-day administration.

INT-01 described significant friction between local accounting software and donor reporting requirements. The organisation relied on local accounting software for compliance but still had to transfer data to Excel for donor reporting, creating extra work and introducing room for error. The same interview also pointed to limited guidance for non-profit-specific compliance questions and reliance on external accountants and peer organisations to interpret taxation requirements. INT-04 highlighted a different but related pressure: the loss of institutional memory when staff leave. Incomplete handovers made it difficult to recover donor portal access, passwords, old proposal logs, and historical documents. INT-06 identified accounting as a major stressor for a young organisation because of the volume and complexity of financial records. INT-02 described reliance on lawyers for casework and showed how funding shortages can affect critical legal and advocacy projects.

Variation: The pattern varies by organisational age, size, and risk profile. Older organisations may have more established administrative routines, but they also carry legacy systems, historical records, and accumulated donor requirements. Newer organisations may have flatter structures and more flexible tools but often have less formal compliance capacity. Groups facing legal, censorship, or documentation risks need stronger separation between public advocacy materials, sensitive case information, financial records, and donor-related documents.

Why it matters for shared infrastructure: Many legal, compliance, financial, and administrative pressures recur across organisations. Shared legal and compliance clinics, pooled accounting support, donor reporting templates, and trusted referral rosters could reduce pressure immediately. Fiscal hosting may also be useful in some cases, especially for newer or smaller groups, but it should

be carefully assessed because it entails legal responsibility, financial control, and trust. These services should not replace each organisation's own accountability. Instead, they can make compliance less isolating, more consistent, and easier to sustain.

2.2.4 Communications and M&E capacity

Finding: Communications, monitoring, evaluation, and knowledge management work often fall between programme, advocacy, and administrative roles. Organisations need better systems for campaign assets, monitoring data, evidence, evaluation templates, and public communications workflows.

INT-03 described collaboration for joint communications, but also weak internal collaboration features in the organisation's email system. INT-05 described high cognitive load from documentation and cross-referencing across different systems. INT-06 described the need to standardise databases and work plans. INT-08 and INT-09 described heavy media management, shared campaign content, and a common interest in more centralised resource hubs. INT-04 described information being lost in one-to-one chat conversations rather than being archived in organisational systems.

Variation: Media and documentation organisations face large-file and archival problems. Advocacy organisations face monitoring and evidence-management problems. Newer organisations face standardisation challenges. Technical organisations face documentation governance and key-person dependency.

Why it matters for shared infrastructure: Shared M&E templates (proposed), documentation standards, communications calendars, campaign asset protocols, and knowledge bases are low-risk starting points. More sensitive shared databases require stronger governance and data classification before implementation.

3. Tool and infrastructure pain points

3.1 Tool fragmentation and donor-imposed tools

Finding: Many organisations use tools not because they are the best fit, but because donors, partners, legacy habits, cost constraints, or individual preferences push them into fragmented systems.

INT-04 described donor-mandated use of one secure messaging app for some coordination while urgent internal issues still happened elsewhere. INT-08 described a partner requirement to use a Microsoft system, although the team was more familiar with Google Drive. INT-03 described partner-imposed monitoring tools with limited functionality and internal reliance on personal email accounts because official systems lacked collaborative features. INT-07 described attachment to older communication tools and frustration with Google Workspace. INT-01 described accounting software selected for regulatory compliance but difficult to reconcile with donor reporting formats.

Variation: The source of fragmentation differs by organisation type. For some, it is externally imposed, with donors or partners mandating specific platforms (INT-04; INT-08; INT-03). For others, it is internal, driven by long habituation to older tools or reluctance to migrate (INT-07). For finance-facing organisations, the constraint is regulatory, with software chosen to satisfy compliance rather than for usability or compatibility with donor reporting (INT-01). Smaller and less technical organisations feel this most sharply, since they have the least leverage to negotiate tools or fund proper migration.

This should be framed structurally rather than as poor organisational discipline. CSOs operate within donor rules, vendor

markets, compliance requirements, and funding constraints. A small organisation may not have the leverage to choose ideal tools, migrate systems, or pay for proper onboarding.

Why it matters for shared infrastructure: Tool-sharing must not add another layer of fragmentation. Any shared tool should be selected through user testing, low-bandwidth assessment, data classification, exit planning, and support arrangements. The goal is not simply to procure tools collectively; it is to reduce tool burden.

3.2 Connectivity and offline working constraints

Finding: Connectivity is uneven across office spaces, remote work, field settings, public venues, and community contexts. Even organisations with good general internet access face weak spots, hybrid meeting problems, or a lack of wired connectivity for high-bandwidth work.

INT-08 and INT-09 described stable internet in some parts of the office but weak Wi-Fi in meeting areas, making online meetings or screenings difficult. INT-05 described preparing work in advance for offline conditions and syncing later. INT-03 noted that remote or field collaboration sometimes requires physical presence or paid upgrades to meeting tools. INT-01 described fallback reliance on mobile data when office connectivity fails.

Variation: Connectivity problems affect organisations differently. Media organisations need stable bandwidth for large files and screenings. Field-based or community-facing organisations need offline access and resilient communications. Remote teams need lightweight coordination systems. Civic technology groups need reliable servers and development access.

Why it matters for shared infrastructure: Shared infrastructure must be low-bandwidth compatible and usable offline where possible. It should not assume constant cloud access, high-end devices, or staff with specialist technical skills.

3.3 Storage, file sharing, and information management

Finding: Storage and information management are among the clearest cross-cutting pain points. Organisations rely on a mix of cloud drives, personal devices, portable hard drives, local laptops, email, chat apps, NAS devices, websites, and project portals. This creates duplication, missing records, unclear permissions, and loss of institutional memory.

INT-04 described chat apps as places where files, decisions, and coordination can disappear from the organisational archive. The same interview also noted risks when former staff accounts remain active and when historical donor information, passwords, proposal records, and archived documents become difficult to find. INT-03 described files being stored across laptops and portable hard drives, with transmission through email, creating a fragmented information system. INT-08 described managing around 100 physical drives and needing a better way to index and search the data stored across them. INT-09 described an archiving routine where completed event files are downloaded and stored on external drives to manage cloud storage limits and costs. INT-06 and INT-07 described the need to manage different types of information carefully, with INT-07 giving the clearest example of separating public, aggregated, personal, financial, and internal data.

Variation: Organisations handling multimedia need different storage solutions from organisations handling case data, monitoring databases, or sensitive community information. Media organisations need systems for large files, backups, archives, and searchability. Advocacy and documentation organisations need stronger controls for evidence, case records, community data, and legal or donor-related documents. Across these differences, the common issue is information governance: who owns the record, where it lives, how long it is retained, who can access it, and how it is recovered after staff turnover or an incident.

Why it matters for shared infrastructure: Shared backup, indexing, and knowledge management are high-value opportunities, but they must be designed with data classification, encryption, and access control in mind. Low-risk public materials can be shared openly. Sensitive case data, community records, legal documents, donor information, and financial records should be encrypted, strictly separated, access-controlled, and governed by clear retention and recovery procedures.

4. Sustainability and risk concerns

4.1 Funding dependency and the “cliff edge” problem

Finding: Many infrastructure needs are tied to project funding, which creates a cliff edge when grants end. Tools, staff time, subscriptions, consultants, and technical support can disappear even when the underlying need remains. A structural reason sits beneath this: most interviewed organisations receive little or no core or operational funding and run almost entirely on project-based grants. With no stable base to draw on, the everyday costs of keeping infrastructure alive have nowhere to sit except inside time-bound projects, so grants tend to pay for building something but rarely for keeping it running.

In practice, infrastructure is held together internally rather than through funded, dedicated support. The work falls to existing staff, often whoever is most technically confident, with volunteers, pro bono help, or paid external assistance brought in only at certain points or when something breaks. INT-08 described the most technically inclined staff member naturally inheriting responsibility for data, hard drives, and equipment, with minor IT handled in-house and a web developer kept on retainer for emergency server or website issues. INT-03 described staff self-managing IT needs because hiring budgets are limited, and INT-05 described a team that self-hosts its own servers without any dedicated IT support structure. INT-07 described security resting on one person’s manual vigilance. Other gaps are filled by unpaid or external specialists, such as the volunteer lawyers INT-01 relies on for legal aid and the consultants several organisations bring in only for one-off needs (INT-01; INT-04; INT-09). This keeps systems working day-to-day, but it concentrates risk on a few individuals and leaves upkeep dependent on goodwill and spare capacity.

INT-02 described funding shortages that stopped or weakened critical projects and limited access to essential monitoring software. INT-05 described tools as temporary or project-dependent even where the organisation has some core support. INT-06 described the burden of moving from free or low-cost tools to paid subscriptions, including the risk of unpaid bills or debt during cash flow gaps. INT-01 and INT-04 described donor dependency and shifting donor priorities as major concerns. INT-03 pointed to the heart of the matter, noting that technical organisations need ongoing maintenance funding rather than one-off development grants.

Variation: Older organisations may face donor exit or sunset clauses after long-running programmes. Newer organisations frequently operate without any funded base to carry recurring operational costs, leaving them exposed when expenses fall due. Technical organisations face the opposite pressure: funding flows toward building new systems, not toward the ongoing upkeep needed to keep existing ones alive. The common thread is that tools, servers, and trained capacity vanish when a project ends, even though the need does not.

Why it matters for shared infrastructure: Shared infrastructure can lower per-organisation costs, but it still needs reliable funding. A shared model resting on one short grant simply repeats the cliff edge at a larger scale. The deeper question is how project funding can build something lasting rather than standalone systems that are dropped once a grant closes. The interviews point to a few conditions that make this possible when they are built into grant design from the outset. First, projects should feed into shared resources rather than custom ones: a pooled subscription, a common backup system, or a shared platform outlasts any single project because several organisations depend on it, whereas a tool built for one organisation is left unsupported the moment its funding ends (INT-08; INT-09).

Second, upkeep, governance, security review, documentation, and exit plans should be written in as core budget lines, not treated as afterthoughts. Third, every tool a project builds should have a named maintainer, documentation, and a handover plan from day one, which guards against the loss of access and institutional memory that follows when staff or projects move on (INT-04). Fourth, the cost of keeping things running should be spread across several funders or a pooled fund rather than carried by a single grant. The shift required is twofold: from funding projects that happen to build tools towards funding infrastructure that projects contribute to, and from project-only grants towards a funding mix that includes core support. Without some stable operational funding beneath it, even well-designed shared infrastructure will keep meeting the same cliff edge.

