



84

ANNUAL
GENERAL
MEETING



ccNSO Members Meeting

IANA ccTLD Disaster Recovery Session

29 October 2025



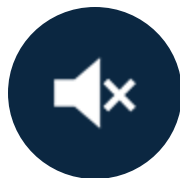
**SPEAK SLOWLY
AND CLEARLY.**



**USE A HEADSET
FOR BETTER
AUDIO AND
INTERPRETATION.**



**RAISE YOUR HAND
IN ZOOM TO JOIN
THE QUEUE.**



**ON SITE? PLEASE
MUTE YOUR ZOOM
AUDIO.**



**REMOTE? PLEASE
TURN ON YOUR
CAMERA WHEN
SPEAKING.**



**SPEAKING IN A
LANGUAGE
OTHER THAN
ENGLISH? LET US
KNOW FOR
INTERPRETATION.**



Have a headset ready!

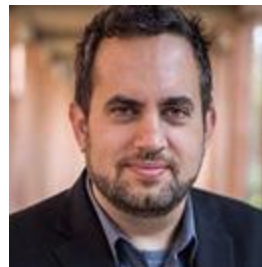
Participants could present, ask questions, or contribute in languages other than English.

IANA Disaster Recovery (DR) Session

Wednesday, 29 October 2025 | 13:15-14:30 local, UTC +0

Session chair: Peter Koch (.de), Chair ccNSO Study Group on IANA DR

- **TLD-OPS perspectives** | Régis Massé (.fr), Chair TLD-OPS Standing Committee
- **IANA perspectives** | Kim Davies (ICANN), VP, IANA Services & President, PTI
- **About Emergency Back-end Registry Operators (EBERO) and the ICANN ESCROW Program** | Francisco Arias (ICANN), VP, GDS Technical Services
- **Observation by AFNIC CTO** | Régis Massé (.fr)
- **ccTLD perspectives** | moderated by Peter Koch



TLD-OPS Perspective

Régis Massé (.fr), Chair TLD-OPS Standing Committee

TLD-OPS Working Group

◆ Definition and General Role

- TLD-OPS is the operational security community for top-level domain (TLD) registries within the ICANN ecosystem
- It provides a trusted platform for cooperation and information sharing among TLD operators to manage security incidents, enhance DNS resilience, and coordinate responses to threats
- Participation is restricted to authorized technical contacts of ccTLD registries

◆ Main Objectives

- Facilitate coordinated responses to DNS-related security incidents
- Provide secure emergency communication channels between ccTLD operators
- Share best practices on operational security and incident response
- Enhance global DNS operational continuity through collaboration and mutual support
- Enables rapid, secure information exchange during crises, minimizing operational disruptions

Business Continuity (BC) versus Disaster Recovery (DR)

- ◆ **What is Business Continuity?**

Business Continuity is the capability of an organization to continue delivery of products or services that are important to the ccTLD registry operator's business and stakeholders at acceptable, predefined levels following a disruptive incident

- ◆ Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) are related but not interchangeable

The former consists of a plan of action focussing on delivering regular business during a crisis ; the latter is a subset and involves procedures to restore vital systems in the shortest time possible that the business requires

- ◆ Differently said a Business Continuity Plan will contain references to a number of Disaster Recovery Plans

TLD-OPS DR/BCP Deliverables

◆ DR/BCP Playbook:

- TLD-OPS developed a series of documents to help ccTLDs with their DR/BCP posture and the tools for a ccTLD to perform their own table top exercise
- Documents translated into several languages

◆ Table Top eXercise documents:

- The Tabletop Exercise (TTX) simulates a crisis scenario, allowing participants to role-play their responses in a structured and interactive environment
- Here's how the exercise works:
 - Group Dynamics and Structure
 - Action Cards
 - Turn-Based Role-Playing
 - Debriefing and Evaluation

<https://icann-community.atlassian.net/wiki/spaces/ccnsowkspc/pages/108404994/TLD-OPS>

DR/BCP Table Top eXercise (TTX) Workshop

- Simulate a registry compromise
- Test the DR/BCP Playbook against the scenario
- Update the DR/BCP Playbook against the gaps, observations and lessons learned
- Two sessions:
 - ICANN 66
 - ICANN 81 (with European TLD-ISAC)





