DIGITAL RESILIENCY GRANTS

CIVICUS CRISIS RESPONSE FUND AND DIGITAL DEMOCRACY INITIATIVE

GUIDELINES AND PROTOCOLS

Why the Crisis Response Fund?

CIVICUS is guided by the 2022 - 2027 Strategic Priorities identified through an extensive consultation process. These Strategic Priorities are to 1) generate timely knowledge and analyses, 2) coordinate targeted advocacy, 3) contribute to stronger emergency and sustained support ecosystems, 4) strengthen public discourse on civic space and reinforce, and 5) build counter-power with the most affected groups and their movements. The Crisis Response Fund (CRF) supports these priorities by mobilising quick, principled and effective responses to events that threaten civil society's fundamental rights to collectively express, associate and organise.

While some threats develop gradually, others materialise swiftly and require an immediate response. The CIVICUS Crisis Response Fund, setm up by CIVICUS in 2007, serves as a mechanism for mobilising quick, principled and effective responses to events threatening civil society's fundamental rights to collectively express, associate and organise. In 2011, CIVICUS joined a coalition of seven international civil society partners administering Lifeline, an emergency fund for civil society established multilaterally by 19 donor governments and independent foundations, to provide additional financial and technical support to embattled civil society around the world.

What is the Digital Democracy Initiative?

The Digital Democracy Initiative (DDI) is an ambitious global effort funded by the Danish Ministry of Foreign Affairs (MFA) and the European Union and implemented in partnership with Access Now, CIVICUS, Digital Defenders Partnership and Global Focus. The Digital Democracy Initiative, launched in March 2023, aims to strengthen and safeguard inclusive democracy under pressure in the digital age by supporting civil society actors, particularly in the Global South, experiment, learn and take action, as well as access and build infrastructure and support ecosystems that help them leverage their digital capacities and resilience.

What are the digital resiliency grants provided by the Crisis Response Fund and the Digital Democracy Initiative?

To help civil society adapt to the new challenges of promoting civic space and more inclusive democracy in the digital age, CIVICUS is deepening and broadening the reach of the Crisis Response Fund by including new digital resiliency grants in collaboration with the Digital Democracy Initiative. These grants are meant to support civil society organisations (formal and informal), groups and social movements facing imminent civic space restrictions, struggles, threats and barriers which prevent them from continuing their work towards more inclusive democracy in domestic and regional settings.

These are rapid-response resiliency grants that provide up to USD 10,000 (ten thousand American dollars) for one organisation submitting a funding application alone, and up to USD 20,000 (twenty thousand American dollars) for joint applications between two or more organisations. The grants must be used in under six months. It is expected to award between 30-40 CRF-DDI digital resiliency grants in 2024.

Guidelines for the use of the CRF-DDI digital resiliency grants

The CRF-DDI digital resiliency grants aim to protect the civil society sector, as a whole, against systemic and imminent threats to its existence and work towards inclusive democracy, with a specific focus on protecting the rights to freedom of assembly, association and expression and responding challenges related to civic engagement in the digital age and responses that use digital technology to counter the threats.

This funding will be used in cases that require immediate action to forestall imminent threats. Although responses should be as immediate as possible, CIVICUS evaluates when, why and how it should respond to particular situations. If the situation under review makes us answer YES to the following questions, CIVICUS will then have sufficient justification to mobilise the Fund's resources:

1. Is it a crisis that requires action to enhance the resilience of civil society actors?
2. Are there systemic threats to civil society?
3. Will our actions be beneficial?
4. Are the proposed actions and initiatives implementable?

1. Is it a crisis?

It is a crisis if the case can be categorised as one of the following:

- Significant deterioration of civic space in the areas of freedom of assembly, association and expression that affect civil society promoting more inclusive democracy in the digital age: for example, urgent response is necessary to prevent the curtailment of civil society activities because there are enough indications that restrictions on civil society are imminent.

- Escalation of existing threats to civil society promoting more inclusive democracy in the digital age: for example, civil society is already suffering from restrictions on its activities. This includes cases where civil society activity has been recently curtailed and situations involving a growing number of threats over a period of time.

2. Are there systemic threats to civil society?

Systemic threats to civil society include those which undermine civil society, in general, in the country or region. This also includes threats to specific sectors of civil society, for example women's groups, environmental organisations, and indigenous movements, among others. An individual attack on an activist would not generally be considered a systemic threat; however, numerous attacks on activists could be part of a campaign to intimidate civil society groups, which would then be considered systemic.

3. Will our actions be beneficial?

In addition to deciding whether a situation has become a 'crisis', we must assess whether a response by CIVICUS will be of assistance and have a positive impact. This must always be considered in consultation with local partners or members where they exist. In countries where CIVICUS does not have members or partners, CIVICUS will consult with other international organisations working on the ground.

