Sound check script

Please read out loud

Hello, my name is - - - and I will be speaking during the session today.

I am testing my audio to confirm that the technical service providers can hear me clearly.

ICANN 86 POLICY FORUM

ccNSO Community Sessions

Resilience Session (2 of 2)

9 June 2026

ICANN | ccNSO

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.

NON-ENGLISH SPEAKER? LET US KNOW FOR INTERPRETATION.

Have a headset ready!

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

Resilience Session (2 of 2)

ccTLD perspectives

Tuesday, 9 June 2026 | 16:30-17:30 local

Session Chair: Annaliese Williams, .au (IGLC Chair)

- Katrina Sataki, .lv
- Seyi Onasanya, .ng

ICANN | ccNSO

https://www.icann.org/en/ccnso/resources/governance/statements-of-interest

TLP: Amber

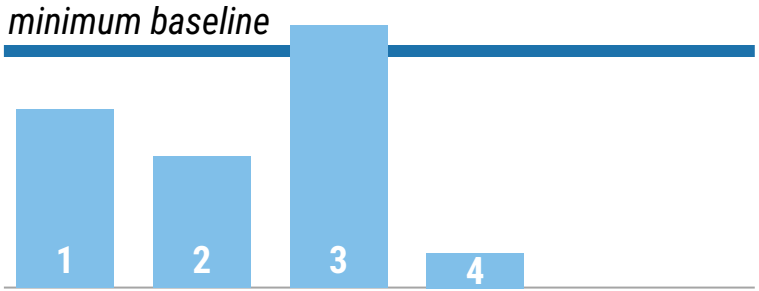
Regulation vs Resilience

Katrina Sataki, NIC.LV

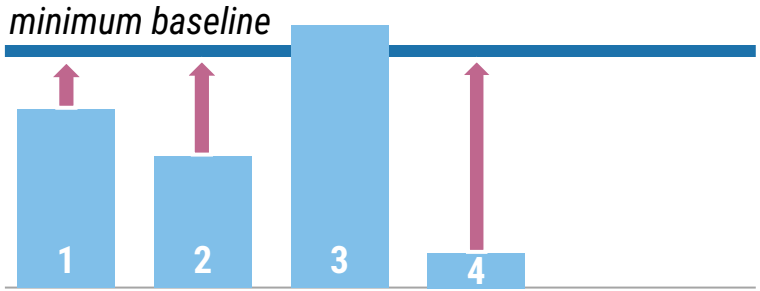
ccNSO Meeting, ICANN86, Seville


GDPR
eIDAS
Cybersecurity Act
NIS2
CRA
DSA
AI Act
National legal acts
ePrivacy

Are you serious about your security?



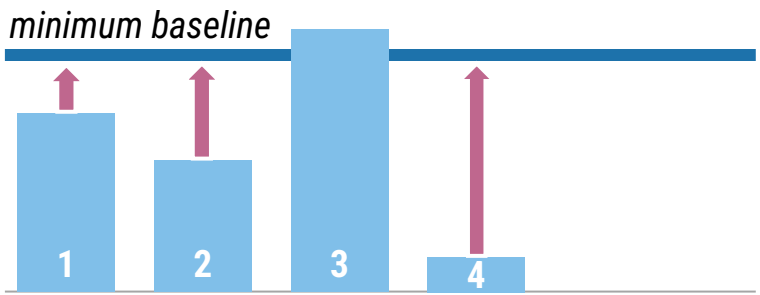
Are you serious about your security?

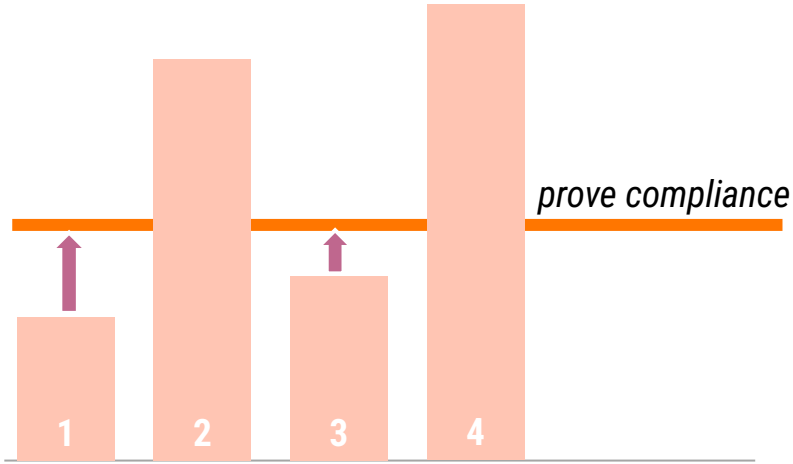


Are you serious about your security?

vs

Can you prove you are serious about your security?





