Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

SSR2 recommendation	SSR2-defined measures of success	Board action
Recommendations the Board approves, subject to prioritization, risk assessment and mitigation, costing and implementation considerations; and recommendations that the Board approves, with the understanding that they are already fully implemented		
1.1: The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations) **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN Board and ICANN org	n/a	The Board approves Recommendation 1.1, subject to prioritization, risk assessment and mitigation, costing and implementation considerations. Under the Bylaws, the SSR2 Review Team is empowered to determine the extent to which ICANN org has completed implementation of the SSR1 recommendations and has done so as part of its final report. To the extent this recommendation is intended to establish a collaborative mechanism to progress implementation of SSR2 recommendations with input from the SSR2 Implementation Shepherds, the Board approves this recommendation. The Board notes, however, that as a formal matter the Bylaws (Section 4.6(b)(iii)) reserve to SSR3 (or other future SSRs) the role of final assessment of the completion of recommendations from prior SSRs, including those that the SSR2 Review Team assessed. The Board directs ICANN's President and CEO, or his designee(s), to undertake a thorough analysis of the SSR2 Review Team's finding pertaining to the implementation of SSR1 recommendations and complete ICANN org's implementation, where appropriate, subject to prioritization, availability of resources, cost-effectiveness, and relevancy of the recommendations given the ever-changing landscape of the security, stability, and resiliency of the Internet's unique identifiers.
4.1: ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	The Board approves Recommendation 4.1, with the understanding that this recommendation is already fully implemented and no further action is required. The Board understands that ICANN org already has policies, plans and programs in place through which Recommendation 4.1 has already been implemented, and the Board continues its oversight role over ICANN org's risk management efforts. The Board is supportive of ICANN org in continuing the risk management activities that it is already carrying out.
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	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1**	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

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**- 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	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.
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. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
9.1: The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse related obligations in contracts, baseline agreements, temporary specifications, and community policies. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN Board	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).	The Board accepts ICANN org's representation that the Contractual Compliance operations that ICANN org has in place already meet the SSR2 Review Team's defined measures of success for Recommendation 9.1. Therefore, the Board approves this recommendation, with the understanding that this recommendation is already fully implemented and no further action is required.
10.1: ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct— ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-	**SSR2-defined measures of success for Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3):** This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date. This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy	To the extent that this recommendation is intended to enhance transparency, accountability, and clarity of ICANN org's work on Domain Name System (DNS) security threat mitigation through its existing contractual and compliance mechanisms, and thereby facilitate ongoing community discussions around definitions of DNS security threats, the Board approves this recommendation subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board notes that these considerations may be particularly important as definitions, procedures and protocols may evolve over time. In this regard, the Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.	ICANN org's Information Transparency Initiative (ITI).
16.1: ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the RDS. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3):** This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.	The Board approves Recommendation 16.1, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ITI.
21.1: ICANN org and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org and PTI	**SSR2-defined measures of success for Recommendation 21: Improve the Security of Communications with TLD Operators (21.1):** This recommendation can be considered implemented when ICANN org and PTI have a next-generation RZMS that involves a robust and secure authentication and authorization model for submission and approval of the requests as well as additional functionality that would enhance the security and stability of the global DNS system. This recommendation can be considered effective when ICANN org mitigates the potential for security and stability issues that involve the misuse of the RZMS through improved identity management procedures.	The Board notes that efforts to implement the new Root Zone Management System are already underway and the Board is supportive of building on existing efforts to enhance security in the Root Zone System. The Board notes that Recommendation 23.2 must be completed before the DNSSEC Practice Statement can be updated as called for in Recommendation 23.1. Further, the Board notes that preparing for an algorithm roll is part of the Public Technical Identifiers (PTI) Strategic Plan. As such, some elements of work associated with these recommendations are already anticipated to take place. The Board approves Recommendations 21.1, 22.1, 22.2, 23.1 and 23.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations.
22.1: For each service that ICANN org has authoritative purview over, including root-zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and	**SSR2-defined measures of success for Recommendation 22: Service Measurements (22.1 - 22.2):** This recommendation can be considered implemented when ICANN org makes the operational status metrics on the services ICANN org supports available to the community. This	

