ICANN Specific Reviews - Second Security, Stability and Resiliency of the DNS Review (SSR2) Recommendations 7.1, 7.2, 7.3 - Implementation Documentation

SSR2 Final Report
https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

Board resolution on SSR2 Final Report
https://www.icann.org/resources/board-material/resolutions-2021-07-22-en#2.a

- Recommendation submitted: January 2021
- Recommendation approved: November 2022
- Implementation completed: N/A

See https://community.icann.org/display/SSR/Implementation for more information on SSR2 implementation.

SSR2 Recommendation 7.1

ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.

SSR2 Recommendation 7.2

ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).

SSR2 Recommendation 7.3

ICANN org should also establish a DR Plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.

Board Action on SSR2 Recommendations 7.1-7.2-7.3

The Board approves Recommendations 7.1, 7.2, and 7.3 as complete [...]. With regards to Recommendations 7.1, 7.2, 7.3, the Board notes that ICANN org is following the Contingency Planning guide for Federal Information Systems (NIST SP 800-34 Rev 1) which is a more integrated approach with, and given, ICANN org’s existing plans and processes. ICANN org does not plan to introduce ISO standards in its processes. [...]

Final Implementation Report

As noted by the Board, ICANN org is following the Contingency Planning guide for Federal Information Systems (NIST SP 800-34 Rev 1), and does not plan to introduce ISO standards in its processes.

ICANN org has in place a Business Continuity Management which includes Disaster Recovery (DR), Business Continuity (BC) and Crisis Management plans that are followed as applicable and are reviewed/updated annually.

The ICANN Disaster Recovery (DR) Plan was developed by Engineering and Information Technology (EIT), has been in place since 2014 and is continuously reviewed, updated, and tested annually with internal reports produced after each test.

All systems provided by ICANN which support PTI operations and root zone management are covered by this DR plan. This DR plan covers Definition of a Disaster (Declaring a Disaster, Purpose, Scope, Version Control Information & Changes), Disaster Recovery Teams & Responsibilities, Disaster Recovery Call Tree, Communicating During a Disaster, Dealing with a Disaster (Disaster Identification and Declaration, DRP Activation, Communicating the Disaster, Standby Facility Activation), Restoring EIT Functionality (Data and Backups, Ransomware Recovery), Plan Testing & Maintenance.

ICANN Org does not share specific details of the DR and BC plan externally as it contains operational internal procedures. This information is confidential due to the nature and objective of these plans.

Rationale

The recommendation was approved as implemented by the ICANN Board.

Timeline

Expected implementation date: N/A
Final implementation date: N/A

Milestones

N/A.