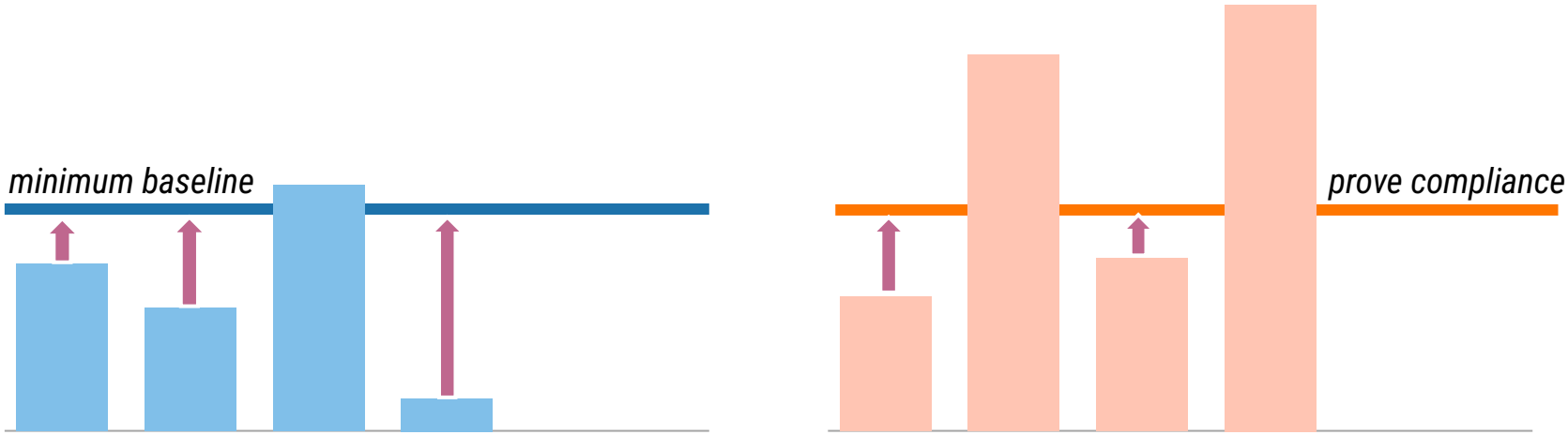

LET'S
HACK THAT
ccTLD


LET'S HACK THAT ccTLD
NO... THEY HAVE STRONG POLICIES

Are you serious about your security?

vs

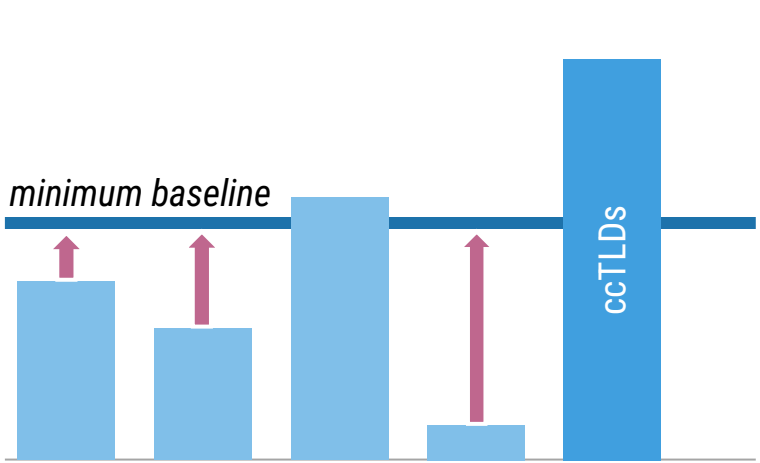
Can you prove you are serious about your security?

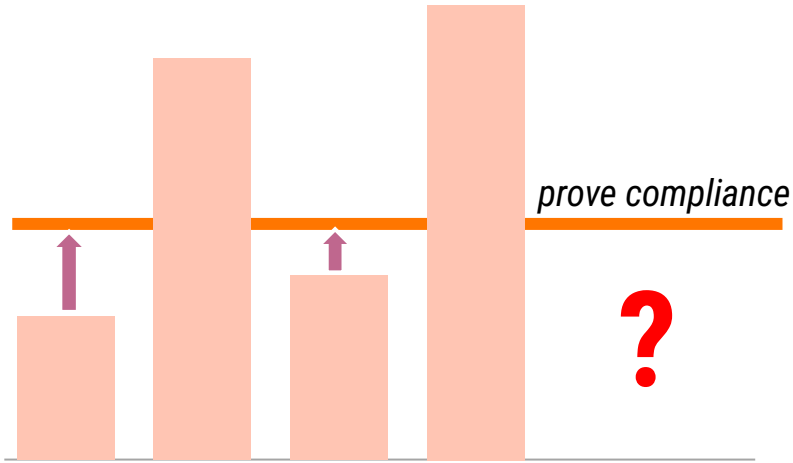


Are you serious about your security?

vs

Can you prove you are serious about your security?





Security **Compliance**


10000
€

LOSSES + FINES

Security

Compliance

Never let a good crisis go to waste.