4.2 Digital security incidents and data risk

Finding: Digital security risk is not hypothetical. Interviews described incidents of website compromise, login attacks, account access issues, data loss, weak backups, phishing attempts, device exposure risks, and public communications that triggered legal or political pressure. Sensitive details are intentionally generalised here.

INT-03 reported a previous website compromise and described related security measures, including hosting arrangements and security policies. INT-07 described repeated attempts to compromise backend login credentials, suspicious messages, concerns about doxxing and surveillance, and strict separation of sensitive information. INT-02 described data loss and access problems, including website access issues, lost login access, weak backup arrangements, and concern about hardware

exposure during physical incidents. INT-04 described phishing, spam, attempted unauthorised logins, partner website attacks, and security tools that were no longer regularly reviewed. INT-09 described risk assessments and digital security briefings before high-risk activities, along with password and VPN training and access to trusted digital rights expertise through a coalition.

Why it matters for shared infrastructure: A failure of shared infrastructure can cause collective harm. Any shared system that handles sensitive data must include access controls, clear incident-response roles, data portability, exit procedures, and regular security reviews. For some types of data, the safest shared infrastructure may be shared guidance and expert support rather than a shared database.

4.3 Automation and emerging technology (AI) needs

Finding: Some organisations are beginning to look toward automation and artificial intelligence (AI) to reduce manual workload, but they lack the capacity and governance to adopt these tools safely. This is an emerging need, not yet sector-wide.

Two organisations named automation as a top priority. INT-03 described automation as a primary priority for reducing manual work. INT-05 framed its ideal shared infrastructure solution as automation for manual work, alongside shared documentation and capacity building. These organisations were also alert to the risks. INT-05 described exploring AI agents and highlighted the need for next-generation capacity building, data governance, and AI governance. INT-03 flagged the data classification and security risks of using generative AI. A simpler form of the same need appeared in INT-08, which described the need for software to index and log content across multiple external drives automatically.
Variation: Automation needs appear differently across

organisations. More technically engaged organisations are considering AI agents, data governance, and the automation of internal workflows. Media and documentation organisations may need more practical automation, such as indexing drives, organising archives, transcribing interviews, or managing large files. Smaller organisations may benefit from automation that reduces repetitive administration, but may not have the staff time, technical confidence, or governance systems to adopt new tools safely.

Why it matters for shared infrastructure: Automation and AI could ease the manual, repetitive burdens that exhaust small teams, but only with shared technical support, training, and clear data and AI governance. Rather than each organisation experimenting alone with sensitive data, the safer starting point is shared learning, practical guidance, and joint capacity building.

4.4 Core Sustainability Concerns Raised by CSOs

Across interviews, the main concerns were funding uncertainty, digital security, data loss, staff burnout, key-person dependency, legal risk, platform or vendor changes, storage failure, and difficulty sustaining work when projects or people leave. Several organisations worried that critical knowledge sits with one person or in one tool. Others worry that being visible online is necessary for advocacy but also increases the risk of being targeted.

This has a care dimension. Shared infrastructure is often discussed as a technical or financial solution. Still, interview evidence shows it is also about reducing anxiety, preventing burnout, and making sure people do not carry organisational risk alone. Shared infrastructure should therefore include peer support, escalation pathways, and realistic workload expectations, not only software and hardware.

5. Findings: Current sharing practices and existing models

A key finding of this study is that civil society organisations already share a great deal. Shared infrastructure is not a new idea to be introduced from scratch; it is an existing practice that can be made safer, fairer, and more durable.

This sharing extends far beyond tools, money, equipment, or services. Even when organisations are under-resourced and stretched, the interviews show a strong sense of solidarity across parts of the civil society ecosystem. Organisations support each other because they recognise shared risks, shared principles, and shared struggles. This solidarity often manifests through advice, referrals, crisis support, campaign collaboration, public backing, and informal peer care. It is rooted in trust, comradeship, and a common commitment to human rights and civic space. Any shared infrastructure model should build on this existing culture of mutual support, rather than treating sharing as merely a technical or financial arrangement.

- **Knowledge, advice, and referrals.** Organisations ask trusted peers for help with digital security, compliance, legal issues, and operations. INT-09 described quick access to digital rights expertise through a trusted cluster when phones, laptops, social media accounts, or other systems are targeted. INT-01 described shared learning through coalition spaces on regulatory and tax compliance issues, including questions linked to LHDN compliance and accounting systems such as AutoCount & UBS. INT-02 described the value of open knowledge resources, joint training, and shared learning across organisations.

- **Contacts and trusted specialists.** Several organisations rely on referrals to lawyers, accountants, digital rights experts, web developers, security trainers, and other trusted specialists. INT-01 described relying on external accountants and peer organisations to understand legal & tax compliance requirements. INT-02 described working closely with lawyers on cases. INT-08 and INT-09 described using external technical or digital security support when internal capacity was not enough. These referral networks already function as informal infrastructure.

- **Equipment and physical space.** Media and freedom-of-expression organisations already lend cameras, microphones, speakers, projectors, and other gear to trusted partners. INT-08 described equipment loans and shared office or meeting space. INT-09 described a more organised approach: equipment is shared only after basic training, with a sign-out form and return dates. INT-04 described shared physical space for community hubs and legal education activities. These examples show that even informal sharing is safer when there are simple rules for use, care, return, and responsibility.

- **Software access and subscriptions.** Organisations sometimes share software because individual subscriptions are expensive or only needed occasionally. INT-09 described shared and cost-split access to Canva, temporary access to Adobe Premiere for campaign producers, shared Vimeo use, and shared music libraries for video productions. INT-08 expressed interest in pooling subscriptions for transcription tools and audio or music libraries. INT-03 described testing secure collaboration tools such as CryptPad and noted problems with official email systems that pushed staff toward personal Gmail accounts. These examples show that software sharing can reduce costs, but it requires privacy protections, account controls, and clear rules.

- **Campaign content, public resources, and media assets.** Organisations already share campaign materials, raw footage, public education content, toolkits, and selected data. INT-09 described sharing raw footage with a partner so the partner could edit it for advocacy use. The same interview described a shared campaign microsite where several organisations contributed content, blurbs, and toolkits. INT-02 also referred to a shared resource hub and open campaign materials linked to freedom of expression work. INT-06 described sharing public resources, toolkits, databases, and templates with peer groups, including materials managed through Airtable, Google Workspace, GitBook, and websites.

- **Databases, templates, and documentation practices.** Several interviews showed interest in shared documentation and monitoring systems. They also showed why this area needs more care than sharing public materials. INT-06 described efforts to combine databases, including media monitoring information, so that resources could benefit more organisations. INT-05 described past sharing of human rights documentation tools and interest in shared platforms such as Bayanat or Uwazi, as well as shared help desk support, hosting, and technical capacity building. INT-07 described sharing research findings and case studies with trusted peers while keeping personal identifying information and financial data internal. This indicates that shared documentation can be useful, but what can be shared depends on how sensitive the data is.

- **Training and digital security support.** Digital security support is already shared through trusted relationships. However, the interviews also reveal a broader structural problem: many CSOs still depend heavily on proprietary or

commercial platforms because they are familiar, available, donor-recognised, or easier for their teams to use. Organisations described daily reliance on tools such as Google Workspace, Google Drive, Gmail, Microsoft tools, OneDrive, WhatsApp, Adobe, Canva, Vimeo, TeamViewer, and UltraViewer. Some organisations also use stronger or more security-focused tools, including Signal, Bitwarden, YubiKey, VPNs, CryptPad, Mattermost, Bayanat, and Uwazi. However, moving toward more secure, open-source, or rights-respecting tools requires time, training, technical support, and clear organisational policies.

INT-09 described access to digital rights expertise through a coalition when incidents happen, as well as risk assessments and security briefings before high-risk activities. INT-03 described security tools and practices such as VPN, Bitwarden, Kaspersky, DocuSign, training, and experimentation with CryptPad, while also noting that weak official systems led some staff to use personal Gmail accounts. INT-01 described the use of YubiKey, TeamViewer, UltraViewer, WhatsApp, Microsoft tools, OneDrive, and Google Drive in daily operations. INT-04 described digital security risk policies and security tools that needed regular review. INT-05 described the use of Mattermost and interest in shared documentation platforms such as Bayanat or Uwazi. INT-02 described digital security as a major concern and pointed to the need for stronger support.

This suggests that shared digital security training, incident response, tool hardening, and practical migration support may be easier to start with than a shared database for sensitive information. It also shows that shared infrastructure should not simply push CSOs to adopt new tools without

support. Any shift toward secure or open-source platforms requires onboarding, troubleshooting, documentation, and user support; otherwise, organisations may revert to familiar commercial tools even when those tools pose privacy, security, or dependency risks.

- **Crisis and peer support.** Several interviews show that CSOs turn to trusted peers during security, legal, operational, or emotional stress. This support is often informal, but it matters. It helps small teams cope when they lack sufficient staff, money, or specialist support. It also reflects a deeper culture of solidarity. However, this support depends heavily on trusted individuals. It can fail when those people are unavailable, overworked, or leave the organisation.

A repeated need is a shared documentation, monitoring, or archive system. This is not yet fully built. Interviewees described interest in combining monitoring databases, improving documentation tools, creating better archives, and building shared resource hubs. INT-06 described database consolidation as a way to benefit a wider network, using tools such as Airtable, Google Workspace, GitBook, and websites. INT-05 pointed to possible joint use of documentation platforms such as Bayanat or Uwazi, along with shared technical support, shared hosting, AI server or virtual machine resources, and shared help desk support. INT-09 described discussions around shared media monitoring and digital archiving. It also noted that organisations are still organising their own archives using Google Drive, Vimeo, external drives, and Synology NAS. This is one of the clearest shared infrastructure needs, but it requires strong governance, data classification, access control, and long-term maintenance.

Most existing sharing is trust-based and unpaid. This is both a strength and a weakness. It works because relationships already exist. It is fragile because it depends on goodwill, individual staff, informal coordination, and spare capacity. The more organised

examples, such as equipment training, sign-out forms, return dates, temporary software access, password changes, and cost-splitting, show what better governance can look like in practice.

Two gaps are important. First, pooled staff time and shared consultants are still limited. One organisation usually hires external specialists, even when several organisations have similar needs. This creates an opportunity for pooled retainers, shared expert rosters, or jointly funded support for digital security, legal compliance, communications, M&E, and technical maintenance. Second, not all collaboration is easy. INT-02 cautioned that barriers to cooperation can come from deep-rooted structural and principle-based issues, not only from technical capacity. This is an important lesson: shared infrastructure cannot depend on goodwill alone. It needs trust, clear governance, fair cost-sharing, privacy protection, and practical rules for access, risk, responsibility, and exit.

