

Draft Report

ccTLD Disaster Recovery Study Group

The Role of IANA in ccTLD Disaster Recovery

Table of contents

1. Executive Summary	4
2. Introduction and Mandate	5
3. Method and Limitations	5
4. The ccTLD BC/DR Landscape	6
4.1 Introduction	6
4.2 BC/DR and the responsibility of the ccTLD manager	7
4.3 Diversity of the ccTLD landscape	10
4.4 IANA's current role	10
4.5 Where the Study Group's question begins	11
5. Exploring the potential role of IANA	12
5.1 Introduction	12
5.2 The five dimensions	13
5.3 Use case summary	13
5.4 Cross-cutting findings	14
6. Possible Framework and the Role of IANA	16
7. Potential Policy Gaps & Areas for Further Exploration	17
8. Recommendations to the ccNSO Council	18
8.1 Basis for the recommendations	18
8.2 Recommendation 1 — No additional policy is needed at this time	19
8.3 Recommendation 2 — Further study on temporary measures: caretaker and temporary transfer	20
8.4 Observations from the study group	21
ANNEX A Diversity of the ccTLD Landscape	22
Governance Models	22
Operational Model: From completely Outsourced to In-House	22
Size: Domains Under Management	23
The External BC/DR Context Landscape	23
Regulatory Frameworks Affecting ccTLD's BC/DR	23
Impact of Regulatory Frameworks on ccTLDs	24
ANNEX B IANA Fact Finding	30
ANNEX C Use Cases in Detail	34
UC-1 Large Private registry — utility disruption during armed conflict	34
UC-2 Island government ccTLD — total infrastructure collapse	35
UC-3 Academic ccTLD — hurricane and loss of key personnel	36

UC-4 Government registry — prolonged power outage	36
UC-5 Mid-size private registry — political crisis and contested legitimacy	37
UC-6 Large government registry — active war, operator incapacitated	38
ANNEX D References	40
Presentations BC/DR	40
TLD-OPS: Playbook, TTX and Study Group	41
References BC/DR	42
International standards	42
ICANN / ccNSO governance	42
Operational / community reference	42

1. Executive Summary

Why this report

In 2024 IANA asked the ccNSO what role, if any, it should have when a ccTLD suffers a disaster. Following advice from the ccNSO Policy Gap Analysis Working Group (PGA WG), the ccNSO Council established this Study Group to scope the issue and, if warranted, to recommend whether new policy, interpretations or practices are needed. Today there is no documented framework for IANA involvement in ccTLD disaster recovery; past cases have been handled ad hoc.

How the Study Group worked

The Group used a design-thinking approach: it first defined the problem, then tested possible responses against six realistic use cases before converging on recommendations. The evidence base comprised BC/DR definitions and standards, ccTLD experiences shared since 2009, the diversity of ccTLD governance, operating models, size and regulatory environments, and two rounds of fact-finding with IANA. Building on the material collected, 8 use-cases or scenarios were built along five dimensions (regulation, governance, DNS operation, registration service, scale). The use cases were subsequently assessed for what IANA could realistically do.

What was found

Business continuity and disaster recovery are first and foremost the responsibility of the ccTLD manager, including where functions are outsourced. The Study Group's question begins only where a manager's own arrangements fail, are absent or cannot be activated [Section 4.5].

- Preparedness, not the severity of the disaster or the size of the ccTLD, determines whether IANA involvement is needed at all. A well-prepared registry needs almost nothing from IANA even under the most extreme circumstances; an unprepared registry can make IANA the sole actor after man-made or natural disasters. [Section 5.4].
- Pre-arrangements with another ccTLD or trusted entity are the single most effective measure and require no new policy.
- The hardest scenarios concern authority and recognition (contested legitimacy, an incapacitated operator), not technical failure. Existing delegation, transfer and revocation policies were not designed for emergencies, and no clear pathway exists for IANA to take expedited, extraordinary action [Sections 6, 7].

What it recommends [Section 8]:

1. The Study Group concludes that no additional ccNSO policy is required at this stage with respect to the role of IANA in ccTLD disaster recovery Policy would act on the wrong lever; the real leverage lies with preparedness before a disaster.
2. The ccNSO Council should commission follow-up study on whether, and by what method, a temporary measure could be made available when a ccTLD manager is not operational. Such measures could include the appointment of a caretaker and/or a temporary transfer of operational functions. Any temporary measure should not serve as a mechanism for resolving contested legitimacy or for bypassing the standard process.

2. Introduction and Mandate

In 2024, IANA raised several concerns with the ccNSO, including questions regarding IANA's potential role in the disaster recovery of ccTLDs.

In May 2025, the Policy Gap Analysis Working Group (PGA WG) recommended that the ccNSO Council establish a Study Group to explore and advise the Council on what role, if any, IANA might have with respect to ccTLD disaster recovery. The recommendation was based on three considerations:

- IANA currently has no defined role in ccTLD disaster recovery, but there was interest in exploring whether such a role might be appropriate.
- Because no such role currently exists, there is no established policy framework that would constrain the discussion, allowing the issue to be considered from a relatively “blank page.”
- There is significant public interest in ensuring that ccTLDs remain resilient and available when disasters occur. Clarifying whether IANA has a role in supporting this resilience could therefore contribute to ICANN's broader mission of supporting a stable and secure Internet.

Following the PGA WG's recommendation, the ccNSO Council established the Study Group on the Role of IANA in ccTLD Disaster Recovery.

The Study Group was tasked with providing a comprehensive overview of the issues associated with IANA's potential role in ccTLD disaster recovery and defining the scope of those issues. If appropriate, the Study Group was also expected to recommend to the ccNSO Council whether new policy, interpretations, or practices should be considered as potential next steps.

To fulfil this mandate, the Study Group was explicitly tasked with exploring key questions concerning what, if any, requirements should be established around IANA's role in ccTLD disaster recovery and/or in sustaining the ongoing operation of a ccTLD in the event of a disaster or non-compliance with global policies.

The Study Group was also asked to examine situations in which ccTLD managers have sought to establish private arrangements with IANA for special procedures to be followed in an emergency. Such arrangements could, for example, seek to pre-define conditions under which IANA would recognise another party to manage the domain, based on prior mutual agreement.

3. Method and Limitations

The Study Group was established to explore what role, if any, IANA might have in ccTLD disaster recovery. Its initial exploration showed that this question first required a clearer definition of the problem. Business continuity (BC) and disaster recovery (DR) are primarily the responsibility of the ccTLD manager, who is expected to maintain appropriate backup systems,

failover procedures, and recovery plans. The Study Group therefore focused on situations that go beyond conventional BC/DR: when these mechanisms fail or are absent, or when the ccTLD manager itself is no longer able to operate.

The Study Group also recognised that ccTLDs operate in highly diverse regulatory, governance, and operational environments. BC/DR requirements range from relatively detailed regulatory obligations, such as those under the EU's NIS2 framework, to environments where no binding requirements exist. Consequently, both the nature of the problem and the appropriate response may differ significantly among ccTLDs.

To account for this complexity, the Study Group applied a design-thinking approach: exploring the problem broadly, defining it more precisely, developing and testing possible approaches, and ultimately converging on recommendations. The exploration included analysis of BC/DR definitions, historical cases, publicly available IANA materials, relevant regulatory frameworks, and the diversity of ccTLD governance, operational models, and sizes.

This work highlighted several areas requiring further consideration, including the absence of a documented framework for IANA involvement in ccTLD disaster recovery, the use of ad hoc continuity arrangements, and the absence of a public process for emergency pre-arrangements. The Study Group therefore refined the problem statement around whether a framework for possible IANA involvement is needed that can accommodate the diversity of ccTLDs and the environments in which they operate.

The Study Group then tested possible approaches against diverse ccTLD use cases. This led to a three-tier trigger framework for structuring possible responses, ranging from standby through facilitation to potential active involvement in exceptional circumstances. The resulting options informed the Study Group's recommendations.

This methodology was intended to ensure that any proposed role for IANA emerged from an evidence-based understanding of the problem and was tested against realistic scenarios, rather than being assumed at the outset.

4. The ccTLD BC/DR Landscape

4.1 Introduction

The Study Group reviewed the ccTLD business continuity and disaster recovery landscape to establish the context in which a potential role for IANA should be considered. This included the meaning of business continuity (BC) and disaster recovery (DR), experiences within the ccTLD community, IANA's current role, the diversity of ccTLD governance and operational models, and the external regulatory environment.

Four main findings emerged from this exploration:

- BC and DR are primarily the responsibility of the ccTLD manager.
- ccTLDs operate in highly diverse governance, operational and regulatory environments, resulting in different levels of preparedness, capacity and dependency on third parties.
- IANA has an established role in maintaining the root zone and processing delegation-related changes, but there is no standing, generic IANA disaster recovery service or documented framework defining IANA involvement when a ccTLD's own BC/DR arrangements fail.
- The question for the Study Group therefore arises principally when the ccTLD manager's own arrangements are insufficient, fail or are absent, or when the manager itself is no longer able to operate.

This section summarises these findings. More detailed supporting material is included in the annexes.

4.2 BC/DR and the responsibility of the ccTLD manager

Business continuity and disaster recovery are related but distinct concepts:

- **Business Continuity** concerns an organisation's ability to continue delivering essential services during and following a disruption.