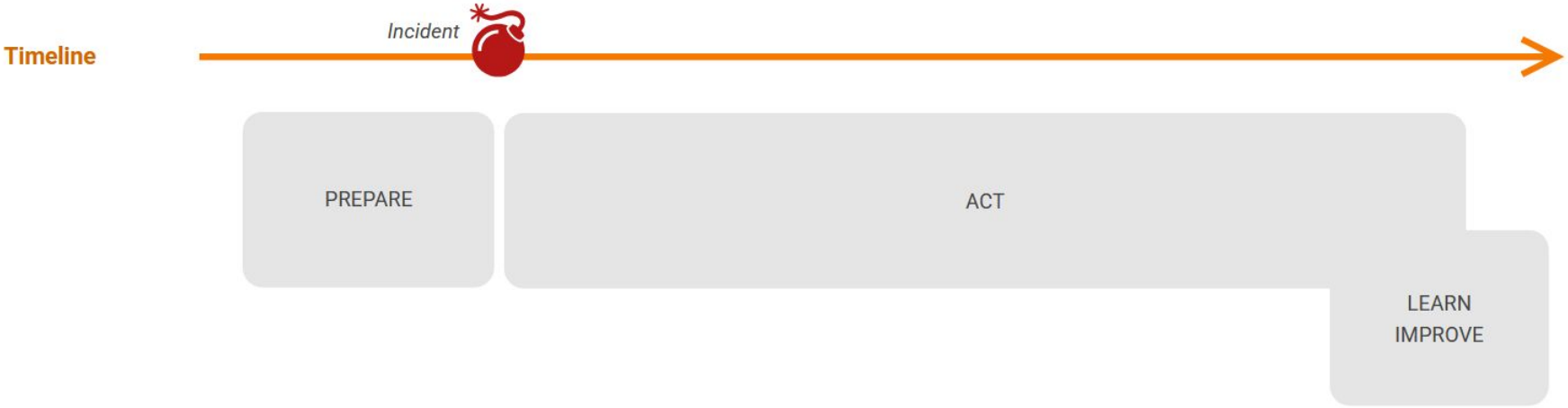
Winston Churchill

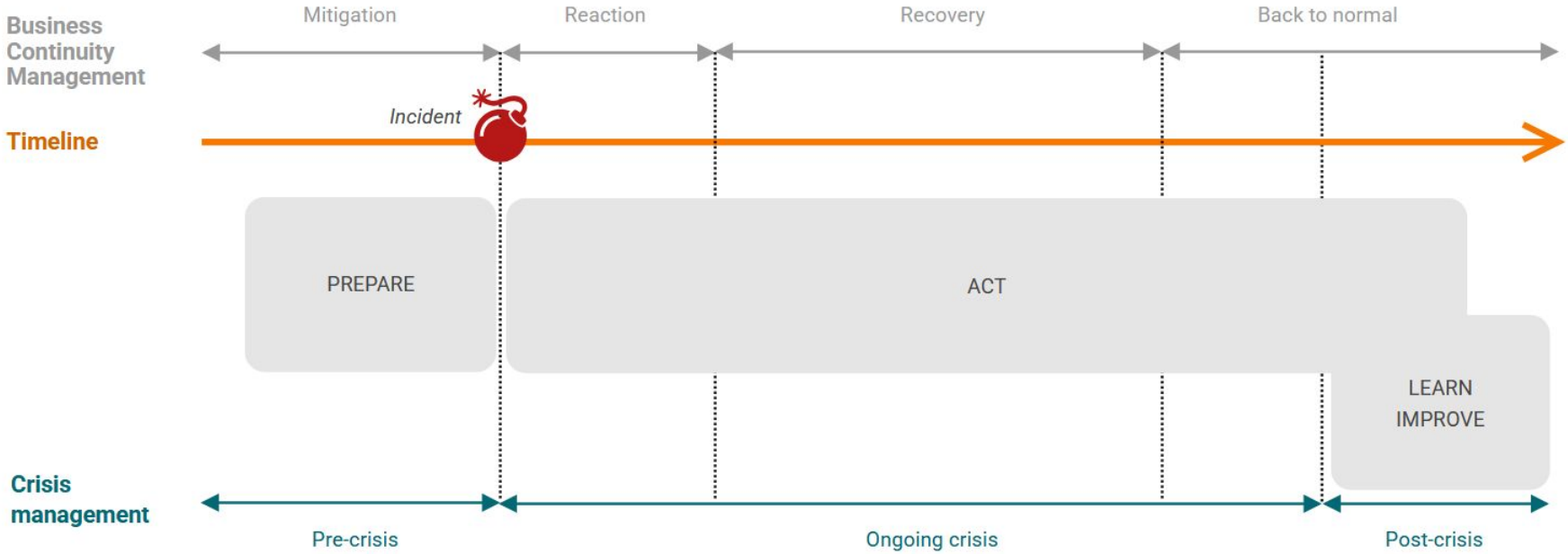
compliance requirement

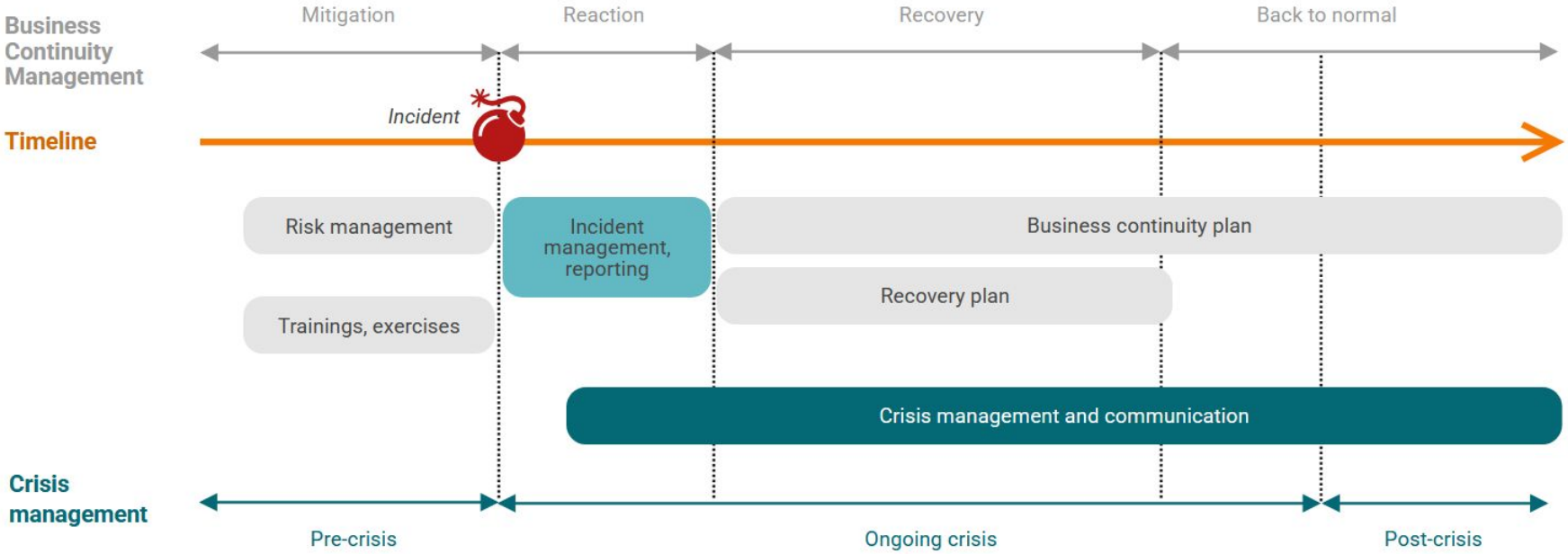
Never let a [redacted] go to waste.