6. Existing shared infrastructure models: a landscape review

The desk review identified several types of shared infrastructure models. Some are technical, such as secure hosting, documentation platforms, digital security helplines, and open-source tools. Others are less technical but just as important to sustainability, such as fiscal hosting, pooled funds, shared spaces, cooperative governance, rapid-response funds, regional networks, and collective care models.

This matters because the interview findings show that CSOs do not only need better tools. They also need trusted people, shared services, legal and financial support, practical governance, safe spaces, emergency support, and long-term maintenance. A useful shared infrastructure model should therefore combine technology, services, governance, funding, and solidarity.

Model/type	What is shared, governance and limitation	Relevance/ lesson
Qurium / Virtualroad.org Secure hosting and digital forensics	**Shared:** Attack-resilient hosting, DDoS protection, website cleaning, circumvention support, digital forensics, and rapid help for media and rights groups under attack. **Governance/funding:** Independent nonprofit foundation model; owns and operates specialist infrastructure. **Limitation:** Highly specialised, with eligibility targeted. It cannot meet every CSO infrastructure need.	Shows how high-risk groups can share resilient hosting and incident support without each organisation having to build it on its own.
Digital Defenders Partnership (DDP)	**Shared:** Incident response funding, sustainable protection grants, community and network funding, regional support, and digital protection resources.	Useful model for pooled emergency response, protection

Model/type	What is shared, governance and limitation	Relevance/ lesson
Digital protection fund and support network	**Governance/funding:** Programme model hosted by Hivos, with regional and network relationships. **Limitation:** Often time-bound and focused on digital protection. It does not replace everyday IT maintenance.	funding, and regional security support.
Access Now Digital Security Helpline Shared incident response service	**Shared:** Free 24/7 technical assistance, incident response, and digital security advice for civil society, journalists, activists, and human rights defenders. **Governance/funding:** Hosted by Access Now as a global helpline service. **Limitation:** Reactive support cannot replace daily security practice, local governance, or internal policies.	A strong example of a trusted, shared help desk for urgent digital security incidents.
CiviCERT Trusted network of civil society responders	**Shared:** Shared infrastructure, threat information, incident response knowledge, peer capacity building, and coordination among trusted civil society security actors. **Governance/funding:** Network and membership model based on trust between responders and infrastructure providers. **Limitation:** Requires high trust, skilled responders, and clear information-sharing rules.	Useful reference for building trusted security coordination across a CSO ecosystem.
HURIDOCS / Uwazi Open-source documentation and evidence system	**Shared:** Open-source database application for organising human rights information, collections, cases, complaints, and evidence. **Governance/funding:** Developed and supported by HURIDOCS, with partner implementation. **Limitation:** The tool still needs good data models, training, hosting, access control, and governance.	Highly relevant to interview needs around documentation, monitoring, archives, and evidence pres-ervation.

Model/type	What is shared, governance and limitation	Relevance/ lesson
The Engine Room Responsible technology advisory support	**Shared:** Research, advice, and practical support on technology, data, responsible tool choices, and organisational digital practices. **Governance/funding:** Independent nonprofit support model with a distributed team. **Limitation:** Mostly advisory and project-based, not permanent shared infrastructure.	Useful for participatory tool selection, responsible data decisions, and transition planning.
Greenhost Ethical hosting provider	**Shared:** Sustainable web hosting, VPS, secure internet services, and open-source-oriented hosting support. **Governance/funding:** Mission-driven hosting provider. **Limitation:** Commercial pricing and Europe-based infrastructure may not fit all small or high-risk CSOs.	Useful model for rights-aligned hosting criteria and responsible service provision.
May First Movement Technology Cooperative / member-run technology model	**Shared:** Movement technology infrastructure, hosting, email, lists, collaboration tools, and member support. **Governance/funding:** Member-run and movement-rooted democratic governance model. **Limitation:** Requires active member participation, governance capacity, and shared political alignment.	Strong cooperative model for collective control of technology, not just vendor-based service provision.
Co-op Cloud Cooperative open-source cloud model	**Shared:** A software stack that helps small service providers, tech cooperatives, community groups, and nonprofits self-host open-source apps such as Nextcloud, WordPress, and Jitsi. **Governance/funding:** Federated/ open-source commons model used by cooperative and community service providers.	Useful for CSOs that want alternatives to Big Tech platforms but need shared technical support to make them usable.

Model/type	What is shared, governance and limitation	Relevance/ lesson
	Limitation: Requires technical hosting capacity and ongoing maintenance.	
Open Collective/ fiscal hosting Fiscal hosting and shared administration	**Shared:** Legal and financial infrastructure to receive funds, manage budgets, issue receipts, pay expenses, and keep transparent records for groups without their own legal entity. **Governance/funding:** Platform plus fiscal host. Governance depends on host rules and collective agreements. **Limitation:** Legal fit is jurisdiction-specific. Not all hosts are suitable for high-risk human rights work.	Useful for pooled funds, shared administration, coalition fundraising, and smaller groups without formal registration.
Platform 6 fiscal hosting Cooperative fiscal hosting model	**Shared:** Open and transparent money handling for new or emerging cooperative projects without requiring an immediate bank account or legal entity. **Governance/funding:** Cooperative support model using Open Collective fiscal hosting infrastructure. **Limitation:** Built mainly for cooperative projects; adaptation would be needed for high-risk CSOs or cross-border rights work.	A useful example of combining fiscal hosting with cooperative values and transparent financial practices.
Community Spaces Network Shared physical space and social purpose real estate	**Shared:** Peer learning, tools, templates, consulting, and knowledge for developing and operating nonprofit shared spaces and community-serving spaces. **Governance/funding:** Membership organisation of social purpose real estate practitioners; fiscally sponsored by Tides Centre. **Limitation:** Physical shared space poses challenges for cost, safety, accessibility, and location.	Useful for CSOs considering shared offices, meeting rooms, equipment storage, community hubs, or safe spaces for convening.

Model/type	What is shared, governance and limitation	Relevance/ lesson
EngageMedia / Cinemata Regional open-source media platform	**Shared:** Secure, open-source, ad-free, privacy-respecting video platform for social and environmental films across Asia-Pacific. **Governance/funding:** Hosted and maintained by EngageMedia with open-source/community-facing development. **Limitation:** Requires long-term technical maintenance, moderation, governance, and sustained funding.	Strong regional example of shared media infrastructure that offers an alternative to Big Tech platforms.
Sinar Project / Enabling Tech Local civic tech and capacity-building model	**Shared:** Technical literacy, civic tech capacity, digital rights support, open tools, and bridges between technologists and civil society. **Governance/funding:** Local nonprofit and project-based community model. **Limitation:** Small-team capacity and project funding can limit scale and continuity.	Highly relevant for Malaysia and Asia-Pacific CSOs needing local, context-aware technical support.
Association for Progressive Communications (APC) Membership network and ecosystem coordination	**Shared:** Network membership, capacity strengthening, convening, advocacy, knowledge exchange, and strategic use of ICTs for social justice. **Governance/funding:** International membership-based network. **Limitation:** A network model supports coordination and learning, but does not provide every operational service directly.	Useful model for ecosystem-level coordination, regional solidarity, and movement-owned digital rights agendas.
FORUM-ASIA Regional human rights network	**Shared:** Advocacy, research, solidarity, member coordination, HRD support, and regional human rights movement infrastructure. **Governance/funding:** Regional membership network of human rights organisations.	Strong Asia-based model for solidarity, referrals, protection pathways, and collective voice.

Model/type	What is shared, governance and limitation	Relevance/ lesson
	Limitation: Focused on human rights advocacy and protection, not general back-office services.	
APCASO Regional community systems network	**Shared:** Advocacy, community systems strengthening, coordination, and support for marginalised communities across Asia-Pacific. **Governance/funding:** Regional civil society network and catalytic platform model. **Limitation:** A sector-specific focus may mean it does not cover all CSO infrastructure needs.	Useful regional model for community-led coordination, shared advocacy, and systems strengthening.
Urgent Action Fund Asia & Pacific Feminist rapid response and care infrastructure	**Shared:** Urgent grants, strategic support, safety and well-being support for women and non-binary activists and movements in Asia-Pacific. **Governance/funding:** Regionally rooted feminist fund and movement-support model. **Limitation:** Focused on feminist movements and urgent support, not routine organisational administration.	Important non-tech model showing that shared infrastructure should protect people, care, and the sustainability of movement.
Lifeline Embattled CSO Assistance Fund Emergency assistance and civic space protection fund	**Shared:** Emergency financial assistance, rapid response advocacy, and resiliency grants for CSOs under threat or attack. **Governance/funding:** Consortium- and donor-supported fund administered through Freedom House and partners. **Limitation:** Short-term emergency support cannot replace long-term sustainability funding.	Useful model for crisis support, legal/security response, and civic space protection funds.

Model/type	What is shared, governance and limitation	Relevance/ lesson
Start Network / National Start Funds Membership-owned pooled funding model	**Shared:** Pooled rapid funding for locally led humanitarian action, with national funds managed closer to affected communities. **Governance/funding:** Membership network with locally led hubs and member-managed funds. **Limitation:** Humanitarian focus; would need adaptation for rights-based CSO infrastructure.	Useful model for pooled funds, local decision-making, and moving resources closer to frontline organisations.
NEAR Network Global South local CSO network	**Shared:** Peer learning, advocacy, local ownership, and collective power among local and national CSOs from the Global South. **Governance/funding:** Movement/ network model rooted in local and national CSOs. **Limitation:** Humanitarian and localisation focus; not a direct service provider.	Useful for principles of local ownership, solidarity, and the shift of power away from externally controlled models.
Numun Fund Feminist technology and movement infrastructure fund	**Shared:** Funding and support for feminist technology infrastructure and movement organising in the Global South. **Governance/funding:** Feminist fund and movement infrastructure model. **Limitation:** Focused on feminist technology movements, not general CSO services.	Useful for seeing technology as movement infrastructure, not only software or platforms.
Amnesty International Security Lab Resource Hub Knowledge hub and referral resource	**Shared:** Digital security resources, risk analysis support, helpline referrals, and tools for civil society, activists, journalists, and HRDs. **Governance/funding:** Hosted by Amnesty International Security Lab. **Limitation:** The resource hub model does not provide full implementation support for every organisation.	A useful example of a curated knowledge base and triage pathway that complements direct support.