In evaluating potential positive impact, some of the criteria to consider are:

- Security: Will our actions place CIVICUS' staff or local members, partners or civil society in general in greater danger?
- Local actions: Will our actions complement and enhance or undermine the work of local civil society?
- Presence of other international actors: Are other international actors already working on this crisis? Would our involvement provide supplementary assistance or make an additional impact?
- Strategic value: Is the country able to influence other countries in the region? Will CIVICUS' work in this country have a positive impact externally or only within the country?

4. Are the proposed actions and initiatives implementable?

The CRF-DDI digital resiliency grants are open to funding responses in contexts where actors can receive and utilise resources towards achieving project goals and objectives. We would not be able to provide support if actors were based in countries or locations where it is just not possible to transfer funding or in a context where the implementation of the grant is not realistic or could place actors in greater danger. For example, this could be the case in some countries where civic space is rated “closed”.

What is the response?

The CRF-DDI digital resiliency grants support the implementation of resiliency responses or activities that proactively avoid and mitigate imminent civic space restrictions, struggles, threats and barriers and/or “help civil society continue to do work” towards more inclusive democracy. These responses could focus on helping mitigate digital threats, threats to digital civic rights, threats to civic engagement and inclusive democracy in the digital space, and broader civic space threats that could be countered or mitigated by using digital technology and building digital resilience.

Prospective resiliency responses or activities under the CRF-DDI digital resiliency grants are envisaged to be under six months in duration and could include (but are not limited to):

- Responses to help civil society actors at risk for their in-person activities start mobilising safely in online spaces to be able to continue their work. This could include training but also creating online spaces and other infrastructure to work in the digital space.
- Training in digital security, digital skills and other relevant areas (for example, training on digital well-being and resilience, which focus on learning how to maintain a healthy relationship with digital technology for civic engagement, understand its positive and negative impacts and develop strategies to cope with challenges) for civil society organisations to build their skills in safely using digital technologies to strengthen civic space and promote inclusive democracy.
- Digital security assessments to help organisations and groups identify digital risks they face and provide expert-led guidance, accompaniment and capacity support to address them.
- Equipment, licenses and other tech tools to strengthen the digital security and protection of the civil society organisation or group at risk.
- Legal and other responses to directly counter online attacks and harassment and criminalisation and prosecution of online expression.

- Psychosocial support in case of online attacks and harassment and to build digital well-being and resilience of civil society actors at risk.
- Responses to promote digital access and equality particularly among marginalised civil society groups and when digital exclusion represents a risk or threat to their work and rights.
- Preemptively creating a strategy to respond to the threat of local restrictive legal and regulatory frameworks that risk the exercise of civic freedoms and rights in the digital space.

What cannot be funded?

- The CRF-DDI digital resiliency grants are designed to protect the civil society sector against systemic threats but do not provide emergency assistance for critically urgent situations that require immediate support. Partners can expect a 4–6-week turnaround in processing their application, contracting and initial disbursement of funds.
- The CRF-DDI digital resiliency grants do not provide resources for individuals. When possible, these cases will be referred to CRF partners, including the Freedom House and Frontline Defenders. Click here to read more about the funds available to individual human rights defenders under the Lifeline Embattled CSO Fund.
- The CRF-DDI digital resiliency grants do not fund responses for advocacy activities or other projects that are not specifically resiliency responses to threats as detailed in this document and do not provide core organisational funding.

Who can apply for a grant?

The use of the CRF-DDI digital resiliency grants can be proposed by any civil society organisation, group, movement and collective working towards inclusive democracy and facing a situation of crisis that meets all the following eligibility criteria:

- Applicants must be a local civil society organisation, group or social movement (formal or informal) working to expand civic and democratic freedoms and promote inclusive democracy in the digital age.
  - Our definition of local civil society: diverse civil society actors (individuals, organisations, human rights defenders, grassroots groups, among others) established and operating in their own country, led by and primarily accountable to the local constituents they serve or represent.
  - Priority is given to unrepresented or marginalised actors, including women, youth, informal civil society, grassroots groups and LGTBIQ+ groups, among others.

- Applicants must be based in a global south country receiving Official Development Assistance from the Organisation for Economic Co-Operation and Development's Development Assistance Committee (click here to check the list of countries).
    - Priority is given to countries where civic freedoms are restricted, particularly those with "Obstructed" and "Repressed" civic space ratings, according to the CIVICUS Monitor. Review the CIVICUS Monitor ratings: https://monitor.civicus.org/

- Applicants must be facing a verifiable imminent civic space threat or emergency or a need for enhanced digital resiliency to ensure effective civil society action towards inclusive democracy. Evidence of the risk from the last three to six months is required.
    - Our definition of imminent threat or need: real danger that is likely to occur or about to happen almost immediately or in a very short period of time. An imminent need is something necessary to do or get almost immediately or in a very short period. Applicants do not have to be in a severely critical situation to be eligible.