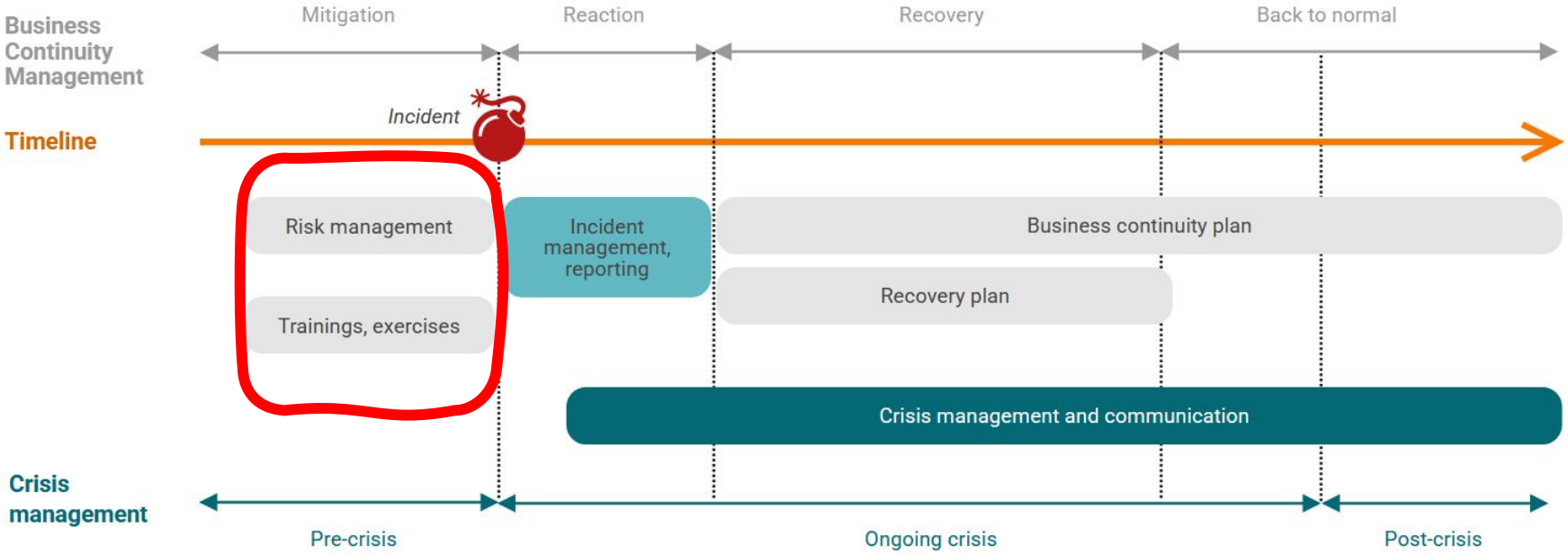
[redacted]