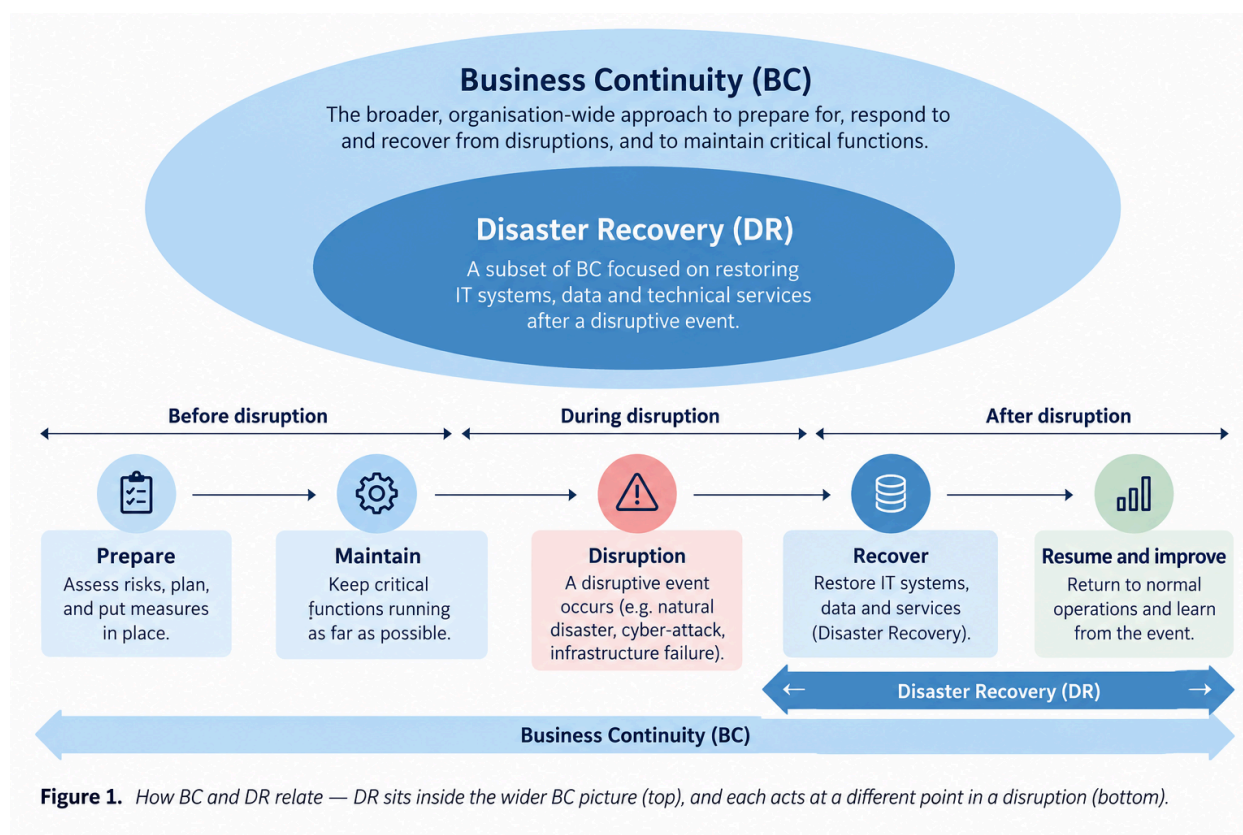
It is the wide discipline, among others defined in ISO 22301:2019. It keeps the whole organization working during and after a problem. It covers people, processes, communication, and partners — not only computers.

- **Disaster Recovery** is a component of BC and focuses more specifically on restoring systems and data following a failure.

DR is the focus of ISO/IEC 27031 (ICT readiness) and ISO/IEC 24762 (DR services).

In simple terms, BC asks how an organisation continues to operate, while DR addresses how its systems are restored. The two must work together — DR without BC may restore systems that no longer match business needs; BC without DR may set goals the technology cannot meet.

	Business Continuity (BC)	Disaster Recovery (DR)
Focus	The whole organization	IT systems and data
Main question	How do we keep operating?	How do we restore the systems?
Covers	People, processes, communication, partners	Backup, failover, system rebuild
Owner	Senior management	Technical team or provider



For the purposes of the Study Group, the important distinction is between the ccTLD manager's responsibility for its own BC/DR arrangements and circumstances in which those arrangements no longer provide a workable solution.

Shared Experiences

The ccTLD community has considered BC/DR for many years and has shared experiences from a wide variety of disruptions, including natural disasters, infrastructure failures, crime, pandemics and armed conflict. Since 2009, presentations at ccNSO meetings have demonstrated how ccTLD managers of different sizes and operating models prepare for and respond to disruptions.

Early discussions at the ccNSO meeting in Sydney in 2009 focused on preparedness. EURid (.eu) presented its approach to business continuity, from identifying crisis scenarios to developing and testing a DR plan; DENIC (.de) addressed registry redundancy; and .cr and .mx demonstrated how smaller registries can develop practical contingency arrangements with limited resources.

Subsequent discussions increasingly drew on experience from actual events. Following the 2010 earthquake in Haiti, IANA documented how geographic diversity helped .ht maintain DNS resolution despite some name servers in Haiti becoming unreachable. JPRS (.jp) subsequently shared lessons from the 2011 earthquake and tsunami and, in 2018, described an approach

based on geographically separated DR sites, regular switching exercises and distributed DNS infrastructure. At the same meeting, .pr shared its experience following Hurricane Maria.

More recent examples illustrate the widening range of disruptions affecting ccTLDs. At ICANN84 in 2025, AFNIC (.fr) presented a broad threat taxonomy covering natural, cyber, financial, human-resource and supply-chain risks, together with the experience of .mg following the theft of its production equipment. At ICANN86 in 2026, .ua shared its experience of maintaining registry operations under wartime conditions.

These experiences demonstrate the importance of preparedness, including redundancy, geographic diversity, tested recovery procedures and arrangements with third-party providers. The community has also developed practical resources through TLD-OPS, including a DR/BCP Playbook and tabletop exercises.

Emerging Themes

Several themes emerge from these experiences:

- First, the range of risks considered by ccTLD managers has broadened considerably. Discussions have evolved from a primary focus on natural disasters to include pandemics, crime, infrastructure and supply-chain disruption, and armed conflict.
- Second, the experience shared by ccTLDs consistently highlights the importance of preparedness. Geographic and operational diversity, redundancy, tested recovery procedures, access to backups and arrangements with third-party providers can substantially reduce the impact of a disruption. The examples also demonstrate that preparedness is relevant to ccTLDs regardless of their size or operating model.
- Third, the community has increasingly moved from sharing individual experiences towards developing common resources and practical tools. The TLD-OPS Standing Committee, for example, developed the DR/BCP Playbook to assist ccTLDs and has tested and further developed this work through Table Top Exercises (TTX). These exercises use simulated incidents to test decision-making, identify gaps and capture lessons that can subsequently be applied by ccTLD managers.
- Finally, the discussions increasingly raise questions that go beyond the ccTLD manager's own BC/DR arrangements. Where those arrangements are insufficient, fail or are absent, questions may arise about what other actors could do to support continued operation of the ccTLD. The potential role of IANA in such circumstances is the focus of this Study Group.

The Study Group considers BC and DR to be first and foremost the responsibility of the ccTLD manager. BC will normally involve decisions at the organisational and management level, while DR may be delegated to technical teams or service providers. Where functions are outsourced, responsibility nevertheless remains with the ccTLD manager, including ensuring that contractual arrangements adequately support its continuity and recovery requirements.

4.3 Diversity of the ccTLD landscape

There is no single model for managing and operating a ccTLD. The Study Group identified significant differences in governance, operational arrangements, size and regulatory environment.

ccTLD managers include government or national bodies, academic institutions, private companies and non-profit organisations. Their technical and registration functions may be operated entirely in-house, outsourced to third parties, or delivered through a combination of both. ccTLDs also vary considerably in size and organisational capacity.

The external environment is similarly diverse. The Study Group identified a range of regulatory frameworks affecting BC/DR, from binding requirements to voluntary arrangements and environments in which no specific framework exists. Where regulatory frameworks apply, they may establish requirements concerning continuity planning, testing, recovery objectives, incident reporting and organisational accountability. The extent and detail of these requirements vary considerably between jurisdictions.

These differences influence a ccTLD manager's preparedness, available recovery options, dependencies and the actors that may be able to assist when a disruption occurs. They also mean that the consequences of an event cannot be assessed solely by the nature or severity of the disaster, or by the size of the ccTLD.

For the Study Group, this diversity is important because a potential role for IANA cannot be considered on the basis of a single ccTLD operating model or disaster scenario. The different circumstances need to be taken into account when considering whether, when and how IANA might have a role.

Detailed information on the governance and operational models, size distribution and regulatory environments considered by the Study Group is included in Annex [A].

4.4 IANA's current role

IANA's established functions in relation to ccTLDs include maintaining the relevant entries in the DNS root zone and processing delegation-related changes. These functions form part of the normal framework within which ccTLDs operate; they are not themselves disaster recovery.

The Study Group's review found no standing, generic IANA disaster recovery service. Existing public policy and procedural documents address matters such as delegation, transfer and revocation, rather than establishing a specific framework for IANA involvement in ccTLD disaster recovery.

This distinction is important. Under normal circumstances, the ccTLD manager remains responsible for its own BC/DR arrangements. The question of a potential additional role for IANA arises when those arrangements no longer provide a workable solution.