Model/type	What is shared, governance and limitation	Relevance/ lesson
Ethereum Foundation Ecosystem Support Program (ESP) Public-goods grants and ecosystem support	**Shared:** Financial and non-financial support for free, open-source, non-commercial projects that strengthen Ethereum's technical, social, research, education, and public-goods foundations. **Governance/funding:** Foundation-led ecosystem support programme, with grants and support coordinated through the Ethereum Foundation. **Limitation:** Focused on Ethereum. It is not a general CSO funding mechanism, and CSOs would need legal, tax, accounting, volatility, compliance, and reputational review before using crypto-linked funding models.	Useful as an example of public-goods funding for open-source infrastructure and shared maintenance. Indirectly relevant, not a ready-made CSO funding solution.
Filecoin Foundation / FIL Public Goods Funding Decentralised storage and public-goods funding	**Shared:** Grant funding and public-goods support for tools, research, storage, retrieval, data infrastructure, applications, and projects that strengthen the Filecoin ecosystem. **Governance/funding:** Foundation and ecosystem-based funding model, including grants and proactive or retroactive public-goods funding mechanisms. **Limitation:** Focused on Filecoin and decentralised storage. It is not designed for general CSO operations, and crypto-linked funding may create compliance, accounting, volatility, data protection, and donor-trust concerns.	Useful for thinking about decentralised storage, public-goods funding, open-source tools, archives, and long-term infrastructure maintenance.
Gitcoin Grants / Quadratic Funding Community-backed public-goods funding	**Shared:** Crowdfunding, matching grants, quadratic funding, retroactive grants, and grants-management infrastructure for public goods and open-source projects.	Useful as an example of community-backed pooled funding and participatory allocation.

Model/type	What is shared, governance and limitation	Relevance/ lesson
	Governance/funding: Community-based public-goods funding model using matching pools, community donations, and allocation mechanisms such as quadratic funding. **Limitation:** Stronger fit for open-source and Web3 public goods than general CSO services. Requires technical knowledge, wallets, public campaigning, fraud controls, and compliance review.	Exploratory for CSOs, not a ready-made solution.

This landscape shows that no single model solves every need. The strongest models are not only technical. They combine trust, governance, funding, maintenance, and clear accountability. Secure hosting models are useful for websites and for defending against digital attacks. Documentation platforms are useful for evidence and archives. Fiscal hosting helps with money and legal administration. Cooperative models show how infrastructure can be owned and governed by members. Shared space models show how organisations can reduce costs and build relationships. Rapid-response funds and care funds show how shared infrastructure can protect people, not just systems.

Crypto, blockchain, and DAO-based models also deserve careful exploration, but they should not be treated as quick fixes. Some CSOs may be reluctant to explore these models because crypto is often associated with speculation, volatility, scams, unclear regulation, donor concern, and technical complexity. The interviews also show that many organisations already face gaps in accounting, compliance, digital security, and governance. For these organisations, accepting crypto funding or using blockchain-based tools without proper support could create new risks rather than solve existing ones.

At the same time, some blockchain-based models offer useful lessons for shared infrastructure. A DAO, or decentralised autonomous organisation, can allow members to pool funds, vote on priorities, allocate grants, and manage a shared treasury through transparent rules. For CSOs, the most useful lesson is not necessarily the token model itself, but the idea of participatory governance: members can help decide how shared funds are used, who receives support, and what infrastructure should be maintained.

There are real examples worth studying. Big Green DAO is a non-profit-led philanthropic DAO, and Big Green's grantmaking model uses democratic processes where community voices help decide how funding flows to grassroots food organisations. Filecoin Foundation for the Decentralised Web has supported public-interest projects using decentralised storage, including WITNESS, which explored how decentralised web tools could help authenticate and preserve human rights records while protecting privacy, autonomy, and user control. It has also supported the Rohingya Project to preserve cultural heritage materials, including audio recordings, photographs, videos, and written materials. These examples show that blockchain-based funding and storage can be relevant to human rights, archives, cultural memory, and public-interest infrastructure.

For this study, the lesson is clear: shared infrastructure for CSOs should not be designed as one large platform. It should be built as a mixed system of shared knowledge, shared services, shared tools, shared spaces, pooled funds, trusted referrals, and clear governance. Technology is important, but it is only one part of the infrastructure that keeps civil society alive. Crypto, blockchain, and DAO models may be useful in specific cases, especially for public-goods funding, participatory grantmaking, decentralised archives, and community governance. However, they require strong legal review, financial controls, data protection, security planning, and clear rules before CSOs can safely adopt them.

7. Proposed Framework: Resource-Sharing Protocol

7.1 Purpose and principles

This framework is a practical protocol for CSOs that want to share resources without creating new risks, dependencies, or extra work. It is not a proposal for one large shared platform. The interviews show that a single platform would be too risky at the start because organisations differ in trust, technical capacity, data sensitivity, secure funding, and digital security preparedness.

Instead, the framework builds on what CSOs already do, including peer guidance, referrals, equipment, campaign materials, meeting space, and trusted specialists. It aims to make this existing sharing safer, clearer, fairer, and easier to sustain, guided by three key principles:

1. **Start with what is already trusted:** low-risk sharing such as knowledge, referrals, training, and equipment.
2. **Add governance before infrastructure:** Ensure every shared tool, service, fund, or space has clear rules regarding access, cost, maintenance, data, security, and exit strategies.
3. **Build in phases:** Introduce sensitive infrastructure, such as hosting, backups, archives, and databases, only after smaller forms of sharing have been thoroughly tested.

7.2 Levels, categories, and the framework matrix

Sharing works across three levels and four categories.

Level	What it means	Best for
Bilateral (2 orgs)	Two organisations share directly	Simple, high-trust resources: equipment, one subscription, a shared adviser
Coalition (3–10)	An existing cluster or trusted network shares	Pooled services, learning circles, referral rosters, shared subscriptions, security support
Ecosystem (sector-wide)	A resource is open to many organisations	Knowledge commons, pooled funds, sector help desks, shared infrastructure with strong governance

7.3 Risk ladder: what to share first

Risk	Resource type	Examples	Readiness needed
Low	Knowledge & public resources	Templates, toolkits, referral lists, learning calls, equipment sign-out forms	Basic coordination: a rotating maintainer
Medium	Pooled services & subscriptions	Shared security retainer, legal clinic, pooled transcription tool, equipment library	Written agreement; cost-sharing and access rules; confidentiality
High	Systems with sensitive data or money	Shared hosting, backup, documentation database, pooled fund, fiscal hosting	Strong governance; encryption; data separation; legal/ security review; exit rules; maintenance funding

The core rule: never centralise sensitive data, money, or control before the group has tested smaller forms of sharing.

7.4 Minimum governance checklist

Before launching any shared resource, participating organisations should agree on answers to these questions. This single checklist applies to every protocol below.

Question	Practical rule
What are we sharing?	Define it clearly; scope grows only by agreement.
Who controls it?	No shared resource is quietly controlled by one organisation.
Who pays?	Transparent, size-based cost-sharing; smaller orgs not priced out.
Who maintains it?	Every resource has a named maintainer or administrator.
Who can access it?	Clear access levels; remove access when staff or orgs leave.
What data is involved?	Classify as public, internal, sensitive, or highly sensitive.
If something goes wrong?	Define incident response, escalation, and responsibility.
If funding ends?	Plan renewal, handover, or safe closure from the start.
If an organisation leaves?	Set rules for data export, account closure, unpaid costs, and access removal.
How are smaller/higher-risk groups protected?	Equal voice, sliding-scale costs, confidentiality options.
How do we know it's working?	Review usage, safety, fairness, and maintenance yearly.

7.5 Protocols by category

Knowledge resources (lowest risk, best starting point)

Share donor-reporting and compliance templates, tax and e-invoicing guidance, digital-security checklists, tool recommendations, M&E and documentation templates, campaign toolkits, and referral lists. This is grounded in compliance stress and reliance on informal peer advice (INT-01; INT-04; INT-09).

Practical start: 3 to 5 organisations open a shared folder, a referral roster, and a monthly learning call with a rotating facilitator, with little or no additional funding.

Success: Materials are reused, staff save time, and the folder remains up to date after six months.

Tools, systems, and hardware (medium to high risk)

Share pooled subscriptions for occasional tools (transcription, design, audio and video production), equipment, low-risk backup, archive or indexing tools, and, only when ready, open-source hosting and documentation platforms. This is grounded in cost-splitting and equipment loans already practised, plus demand for pooled subscriptions, backup, and a shared, offshore server, alongside strong data-separation concerns (INT-03; INT-05; INT-08; INT-09).

Practical start: One low-risk pilot only, a single pooled subscription with separate organisational accounts, or one equipment sign-out system. Each organisation uses its own account; shared logins are never used for sensitive work.

Success: Costs fall, equipment returns safely, fewer files are lost, and sharing reduces workload rather than adding to it.

Services (strongest opportunity)

Many CSOs need the same support but cannot afford it on their own. Build in stages; start with clinics, retainers, referrals, and assessments before pooled funds or fiscal hosting (which needs legal and financial review).

Shared service	What it covers	Grounded in	Start small (MVP)
Digital-security responder	Incidents + prevention: account compromise, phishing, website attacks, 2FA, backups	NT-02, 03, 07, 08	Shared emergency referral list + quarterly refresher; then a 6-month responder pilot for 4–6 orgs
Security audits & risk assessments	Access review, 2FA, backups, on/offboarding, incident plans	INT-02, 04, 08, 09	One "check-up month" every six months; each org writes down one verbal policy
Legal, compliance & accounting	Tax/e-invoicing, donor reporting, entity status, contracts, data consent	INT-01, 04	Quarterly clinic, one topic each, producing a reusable template
Technical administrator/ help desk	Accounts, access removal, backups, tool support, troubleshooting	INT-01, 03, 05, 08	Tool-and-access map first; then a shared admin for set hours/ month (not a new single point of failure)
Comms, M&E, documenta-tion & archive	Templates, file/ archive rules, monitoring-database design, media indexing	INT-04, 06, 08, 09	Documentation clinic: one shared data-classification guide
Fiscal hosting & pooled funding	Manage funds via a host; pooled fund for shared services	INT-01, 04, 06	One written cost-sharing agreement for one shared service
Automation, AI & data governance	Safe automation, what to never feed AI, data classification	INT-03, 05	One AI/data-use checklist before any AI use with internal data

Success across services: Organisations get support they could not afford alone; incidents are handled faster; smaller groups are not priced out; and the service outlives a single grant.