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

metrics on a single page on the icann.org web site, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior). **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	recommendation can be considered effective when the community sees an increase in the transparency of ICANN org SSR-related operations.	
22.2: ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org		
23.1: PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS. **SSR2 designated priority:** Medium **SSR2 designated owner:** PTI	**SSR2-defined measures of success for Recommendation 23: Algorithm Rollover (23.1 - 23.2):** This recommendation can be considered implemented when PTI updates the DPS to allow the transition from one digital signature algorithm to another and develops a consensus plan for future root DNSKEY algorithm rollovers. This recommendation can be considered effective when ICANN org is prepared for more advanced algorithms to be used for key signing, including any increases of key length and timing for key rollover.	
23.2: As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018. **SSR2 designated priority:** Medium **SSR2 designated owner:** PTI		
24.2: ICANN org should make the Common Transition Process Manual	**SSR2-defined measures of success for Recommendation 24: Improve Transparency and**	The Board approves recommendation 24.2, subject to prioritization, risk assessment and mitigation, costing and

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

easier to find by providing links on the EBERO website. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**End-to-end Testing for the EBERO Process (24.1 - 24.2):** This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.	other implementation considerations. The Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ITI.

SSR2 recommendation	SSR2-defined measures of success	Board action
Recommendations the Board rejects because the recommendation cannot be approved in full		
4.2: ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures). **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	The Board notes that ICANN org has a strong, clearly documented risk management program, but not as envisioned by SSR2, as written. Thus, the Board agrees with the recommendation in principle, and considers the intent of the recommendation achieved through ICANN org's current operations. However, the Board cannot approve the portion of the recommendation that specifies that ICANN org "adopt and implement International Standardization Organization (ISO) 31000 'Risk Management' and validate its implementation with appropriate independent audits…" because it is not clear what risks would be mitigated , nor what benefit would be derived in expanding significant resources to switch from the current risk-management process. The Board supports ICANN org's risk management operations already in place. In light of the above considerations, and the fact that approval of the recommendation would require ICANN org to adopt and implement ISO 31000, while the Board agrees in principle with the intent of the recommendation, the Board rejects recommendation 4.2. The Board encourages ICANN org to continue following industry best practices and look for ways to strengthen its risk management practices as it evolves its operations as part of its continuous improvement.
8.1: ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the	**SSR2-defined measures of success for Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties (8.1):** This recommendation can be considered implemented when ICANN org has included abuse and security specialists in these negotiations and the management of the domain name system aligns with public safety	The Board notes that the aspect of the recommendation that calls for the introduction of a third party into the bilateral negotiation process is not proper or feasible. The Registry Agreement and Registrar Accreditation Agreement do not allow for third-party beneficiaries. The Board notes that ICANN org negotiates in the broader interest of ICANN, including the public interest, and does not represent the interests of the domain industry. The Board also understands that parts of the ICANN community have concerns, as

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

domain name system for end-users, businesses, and governments. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	and consumer interests, and not just those of the domain name industry. This recommendation can be considered effective when a broader and more balanced set of stakeholders are able to have direct input into the contracts negotiated with contracted parties.	reflected through the public comments, about how Contracted Party agreements are negotiated, and acknowledges that it is important to listen carefully to the community as negotiations proceed and decisions are made. ICANN org also has an important enforcement role once items are incorporated into contracts. The Board further notes that recommendation 8.1 is not allowed under the provisions of the RA and RAA. While the agreements do provide for a "Working Group", these have contractually specific meanings that are not aligned with this recommendation. For example, in the case of the RA, a "Working Group" is defined as: "representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i)) Neither the Board or ICANN org is involved in the appointment of these contractual "Working Groups". Further, the Board and ICANN org cannot bring about contractual changes unilaterally. In light of the above considerations, the Board rejects this recommendation. The Board encourages ICANN org to continue bilateral discussions with the contracted parties in a way that enhances the security, stability, and resiliency of the DNS and to strive to have these bilateral discussions be transparent to the general public, in order to continue building trust.
9.4: ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence based Security Improvements).	The Board accepts in principle the idea of improving the tools that the ICANN org Contractual Compliance team has available to it in order to enforce policies that have been adopted by the community. However, the Board cannot approve the part of the recommendation that contemplates "measures that would require changes to the contracts" as such changes cannot be undertaken by either the Board or ICANN org unilaterally. As such, the Board rejects this recommendation given that it is not consistent with the role and authority of ICANN org's Contractual Compliance team. The Board encourages ICANN org's Contractual Compliance team to continue pursuing new tools that will help improve its work.