Consistent with its Terms of Reference, the Study Group considered two broad situations:

- **Reactive involvement:** where the ccTLD manager's own recovery arrangements are absent, exhausted or have failed and assistance outside the ccTLD's normal BC/DR arrangements may be required.
- **Pre-arrangements:** where arrangements are made in advance concerning what should happen, and which parties should be recognised, if specified emergency circumstances arise.

The Study Group also sought factual information from IANA concerning existing arrangements, possible actions and questions of authority. The questions and responses are included in Annex [B].

4.5 Where the Study Group's question begins

The findings above establish an important boundary for the Study Group's work. Business continuity and disaster recovery are first and foremost the responsibility of the ccTLD manager. The Study Group is therefore not examining how individual ccTLD managers should design or operate their BC/DR arrangements. Rather, its focus is on the exceptional circumstances in which those arrangements no longer provide a workable path to maintaining or restoring the operation of the ccTLD.

The severity of a disruption does not, in itself, determine whether IANA may have a role. A ccTLD affected by a major disaster may require little or no IANA involvement if its continuity and recovery arrangements remain effective. Conversely, a more limited disruption may create significant difficulties if recovery arrangements are insufficient or absent, key contacts are unavailable, critical third parties cannot provide the required services, or the ccTLD manager itself is no longer able to operate.

The Study Group's question therefore begins where the ccTLD manager's normal BC/DR arrangements fail, are unavailable, or cannot be activated, and there is no foreseeable path back to workable operations. This can be understood as a failure of the mechanisms intended to mitigate failure. At that point, the situation extends beyond conventional BC/DR and may raise broader questions concerning authority, recognition, changes to root-zone information, temporary operational arrangements, or succession.

To clarify this boundary, the Study Group distinguishes three layers:

- **Layer 1 – ccTLD manager:** The ccTLD manager is responsible for establishing and operating appropriate BC/DR arrangements, including arrangements with third-party service providers where functions are outsourced.
- **Layer 2 – Normal IANA framework:** IANA maintains the relevant root-zone information and processes delegation-related changes in accordance with established policies and procedures. These are routine IANA functions and are not, in themselves, disaster

recovery.

- **Layer 3 – Potential additional IANA involvement:** Exceptional circumstances may arise in which the ccTLD manager's own arrangements no longer provide a workable solution and actions beyond IANA's routine functions may need to be considered. Whether IANA could or should have such a role, under what circumstances, and subject to what authority or safeguards, is the question examined by the Study Group.

Potential involvement could arise reactively, after the ccTLD manager's own recovery arrangements have failed, or through arrangements established in advance for specified emergency circumstances. There is currently no generic policy or framework establishing such a backstop role for IANA.

The Study Group therefore does not start from the assumption that IANA should provide disaster recovery for ccTLDs. Instead, the question carried forward is narrower:

When a ccTLD manager can no longer maintain or restore workable operations through its own arrangements, what actions could IANA potentially take, and would additional policy, procedures or practices be required to enable them?

5. Exploring the potential role of IANA

5.1 Introduction

The previous section in this report established the point at which the Study Group's central question arises: when a ccTLD manager's own BC/DR arrangements no longer provide a workable path to maintaining or restoring operations. This section explores what role, if any, IANA could potentially play in such circumstances.

Rather than considering IANA's potential role in the abstract, the Study Group developed a set of use cases reflecting different ccTLD circumstances and types of disruption. These use cases are intended to test what actions or roles might be relevant in different situations and to identify the conditions that could trigger different levels of involvement.

For each use case, the Study Group considers two related questions:

- What could IANA potentially do in this situation, from an operational or technical perspective?
- Would existing policies, procedures and practices allow such action, or might additional pre-arrangements or policy work be helpful?

The use cases therefore provide a structured way to explore the range of possible IANA involvement and to identify where operational, procedural or policy gaps may exist.

5.2 The five dimensions

Each use case is positioned along five dimensions that together describe the operational context of ccTLDs. These dimensions were chosen because they directly shape both the likelihood of disaster impact and the type of IANA support that would be relevant.

Dimension	Range	Why it matters for BC/DR
Regulatory framework	Strict (NIS 2) ↔ Absent	Determines baseline obligations and enforcement capacity
Governance model	Government related ↔ Private sector	Shapes authority structures and decision-making in a crisis
DNS service	Fully in-house ↔ Fully outsourced	Determines dependency on third parties and resilience options and availability of the zone
Registration service	Fully in-house ↔ Fully outsourced	Affects data custody, continuity of provisioning, and users
Scale (DUM)	Micro (<5 000) ↔ Very large (>5M)	Strong indicator for resource capacity and societal impact of failure

5.3 Use case summary

The table below provides a one-line summary of each use case and the potential IANA role. The full use cases are included in Annex [C].

ID	Profile	Disaster	IANA role
UC-1	Large private registry Strict reg · Private · In-house · >5M	Utility disruption / war	Minimal — standby only
UC-2	Island government No reg · Gov · Outsourced · <5K	Total collapse — cyclone	Central / sole actor
UC-3	Academic, Emerging reg · Academic · Mixed · 5–50K	Hurricane + personnel loss	Coordination / facilitation
UC-4	Government Moderate reg · Gov · In-house · 100–500K	Prolonged power outage	Advisory / technical facilitation
UC-5	Private NGO Moderate	Political crisis / contested	Gatekeeper — legitimacy

	reg · Private · Mixed · 500K–2M	authority	decision
UC-6	Gov Strong reg · Gov · In-house · 1–5M	War ? operator incapacitated	Emergency authority

5.4 Cross-cutting findings

Comparing the six use cases reveals four findings that could inform the study group's deliberations:

A. Preparedness, not disaster severity, determines the outcome

UC-1 involves armed conflict and data centre destruction — yet IANA's role is minimal because the operator is well-prepared. UC-2 involves a cyclone affecting fewer than 5 000 domains — yet IANA becomes the central actor because no other mechanism exists.

The key variable is the preparedness of the ccTLD manager, rather than the severity of the event itself. This suggests that the most effective and important measures are those taken before a disaster occurs, including establishing minimum preparedness standards and facilitating appropriate pre-arrangements.

B. The hardest scenarios involve contested legitimacy, not technical failure

UC-5 and UC-6 demonstrate that for IANA the most difficult role will not be about service continuity, but about authority and recognition. The existing IANA policies on delegation, transfer, and revocation were not designed for emergency conditions.

C. Pre-arrangements are the single most effective intervention

In UC-2 and UC-3, the absence of a simple pre-agreed backup arrangement — with a neighboring ccTLD or other entity — created the conditions to look at IANA to become the sole actor.

A pre-arrangement with another ccTLD manager or other entity, requiring only modest administrative effort before a disaster occurs, could reduce reliance on IANA as the central actor and limit its role to occasional monitoring. The study group seeks feedback on whether a tiered pre-arrangement framework, as outlined in Section 6, as a concrete recommendation is advisable.

D. Scale (DUM) is a misleading proxy for risk or priority

UC-6 involves millions of domains and is the most geopolitically complex use case. UC-2 involves fewer than 5 000 domains but is arguably the most operationally urgent for IANA to take action because no other actor is available. Any IANA support framework that prioritizes

and is based on scale alone will misallocate resources. The framework must account for operator capacity, governance model, and the availability of alternatives — not scale alone.

In summary: The use cases demonstrate that the potential need for IANA involvement is determined primarily by the ccTLD manager's preparedness and ability to recover, rather than by the severity of the disaster or the size of the ccTLD. Effective preparedness and pre-arrangements can significantly reduce or avoid the need for IANA involvement. Where these mechanisms fail or are absent, however, a potential additional role for IANA may arise.

The BC/DR picture: preparation decides the outcome

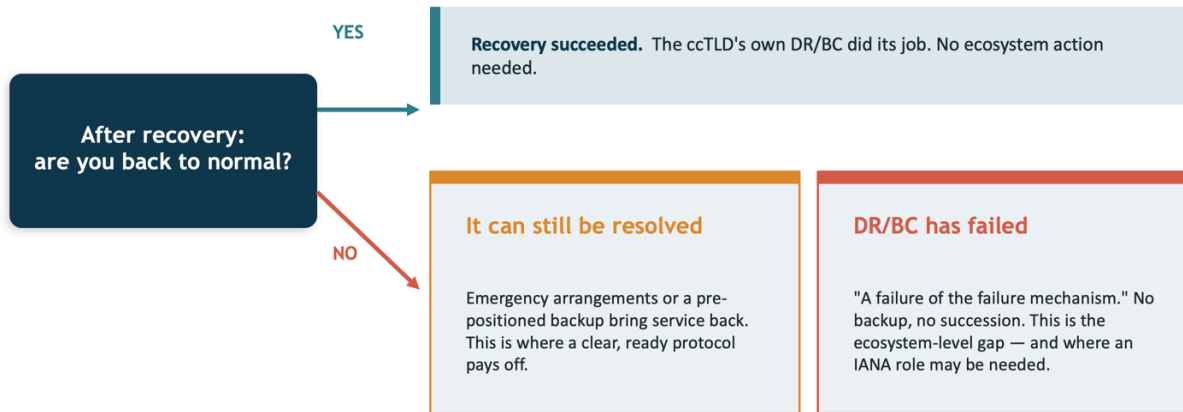


What you do BEFORE the event decides whether you return to normal AFTER it.