Spaces and coordination

Share meeting rooms, co-working days, event logistics, equipment storage, campaign coordination, shared calendars and action logs, peer-care check-ins, and, carefully, community hubs. This is grounded in shared office or meeting space, equipment loans, and cluster coordination that are already underway (INT-04; INT-08; INT-09).

Practical start: One monthly coordination meeting with rotating facilitation, a shared action log, and occasional room-sharing. A permanent physical hub comes only after security planning, because concentrating organisations can raise the risk of raids and cut costs (INT-04; INT-09).

Success: Members attend, follow-ups happen, duplication falls, and the group responds to threats faster.

7.6 Models to learn from

- **Digital security & rapid response:** Access Now Digital Security Helpline; Digital Defenders Partnership; CiviCERT; Qurium / Virtualroad.
- **Documentation, data & tech advice:** HURIDOCS / Uwazi; The Engine Room.
- **Hosting & open technology:** Greenhost; May First Movement Technology; Co-op Cloud; Cinemata (EngageMedia).
- **Fiscal hosting & pooled funds:** Open Collective; Tides.
- **Security guidance:** Amnesty Tech Security Lab.

- **Regional coordination & care:** FORUM-ASIA; Urgent Action Fund Asia & Pacific; Association for Progressive Communications.

Emerging funding models are exploratory only; treat with caution.

A set of "public-goods" and decentralised funding models has emerged from the open-source and web3 world, including Gitcoin Grants and quadratic funding, the Ethereum Foundation Ecosystem Support Program, Filecoin Foundation grants, and DAO-inspired participatory grantmaking, where a community allocates a shared pool of funds through transparent, often token-based voting.

> Caution: These models were not raised by any interviewee and sit largely outside the human rights CSO context covered by this study. They can carry legal, tax, currency-volatility, security, and reputational risks, and several depend on cryptocurrency infrastructure that may be unsuitable or unsafe for organisations operating under surveillance or financial scrutiny. They are included only as references to study, not as recommendations. Any consideration should follow a full legal, tax, accounting, and security review and should never replace stable, mission-aligned funding.

7.7 Cross-cutting rules

Always: Start small, write down basic rules, and separate sensitive data. Assign a named owner to every resource and budget for maintenance, not just the initial setup. Protect smaller and higher-risk groups, set clear exit rules, reuse existing services instead of rebuilding them from scratch, and review the setup annually.

Avoid at the start: Do not implement a single shared database for all sensitive data, or a shared server without backup or exit options. Avoid having a single organisation hold all control, using shared logins for sensitive work, or pushing an open-source migration without providing training and a dedicated help desk.
Additionally, steer clear of infrastructure that depends entirely on a single short grant, a shared physical hub without proper security planning, fiscal hosting without thorough legal and accounting review, and AI or automation without data-classification rules.

These complex setups may become possible later, but only once trust, governance, technical capacity, and sustainable funding are firmly in place.

8. Recommendations

These are organised by timeline and actor and designed for CSOs with limited staff, funding, and technical capacity. The central message: do not build one large platform first. Start with low-risk sharing, move to pooled services and shared tools, and only later develop secure hosting, backup, documentation systems, pooled funds, or fiscal hosting.

8.1 Priority starting package (launch within 6 months)

Action	Includes	Why it matters
Monthly peer learning circle	One practical session/month on tools, compliance, security, storage, or campaigns	Builds on existing trust
Shared knowledge folder	Templates, compliance notes, tools, security checklists, and referral contacts	Cuts duplicated work; preserves memory
Trusted referral roster	Lawyers, accountants, security responders, web developers, trainers	Gives small orgs somewhere to turn
Simple sharing rules	Sign-out forms, return dates, cost-splitting, access and password rules	Makes existing sharing safer
Digital-security refresher	Basic training, access review, 2FA, password manager, one written procedure	Responds to repeated incidents
Storage & access mapping	Map where files, accounts, drives, and backups live	Shows what is most at risk first

8.2 Immediate actions (0-6 months): little or no new funding

#	Recommendation	Who leads	What success looks like	Category
1	Start a monthly peer learning and problem-solving circle	3–5 trusted CSOs in a cluster	Regular turnout; one improvement shared each month	Knowledge
2	Build a shared knowledge folder with a rotating maintainer	Participating CSOs	Folder used, updated, reviewed; less duplication	Knowledge
3	Build a trusted referral roster	Participating CSOs	Orgs know who to call in a crisis	Services
4	Write down simple rules for existing sharing (sign-out, returns, password changes, cost-splitting)	Participating CSOs	Equipment and tools shared with fewer disputes/ losses	Tools/ spaces
5	Run a security refresher; write down one verbal policy	Networks + a security partner	Each org has one written, practised procedure	Services
6	Map storage, backup, accounts, and access risks	CSOs + technical help if available	Orgs know where key files and access live	Tools/ systems
7	Create a staff-handover checklist (passwords, donor portals, files, subscriptions)	Participating CSOs	Fewer access problems when staff leave	Knowledge/ governance

8.3 Short-term actions (6-18 months): modest funding or a pilot

#	Recommendation	Who leads	What success looks like	Category
8	Pilot one pooled subscription for an occasional tool	3–5 CSOs	Lower cost; separate accounts/ workspaces used	Tools/ systems
9	Create a shared equipment protocol (cameras, mics, projectors, drives)	Media/ campaign orgs	More groups use gear without damage or unfairness	Tools/spaces
10	Pool funds for a shared part-time security/ technical responder	EngageMedia or a regional convener + members	Members get triage, backup advice, and troubleshooting	Services
11	Hold quarterly legal/ compliance/finance clinics	CSO coalition + legal/ accounting partners	Common questions answered early turned into guidance	Services
12	Develop a plain-language shared-resource agreement template	EngageMedia or a regional convener + CSOs	At least one cluster uses it for a real resource	Governance
13	Run a data-classification and backup exercise (low-risk files first)	Technical partner + CSOs	Public/internal/ sensitive data separated; backups tested	Tools/ systems
14	Test one open-source/ rights-respecting tool with onboarding	Technical partner + CSOs	Staff use it confidently; less dependency, no extra burden	Tools/ systems
15	Run a documentation and archive clinic	Data partner + CSOs	Better file naming, structure, access, and retention	Knowledge/ tools
16	Create an AI and data-use checklist	Data-governance partner + CSOs	Orgs know what must never go into AI tools	Governance/ capacity

8.4 Medium-term actions (18 months+): stronger governance and funding

#	Recommendation	Who leads	What success looks like	Category
17	Establish a pooled technical administrator/help desk	Engage-Media, technical partners, or coalition	Reliable support for accounts, backups, tools, and hosting	Services
18	Develop shared secure backup or hosting (only for ready orgs)	Technical partner + governance group	Data separated, encrypted, access-controlled, restorable	Tools/ systems
19	Pilot a shared documentation/ monitoring/archive system (non-sensitive or classified data first)	Coalition + data partner	Agreed materials are safely stored, searched, and retrieved	Tools/ systems
20	Create a pooled fund so shared services survive any one grant	Funders, backbone org, CSOs	Services funded through mixed sources	Services/ funding
21	Explore fiscal hosting for smaller/newer groups (with legal/ accounting review)	Backbone org, legal partner, funders	Small groups access funds/ admin without unsafe risk	Services
22	Pilot a safe shared physical hub (only after security planning)	Coalition + funders	Space used without increasing exposure	Spaces
23	Build a sector coordination mechanism giving smaller/higher-risk groups a real voice	Networks and coalitions	Faster collective response; decisions not dominated by large orgs	Coordination
24	Diversify and pool funding sources (with legal, tax, and compliance review); treat emerging public-goods or participatory (DAO-inspired) models as exploratory only	Funders, Engage-Media, advisers	Less single-donor dependency; risks understood before adoption	Funding/ governance

8.5 Recommended next steps for Malaysian civil society organisations

These steps are best taken collectively across the Malaysian civil society network, with trusted peers convening, testing, connecting, and supporting one another. No single organisation should own or control all shared infrastructure, since concentrating too much control would reproduce the single-point-of-failure risks that interviewees described (INT-04; INT-05).

#	Recommendation	What success looks like
1	Convene a small pilot group (3–5 CSOs) to test the starting package	A pilot group is active within six months
2	Develop and share the shared-resource agreement template	CSOs reuse it instead of starting from zero
3	Broker access to existing services (helplines, funds, fiscal hosts, tools)	CSOs don't duplicate what already exists
4	Pilot pooled security/technical support	Faster support; less reliance on one internal staffer
5	Support safer tool choices with onboarding and documentation	Orgs move off risky tools without losing usability
6	Advocate with funders for maintenance, coordination, and core costs	Funding lasts beyond one project cycle
7	Protect decentralised governance	Infrastructure stays group-owned, with smaller groups protected
8	Document and share lessons	Other clusters can adapt the model

8.6 Roles for other actors

Actor	Recommended role
Participating CSOs	Start with honest, low-risk sharing; follow agreed-upon rules; protect sensitive data; don't overload a single organisation.
Networks & coalitions	Host coordination, protect smaller members, document practices, provide neutral decision spaces.
Funders	Fund infrastructure, maintenance, technical administration, security review, and core costs; avoid imposing fragmenting tools.
Technical partners	Shared guidance on tax, e-invoicing, donor reporting, entity status, contracts, liability, data protection, and fiscal hosting.
Legal & compliance partners	Shared guidance on tax, e-invoicing, donor reporting, entity status, contracts, liability, data protection, and fiscal hosting.
Digital-security providers	Incident response, audits, tool hardening, backup advice, risk assessments, practical training.
Documentation & data partners	Help classify data, improve archives, design documentation systems, and avoid unsafe centralisation.
Movement-support organisations	Support care, burnout prevention, succession, and peer support so sustainability isn't only about funding or technology.

8.7 Overall recommendation: A practical way forward

The overall recommendation of this study is that shared infrastructure should be treated as a long-term resilience strategy for civil society, not as a one-off technical project. The interviews show that CSOs are already sharing in many ways: advocacy and solidarity, peer support, trusted referrals, equipment, campaign materials, meeting spaces, digital security contacts, and specialist support. This existing culture of solidarity is the strongest foundation for any future shared infrastructure model.

However, goodwill alone is not enough. Informal sharing is useful, but it remains fragile when it depends on overworked staff, personal relationships, unpaid coordination, short-term grants, and one or two technically confident people. If shared infrastructure is to become reliable, it must be supported by clear governance, sustained funding, technical maintenance, and fair participation rules.