IANA Perspective

Kim Davies (ICANN), VP, IANA Services & President, PTI

Emergency Back-end Registry Operators (EBERO) and the ICANN ESCROW Program

Francisco Arias (ICANN), VP, GDS Technical Services

NEW gTLD PROGRAM: NEXT ROUND

Business Continuity in gTLDs

Francisco Arias | 29 October 2025



gTLD

Data Escrow

- Allows ICANN to restore registry services in case of catastrophic failure by the registry
- gTLD registries are required to escrow registration data with an ICANN-approved Data Escrow Agent (DEA)
- Required to be deposit daily either as a full or differential deposit
- Deposits follow RFCs 8909 and 9022 format
- The gTLD registry agreements specify what data is required to be escrowed
- More information: <https://www.icann.org/en/contracted-parties/registry-operators/services/data-escrow>

SLA Monitoring - SLAM

- Zabbix monitoring platform plus custom code
- Monitors registry and registrar's compliance with their SLAs
- Other parts of the code developed internally
- Probe node network consists of ~40 probe nodes distributed globally
- Centralized servers that compile, analyze and act on the data collected by the probe nodes
- A Network Operations Center operating 24/7
- ICANN staff on-call 24/7

Monitoring System API - MoSAPI

- REST API that allows registries and registrars to retrieve information:
 - Collected by the SLAM
 - Produced by Domain Metrica - <https://domainmetrica.icann.org/>
- Available for both gTLDs and ccTLDs
- A ccTLD can request via globalSupport@icann.org, which will be authenticated relying on the ccTLD contacts in IANA
- More information at <https://www.icann.org/mosapi/>

Emergency Thresholds

Critical Function	Emergency Threshold
DNS Service	4-hour total downtime / week
DNSSEC proper resolution	4-hour total downtime / week
EPP*	24-hour total downtime / week
RDAP	24-hour total downtime / week
Data Escrow	failed to submit at least one full deposit in a consecutive 8-day period starting on any given Sunday**

* Not implemented yet

** Proposed for next round

The matrix presents the emergency thresholds that, if reached by any of the services, for most gTLDs, would cause the emergency transition of the TLD to an emergency operator

Emergency Back-End Registry Operator - EBERO

- ICANN maintains three EBERO providers under contract that are ready to be activated 24/7
- An EBERO provider can be temporarily activated if a critical function of a gTLD reaches any of the emergency thresholds
- EBEROs provide the five critical functions that gTLDs are required to offer: DNS, DNSSEC, EPP, RDAP, Data Escrow
- Since the delegation of the 2012 round gTLDs, ICANN has taken 7 gTLDs to EBERO