Preparation is the most leveraged step — and the part the ccTLD can most directly influence

The key question: do you return to normal?

Normal = both DNS resolving AND registration working again.



This fork is the "?" in the BC/DR model and the role IANA potentially can play – the space the Study Group is exploring.

6. Possible Framework and the Role of IANA

This section sets out the tiered, proportionate framework: principles, triggers, tiered IANA roles, escalation, boundaries, policy and transparency safeguards. Based on the six use cases, the following three-tier trigger framework was developed to consider the potential role for IANA. Trigger tiers are defined by operator status, not by the nature of the disaster.

Tier	Operator status	IANA role	Example use cases
Tier 1	Operational, taking recovery steps	Standby — monitor and provide named contact	UC-1
Tier 2	Partially operational or key contacts unavailable	Advisory — guidance, facilitation, temporary measures	UC-3, UC-4
Tier 3	Not operational or legitimacy contested	Active — if needed emergency delegation, credential management, authority determination	UC-2, UC-5, UC-6

This framework aligns with the observation from the study group's factfinding material that the type of disaster is less important than the operational status of the ccTLD manager. It also maps to existing IANA administrative capabilities: Tier 1 requires no new policy; Tier 2 requires facilitation protocols and pre-arrangement templates; Tier 3 potentially requires new emergency practices/policy and authority frameworks.

The potential role of IANA under this tiered approach is also linked to issues that will be considered by other Study Groups, as per the Final Report of the PGA WG:

- **Study Group on Local Presence.**

This work will consider the level of involvement of the ccTLD Manager. There is a wide gamut of operational situations for ccTLD managers: Some are responsible for every aspect of the ccTLD, from policy setting to technical platform to operations and providing direct registrations services. Should minimum obligations be defined regarding the functions a manager must perform directly?

- **Study Group on Resignation.**

This work will consider the absence of a specified policy on how a ccTLD manager, or a public point-of-contact, can resign from their role. It is assumed and operationalized that any time a ccTLD manager or a contact no longer wishes to perform their role, they will be replaced by a change request that identifies their successor.

It should also be noted that the caretaker mechanism for the .lb (Lebanon) top-level domain provides an example of how some of these scenarios could potentially be addressed, where needed. The exchange of correspondence between IANA and the ccNSO Council regarding this mechanism may therefore provide a useful reference. At the time, however, the ccNSO Council did not consider that it had a specific role with respect to the individual case.

Read more:

- <https://itp.cdn.icann.org/en/files/council/davies-to-reynoso-13jul23-en.pdf>
- <https://itp.cdn.icann.org/en/files/council/response-to-kim-davis-creation-of-caretaker-for-lb-02-08-2023-en.pdf>

7. Potential Policy Gaps & Areas for Further Exploration

Several questions remain open:

- how to distinguish disaster recovery from situations requiring a standard transfer or need for a caretaker;
- who has the authority to declare an emergency and what authority would IANA have to act;
- whether a caretaker mechanism or an EBERO-style arrangement - adapted for ccTLDs, possibly without full data escrow - could be appropriate.

These rare edge cases require further consideration. At the same time, care should be taken to avoid over-specifying arrangements for scenarios that are unlikely to occur.

8. Recommendations to the ccNSO Council

8.1 Basis for the recommendations

The Study Group was asked to provide an overview of the issues associated with a potential role for IANA in ccTLD disaster recovery and, if appropriate, to recommend to the ccNSO Council whether new policy, interpretations or practices should be considered. Its work narrowed the question to the exceptional situation in which a ccTLD manager can no longer maintain or restore workable operations through its own arrangements. The recommendations below follow from the findings of that work. Each recommendation is linked to the findings on which it rests; the findings themselves are numbered here for traceability.

Finding	Statement	Where in the report
F1	Business continuity and disaster recovery are first and foremost the responsibility of the ccTLD manager, including where functions are outsourced.	Sections 4.2, 4.5 (Layer 1)
F2	ccTLDs operate in highly diverse governance, operational and regulatory environments; preparedness, capacity and dependencies differ accordingly.	Section 4.3, Annex A
F3	IANA's established functions in relation to ccTLDs include maintaining the relevant entries in the DNS root zone and processing delegation-related changes. The Study Group's review found no standing, generic IANA disaster recovery service for situations where a ccTLD manager's BC/DR arrangements are absent or have failed, or for establishing advance arrangements for emergencies.	Section 4.4, Annex B (Q2, Q4)
F4	Preparedness, not disaster severity or scale, determines whether IANA involvement is needed at all.	Section 5.4
F5	Pre-arrangements between the ccTLD manager and another ccTLD or trusted entity are the single most effective intervention.	Section 5.4, Annex B (Q1)
F6	The hardest scenarios concern authority and recognition (contested legitimacy, incapacitated operator), not technical failure. Existing delegation, transfer and revocation policies were not designed for emergency conditions, and policy is not clear on a pathway for IANA to take extraordinary action on an expedited basis.	Section 5.4, Section 7, Annex B (Q3), UC-5, UC-6
F7	A three-tier response can be mapped to existing IANA capabilities: Tier 1 (standby) requires no new policy; Tier 2 (advisory/facilitation) requires protocols and templates; only Tier 3 (active) would potentially require new emergency practice or policy.	Section 6

8.2 Recommendation 1 — No additional policy is needed at this time

RECOMMENDATION 1

The Study Group concludes that at this stage no additional ccNSO policy is required with respect to the role of IANA in ccTLD disaster recovery, and the ccNSO Council should not initiate a Policy Development Process on this topic.

Rationale

1. The responsibility for BC/DR rests with the ccTLD manager, and the leverage is before a disaster.

The use cases show that a well-prepared manager renders IANA's operational role close to zero even in the most extreme cases, while an unprepared one makes IANA the sole actor even for a micro event. Policy binding IANA would act on the wrong lever: it cannot substitute for preparedness, and it risks signalling that a backstop exists where the report finds none.

2. What is needed most can be achieved without a new policy.

Pre-arrangements with another ccTLD or a trusted third party are a private matter for the manager and do not require new policy, as IANA also confirmed. Any arrangements needed could be addressed through protocols, templates and guidance rather than through new policy.

3. Diversity argues against a single generic rule.

The ccTLD landscape ranges from highly regulated, in-house operated, multi-million-domain registries to unregulated, fully outsourced registries operated by only one or two people (Annex A). Size alone is therefore not a reliable indicator of risk or preparedness. A generic policy designed around one operating model could over-specify requirements for many ccTLDs, while failing to address the needs of others. The Study Group therefore cautions against over-specifying arrangements, particularly for scenarios that are unlikely to occur.

4. The residual hard cases are not disaster recovery questions.

The use cases demonstrate that situations involving contested legitimacy, or an incapacitated operator alongside a competing claim to authority, raise questions of delegation, transfer and revocation, rather than disaster recovery. These matters fall under [RFC 1591](#), as interpreted by the [Framework of Interpretation](#) (FOI), and may also intersect with the work of future Study Groups on Resignation and Local Presence. Creating a separate disaster recovery policy would not resolve these questions and could risk creating a parallel route around the standard process. See recommendation 2 below.

8.3 Recommendation 2 — Further study on temporary measures: caretaker and temporary transfer

RECOMMENDATION 2

The ccNSO Council should commission a focused follow-up study on whether, and by what method, a temporary measure could be made available when a ccTLD manager is not operational. Such measures could include the appointment of a caretaker and/or a temporary transfer of operational functions.

The study should emphasize the temporary character of any such measure.

Its purpose is either to:

- stabilize the situation so that operations can return to normal under the existing manager, or
- hold the ccTLD in a stable state while a transfer is prepared according to the basic rules (RFC 1591, the Framework of Interpretation and the standard IANA transfer process).

Any temporary measure should not serve as a mechanism for resolving contested legitimacy or for bypassing the standard process.

Rationale

The report identifies a residual gap that neither preparedness nor existing policy clearly addresses: what happens when a ccTLD manager is no longer operational and no pre-arrangement exists? In such circumstances, there is no clearly defined pathway for IANA to take temporary or expedited action, to maintain stable operation of the ccTLD.

Several questions remain open, including:

- How to distinguish disaster recovery from a standard transfer?
- When could a caretaker or temporary transfer of operational functions be appropriate?
- Who could determine that circumstances justify such a measure?
- What safeguards would be needed to ensure that any intervention remains temporary?

The caretaker concept has been used previously. The related correspondence between IANA and the ccNSO Council shows both that such an instrument is possible and that aspects of its application remain unsettled. Further, IANA has noted that ICANN's mission may permit some form of emergency response in the absence of explicit policy, while indicating that it has generally not taken the lead in such situations.

Without further consideration, a future case would therefore risk being addressed on an ad hoc basis. A focused follow-up study would allow to examine whether a temporary mechanism is needed and, if so, how it could operate without creating an alternative route for resolving contested legitimacy or bypassing the established delegation and transfer framework.

8.4 Observations from the study group

OBSERVATION 1

The ccNSO Council is advised to:

- support the Study Group's advice to ccTLD managers and TLD-OPS to incorporate the identified use cases and potential role of IANA into their DR/BC playbooks and tabletop exercises; and
- bring the report to the attention of ccTLD managers, encouraging them to consider its findings in their own BC/DR planning.