The way forward should therefore be practical and phased. CSOs should not begin by building one large shared platform or centralised system. A platform may look efficient, but without staff time, financial resources, technical support, security safeguards, and long-term maintenance, it can quickly become another burden. It may also create new risks if sensitive data, passwords, archives, or organisational records are centralised too early.

Instead, the first step should be to strengthen what already exists. CSOs can begin with low-risk sharing: knowledge folders, referral rosters, learning circles, digital security refreshers, equipment protocols, and simple shared-resource agreements. These actions are realistic because they do not require major funding or complex technology. They help build the habits, trust, and governance needed for deeper sharing later.

The next step is to invest in shared services. The strongest need emerging from the study is not only for more tools but also for people who can help maintain them. Shared digital security responders, technical administrators, legal and compliance advisers, accountants, documentation support, and M&E support may be more valuable in the short term than building new platforms. These services reduce pressure on small teams and prevent organisational risk from falling on one exhausted person.

Just as important as what is shared is how it is owned and governed. The more durable models are defined not by their technology but by how a group of organisations agrees to run something together. Collective approaches, in which members jointly own, govern, and sustain the resources they depend on, offer a way to share infrastructure without handing control to any single organisation. The PurpleCode Collective in Indonesia is one living example: a feminist collective working at the intersection of feminism, human rights, and technology, it organises around shared values, open membership, and care for marginalised communities rather than around a single funded project and runs a free, donation-sustained community space that members use to gather, learn, and build together. Building governance of this kind, with clear membership, decision-making, and cost-sharing rules, should be treated as core infrastructure in its own right because it addresses the very fragility the interviews described, in which shared arrangements collapse when one person leaves or a grant ends.

Only after these foundations are in place should CSOs move toward more complex shared infrastructure, such as shared hosting, secure backup, documentation platforms, archive systems, pooled funds, fiscal hosting, or DAO-inspired public-goods funding models. These models may offer real value, but they require legal review, data governance, security planning, financial controls, and clear exit rules. They should be explored carefully, not adopted because they appear innovative.

This study also shows that shared infrastructure depends heavily on organisational resilience. A shared system cannot be stronger than the organisations and people expected to run it. If CSOs are underfunded, understaffed, and operating from one project cycle to the next, they will struggle to sustain even the best-designed infrastructure. For this reason, funders and backbone organisations must support core costs, coordination, maintenance, technical administration, security review, and staff capacity, not only visible project outputs.

Shared infrastructure is not only about technology. It is about protecting the people, relationships, knowledge, tools, spaces, and systems that keep civil society alive. Technology can support this work, but it cannot replace trust, care, governance, and sustained resources.

The recommended way forward is to start small, build trust through practice, fund maintenance from the beginning, protect smaller and higher-risk organisations, and grow only when governance and capacity are ready. Shared infrastructure should reduce the burden on CSOs, not create another burden. If built carefully, it can help civil society move from isolated survival toward collective resilience.

Directions for further research

This study was deliberately scoped to civil society organisations operating in Malaysia, and its findings reflect that context: a specific funding environment, an "obstructed" civic space, and a particular set of trusted networks. Several questions fall outside that scope and would benefit from further work.

The first is comparative. Future research could examine how civil society groups in other countries, particularly those facing similar political pressures, sustain shared resources over time, and how far collective and cooperative models of ownership, well-established in

other sectors but rarely tested in civil society infrastructure, can be adapted to the Malaysian context. This would allow CSOs to learn from working examples rather than designing governance from scratch.

A second direction would move from descriptive research toward applied research. Rather than only mapping needs and risks, future work could pilot one element of the starting package with a small group of organisations and study what happens in practice: how governance rules hold up, where coordination breaks down, what maintenance really costs, and what makes participants trust or abandon a shared arrangement. This learning-by-doing approach would turn the recommendations in this report into tested practice and generate evidence that funders and CSOs can use to decide what is worth scaling.

A third direction looks not outward to other countries but inward, to grassroots and Indigenous communities that have sustained collective organising for decades without formal structures, project funding, or digital systems. The Jaringan Kampung Orang Asli Semenanjung Malaysia (JKOASM), a network of Orang Asli villages spanning multiple states and tribes in Peninsular Malaysia, has advocated for ancestral land and Indigenous rights for well over a decade, coordinating across great distances and sustaining collective action grounded in customary law and traditional belief rather than in offices, grants, or technology. Community-owned structures of this kind, held together by shared values, kinship, and long-term commitment, embody a form of resilience that formal CSOs often struggle to maintain. Research into how such networks organise, make decisions, pass on knowledge, and endure could offer civil society valuable lessons about what makes collective infrastructure last, lessons rooted in local and Indigenous practice rather than imported models.

Finally, there is scope to build on existing local capacity. Sinar Project, recognised in this study as a trusted civic-tech and digital-rights actor within the wider network, is a natural partner for continuing this work, whether by translating the proposed Resource-Sharing Protocol into concrete tools and pilots, providing the technical administration and documentation support interviewees identified as missing, or helping host and govern early shared services in a way that keeps ownership distributed across the network. The precise shape of that role would be an early task for any follow-on phase, developed with the organisations involved rather than decided in advance.

Appendix A: Interview Log

Identifying columns have been generalised to protect respondents. Two pairs of interviews come from the same organisations (INT-06/INT-07 and INT-08/INT-09).

ID	Org type	Org size	Key themes raised
INT-01	Human rights (finance/admin)	Small–medium	Accounting/compliance friction; e-invoicing; no internal IT; pooled subscriptions; funding loss
INT-02	Human rights (programme)	Small	Physical-raid unpreparedness; lack of backups; trust/principle barriers; digital audit; resource pooling
INT-03	Media freedom / digital rights (finance)	Small–medium	ERP and email friction; fragmented storage; off-shore servers; website compromise; technical capacity as primary barrier
INT-04	Youth/democracy / legal reform (leadership)	Small–medium	Institutional-memory loss; donor-imposed tools; sunset clauses; e-invoicing risk; governance of shared access
INT-05	Digital rights / civic tech (KM lead)	Small	Self-hosting without IT support; key-person dependency; shared help desk / SOC; shared hosting; automation
INT-06	LGBTQI advocacy	Small	Remote-team friction; varied security protocols; shared databases; cost burden of paid tools; legal risk from public content
INT-07	LGBTQI advocacy	Small	Brute-force attacks; doxxing/surveillance; manual security; redundancy (Plan A/B); fear of data leaks in sharing
INT-08	Film/media (programme)	Small	~100 hard drives; donor-imposed tools; pooled subscriptions; off-site encrypted backup; need for technical administrator; raids
INT-09	Film/media (leadership)	Small	Equipment-sharing with sign-out forms; offshore open-source server; physical hub; verbal-only policies; state investigation fears.

Appendix B: Cross-Interview Comparison Matrix

This matrix is the evidence base for the findings section. “Y” = yes, “P” = partial, “N” = no.

Theme / question	01	02	03	04	05	06	07	08	09
Existing resource sharing (Y/P/N)	P	P	Y	P	Y	Y	P	Y	Y
Donor- or partner-imposed tools	Y	P	Y	Y	N	P	P	Y	Y
Dedicated internal IT capacity	N	N	N	N	N	N	N	N	N
Digital security posture (strong/basic/none)	Basic	Basic	Strong	Basic	Basic	Basic	Strong	Basic	Basic
Experienced a security/ physical incident	N	Y	Y	Y	N	Y	Y	Y	Y
Lost access when the funding/project ended	Y	Y	P	Y	Y	P	P	Y	P
Automation / AI interest	N	N	Y	N	Y	N	N	P	N
Wellbeing / key-person concern	N	P	P	Y	Y	P	P	N	P
Most-desired shared resource	Sub./DB	Audit	Hosting	Hub/ exp.	Helpdesk	DB/subs	Server	Subs/backup	Hub/server
The top-named barrier to sharing	Cost	Trust	Tech	Gov.	Cost/cap.	Cost	Data risk	Tech	Tech
Primary sustainability concern	Funding	Funding	HR/cap.	Donor dep.	Key person	Funding	Security	Funding	State risk

Reading the Matrix: Every interviewed organisation lacks dedicated internal IT, most have experienced an incident, and most have lost access when funding ended. The most frequently named barriers are technical capacity, cost, and governance, rather than an unwillingness to share. The most desired resources cluster around shared hosting and servers, pooled subscriptions, shared help-desk or security services, and a shared hub. Interest in automation and AI is concentrated in the most technical organisations, while wellbeing and key-person concerns appear most sharply where survival rests on one or two people.

Appendix C: Digital Sovereignty Readiness Assessment

As part of this study, civil society organisations in Malaysia were invited to complete Sinar Project's Digital Sovereignty Readiness Assessment, an instrument adapted from the Red Hat readiness model for civil society needs. The assessment measures the extent of an organisation's practical control over its data, systems, and digital infrastructure across seven domains. Three organisations completed the assessment. Their responses are presented here in an anonymised form, identified only by the broad area of work.

Participation was voluntary, and respondents consented to the use of their anonymised data for research. With only three responses, the results are illustrative rather than representative; they are included to complement the interviews with a structured, comparable snapshot of digital sovereignty readiness.

Participating organisations

The three respondents were a research-focused CSO and a legal and human rights CSO, both based in the Klang Valley / Peninsular Malaysia, and an advocacy organisation based in East Malaysia (Sabah). Two had between six and ten staff; the third had fewer than five. All identified their profile as civil society.

Anonymised label	Area of work	Location	Staff size	Respondent role
Research CSO	Research	Peninsular (WP)	6–10	Head of Organisation
Legal & human rights CSO	Legal and human rights	Peninsular (WP)	6–10	Project staff
East Malaysia advocacy CSO	Advocacy and rights	Sabah	Under 5	Head of Organisation

Overall readiness

Overall weighted scores were low across all three organisations, ranging from 15% to 47%. The East Malaysia advocacy CSO scored highest at 47% (Defined), the research CSO followed at 27% (Managed), and the legal and human rights CSO scored 15% (Initial). The weighting reflects the relative importance assigned to each domain, with data, operational, and open-source sovereignty weighted most heavily.