NEW gTLD PROGRAM: NEXT ROUND

gTLD

Q&A

Visit us at <https://newgtldprogram.icann.org>



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin.com/company/icann



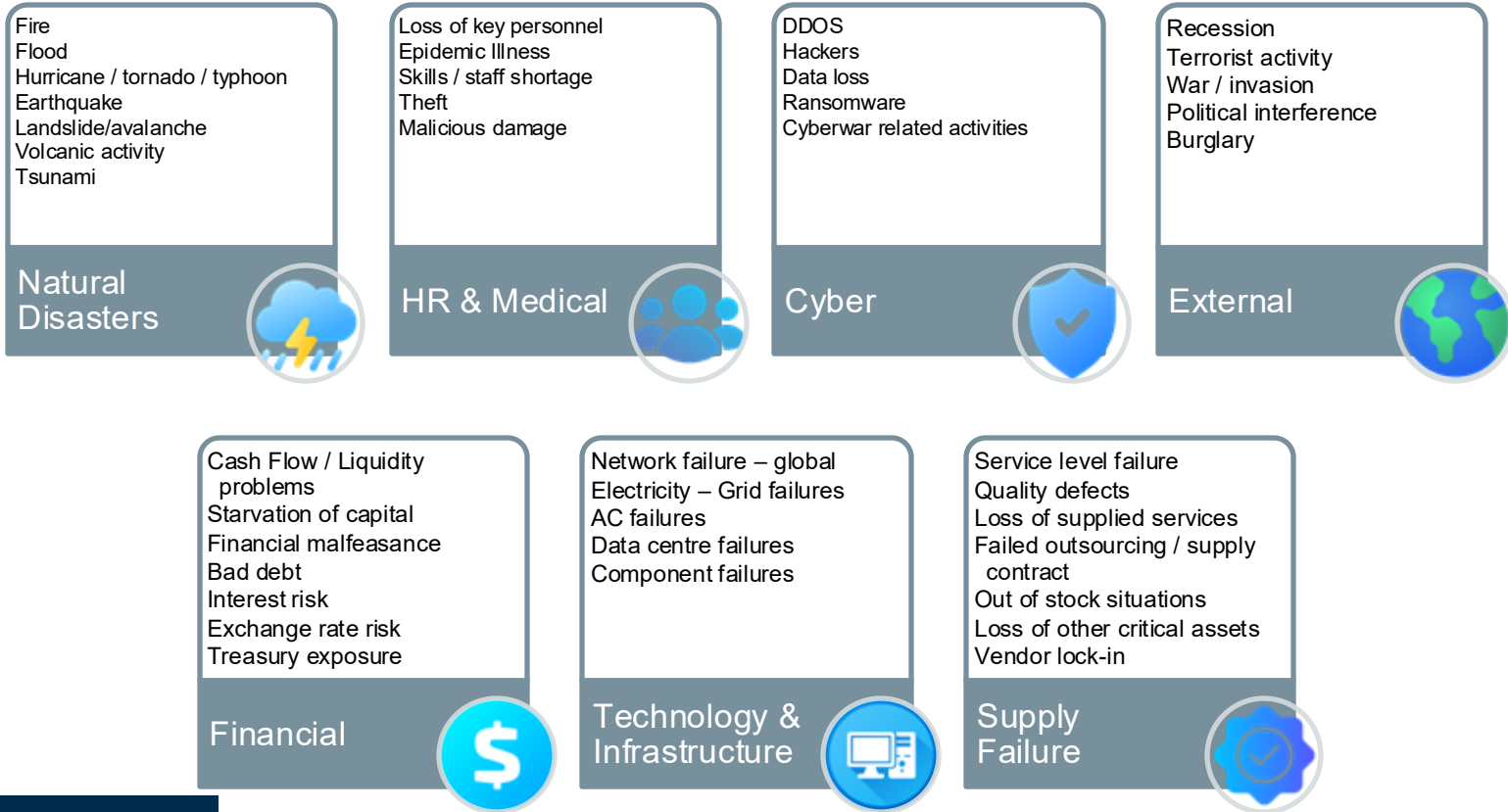
instagram.com/icannorg



Observation by AFNIC CTO

Régis Massé (.fr)

Threat categories / Illustrative examples



A recent example

- ◆ **The attack on the nic.mg registry**

The nic.mg registry was burglarized on the night of September 25, 2025: all computer and electrical equipment was stolen, leaving no production tools in the offices

- ◆ The DNS resolution infrastructure was not affected
- ◆ With great courage, the registry team has:
 - Implemented recovery procedures
 - Deployed a new recording infrastructure at a local operator
 - Reinstalled Cocca, used external backups, and restarted registration services within a few days
- ◆ The registry should be fully operational again by the end of the year



.ac Ascension Islands	.cu Cuba	.hm Heard and McDonald Islands	.ms Montserrat	.so Somalia
.ag Antigua and Barbuda	.cx Christmas Islands	.io British Indian Ocean Territory	.mv Maldives	.sr Suriname
.ai Anguilla	.dj Djibouti	.jm Jamaica	.nc New Caledonia	.ss South Sudan
.ao Angola	.er Eritrea	.kg Kyrgyzstan	.ne Niger	.st Sao Tome and Principe
.aq Antarctica	.es Spain	.kn Saint Kitts and Nevis	.nf Norfolk Island	.sz Swaziland
.bd Bangladesh	.et Ethiopia	.kp Korea, Democratic People's Republic	.np Nepal	.tc Turks and Caicos Islands
.bj Benin	.fk Falkland Islands	.ky Cayman Islands	.nr Nauru	.tg Togo
.bs Bahamas	.ga Gabon	.kz Kazakhstan	.om Oman	.tj Tajikistan
.bt Bhutan	.gf French Guiana	.lr Liberia	.pf French Polynesia	.tm Turkmenistan
.bz Belize	.gn Guinea	.ly Libya	.pk Pakistan	.tv Tuvalu
.cd Congo, the Democratic Republic of the	.gq Equatorial Guinea	.mh Marshall Islands	.pw Palau	.vc Saint Vincent and the Grenadines
.cf Central African Republic	.gs S. Georgia & the S. Sandwich Islands	.ml Mali	.sc Seychelles	.ve Venezuela
.cg Congo, Republic of	.gw Guinea-Bissau	.mm Myanmar	.sd Sudan	.ws Samoa
.ck Cook Islands	.gy Guyana	.mp Northern Mariana Islands	.sh Saint Helena, Ascension and Tristan da Cunha	.zw Zimbabwe
.cm Cameroon		.mq Martinique	.sl Sierra Leone	

Questions?

ccTLD perspectives

Mentimeter polling

Thank you!

Next session: Q&A with candidates ccNSO Council and Board Seat 11