OBSERVATION 2

A formal active IANA role in escrow arrangements or formal decision making etc would need mandate, funding and validation that are not in place.

IANA has indicated that taking on functions such as acting as an escrow agent or similar roles would require an appropriate policy basis, resourcing and prioritization, none of which are currently planned. It has also noted that the diversity of ccTLD operating models makes gTLD-style escrow and standardized restoration mechanisms poorly suited to the ccTLD environment. The proportionate course is therefore to clearly identify the remaining gap and subject it to focused further study, rather than initiate a policy process whose need and scope have not yet been established. .

ANNEX A | Diversity of the ccTLD Landscape

Governance Models

ccTLD governance falls into three broad types:

- Government or national bodies: about 85 ccTLDs
- Academic or university operators: about 37 (a legacy of early Internet delegations),
- Private, NGO, or commercial operators: about 133.

Distribution varies by region. Government operators are common across Africa, the Pacific, and the Caribbean, and also run some large strategic registries. Private and NGO operators dominate Europe and most large registries, while academic operators cluster in mid-size registries.

Governance model	Approx. ccTLDs	Where concentrated
Government / national body	~85	Africa, Pacific, Caribbean; some large strategic
Academic / university	~37	Mid-size registries; legacy delegations
Private / NGO / commercial	~133	Europe; most large registries

Operational Model: From completely Outsourced to In-House

Operations run along a spectrum from fully in-house to fully outsourced. Overall, roughly 55 ccTLDs are fully in-house, about 78 use a mixed model, and about 122 are fully outsourced. Outsourcing is the most common model globally.

The regional pattern is strong: European registries are mostly in-house, while the Pacific, Caribbean, and Africa are heavily outsourced. This matters because when operations are outsourced, the ccTLD's resilience duty passes through a third party.

Region	In-house %	Mixed %	Outsourced %
EU / EEA	78	18	4
Asia-Pacific	42	30	28
MENA	25	38	37
Latin America	15	32	53
Africa	8	18	74
Caribbean	5	12	83
Pacific	2	8	90

Size: Domains Under Management

Scale correlates with region and operational capacity, included, but not limited to BC/DR. As noted by the 2nd ccNSO Finance WG, ccTLDs vary considerably in scale. About 140 ccTLDs manage fewer than 20,000 domains, about 85 manage between 20,000 and one million, and about 30 manage more than one million. The largest registries manage several million domains each.

Not only do ccTLDs vary in size, there is also a huge diversity across the various geographic regions. The largest registries are concentrated in Europe and a few large economies, while the smallest are common in the Pacific, Caribbean, and parts of Africa — often run by teams of only one or two people.

Size band (domains)	Approx. ccTLDs	Typical regions
Fewer than 20,000	~140	Pacific, Caribbean, parts of Africa, small territories
20,000 – 1 million	~85	Mixed; emerging and mid-size markets
More than 1 million	~30	Europe, large economies (e.g. major national registries)

References: ccNSO Finance WG overview.

The External BC/DR Context Landscape

In this section the regulatory context is sketched. It covers a summary of the Study Group's findings of the regulatory frameworks affecting ccTLD BC/DR, a distribution of regulatory coverage across regions, and the impact of those frameworks on ccTLDs.

Regulatory Frameworks Affecting ccTLD's BC/DR

The Study Group identified a wide range of frameworks relating to BC/DR. They range from binding regimes over voluntary arrangement to no framework at all. Only one framework explicitly names DNS service providers and TLD registries as in-scope entities.

All frameworks converge on the same core requirements: documented plans, testing, recovery objectives, and incident reporting. Differences are sharp in detail — incident reporting ranges from 2 hours (Singapore) to 72 hours (EU/Canada) — and a clear trend places accountability at board level.

7.2 Regulatory Coverage Across Regions

Summary - The impact of Regulatory Frameworks is highly uneven across the roughly 250+ ccTLDs. A minority sit under strict regimes, while about 100 operate under minimal, voluntary, or no regulation, and the gap is widest for the smallest registries.

Regulatory tier (regulatory strength)	Approx. ccTLDs	Typical regions
Strict (8–10)	~	EU / EEA
Strong national (6.5–8)	~49	Parts of Asia-Pacific, mature economies
Emerging / moderate (4–6.5)	~50	Latin America, parts of Asia, MENA
Minimal / voluntary (2–4)	~50	Africa, parts of Asia, Caribbean
No regulation (0–2)	~50	Pacific, small territories, least-served

Impact of Regulatory Frameworks on ccTLDs

This part provides an overview of how the frameworks above actually affect ccTLD operators in practice — for example new obligations, board-level accountability, and the burden on small or outsourced registries.

Tier 1 – Direct Impact

These two frameworks clearly cover ccTLDs today. Compliance is mandatory and not optional.

EU NIS 2 Directive (2022/2555)

Summary	EU-wide cybersecurity law for essential services. It is the only framework that names DNS providers and TLD registries directly. A special regulation (2024/2690) adds technical rules just for DNS and TLD operations.
Who is covered	All EU ccTLDs (.de, .nl, .fr, .eu and others) as “essential entities”. Non-EU ccTLDs offering services in the EU can also be covered.
ccTLD duties	Written BC and DR plans; business impact analysis; recovery time targets (RTO/RPO); tested backups; crisis management; report incidents within 24 hours; assess your suppliers (including your secondary DNS provider).
Who is accountable	The registry’s management. Board members can be personally liable.
Penalties	Up to EUR 10 million or 2% of worldwide turnover.

China Cybersecurity Law + MLPS 2.0

Summary	China's core cybersecurity law. It applies to every "network operator", which automatically includes the .cn registry (CNNIC). MLPS 2.0 makes BC/DR one of nine mandatory control areas.
Who is covered	.cn and any DNS infrastructure operating in mainland China.
ccTLD duties	DR backups of critical systems; emergency response plans with regular drills; keep registry data inside China; national DR standard (GB/T 20988) sets recovery levels with fixed RTO/RPO values.
Who is accountable	The operator and its managers personally.
Penalties	From January 2026: RMB 1–5 million or 1–5% of yearly revenue; licences can be revoked.

Tier 2 – Possible High Impact

These laws use broad terms — critical infrastructure, essential services, digital infrastructure — that may very likely include the national ccTLD. Designation decisions are made by the regulator.

Chile – Cybersecurity Framework Law 21.663

Summary	Latin America's first complete cybersecurity law (in force 2025). A new agency (ANCI) designates "essential service providers" and "operators of vital importance". Digital infrastructure and digital services are on the list.
Why ccTLD relevant	.cl (NIC Chile) is a strong candidate for designation.
ccTLD duties	Security management system aligned with ISO 27001; continuity plans certified and re-checked by ANCI every 2 years; a named cybersecurity delegate; alerts within 3 hours, full reports within 72 hours.
Penalties	Up to about USD 3.2 million.

Australia – SOCI Act

Summary	Covers 11 critical infrastructure sectors with an "all hazards" approach (cyber, physical, personnel, supply chain).
Why ccTLD relevant	.au likely fits the communications or data-processing sectors. Important: .au is fully outsourced to Identity Digital (US). auDA stays accountable for duties its provider performs.

ccTLD duties	A risk management program covering all hazards; incident reports to the national cyber centre; possible extra duties (exercises, vulnerability checks) if named a “system of national significance”. Government can step in during serious incidents.
Penalties	Significant fines; direct government intervention powers.

Singapore – Cybersecurity Act (2024 amendment)

Summary	Protects critical information infrastructure. The 2024 update adds “foundational digital infrastructure”, a term that fits DNS well.
Why relevant ccTLD	.sg (SGNIC) may be designated as CII or foundational digital infrastructure.
ccTLD duties	Measures to keep essential services running; follow codes of practice; report incidents within 2 hours — the fastest deadline in the world, which requires 24/7 monitoring.
Penalties	Up to SGD 100,000 and/or 2 years imprisonment; daily fines for continuing breaches.

Kenya – CII Regulations 2024

Summary	Detailed regulations under the Computer Misuse and Cybercrimes Act. The most explicit BC/DR duties in Africa.
Why relevant ccTLD	Telecommunications is a CII sector; .ke (KENIC) may be designated.
ccTLD duties	Develop, test, and update BC and DR plans; yearly business impact analysis, risk assessment, and internal audit; a risk register; joint exercises with the national committee (NC4); a security operations centre; report incidents within 24 hours.
Penalties	Fines up to KSh 5 million and/or up to 10 years imprisonment.

Saudi Arabia – NCA Essential Cybersecurity Controls

Summary	Mandatory controls for government bodies and critical national infrastructure, with a resilience domain built on business continuity management.
Why relevant ccTLD	.sa (SaudiNIC) likely counts as critical national infrastructure.
ccTLD duties	Bring cybersecurity into your continuity plans; DR plans; regular backups; simulations and drills; periodic reviews. Aligned with ISO 27001 and NIST CSF.

Penalties

Fines and licence revocation (since December 2024).

One obligation to Watch: Incident Reporting Speed

Reporting deadlines are the hardest BC/DR duty in practice. They are short, fixed, and cannot be delegated: the ccTLD must report even when a provider runs the systems. If your ccTLD outsources operations, your contract must force the provider to alert you fast enough to meet the deadline.