- Proposals must be for resiliency activities and responses that help avoid, counter, mitigate and/or navigate civic space threats to civil society actors promoting inclusive democracy or civil society at large by using digital technology or activities to enhance their digital resilience. Responses/proposals for advocacy activities, core funding and other purposes are not accepted.
    - Our definition of resiliency activities and solutions: those that are designed to help civil society actors cope with imminent challenges and crises and continue doing their work.

- Responses/proposals should be implemented in under six months.

- Applicants must have an organisational bank account with the ability to receive funds from a CIVICUS bank account based in the United States of America. If an appropriate organisational bank account does not exist, the applicant can submit a written request to use a fiscal sponsor or receive funds into an alternative account.

- Applicants must be able to plan and track the use of CRF-DDI grant funding. This includes providing receipt-based financial reports to CIVICUS every month.

- Applicants should not have received funding from the CIVICUS Crisis Response Fund in the last two years.

*Applicants do not need to be CIVICUS members or partners to apply for the grants, but members and partners are welcome to apply.

Protocols for the use of CRF-DDI digital resiliency grants

Interested applicants must follow these steps to apply for a CRF-DDI digital resiliency grant and use the funds if approved:

- Requests will be submitted via the online form available on the CRF-DDI digital resiliency grants webpage and should provide all necessary information to allow the request to be properly evaluated.
- Only in circumstances where partners feel unsafe or do not have access to the internet, they can either submit an application via this email: ddiresiliencygrants@civicus.org.
- Important budget regulations: partners can apply for personnel and other core overhead costs (such as rent) in their funding request. Given that the grants prioritise an emergency and urgent response, the majority of funds (60%) requested must cover project activities for implementation. Subsequently, up to 30% of the budget can be dedicated to personnel and up to 10% to other overhead costs.
- Requests will be evaluated by the CRF-DDI team according to the eligibility criteria presented above. Relevant partners and members will be consulted in evaluating the requests.
- Applicants who do not meet the eligibility criteria will be notified and, when possible, referred to funding partners in our networks.
- Eligible applications will go through careful review and due diligence. The CRF-DDI team will be in touch with the applicant and might request additional information and small modifications to the proposed activities and budget.
- If the review and due diligence are not successful, the applications will be rejected.
- Applications successful in the review and due diligence processes will be approved. Applicants will be notified and start the contracting process. Contracts will detail the project activities, budget, deadlines, reporting requirements and any other detail regarding the sub-granting agreement.
- Payments: the CRF-DDI digital resiliency grants are issued through a tranche system. Upon signing the sub-partnership agreement, partners receive a first tranche payment of 40% of the grant. After submitting interim progress reports (narrative and financial), a 30% payment is disbursed. The remaining 30% is paid after summitting the final narrative and financial reports. Payments are usually received within 14-20 working days after approving the reports.
- Reporting requirements: partners are required to submit monthly financial and narrative updates and participate in monthly check-in calls; one or two interim financial reports (depending on the length of the grant); final narrative and financial reports and an impact report as part of their undertaking in the implementation of the grant.

- Budget changes: in the event of unforeseen circumstances, partners are permitted to make budget reallocations across each budget line. The total changes must not exceed 10% of the overall budget and must be reported to the CRF-DDI officer. When changes greater than 10% are required, partners must submit an amended budget to the CRF-DDI officer for approval. Partners are not authorised to spend more than the approved budget in the contract.
- Deadline changes: the contract period for CRF-DDI digital resiliency grants is six months. If a partner faces a delay and requires a project extension, they must request it at least one month before the project-end-date registered in the contract. The CRF-DDI team will then decide case-by-case if a no-cost extension is approved.

Cross department and unit involvement in the response

In addition to funding, CIVICUS is able to provide additional support across its clusters for the overall enhancement of envisaged project activities. This may include:

- Identifying partners and networks for additional coordination during the project.
- Identifying possible crises.
- Developing new media contacts in countries and regions where CIVICUS has not worked previously.
- Raising awareness among networks.
- Mobilising partners and networks to support campaigns.
- Providing convening space to address issues.
- Assisting with the development of long-term initiatives in particular countries.

MORE INFORMATION

If you have any questions related to funding applications, please email ddiresiliencygrants@civicus.org

Visit the main webpage of the Crisis Response Fund to explore other funding opportunities: https://www.civicus.org/index.php/what-we-do/defend/crisis-response-fund

Learn more about the Digital Democracy Initiative: web.civicus.org/DDI

WITH THE SUPPORT OF

Co-funded by the European Union

MINISTRY OF FOREIGN AFFAIRS OF DENMARK
Danida