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

10.2: Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3):** This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date. This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.	The Board rejects Recommendation 10.2, as neither ICANN org nor Board can unilaterally establish a cross-community working group. However, the Board notes that the community continues its discussions over DNS security threat mitigation. Discussions include questions around the definitions and scope of DNS security threats that can be considered as coming within ICANN's remit and the extent to which policy or other community work may be required to supplement efforts already underway, such as industry-led initiatives. The Board is fully supportive of this effort and remains committed to this important work through facilitation and the convening of diverse relevant groups with diverse viewpoints. The Board rejects Recommendation 10.3 due to its dependencies on Recommendation 10.2; however, the Board supports using consensus definitions consistently.
10.3: Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page. **SSR2 designated priority:** High SSR2 designated owner: **ICANN org**		
17.2: The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN community and ICANN org.	**SSR2-defined measures of success for Recommendation 17: Measuring Name Collisions (17.1 - 17.2):** This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption mechanism is successful. The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios. This recommendation must be completed before the next round of gTLDs.	The Board rejects Recommendation 17.2, as the Board does not have the authority to develop policy. The Board notes that the community has already conducted extensive policy work concerning the process for handling name collisions for the next round of New Generic Top-Level Domains (new gTLDs), and the Security and Stability Advisory Committee (SSAC) Name Collision Analysis Project (NCAP) is another significant community effort already underway that is expected to result in additional useful information for the Board and community on the topic. Given the ongoing work in this area, including the NCAP studies, the Board understands that the results of those studies may have implications for SSR in the context of a future round of new gTLDs.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board rejects		
2.1: ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security	**SSR2-defined measures of success for Recommendation 2: Create a C-Suite Position**	The Board notes that it has an oversight role; it is the responsibility of the ICANN President and CEO to structure ICANN

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**Responsible for Both Strategic and Tactical Security and Risk Management (2.1 - 2.4):** This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations. This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.	org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. The Board supports ICANN org's decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible.
2.2: ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		In addition ICANN org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-Suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. The CEO Risk Management Committee is therefore a mechanism that provides ICANN org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures that ICANN org intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost.
2.3: ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		In light of the above considerations, the Board rejects Recommendations 2.1, 2.2, 2.3 and 2.4. However, the Board agrees with increased reporting and periodic communication of SSR activities. This is already partially performed as part of the current annual planning process but could be enhanced consistently with the presumed intent of the Recommendation 2.2
2.4: ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and		

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
14.1: ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2):** SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.	The Board notes that Temporary Policies can only be established by the Board upon specific requirements, such as when the Board "reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registrar Services, Registry Services, the DNS or the Internet." The Board notes that Recommendation 14.1 does not provide such emergency grounds, and as such rejects this recommendation and the recommendations dependent on its implementation (14.3, 14.4, 14.5, 15.1 and 15.2). Further, the Board notes that, while it can request an Issue Report and Policy Development Process (PDP) be done by the Generic Names Supporting Organization (GNSO), an Expedited Policy Development Process (EPDP) can only be launched by a GNSO Council vote, and only in specific circumstances. The Board notes that Recommendation 15.1 does not meet these requirements. The Board, consistent with its action on the Competition, Consumer Trust, and Consumer Choice (CCT) Review Team recommendations, will not take the place of the community within the multistakeholder model and initiate a PDP upon a Specific Review team's recommendation. As such, even without dependency on Recommendation 14.1, the Board would not be in a position to approve Recommendations 15.1 and 15.2.
14.3: Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and then issue a notice to the relevant party. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
14.4: ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Compliance should move to the de-accreditation process. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
14.5: ICANN org should consider offering financial incentives:		

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
15.1: After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported EPDP to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
15.2: The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board determines to be pending, likely to be approved once further information is gathered to enable approval		

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

5.4: ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	While implementation of the recommendation appears feasible, the Board requires clarification on several elements of this recommendation in order to accurately assess resource requirements and enable approval. For example, the required granularity of the reports expected by the SSR2 Review Team, and what entities the SSR2 Review Team envisioned ICANN org report out to "beyond" the ICANN community are not clear. The Board directs the ICANN President and CEO, or his designee(s) to seek clarifications from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendation 5.4 can be approved.
19.1: ICANN org should complete the development of a suite for DNS resolver behavior testing. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org **19.2:** ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 19: Complete Development of the DNS Regression Test Suite (19.1 - 19.2):** This recommendation can be considered implemented when ICANN org finishes developing a publicly accessible test suite for community testing and research into resolver behavior. This recommendation can be considered effective when there is a test suite available with an annual update cycle that helps ensure the integrity and global availability of the DNS.	The Board notes that the SSR2 Review Team's discussion and recommendations in the Final Report refer to three different things: a "DNS testbed"; a "regression test suite"; and "a suite for DNS resolver behaviour testing." While any of these may be feasible, the Board requires clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent in order to accurately assess resource requirements. The Board directs the ICANN President and CEO, or his designee(s), to seek clarifications from the SSR2 Implementation Shepherds on elements of these recommendations that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendations 19.1 and 19.2 can be approved. Further, the Board understands that the testbed would operate indefinitely so as to be applicable to future changes in resolvers. If the Board eventually approves this recommendation, maintenance of a testbed environment would have to be a persistent budget item in all future budget cycles for continued development and upkeep.
20.2: ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root KSK rollover process. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 20: Formal Procedures for Key Rollovers (20.1 - 20.2):** This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process. This recommendation	While the recommendation appears feasible and the Board believes that table-top exercises would be beneficial, more information is needed to understand what the SSR2 Review Team intended to be targeted in the table-top exercises following the Root key signing key (KSK) rollover process. The Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