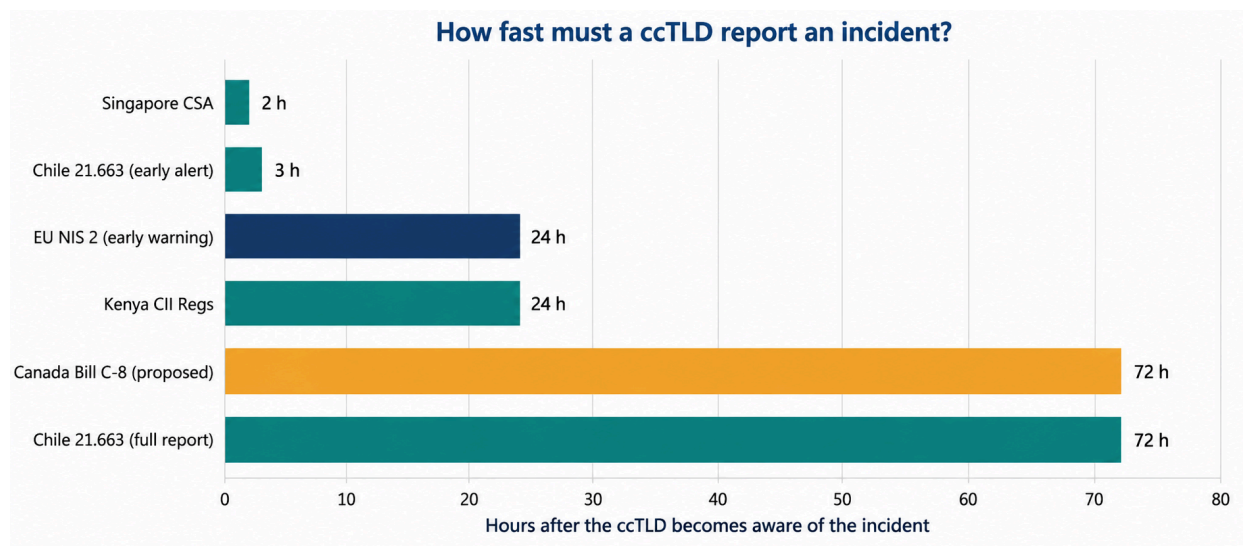


Figure 2: Reporting deadlines across the frameworks that (likely) cover ccTLDs.

Tier 3 – Emerging Impact

Framework	Summary	What is relevant for the ccTLD
Canada – Bill C-8 (CCSPA)	Canada's first federal cyber law for critical infrastructure. Still in Parliament (second reading, early 2026).	.ca (CIRA) could be designated under telecommunications. Duties would include a cyber security program, supply-chain checks, and 72-hour reports. CIRA should follow the designation process now.
Brazil	No single cyber law yet. Communications is a critical sector on paper. Bill 4752/2025 would create a national cyber authority.	.br (NIC.br) has no BC/DR duty today, but LGPD already applies to registrant data. If the bill passes, explicit duties may follow. NIC.br's own anycast network is a resilience strength.

Nigeria	Critical infrastructure order (2024) and cloud policy (2025) exist, but enforcement is weak.	.ng could be designated as critical infrastructure. Special issue: .ng runs on CoCCA's shared platform in Paris — future data localisation rules could conflict with this setup.
----------------	--	--

Tier 4 – Low or Indirect Impact

Framework	Why the impact is low — and when it can still matter
UK Operational Resilience	Same pattern as DORA: only relevant if the ccTLD or its provider is a “critical third party” to UK financial firms.
US NIST CSF 2.0	Voluntary framework, no penalties. Useful as a free, well-documented BC/DR playbook. Often referenced in contracts.
Japan	No DNS-specific rules. .jp follows general guidelines; data protection law applies to registrant data.
South Africa	Strong rules exist, but only for the financial sector. .za has general cybercrime and privacy duties, no BC/DR mandate.
Mexico	No binding cyber law. A national plan (2025–2030) may later create a critical infrastructure list that includes DNS.
Caribbean (CARICOM)	The regional action plan (CCSCAP 2025) is not binding. Island ccTLDs face almost no legal BC/DR duties today.
AU Malabo Convention	A continental framework without DNS provisions or an enforcement body. Impact depends entirely on national laws.

Key References

- Directive (EU) 2022/2555 (NIS 2) and Commission Implementing Regulation (EU) 2024/2690
- Cybersecurity Law of the PRC (2017, revised 2025); GB/T 22239-2019; GB/T 20988-2007
- Chile Law No. 21.663 (2024); Decree DS No. 295 (2025)
- Australia Security of Critical Infrastructure Act 2018; Cyber Security Act 2024
- Singapore Cybersecurity Act 2018; Cybersecurity (Amendment) Act 2024
- Kenya CII and Cybercrime Management Regulations (L.N. 44 of 2024)
- Saudi Arabia NCA ECC-2:2024; NCA Regulations (December 2024)
- Canada Bill C-8 (Critical Cyber Systems Protection Act, 2025)
- Brazil LGPD (Law 13,709/2018); Bill 4752/2025; Decree 10,569/2020
- Nigeria CNII Designation Order 2024; National Cloud Policy 2025

Companion documents: Global Comparison of BC/DR Regulatory Frameworks; Roles of ccTLDs Under BC/DR Frameworks; ccTLD Outsourcing Continuum; BC/DR Regulatory Exposure of ccTLD Outsourced Functions (all February 2026)

ANNEX B | IANA Fact Finding

April 2026 consultation on triggers for IANA engagement

Q1. What triggers IANA's engagement in a disaster scenario?

IANA's involvement in a disaster scenario is either triggered by the request for a root zone change, often associated with a call to our root zone emergency call center; or we become aware of a significant crisis in a country and make enquiries either directly or through trusted third parties (e.g. ICANN's regional engagement personnel, capacity building partners, etc.) and then confirm there are impactful issues happening. When we become aware of issues we try to informally support resolution where we are equipped to do so, even if it is not a formal contractual requirement.

Q2. What is IANA mandated to do?

IANA's mandate as specified in the IANA Naming Functions contract is generally to process root zone change requests according to the service level agreements, which do contain provisions to do so on an expedited basis for emergencies.

(Use case/scenario testing Use case/scenario testing)

Taken from the use case doc: Triggers for IANA engagement

- *Primary nameserver fails and zone cannot be updated.*
- *No technically authorized person is reachable within 48 hours.*
- *University leadership formally requests IANA assistance.*

A: For nameserver failure, IANA has no obligation or practice to proactively monitor nameserver operation and to trigger resulting actions. Any effort along these lines would be voluntary but is not informed by any policies or expected procedures.

The onus on having sufficient authorizing personnel approve a root zone change is on the TLD manager, not IANA. While we may make enquiries and help facilitate a good resolution, that is at our discretion. Ultimately, if authorizing personnel need to be replaced then there are processes to allow the ccTLD manager to replace them. In a disaster scenario, this may be challenging if the parties don't have reliable forms of communication and/or there is an inability for IANA to satisfactorily verify the authenticity of the communication.

September 2026 consultation on technical aspects

The ccNSO DR Study Group sought further clarification on the technical aspects of the issue. The Study Group first aimed to understand what actions IANA could hypothetically take, or what role it could play, from a technical perspective.

triggers for IANA engagement

Situation (1): The ccTLD Manager has made some pre-arrangements

Pre-arrangements might include:

- Depositing on a regular basis zone file, copy registry database with the data on registered domain names and their registrants with third parties (not IANA)
- Conditions (trigger events) to use deposits
- Names and contact details of persons authorized to act as admin & tech contact to make changes in IANA database
- Authorized DNS provider (similar to EBERO function for gTLDs)
- Authorized provider of EPP-service (similar to EBERO function for gTLDs), registration data service (whois)
- Any arrangements regarding DNSSEC ?

Q1. Do we miss any pre-arrangements that might be important?

Depending on the definition and the scope of what are considered pre-arrangements, part of a comprehensive approach would be exercising the assets that are being deposited. This would include validating their correctness (i.e. catching mistakes in the deposits, or a lack of timely deposits). For example, ICANN performs exercises that test the capabilities of the end-to-end process for EBERO. Given in the ccTLD environment this would be even more complex (i.e. heterogenous operating environments, differing registry structures, unique registry policies etc.) it would be even more critical to validate escrowed data could actually lead to successful restoration. Given the customization many ccTLDs have, they may not be well suited to the approaches used in the gTLD space where there is a standard escrow format and business model, and therefore alternative registry operators are less likely to be able to restore operations on standardized platforms in a straightforward way. Therefore an escrow approach may involve escrowing the custom registry software the ccTLD uses to operate on the registry database and perform core functions.

Additional clarifications:

On Q1, pre-arrangements can mean a lot of things. One kind of pre-arrangements if the ccTLD manager asking IANA in advance to take certain actions with their prior authorization. We don't have a policy basis to allow such pre-arrangements that is designed to subvert normal analysis and decision making, but presumably the purpose of such arrangements is to pre-authorize some course of action in advance that would be put in place quickly. So while we've been asked (e.g. "If my ccTLD becomes inoperative, I want to pre-approve transferring/redelegating it to this other organization") we do not see there is a path to do that under current policy and practices.

On Q1, if pre-arrangements just means escrow, that can be a private matter for the ccTLD, but they need to think about release conditions e.g. who can access it and how would that party put it into effect.

Q2. Can hypothetically IANA play any of the roles mentioned above (i.e. store deposits, signal trigger event to use deposits, recognise pre-authorized persons etc) on ?