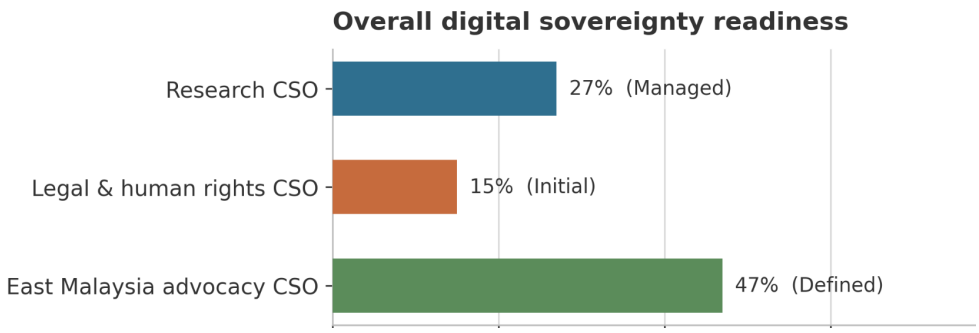

Figure C1. Overall weighted digital sovereignty readiness score by organisation.

Readiness by domain

The domain breakdown shows that strengths and weaknesses were unevenly distributed, with no single organisation strong across the board. The research and legal & human rights CSOs scored highest on data sovereignty (both 67%) but had little or no operational, open-source, or executive-oversight readiness. The East Malaysia advocacy CSO showed almost the reverse pattern: full marks on technical sovereignty (100%) and moderate-to-good scores on operational, open-source, and executive-oversight readiness (each around 67%), but no measured data-sovereignty controls (0%). Managed services were weak across all three, scoring zero for two organisations and 33% for the third.

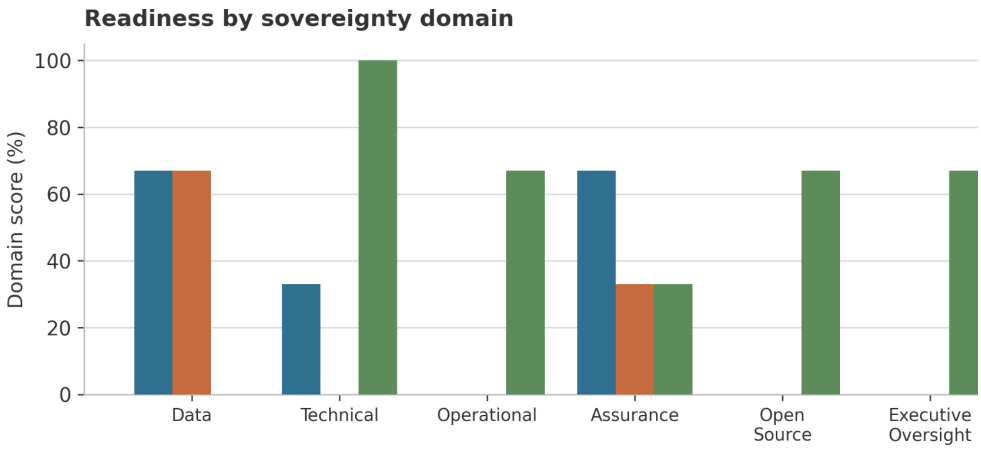

Figure C2. Readiness across the seven sovereignty domains, by organisation.

Domain scores in detail

The table below reproduces the per-domain results in the assessment's own format, showing the raw score out of three, the domain weighting, and the resulting percentage for each organisation.

Domain (weight)	Research CSO	Legal-empowerment CSO	East Malaysia rights CSO
Data Sovereignty (2.0x)	2/3 —67%	2/3 — 67%	0/3 — 0%
Technical Sovereignty (1.5x)	1/3 — 33%	0/3 — 0%	3/3 — 100%
Operational Sovereignty (2.0x)	0/3 — 0%	0/3 — 0%	2/3 — 67%
Assurance Sovereignty (1.0x)	2/3 — 67%	1/3 — 33%	1/3 — 33%
Open Source (2.0x)	0/3 — 0%	0/3 — 0%	2/3 — 67%
Executive Oversight (1.0x)	0/3 — 0%	0/3 — 0%	2/3 — 67%
Managed Services (1.5x)	1/3 — 33%	0/3 — 0%	0/3 — 0%
Overall (weighted)	27% — Managed	15% — Initial	47% — Defined

Results

Three patterns stand out. First, no organisation scored above 50% overall, suggesting that digital sovereignty, meaning genuine control over where data lives, who can access it, and whether systems can keep running if a provider or platform becomes unavailable, is an early-stage concern for these groups. Second, the strengths are mirror images: the Peninsular organisations were stronger in data handling but weaker in technical and operational independence. In contrast, the East Malaysia organisation was technically self-reliant but had not formalised data controls. This suggests that organisations could learn a great deal from one another, which is precisely the kind of exchange shared infrastructure is meant to enable. Third, managed services scored low across all three, reinforcing the study's broader finding that the gap is less about tools than about sustained technical support for running them.

Two respondents also marked individual questions as "don't know," covering disaster-recovery planning for geopolitical scenarios, data-residency compliance, and awareness of national sovereignty standards. These gaps in awareness are themselves a finding: several of the controls the assessment asks about were unfamiliar, which points to a need for plain-language guidance as much as for technical capacity.

Source: Sinar Project Digital Sovereignty Readiness Assessment (dsra.sinarproject.org), responses collected June 2026. Organisation names have been removed and replaced with descriptive labels.

Appendix D: Use Cases

These use cases document recurring day-to-day workflows drawn from the interviews (INT-01 to INT-09). They follow a standard use-case format and are intended to ground the report's findings and the proposed resource-sharing protocol in concrete operational practice. The revision history below applies to all five.

Version	Date	Description	Author
Initial Documentation	2026-06-29	Initial use cases from interviews	Khairil Yusof, Sinar Project

Use Case: Project Coordinator - Coordinating Programme and Events

Primary Actor:

Programme Coordinator

Stakeholders and Interests:

- Organisation head - Progress and status on project implementation
- Funders - Progress and status on project implementation

Preconditions:

- Internet Access for both parties
- Mobile Phone with WhatsApp

Success Guarantee (Postconditions):

Able to successfully follow up on project implementation coordination tasks with partners.

Main success Scenario (Basic Flow):

1. Review the checklist of follow-up tasks with partners, including the calendar
2. Communicate with partners on the status of the task through WhatsApp and email
3. Coordination task completed with partners

Extensions (Alternate Flows):

2. Follow up in person if unable to contact remotely

Special Requirements:

- Must keep coordination and event participation to share with donors and funders.
- Must use WhatsApp as the main form of communication due to widespread use by partners and beneficiaries

Technology and Data Variations List:

- Use of WhatsApp
- Email for more secure communications, and use Proton Mail

Frequency of Occurrence:

- Multiple times daily

Open Issues:

- Need more information from the user on the specific details of the coordination tasks.
- Danger of doxxing from the use of WhatsApp and confiscation of mobile phones
- Transient nature of WhatsApp content, and possible loss of data vs email
- UI of Google Workspace is complicated and messy, making it difficult to find things, including calendars and events

- Shared tools for coordination would be helpful, but also risky, as a single point of failure
- A resource pool for LGBTQ groups to seek mental health services with other partners
- Access to the website backend due to also being a designer, which is under constant brute force assault

Use Case: Administrative/Finance Officer - Manage and update project operations status

Primary Actor:

Administrative and Finance Officer

Stakeholders and Interests:

- Organisation head - Interested in the status of the project, including resources allocated and spent
- Statutory compliance bodies (SSM, KWSP, etc.) - Project and organisational resources.
- Funders and donors - Project implementation status and financials

Preconditions:

- Internet connection
- ERP system online
- Vendor hosting for email

Success Guarantee (Postconditions):

- Able to review tasks by email and manage project deliverables and finances on a custom open-source ERP system

Main success Scenario (Basic Flow):

1. Log in to the office virtual workspace
2. Check emails for pending tasks
3. Log in to the ERP system and update the status of projects, resources and expenditures

Extensions (Alternate Flows):

None specified.

Special Requirements:

None specified.

Technology and Data Variations List:

- Use of customised open source ERP system (undefined)
- Use of email hosting services from a local hosting provider
- Company Limited by Guarantee (CLBG) financial reporting requirements

Frequency of Occurrence:

Daily, multiple times.

Open Issues:

Any open-ended issues and questions related to this user story

- Open source ERP was used, and customisations were not shared
- Mentioned that workflows for ERP project management may not match existing workflows and cause friction,
- The email provider doesn't provide other productivity services and integrations such as a calendar and syncing to mobile devices

- Due to a lack of internal IT support, a joint support group was raised, but the user is unaware that such a group already exists (FOE Cluster IT working group)
- Use of locally hosted and custom open source solutions, but without dedicated in-house IT support. This is a high-risk issue. What are the current arrangements for technical support and maintenance?

Use Case: Coordinator/Director - Collaborating and Sharing Media Content with Partners

Primary Actor:

Organization Coordinator

Stakeholders and Interests:

Project and Network Partners - Coordination of project implementation and events.

Project Partners - Access to media content

Preconditions:

- Local or cloud storage space for videos
- Online video sharing platforms Cinemata, Vimeo, and YouTube

Success Guarantee (Postconditions):

- Able to upload and share project media and documents with partners for the duration of the project
- Able to download online shared project media and documents, to save to offline storage and remove online

Main success Scenario (Basic Flow):

1. Coordinate with partners on media and project documents created by partners or by the user
2. Share media on a cloud platform with private access to partners only
3. Upon completion of a project, download it to external storage and delete it from cloud storage to free up space.

Extensions (Alternate Flows):

2. Possible loss of cloud storage services such as Google, to fall back to self-hosted Cinemata or file-sharing services.

Special Requirements:

Require secure, private, shared storage spaces for each project and for managing partner access.

Technology and Data Variations List:

- Google Drive services are currently implemented with paid storage for sharing project media and documents
- Cinemata, Vimeo for uploading videos
- Offline copies of videos and media are stored on various external storage devices
- Signal for messaging, WhatsApp for community communications.
- Use of Adobe Premiere Creative Suite

Frequency of Occurrence:

Daily.

Open Issues:

- Staff prefer using Canva, but there are no licenses for it. Willing to use own money to accomplish tasks in Canva. Explore open source options.
- Meetings and coordination with a very large number of partners (40+) are required to do this daily task.
- High external storage costs may affect this use case. If hosted, the user requires private, secure storage spaces.

Use Case: Coordinator - Project management reporting

Primary Actor:

Head of organization/Coordinator

Stakeholders and Interests:

- Funders - Interested in good project documentation
- Board of Directors - To review whether the organisation is run well

Preconditions:

- Access to documentation and files needed for project documentation, both digital and hard copy

Success Guarantee (Postconditions):

Project documentation on the status of project activity implementation and impact is sufficiently complete to satisfy the reporting requirements of funders and other stakeholders.