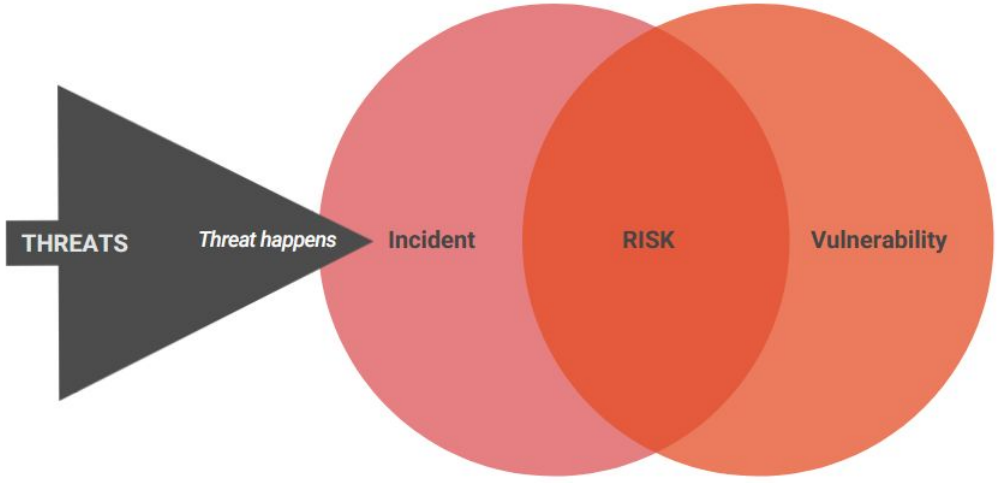
Timeline

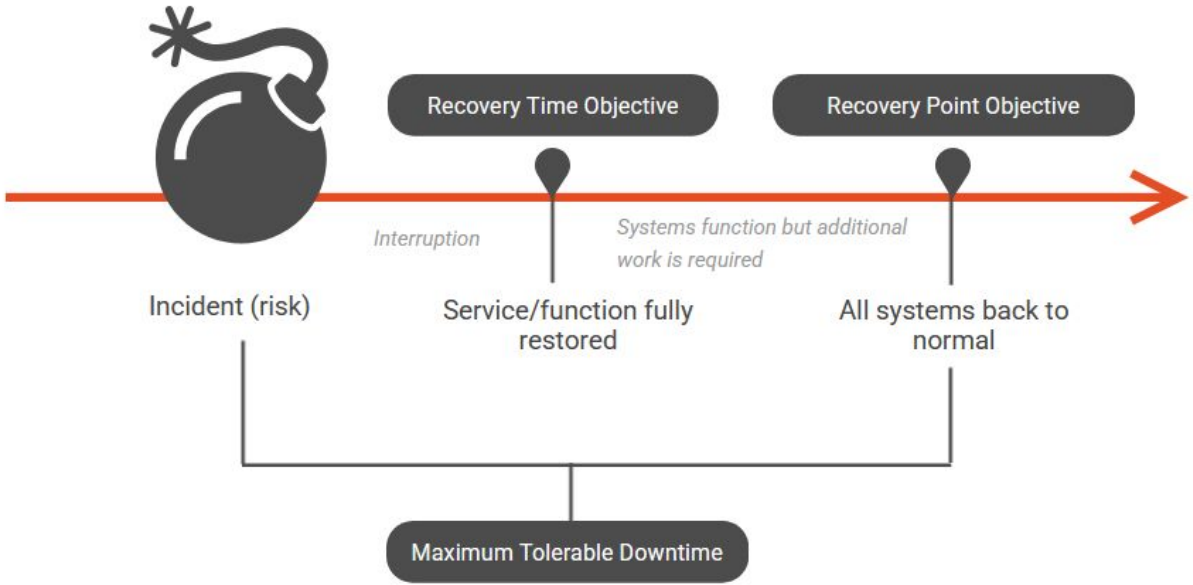

Timeline
Incident
PREPARE
ACT
LEARN
IMPROVE

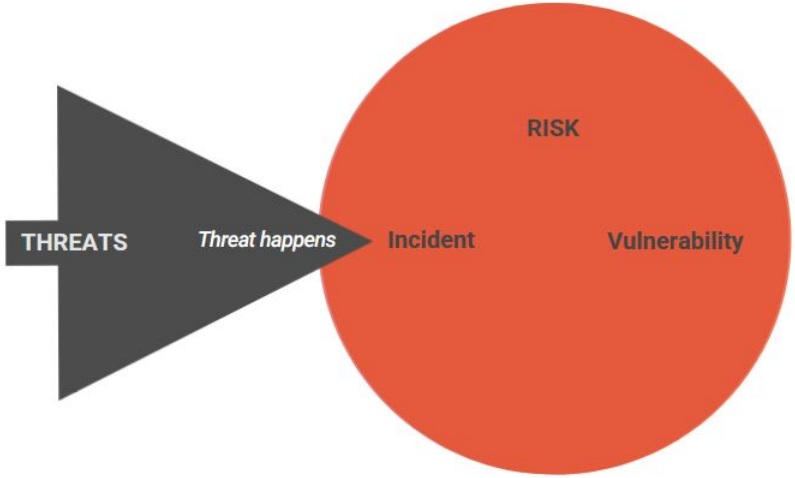

Business Continuity Management
Mitigation
Reaction
Recovery
Back to normal
Timeline
Incident
PREPARE
ACT
LEARN
IMPROVE
Crisis management
Pre-crisis
Ongoing crisis
Post-crisis


Business Continuity Management
Mitigation
Reaction
Recovery
Back to normal
Timeline
Incident
Risk management
Incident management, reporting
Business continuity plan
Recovery plan
Trainings, exercises
Crisis management and communication
Crisis management
Pre-crisis
Ongoing crisis
Post-crisis

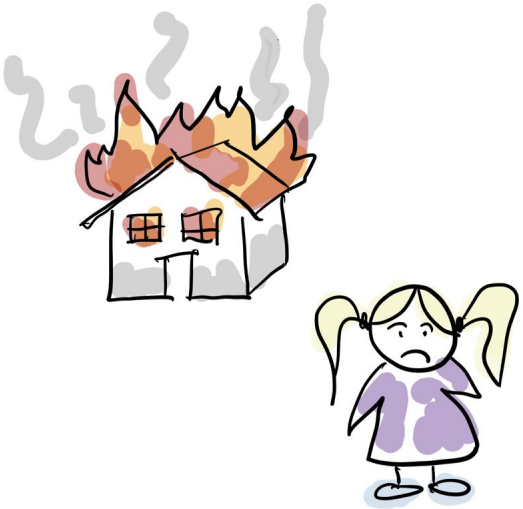

Business Continuity Management
Mitigation
Reaction
Recovery
Back to normal
Timeline
Incident
Risk management
Trainings, exercises
Incident management, reporting
Business continuity plan
Recovery plan
Crisis management and communication
Crisis management
Pre-crisis
Ongoing crisis
Post-crisis


THREATS
Threat happens
Incident
RISK
Vulnerability


Recovery Time Objective
Recovery Point Objective
Interruption
Systems function but additional work is required
Incident (risk)
Service/function fully restored
All systems back to normal
Maximum Tolerable Downtime

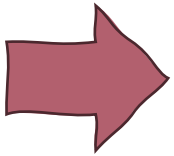

RISK
THREATS
Threat happens
Incident
Vulnerability

What if you lose… EVERYTHING?



