ICANN Specific Reviews - Second Security, Stability and Resiliency of the DNS Review (SSR2) Recommendations 5.1-5.2 - 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: July 2021
- Implementation completed: February 2024

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

SSR2 Recommendation 5.1

ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement.

SSR2 Recommendation 5.2

Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies.

Board Action on SSR2 Recommendations 5.1-5.2

The Board accepts ICANN org's representation that, once migration to the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework is fully complete, Recommendations 5.1 and 5.2 will be implemented. Therefore, the Board approves recommendations 5.1 and 5.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations, noting that substantial parts of the recommendation are already being addressed or will be addressed once ICANN org's migration to the NIST Cybersecurity Framework is fully complete.

Final Implementation Report

In regards to Recommendation 5.1 specific to the implementation of an ISMS, ICANN org uses the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as its Information Security Management System (ISMS) and risk management

framework. The NIST CSF framework was chosen because it focuses on using business drivers to guide cybersecurity activities, and the consideration of cybersecurity risks as part of the organization's risk management process. The framework also helps foster risk and information security management communications among internal and external stakeholders, as well as between senior executives, business and operations. The framework is designed to complement existing business and information security operations, provides a common language for managing information security risk and can be tailored to an organization’s needs.

Usage of the NIST CSF to manage information security risk was effectively integrated into the ICANN E&IT information security risk management program in 2019, and is a cyclical and continual practice to help manage information security risk at ICANN org.

In regards to the Recommendation 5.1 specific to a roadmap and milestone dates for obtaining certifications and areas targeted for continuous improvement, recommendations from a successful audit of the NIST CSF implementation are analyzed and prioritized by the ICANN org and tracked in a database following ICANN E&IT internal recommendations tracking process. A road map and milestones dates for continuing to comply with the NIST CSF are included in the ICANN Org’s Project Management Schedule where they are tracked appropriately.

In regards to Recommendation 5.1 specific to the audit and certification by a third party, the NIST CSF does not provide certifications for adherence, but offers guidance on using third party audit and assessment tooling. In 2020, ICANN org chose to utilize the Baldrige CyberSecurity Excellence Builder (BCEB) for internal assessments, and cybersecurity maturity assessments for external assessments. These external cybersecurity maturity assessments provide informative references which are mapped to the NIST CSF Functions and Categories to provide a current profile, a target profile and a gap analysis to be used by ICANN org to analyze and prioritize gaps and action plans. The first external maturity assessment was successfully conducted in August 2023 and will be repeated every two years and/or as needed.

The next cycle of the internal assessment using BCEB is anticipated to take place before the end of calendar year 2024. After the completion of the internal assessment, ICANN org will focus on the creation of the current framework profile, a target framework profile, gap determination, analyzation and prioritization, and an action plan to reach the target profile. The external and internal security assessments are both part of the cyclical process ICANN implemented in 2019.

In regards to Recommendation 5.2 specific to a plan for certifications and training requirements in the organization, management of such and justification of how they fit into ICANN org's security and risk management strategies, the ICANN org’s security and risk management strategies include necessary training and certifications identified through NIST CSF. NIST CSF generates reports that include an understanding of the ICANN org

information security workforce profile, their capabilities, how they support the strategic objectives and action plans and how they prepare for changes in capability needs. These outcomes drive necessary training and certifications needs for the workforce responsible for managing information security risk at ICANN; E&IT engineers, all staff, specialty training for specific engineering needs, etc.

All ICANN org staff currently undergo an annual compulsory general cybersecurity training.

Rationale

The rationale for the implementation is to use an established risk driven framework for information security practices and programs.

Timeline

Expected implementation date: N/A
Actual implementation date: August 1 2023

Milestones

- NIST CSF integrated with ICANN E&IT information security risk management program: 2019
- External Information Security Maturity Assessment: Aug 1 2023