Main success Scenario (Basic Flow):

1. Review the calendar for upcoming meetings and project deadlines
2. Meeting with the team to organise project tasks and priorities
3. Collecting information and documentation needed to write project reports
4. Write project reports with complete supporting documentation

Extensions (Alternate Flows):

3. Documents missing or inaccessible. Reporting is still done, but incomplete.

- Additional time to track down missing documents.

Special Requirements:

None specified.

Technology and Data Variations List:

- Data and documentation needed for reporting are shared, but the details of the data and the required documentation are not provided.

Frequency of Occurrence:

- Daily. Any delays and problems are compounding.

Open Issues:

Any open-ended issues and questions related to this user story

- Lack of documentation and playbooks for proper project documentation for new staff
- Project documentation is incomplete, missing or not captured

- Project documentation can be stored on messaging apps like WhatsApp
- Meetings take up a lot of time. This is a recurring issue.
- Running out of storage on laptop
- Need samples of project reporting documentation to analyse user requirements.

Use Case: Project Manager and Event Coordinator - Publish website content (Video)

Primary Actor:

Website Content Manager (Primary role as Project Manager)

Stakeholders and Interests:

- Organisation head - Project content is published and disseminated online on websites and social media
- FOE Cluster partners - Joint project content is published and disseminated on social media channels and campaign websites
- Lead campaigner - Videos are edited and published online
- Implementing partners - Access to raw video material and music

Preconditions:

- Internet connection
- Working website and hosting server
- Adobe Cloud / Premiere Pro subscription
- The laptop is good enough to run video editing software

Success Guarantee (Postconditions):

Successfully edit video to upload to website or social media for campaigns

Main success Scenario (Basic Flow):

1. Coordinate with campaign partners for content and communication items
2. Edit graphics and videos on a laptop
3. Coordinate with campaign managers and partners on video publication.
4. Publish on website and social media outlets.

Extensions (Alternate Flows):

None specified.

Special Requirements:

None specified.

Technology and Data Variations List:

- Adobe Cloud and Creative Tools
- Laptop hardware capable of editing videos
- Upload to platforms including YouTube, Cinemata and Vimeo
- Bitwarden to manage passwords. Passwords are changed once a month for security.

Frequency of Occurrence:

How often is this task done? It provides insights into scalability, staffing and technical requirements.

Daily.

Open Issues:

- Using their own accounts for Adobe Premiere Pro, an office license only for 2 computers at a time, but the user and others are already familiar with it
- Using own computer, which is underpowered, the office MacBook is shared
    - Need better equipment for video editing, such as large monitors
- This user is also managing backups, which are currently on physical devices
- WhatsApp is the main software for communications
- Older project videos and outputs are stored on a network-attached storage (NAS). Still, newer projects are stored on various external storage devices such as portable hard disks or SSD, which are tracked manually.
    - Related issue: AI consumer storage shortages and costs should be raised as a potential issue for this use case
- Multiple roles, which could be further split into different use cases
- Learning new video editing software such as DaVinci Resolve is a barrier
- Shared subscriptions/sponsorship model suggested. Frustrated with workarounds because no budget for some services/software
    - (Interviewee asked a question about whether this has been done anywhere else). Yes. Code4All has a solution in which they negotiate with Adobe for several free licenses for members.
- WiFi is poor; prefer wired Ethernet for better devices.No IT staff to implement better networking equipment.

Appendix E: External Resources, Tools, and Platforms

Background and context sources

1. Malaysiakini – Operasi Lalang: news archive on the 1987 Operasi Lalang arrests, cited for historical context on civic repression (https://www.malaysiakini.com/news/399846)
2. CIVICUS Monitor – Malaysia: civic space rating and country profile for Malaysia (rated "obstructed") (https://monitor.civicus.org/country/malaysia/)
3. OHCHR – Foreign aid cuts report (2025): UN report on how foreign aid cuts threaten the global human rights ecosystem (https://www.ohchr.org/en/stories/2025/09/report-foreign-aid-cuts-threaten-global-human-rights-ecosystem)
4. CIVICUS – 2025 State of Civil Society Report: annual global review of civic space and civil society trends (https://publications.civicus.org/publications/2025-state-of-civil-society-report/)
5. OECD – Cuts in Official Development Assistance (2025): analysis of declining global development aid (https://www.oecd.org/en/publications/2025/06/cuts-in-official-development-assistance_e161f0c5/full-report.html)
6. Freedom House – Freedom on the Net 2025: global report on internet freedom and pressure on encrypted and anti-censorship tools (https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet)

Documentation and data tools

7. Bayanat: open-source human rights data and documentation platform (https://bayanat.org/)
8. Uwazi: open-source database tool for organising human rights information, cases, and evidence (https://uwazi.io/)

9. HURIDOCS – Uwazi initiative: HURIDOCS programme developing and supporting the Uwazi documentation tool (https://huridocs.org/initiatives/developing-uwazi-a-human-rights-database-tool/)

Secure hosting, digital security, and rapid response

10. Qurium / Virtualroad.org: attack-resilient secure hosting, DDoS protection, and digital forensics for media and rights groups under attack (https://www.qurium.org/)
11. Digital Defenders Partnership (DDP): digital protection fund and support network for civil society, hosted by Hivos (https://www.digitaldefenders.org/)
12. Access Now Digital Security Helpline: free 24/7 incident response and digital security advice for civil society, journalists, and activists (https://www.accessnow.org/help/)
13. CiviCERT: trusted network of civil society digital security responders and infrastructure providers (https://www.civicert.org/)
14. Amnesty International Security Lab – Resource Hub: digital security resources, risk analysis, and helpline referrals for civil society and HRDs (https://securitylab.amnesty.org/digital-resources/)

Technology advisory

15. The Engine Room: research, advice, and practical support on responsible technology, data, and tool choices (https://www.theengineroom.org/about/)

Hosting and open/cooperative technology

16. Greenhost: mission-driven ethical web hosting, VPS, and secure internet services (https://greenhost.net/)
17. May First Movement Technology: member-run cooperative providing movement technology infrastructure, hosting, and collaboration tools (https://mayfirst.coop/)

18. Co-op Cloud: cooperative open-source software stack for self-hosting apps such as Nextcloud, WordPress, and Jitsi (https://coopcloud.tech/)

Fiscal hosting and pooled funds

19. Open Collective – Fiscal Hosting: legal and financial infrastructure for groups to receive and manage funds transparently (https://opencollective.com/fiscal-hosting)
20. Platform 6 – Fiscal Hosting: cooperative fiscal hosting model using Open Collective infrastructure (https://platform6.coop/platform-6-fiscal-host-open-collective)
21. Tides: fiscal sponsor and administrative host for nonprofit and social-purpose projects (https://www.tides.org/)
22. Start Network – National Start Funds: membership-owned pooled rapid funding for locally led action (https://startnetwork.org/funds/national-start-funds)

Shared space

23. Community Spaces Network: peer learning, tools, and resources for developing nonprofit shared and community spaces (https://communityspaces.org/about-us/)

Media platforms

24. Cinemata (EngageMedia): secure, open-source, ad-free, privacy-respecting video platform for social and environmental films in Asia-Pacific (https://cinemata.org/)

Local civic tech (Malaysia)

25. Sinar Project: Malaysian civic-tech and digital-rights organisation; research collaborator on this study (https://sinarproject.org/)
26. Sinar Project – Enabling Tech: civic-tech capacity building and digital-rights support bridging technologists and civil society (https://sinarproject.org/projects/enabling-tech)

Regional networks, coordination, and care

27. Association for Progressive Communications (APC): international membership network for the strategic use of ICTs for social justice (https://www.apc.org/en/about/who-we-are)
28. FORUM-ASIA: regional human rights network providing advocacy, solidarity, and human rights defender support (https://forum-asia.org/)
29. APCASO: regional community systems network supporting marginalised communities across Asia-Pacific (https://apcaso.org/about-us/)
30. Urgent Action Fund Asia & Pacific: feminist rapid-response fund and well-being support for women and non-binary activists (https://uafanp.org/)
31. NEAR Network: Global South network of local and national CSOs promoting local ownership and collective power (https://near.ngo/)
32. Numun Fund: feminist fund supporting feminist technology infrastructure and movement organising in the Global South (https://numun.fund/)

Emergency assistance

33. Lifeline Embattled CSO Assistance Fund: emergency financial assistance, rapid response, and resiliency grants for CSOs under threat (https://freedomhouse.org/programs/emergency-assistance-and-thematic-programs/lifeline-embattled-cso-assistance-fund)

Collective governance and community models

34. The PurpleCode Collective: Indonesian feminist collective working at the intersection of feminism, human rights, and technology (https://home.purplecodecollective.net/wp/)
35. JKOASM (Jaringan Kampung Orang Asli Semenanjung Malaysia): network of Orang Asli villages advocating for

ancestral land and Indigenous rights in Peninsular Malaysia (https://ms.wikipedia.org/wiki/Jaringan_Kampung_Orang_Asli_Semenanjung_Malaysia)

Emerging, public-goods, and decentralised funding models (exploratory only)

36. Ethereum – DAO explainer: introduction to decentralised autonomous organisations and participatory treasury governance (https://ethereum.org/dao/)
37. Ethereum Foundation – Ecosystem Support Program (ESP): grants and support for free, open-source, public-goods projects (https://esp.ethereum.foundation/applicants)
38. Filecoin Foundation – FIL Public Goods Funding: grants for tools, research, storage, and data infrastructure (https://fil.org/grants)
39. Gitcoin Grants / Quadratic Funding: community-backed matching grants and quadratic funding for public goods and open-source projects (https://gitcoin.co/mechanisms/quadratic-funding)
40. Big Green DAO: nonprofit-led philanthropic DAO using democratic grantmaking for grassroots food organisations (https://dao.biggreen.org/home)
41. Big Green – Grantmaking: Big Green's community-driven grantmaking model (https://biggreen.org/grantmaking/)
42. Filecoin Foundation for the Decentralized Web (FFDW): foundation supporting decentralised-web tools for public-interest and human rights projects (https://ffdweb.org/)
43. WITNESS × FFDW: collaboration using decentralised-web tools to authenticate and preserve human rights records (https://www.witness.org/ffdw-and-witness-collaborate-to-preserve-authentic-human-rights-records/)
44. Rohingya Project × FFDW: collaboration preserving Rohingya cultural heritage materials using decentralised storage (https://ffdweb.org/blog/ffdw-and-rohingya-project-working-together-to-empower-cultural-preservation-and-digital-legacy)