Hypothetically yes, but it would need to be enabled through appropriate policy and procedural elements to enable it, plus associated resourcing and prioritization. As noted in prior discussions, pre-authorization of persons is something the trust model likely supports today - if the current model is insufficient for this purpose it could be explored what needs to be adapted.

Additional clarifications:

On Q2, we could hypothetically act in some of these roles, but notwithstanding the above (i.e. contradicts existing policy) things like being an escrow agent would need a mandate and funding. It would presumable cost money to do that we do not have planned.

Q3. Even if IANA cannot play any of the roles above, what would IANA need to be able to do for each of the above pre-arrangements to be effective?

Fundamentally changes to any TLD operator are manifested through changes to the root zone and associated database, and in an emergency scenario the ability to change the NS and DS records are likely the most critical. Under existing conditions, the ccTLD manager needs to have enough personnel inducted into IANA's systems such that they can operate in a conceived scenario and properly authorize such changes. When there is a fundamental failure, such as in the recent scenario that predicated this work, the policy is not clear on any specific pathway IANA has to take extraordinary action, particularly on an expedited basis in an emergency.

Situation (2): There are no pre-arrangements in place

Q4. Is there anything that can be done to ensure DNS-resolution? Availability of other services (registration service, etc)?

It is unclear if the question is related to what the current policy construct provides for. There is no explicit role for IANA, however we note that it is part of ICANN's overall mission to preserve the stability of the Internet's unique identifier systems and some kind of emergency response could be foreseen in lieu of explicit governing policy. We note that in prior circumstances IANA has been involved in facilitating or advising on emergency restoration of DNS-related data to help sustain resolution operations, however generally speaking it has not taken lead in such scenarios.

Q5. Does it make a difference from IANA's perspective for situations where national legislation directly or indirectly assumes governmental and/or regulator responsibility?

Under existing application of policy, local governments cannot use regulation to supersede IANA operational requirements, that is to compel IANA to take direction solely from the government. Governments are expected to exercise their regulatory or legal powers in jurisdiction within the country. IANA still requires ccTLD managers to comply with a variety of factors beyond compliance with local laws, such as demonstrating operational competency.

Urgency

In terms of urgency, the Study Group identified the following priorities:

- Urgent – Ensure continued DNS resolution (SC-2, SC-3, SC-4 and SC-6): The immediate priority is to ensure that existing domain names continue to resolve.
- Mid-term – Restore or maintain the registration service function (SC-2 to SC-6): The priority is to ensure that domain names can be renewed, which is the most critical function, followed by the ability to update existing registrations and register new domain names.
- Long-term – Address legitimacy issues (SC-5 and SC-6): Where relevant, longer-term measures would need to address questions concerning the legitimacy and authority to operate or manage the ccTLD.

Q6. Does IANA have any comments on the priorities?

Enabling “status quo” resolution we would agree is the top priority, however intrinsic to this is the ability to facilitate changes to delegation data in a reasonable timeframe. This is particularly necessary as NS and DS record changes may be necessary to preserve resolution operations for children of the zone. This should be considered as distinct from renewal operations — we could foresee in emergency operations the need to explicitly renew domains could be deferred to later so long as domains don’t expire as a result.

ANNEX C | Use Cases in Detail

Each use cases below is presented in a structured format:

- a profile covering the five operational dimensions,
- the disaster scenario,
- the impact on BC/DR capabilities,
- Potential role for IANA, if any, and,
- Study Group observations note.

Each of these use cases is built on the presumption that disaster recovery is fully the responsibility of the ccTLD manager. This is distinct from the situation of IANA having a pre-defined general, policy based role with respect to business continuity/disaster recovery above and beyond the role of a ccTLD manager. The latter is about what happens at the ecosystem level when a ccTLD's own disaster recovery provisions are insufficient, fail or are absent, or any other scenario where IANA steps in. Such a scenario is essentially a failure of the failure mechanism, sits outside conventional BC/DR planning scope, and raises fundamental questions in several policy areas (specifically transfer and revocation).

UC-1 | Large Private registry — utility disruption during armed conflict

Profile across five dimensions

Regulatory framework	Strict — NIS 2 (score 9/10)	 9/10
Governance model	Private / NGO operator (score 8/10)	 8/10
DNS service	Fully in-house (score 9/10)	 9/10
Registration service	Fully in-house (score 9/10)	 9/10
Scale (DUM)	Very large — >5 million domains (score 10/10)	 10/10

Disaster scenario

A sustained artillery/drone campaign targeting national critical infrastructure disables two of three data centres and cuts power to the primary metropolitan area for 11 days. Internet exchange points partially fail. Key technical staff is incapacitated.

Impact on BC/DR

The registry's documented BC/DR plan activates. The tertiary data centre, geographically dispersed, takes over within 2 hours — (as required under the NIS 2 RTO envelope). DNSSEC signing continues. Registration provisioning degrades to read-only mode.

Potential IANA role: Minimal active role

Observations This ccTLD has strong self-sufficiency. IANA's role is essentially standby. The main risk is administrative: if the corporate entity becomes legally inoperative due to wartime law, a re-delegation request may arise — which is a lengthy process IANA should anticipate. This use case illustrates that a well-resourced, well-regulated operator renders IANA's operational role close to zero.

UC-2 | Island government ccTLD — total infrastructure collapse

Profile across five dimensions

Regulatory framework	Absent — no formal framework (score 1/10)		1/10
Governance model	Government — 1 to 2 staff (score 2/10)		2/10
DNS service	Fully outsourced to regional provider (score 1/10)		1/10
Registration service	Fully outsourced to regional provider (score 1/10)		1/10
Scale (DUM)	Micro — fewer than 5 000 domains (score 1/10)		1/10

Disaster scenario

A category-5 cyclone makes direct landfall. The government ministry building is destroyed. Both staff members authorized as admin/tech contacts are unreachable for weeks. The DNS outsourcing provider is also affected. The submarine cable is severed.

Impact on BC/DR

The ccTLD ceases to function as a registry. The outsourced DNS provider cannot receive authoritative instructions. No succession plan exists. No data escrow arrangement is in place, meaning registration data may be permanently lost. The country's government email, health systems, and emergency services that rely on the ccTLD go dark.

Potential IANA role: Central and potentially sole actor

Observations This is the scenario most likely to require a formal IANA emergency procedure. Pre-arranged agreements with a neighboring ccTLD, would dramatically reduce response time. IANA or others could develop a pre-agreed protocol for this class of event — such a protocol does not currently exist.

UC-3 | Academic ccTLD — hurricane and loss of key personnel

Profile across five dimensions

Regulatory framework	Emerging — CARICOM CCSCAP guidance (score 3.5/10)		4/10
Governance model	Academic / university operator (score 3/10)		3/10
DNS service	Mixed — university primary plus outsourced backup (score 4/10)		4/10
Registration service	Outsourced to regional provider (score 2/10)		2/10
Scale (DUM)	Small — 5 000 to 50 000 domains (score 3/10)		3/10

Disaster scenario

A major hurricane causes the university campus to flood. The server room, located on the ground floor, is destroyed. The sole DNS administrator — a faculty member — is injured and hospitalized. The vice-chancellor has no technical knowledge of the ccTLD. The outsourced registration provider on a neighbouring island is also affected.

Impact on BC/DR

DNS resolution fails within 48 hours as the primary nameserver managed by the ccTLD goes offline. The outsourced, secondary nameservers are still functional but cannot receive zone updates. Registration provisioning halts. The university has no succession plan. CARICOM's CCSCAP framework provides guidance but imposes no binding obligation and provides no emergency funding.

Potential IANA role: Coordination and facilitation

Observations A key risk here is ambiguity about who can authorize changes in the absence of named contacts. IANA needs a clear policy on what constitutes sufficient authority in an emergency. A pre-existing tri-party agreement — involving IANA, the university, and a regional backup operator — would have resolved this situation before the hurricane struck.

UC-4 | Government registry — prolonged power outage

Profile across five dimensions

Regulatory framework	Moderate — national cybersecurity framework (score 5/10)		5/10
-----------------------------	--	---	------

Governance model	Government ministry (score 6/10)		6/10
DNS service	In-house at ministry data centre (score 7/10)		7/10
Registration service	Mixed — in-house plus contracted provider (score 5/10)		5/10
Scale (DUM)	Medium — 100 000 to 500 000 domains (score 6/10)		6/10

Disaster scenario

A nationwide infrastructure crisis causes rolling blackouts lasting six weeks. The ministry's backup generator runs out of fuel after 72 hours. A cloud migration program is incomplete. Staff can work remotely but cannot access on-premise systems. The contracted registration platform is in a local colocation facility that also loses power.

Impact on BC/DR

DNS resolution continues for approximately 48 hours on cached TTLs, then degrades. Registration provisioning halts entirely. The ministry has a partially documented DR plan that assumes a maximum outage of 24 hours — not six weeks. The national telecommunications authority issues emergency powers to the ministry but cannot restore power.

Potential IANA role: Advisory and technical facilitation

Observations This case illustrates a gap between the existence of a regulatory framework and its effectiveness. A national framework is in place but does not mandate off-site backup or cloud redundancy. IANA's potential advisory role could have high leverage: proactive pre-disaster guidance and minimum standards requirements could prevent this scenario entirely.