Are your priorities really priorities?

Priority 1
Priority 2
Priority 3
Priority 4
Priority 5
…



New priority 1
New priority 2
New priority 3
New priority 4
New priority 5
…

Three lessons learned

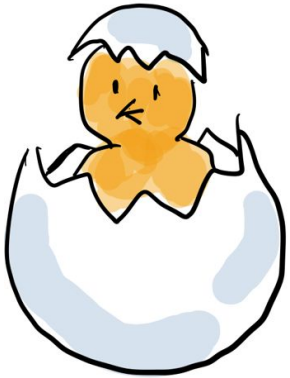
#1 Every incident starts with

Persistent Attempts to Neutralize the Impact of the Crisis!

#1 Every incident starts with **Persistent Attempts to Neutralize the Impact of the Crisis!**

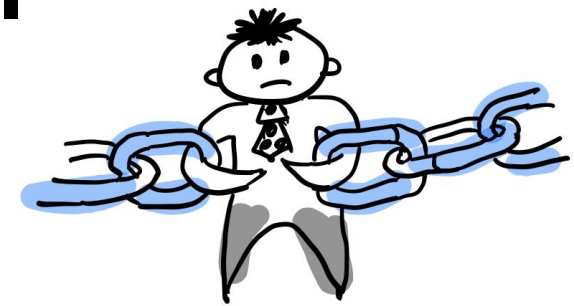
#2 “Are we there yet?”

#3 Every incident will teach you something!



+ one more

If you have to choose between real security and compliance, go for the real stuff!



THANK YOU AND BE SAFE!

NIGERIA INTERNET REGISTRATION ASSOCIATION (NiRA)

Building ccTLD Resilience in a Changing Regulatory Environment: The .ng Experience

Presented at:

ICANN86 Policy Forum in Seville, Spain, from 9th June 2026 | ccTLD Testimonial Session | ccNSO Members Meeting by Seyi Onasanya, COO, NiRA

The .ng Context — Nigeria's Digital Identity Layer

> **".ng is more than a domain extension; it is Nigeria's trusted digital identity infrastructure."**

Digital Sovereignty: Nigeria's digital independence relies on the integrity of our domain infrastructure (**Localising Data** – data sovereignty & data residency, **Strict Hosting** and Securing borders)

Public Interest Stewardship: NiRA manages the .ng namespace to guarantee stability, security, and global integration.

3-Tier Model: Operations run on the secure Registry–Registrar–Registrant pipeline to ensure market efficiency.

241,985
Active .ng Domains

164
Accredited Registrars

Source - https://dashboard.register.ng/

Why Resilience Matters for .ng

“As Nigeria’s digital usage grows, the resilience of .ng becomes central to trust in the national digital economy.”

Rapid Scale: Rapidly expanding digital economy means critical public services, trade, and payment networks rely on DNS stability.

Beyond Technical: Disruption is not just a downtime issue—it has immediate national security, economic, and sovereign reputation costs.

Sovereign Core: .ng underpins Africa's largest digital economy.

Population

220M+

Total national population driving massive digital consumption and identity growth.

Internet Subscription

144.8M

Active internet subscriptions expanding the security perimeter daily.

internet traffic reportedly grew from **517,670.15 TB in January 2023** to **1,385,536.04 TB in January 2026**, showing the scale of digital usage growth

Digital Economy

₦7t

Digital economy contribution to Nigeria GDP

Broadband Penetration

50.58%

Broadband penetration scaling up real-time enterprise and citizen traffic.

Sources: World Bank Population Data; NCC industry data/Spectrum Roadmap 2026; Punch analysis of NCC internet traffic data, March 2026

Regulation as a Driver of DNS Resilience and .ng Adoption

For .ng, regulation is not only a compliance issue; it is a resilience tool when properly shaped through early engagement with policymakers

Sovereign and global demands are shifting operational boundaries. In Nigeria, this translates to dense regulatory policies affecting registration integrity.

Data Protection & Privacy

Enforced under the Nigeria Data Protection Act (NDPA) signed 12 June 2023. Strengthens trust in registrant data handling

Cybercrime Prevention

Strengthened via the amended Cybercrimes Act of 2024. Imposes legal penalties and coordinates fast DNS abuse mitigation. Supports structured response to DNS abuse and online fraud

Sovereign Strategy

NITDA's Strategic Roadmap & Action Plan (2024–2027) focuses on robust infrastructure and trade innovation.

Emerging Bill

National Digital Economy & eGovt Bill (awaiting final passage). Positions .ng as national digital infrastructure. Opportunity to embed .ng and .gov.ng adoption into public-sector digital services.

Public Procurement/Government Identity

Encourages trusted local digital presence for public institutions and vendors

Data Protection | Cybersecurity | Digital Economy | Public Sector | Law Enforcement | DNS Abuse | Consumer Trust

Engaging Lawmakers: Turning Regulation into DNS Resilience

Engage

- Strategic engagement with Senate and House committees on ICT, digital economy, and communications.
- Briefing lawmakers on .ng as national digital identity and critical DNS infrastructure.
- Building understanding of DNS, ccTLD governance, data sovereignty, and digital trust

Influence

- Participation in Senate/public hearing processes.
- Submission of inputs to the National Digital Economy and E-Governance Bill.
- Advocacy for formal recognition of .ng in national digital policy frameworks.
- Push for stronger public-sector use of .gov.ng and .ng-based digital identity.

Institutionalise

- Embed .ng adoption into legislation, policy, procurement, and government digital service delivery.
- Encourage public institutions, regulated sectors, and government contractors to use trusted Nigerian digital identity.
- Strengthen national resilience by reducing dependence on foreign digital identifiers for official services

Legislative engagement>Policy recognition>Public sector adoption>stronger DNS resilience

African Operational Realities

Resilience Cannot Be Imported

Africa cannot copy resilience models built for other operational environments. True resilience is local, scalable, and responsive to regional power and infrastructure realities.

- Nigeria and African ccTLDs face realities that demand adaptive, practical, scalable and cost-aware resilience not imported models require custom, cost-aware architectures.
- NiRA proactively structures data protocols, registrar auditing, and reporting frameworks to translate legal obligations into secure operational processes.
- Strategic focus moved from keeping services online to ensuring survivability under stress and adapting to evolving realities

Operational Challenges

Unstable power, frequent fiber cuts, infrastructure gaps, talent shortages, and high cross-border latency, CAPEX limits

Regulatory Complexity

Rapidly evolving regulations require ccTLDs to translate legal obligations into clear operational processes.

Nigeria's response

Adaptive, practical, scalable, cost-aware resilience became Nigeria's sovereign journey. Foundation is security and resilience starts with security

Historically the focus was:

- Uptime
- redundancy
- DNS availability

The threat landscape evolved

- ransomware
- BGP hijacks
- DNS abuse
- Business Email Compromise (BEC) etc

.ng's Four-Pillar Framework

.ng resilience strategy combines infrastructure, policy, institutional capacity, and ecosystem readiness.

01

Technical Resilience

Signed DNSSEC: Fully signed zone deployment.

Continuous Monitoring: Real-time DNS infrastructure monitoring

Secure Posture: Advanced incident readiness mitigations.

02

Policy Resilience

Policy Update: Review and update of registry policies

Law/Policy maker proactive engagement

Alignment - NDPA and cybersecurity obligations

Registrar compliance and audit frameworks

DNS Abuse Mitigation Enforcement – lawful escalation procedures

03

Institutional Resilience

Board Engagement: Direct strategic alignment.

Internal Roles: Specialized compliance enforcement positions

Capacity Building: Technical secretariat training.

ng Academy Learning Management Platform (LMS)

Tech Convergence – our Flagship even to engage law makers, policy makers and the ecosystem

04

Ecosystem Resilience

Joint Briefings: Ongoing regulatory updates.

Registrar Forums: Frequent technical alignment bootcamps.
Registrar capacity development programs
Technical knowledge-sharing workshops

Public Sector: Coordinated policy engagement networks.
Law & Policy makers engagement

DNSSEC as a Trust and Resilience Milestone

“DNSSEC is not just a technical upgrade; it is a trust signal for Nigeria’s digital economy.”

DNSSEC Milestone	Current Status	Next Phase
.ng Zone fully signed with cryptographic keys	Completed Feb 2026	Zone fully signed and operational
Registrar Readiness & Onboarding	registrars technically ready - ongoing	Enabling secure DNSSEC for .ng domains
Registrant Enablement	training sessions - ongoing	Rolling out DNSSEC to domain holders

.ng Stakeholder Engagement —Collective Governance for DNS Resilience

“DNS resilience is no longer only technical engagement alone. It is increasingly shaped by the legal and policy environment, and this requires strategic collaboration across Nigeria’s digital ecosystem.”

NCC Alignment
National infrastructure resilience, routing compliance, and critical backbone protections.

NITDA Coordination
Aligning digital cybersecurity and sovereign data governance guidelines.

EFCC Partnerships
Fast-tracked reporting and direct mitigation of cyber fraud domains.

ISP & Exchange Points
Localizing national routing networks to withstand subsea fiber blackouts.

Legisla

Digital Infrastructure (DNS Resilience Impacts Economic Interdependence)

16% - 18%

Digital economy Contribution to Nigeria GDP

With Nigeria's non-oil sector driving 96.08% of GDP expansion, DNS infrastructure resilience functions as the base of national transactional security. There is target to increase contribution to 21% of GDP by 2030

Source – The Guardian(August 2025)

Lessons from the .ng Experience – an evolving resilience journey

01 Early regulatory engagement helps policy makers understand the DNS realities before obligations are made thereby facilitating realistic implementation by the Registry

02 Comprehensive Readiness: Infrastructure stability must be integrated with institutional, legislative, and operational alignment.

03 ccTLD adoption and public policy: When national digital policy recognises the ccTLD, adoption becomes part of identity, trust, procurement, e-government, and digital sovereignty. This accelerates adoption

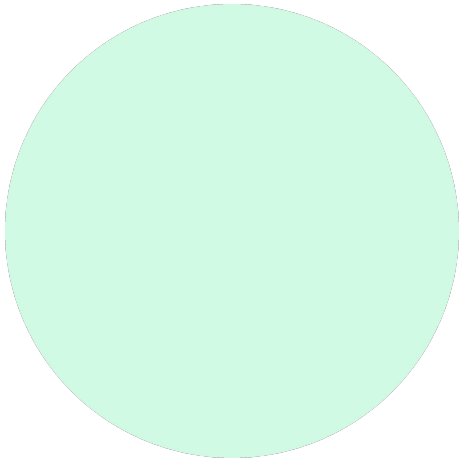
04 Policy only improves resilience when it becomes clear procedures for registrars, registrants, abuse response, data handling, and compliance

05 DNS resilience is now a governance issue. Technical stability remains essential, but legal clarity, policy alignment, institutional trust, and stakeholder coordination are now equally important.