UC-5 | Mid-size private registry — political crisis and contested legitimacy

Profile across five dimensions

Regulatory framework	Moderate — national framework plus LACTLD guidance (score 4.5/10)		5/10
Governance model	Private NGO with government adjacency (score 5/10)		5/10
DNS service	In-house primary plus outsourced secondary (score 6/10)		6/10
Registration service	In-house (score 6/10)		6/10

Scale (DUM) Large — 500 000 to 2 million domains (score 7/10)  7/10

Disaster scenario

A constitutional crisis leads to a change of government. The new administration issues a decree nationalizing the ccTLD and appointing a new operator. The existing operator — a non-profit — refuses to comply and retains physical control of the registry infrastructure. Both parties contact IANA claiming to be the legitimate operator.

Impact on BC/DR

DNS resolution continues — the technical infrastructure is intact. Registration contracts are in legal limbo and Registration provision deteriorates. Registrars are uncertain whether to accept provisioning instructions The legitimacy of any change request to IANA is contested. . . The situation could remain unresolved for months or years.

Potential IANA role: Gatekeeper — contested legitimacy requires administrative resolution

Observations This is the boundary case between disaster recovery, transfer and revocation. IANA's potential role is ambiguous: not technical but judicial-administrative. The risk is that maintaining the status quo — the current operator — is itself a political choice. The study group should consider whether this scenario falls within its scope or requires a separate approach, is addressed through RFC1591 as interpreted by the Fol, or should be addressed in other way (for example advising Council of additional GAP)

UC-6 | Large government registry — active war, operator incapacitated

(composite scenario)

Profile across five dimensions

Regulatory framework	Strong national — government decree framework (score 7/10)	 7/10
Governance model	Government / state authority (score 9/10)	 9/10
DNS service	In-house at state data centre (score 8/10)	 8/10
Registration service	In-house — state authority (score 8/10)	 8/10
Scale (DUM)	Large — 1 to 5 million domains (score 8/10)	 8/10

Disaster scenario

Active military conflict results in the destruction of the primary state data centre. The secondary site is in occupied territory. The ccTLD authoritative leadership is off the radar (whereabouts unknown, or incapacitated in another way). A government-in-exile claims authority. DNS resolution is failing. A third party — a foreign operator — offers to host the zone temporarily. Simultaneously, technical credentials held by staff in occupied territory are at risk of compromise.

Impact on BC/DR

DNS resolution for a large national ccTLD fails, affecting millions of domains including commercial, governmental, medical, and civilian services. The government-in-exile is internationally recognized but has no remaining technical capacity. Technical staff under the occupying authority attempt to modify root zone records using the original credentials.

Potential role IANA: Emergency authority — highest stakes scenario

Observations This is the most complex and highest-stakes scenario. IANA acting here is unprecedented and carries geopolitical risk. The study group could explicitly address this situation, either itself or defer to one of the other Study Groups

ANNEX D | References

Presentations BC/DR

Sydney, ICANN35 (June 2009) – ccNSO Members Meeting

Business Continuity under .eu – G. Seppia (EURid):

<http://syd.icann.org/files/meetings/sydney2009/presentation-ccnso-members-seppia-24jun09-en.pdf>

Redundancy for Registry Services – S. Dolderer (.de):

<http://syd.icann.org/files/meetings/sydney2009/presentation-redundancy-registry-dolderer-24jun09-en.pdf>

Attack & Contingency Response Planning, a small-registry case – L.D. Espinoza (.cr):

<http://syd.icann.org/files/meetings/sydney2009/presentation-ccnso-members-espinoza-24jun09-en.pdf>

Contingency Actions for the Operations of .mx – O. Robles (.mx):

<http://syd.icann.org/files/meetings/sydney2009/presentation-ccnso-members-mx-24jun09-en.pdf>

Session abstracts: <https://ccnso.icann.org/en/meetings/sydney/abstracts.htm>

Haiti (.ht), January 2010 – IANA operational account

“Situation in Haiti and the DNS” – Kim Davies (IANA), ICANN blog, 14 Jan 2010:

<https://www.icann.org/en/blogs/details/situation-in-haiti-and-the-dns-14-1-2010-en>

Operational detail (name-server failover to Australia) – NANOG mailing list, Jan 2010:

<https://seclists.org/nanog/2010/Jan/600>

Background: IANA Report on Redelegation of .HT (2004):

<https://www.iana.org/reports/2004/ht-report-13jan04.html>

JPRS (.jp) natural-disaster presentations

JP Experience of Earthquake, Tsunami, and Nuclear Plant Accident – H. Hotta, ICANN41 Singapore (2011):

<https://archive.icann.org/en/meetings/singapore2011/bitcache/JP%20Experience%20of%20Earthquake,%20Tsunami,%20and%20Nuclear%20Plant%20Accident%20-%20Hiro%20Hotta,%20.jp-vid=25867&disposition=attachment&op=download.pdf>

Natural Disaster: .JP’s Experience and Preparation – H. Hotta, ICANN61 San Juan (2018):

<https://ccnso.icann.org/meetings/sanjuan61/presentation-jp-experience-14mar18-en.pdf>

San Juan, ICANN61 (March 2018) – host registry, post-Maria

.PR Puerto Rico Top Level Domain – P. Rodriguez (nic.pr), Tech Day:

<https://ccnso.icann.org/meetings/sanjuan61/presentation-tech-day-pr-tld-12mar18-en.pdf>

Pandemic-era ccTLD News sessions (2020–2022)

COVID-19: a force majeure – M. Dias (.pt); Impact on .GE – S. Khidasheli (.ge); .ng registry-registrar practices – E. Iyortim (.ng); slides via the ccNSO Webinars archive: <https://icann-community.atlassian.net/wiki/spaces/ccnsowkspc/pages/108402879/ccNSO+Webinars>

Dublin, ICANN84 (October 2025) – IANA ccTLD Disaster Recovery session

Session deck (incl. BC/DR definitions, threat taxonomy, and the .mg case) – P. Koch (chair), R. Massé (.fr / TLD-OPS), K. Davies (IANA), F. Arias (ICANN): https://static.sched.com/hosted_files/icann84/b9/Disaster%20Recovery%20.pdf

Seville, ICANN86 (June 2026) – ccTLD News session

.ua (Hostmaster) on registry continuity under wartime conditions; session listing: <https://icann86.sched.com/>

Background on the 2022 relocation of .ua name servers: <https://hostmaster.ua/news/?pr20220226>

ICANN's response declining Ukraine's request to remove Russia's ccTLDs (governance, not DR, episode): <https://www.internetsociety.org/resources/2022/impact-of-ukraines-requests-to-block-russias-access-to-the-internet/>

TLD-OPS: Playbook, TTX and Study Group

DR & BC Playbook release announcement (Dec 2019): <https://ccnso.icann.org/en/announcements/announcement-17dec19-en.htm>

TLD-OPS workspace (Playbook, TTX toolkit, translations): <https://icann-community.atlassian.net/wiki/spaces/ccnsowkspc/pages/108404994/TLD-OPS>

DR/BCP drafting-team status – J. Latour (.ca), ICANN65 (2019): <https://ccnso.icann.org/sites/default/files/field-attached/presentation-tld-ops-cctld-security-stability-25jun19-en.pdf>

ccNSO Disaster Recovery Study Group: <https://icann-community.atlassian.net/wiki/spaces/ccnsowkspc/pages/511541357/ccNSO+Disaster+Recovery+Study+Group>

Disaster Recovery Study Group 2026: <https://icann-community.atlassian.net/wiki/spaces/ccnsowkspc/pages/613122062/Disaster+Recovery+Study+Group+2026>

Purpose: Survey instrument and results, interview programme (roles, not names), regulatory frameworks comparison table, landscape data tables, glossary, and membership and background material.

References BC/DR

Sources for the definitions, standards, and governance points above

International standards

- ISO 22301:2019 — Security and resilience: Business continuity management systems — Requirements. International Organization for Standardization.
- ISO 22313:2020 — Security and resilience: Business continuity management systems — Guidance on the use of ISO 22301.
- ISO/TS 22317:2021 — Security and resilience: Business continuity management systems — Guidelines for business impact analysis.
- ISO/TS 22330:2018 — Security and resilience: Business continuity management systems — Guidelines for people aspects.
- ISO 22320:2018 — Security and resilience: Emergency management — Guidelines for incident management.
- ISO/IEC 27031:2011 — Information technology: Security techniques — Guidelines for ICT readiness for business continuity.
- ISO/IEC 24762:2008 — Information technology: Security techniques — Guidelines for ICT disaster recovery services.
- ISO/IEC 27001 — Information security management systems — Requirements (referenced as the parent family for ISO/IEC 27031).

ICANN / ccNSO governance

- Terms of Reference — IANA role in ccTLD Disaster Recovery Study Group, *Draft June 2025, adopted by the ccNSO Council*. Source of the scope statements on ccTLD-manager responsibility, IANA's reactive role, and private pre-arrangements.
- Final Report of the PGA Working Group — background material cited by the Study Group Terms of Reference.
- IANA's Topic Areas for ccTLD Policy Reviews — background material cited by the Study Group Terms of Reference.
- ccNSO TLD-OPS (Technical Operations) Committee background material — the operational-security community the Study Group is encouraged to engage.

Operational / community reference

- ICANN registry framework and IANA function — root-zone management and delegation of ccTLDs (Layer 2 of the layered model).
- DNS-OARC — operational coordination body relevant to registry resilience and mutual support.