From ccTLD Stability to Digital Trust

NiRA has evolved from a domain registry operator into a resilience orchestrator, cybersecurity catalyst, and positioning towards being Nigeria's core critical digital infrastructure and critical stakeholder in DNS national policy conversations

> "a ccTLD becomes more resilient when the national policy environment recognises it as trusted digital identity infrastructure."



Thank you!

NIRA | .ng
Nigeria Internet Registration Association
Your Nigerian Identity Online

https://academy.ng/ https://nira.org.ng/ https://dashboard.register.ng/ https://www.linkedin.com/company/nigeria-internet-registration-association-nira-/

mentimeter

Preview the questions here:

https://drive.google.com/file/d/1rXdbquJDYkZkrxofpQDf4FJLu_5e4kgy/view?usp=sharing

ccNSO & resilience

https://www.icann.org/en/ccnso/committees-and-working-groups

Internet Governance Liaison Committee (IGLC)

Enhances ccTLD participation in global IG discussions, processes

2026 focus:

- Resilience
- The Future of Internet Governance
- Sovereignty
- Online harms

Disaster Recovery Study Group (DR SG)

Explores IANA's role, if any, in ccTLD disaster recovery

@ICANN86

- Wednesday | 10:00—11:15
  Update & consultation
- Thursday | 10:00-11:15
  Work session

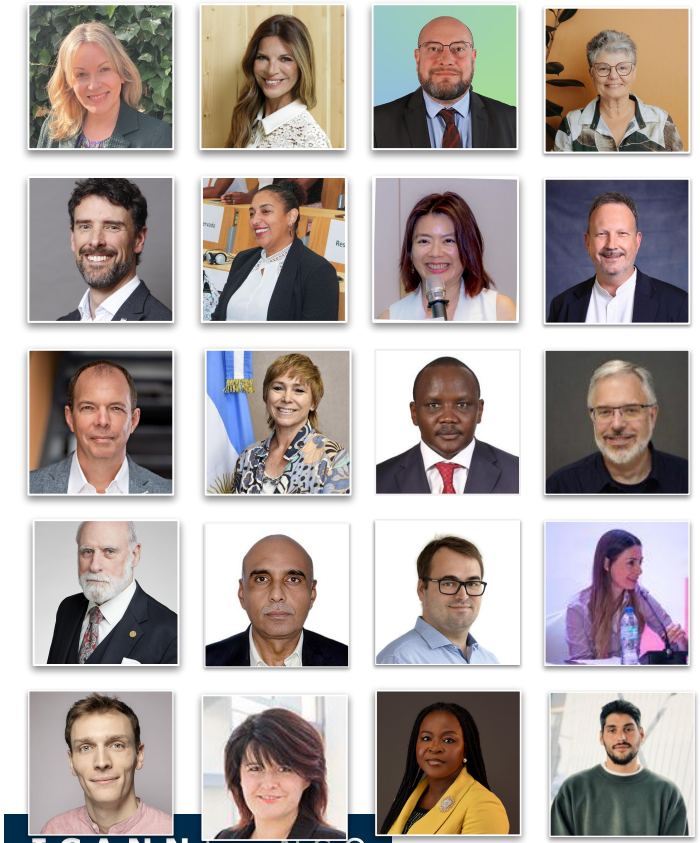
TLD-OPS

A trusted, members-only security and incident response network for ccTLDs

Enables ccTLDs to:

- securely share threat alerts,
- collaborate on DDoS mitigation,
- look up contacts to respond to infrastructure incidents.

Recent IGLC sessions



ICANN83
20 years of WSIS implementation by ccTLDs

ICANN84
WSIS+20 and beyond: a future built by ccTLDs

ICANN85
Regulations impacting ccTLDs

ICANN86
Resilience

https://www.icann.org/en/ccnso/committees-and-working-groups/internet-governance-liaison-committee-iglc

ICANN | ccNSO

About TLD-OPS and its work for the ccTLD community

Global technical incident response community for and by ccTLDs, open to all ccTLDs (ASCII and IDN)

Brings together 400+ people who are responsible for the operational security and stability of 200+ different ccTLDs

Enable ccTLD operators to collaboratively detect and mitigate incidents that may affect the operational security and stability of ccTLD services and of the wider Internet

Raise the security maturity level of ccTLDs: develop a self-assessment maturity model and high-level frameworks to help those with less experience

Disaster Recovery Study Group

Potential role of IANA in ccTLD business continuity and disaster recovery (BC/DR) scenarios

- 6 use cases, each with 5 dimensions:
  - regulatory framework,
  - governance model,
  - DNS service delivery,
  - registration service delivery,
  - domain scale (DUM)
- simulates a severe disruptive event such as infrastructure failure, natural disaster, or armed conflict.

Identifying gaps in current policy

Defining triggers for IANA engagement

Proposing a tiered, proportionate framework

Interested in joining any of the working groups or learning more?

ccnsosecretariat@icann.org

https://community.icann.org/x/4QciCw

Thank you!

Mentimeter poll

- Satisfaction survey
- Bart Tales