	can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable. This recommendation must be completed in conjunction with each key rollover.	inform the Board's decision on next steps and whether Recommendation 20.2 can be approved.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations that the Board determines to be pending, holding to seek clarity or further information		
3.1: The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation SSR2-defined measures of success for Recommendation 3: Improve SSR-related Budget Transparency (3.1 - 3.3):** This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.	The Board notes that, as written, successful implementation of Recommendations 3.1 - 3.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent, and if implementation of these recommendations can be considered effective after the Board rejects Recommendation 2, thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendations 3.1, 3.2, and 3.3 to that new office. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
3.2: The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN Strategic Plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN Board and ICANN org		
3.3: The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN Board and ICANN org		
4.3: ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when	The Board notes that as written, successful implementation of Recommendation 4.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a CSO or CISO at

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications). **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. In light of this dependency on Recommendation 2, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective after the Board rejects Recommendation 2 thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendation 4.3. The Board has a concern with accepting a recommendation for which implementation can never be deemed successful or effective. Further, the Board notes it is the responsibility of the ICANN President and CEO, or his designee(s), to structure ICANN org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. In addition, it is not clear as to what the SSR2 Review Team envisioned would be mitigated, nor what cost/benefit would be derived from the recommended structure. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
5.3: ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	The Board understands that ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented which meets industry-standard requirements. In order to accurately assess resource requirements and feasibility, the Board requires clarification from the SSR2 Implementation Shepherds as to if the SSR2 Review Team's intent was to expand this risk assessment to all ICANN org vendors and service providers. The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherd as to the SSR2 Review Team's intended scope of this recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
7.1: ICANN org should establish a Business Continuity Plan for all the	**SSR2-defined measures of success for Recommendation**	The Board notes that the SSR2 Review Team states successful measures of

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5):** This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.	implementation for these recommendations as: "This recommendation can be considered implemented when ICANN org's Business Continuity (BC) and Disaster Recovery (DR) plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational." The Board is placing Recommendation 7.4, which calls for the "non-U.S., non-North American site" into "pending, likely to be rejected unless additional information shows implementation is feasible."
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 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		As such, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of these recommendations can be considered effective in the event that the Board rejects Recommendation 7.4 regarding opening a non-U.S., non-North American site, and that portion of the success measure cannot be achieved. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
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. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
7.5: ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
9.3: ICANN org should have compliance activities audited externally at least annually and	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce**	The Board notes that some elements of this recommendation are not clear, such as what would be audited, against what

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

publish the audit reports and ICANN org response to audit recommendations, including implementation plans. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community.	criteria, by whom, or why an external auditor would be required. The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the SSR2 Implementation Shepherds on elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
11.1: The ICANN community and ICANN org should take steps to ensure that access to CZDS data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN community and ICANN org	**SSR2-defined measures of success for Recommendation 11: Resolve CZDS Data Access Problems (11.1):** This recommendation can be considered implemented when ICANN org and the community makes access to CZDS data available in a timely manner and without unnecessary hurdles to requesters. This recommendation can be considered effective when ICANN org reports a decrease in the number of zone file access complaints and improves the ability for researchers to study the security-related operations of the DNS.	The Board notes that some elements of this recommendation are not clear. For example, the Board notes that ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the [Centralized Zone Data Service] CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default." It is not clear what additional work is needed to sufficiently implement the SSR2 Review Team's Recommendation 11.1 or how the existing work already being performed on CZDS access is insufficient. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
12.1: ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org **12.2:** ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN web site. ICANN org should terminate any contracts that do not	**SSR2-defined measures of success for Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (12.1 - 12.4):** This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data. This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.	The Board acknowledges the extensive community and ICANN org efforts currently going on around DNS security threats. The Board directs the ICANN President and CEO, or his designee(s), to evaluate how this grouping of recommendations, along with other recommendations that pertain to DNS security threats should be considered in a coordinated way, including through ICANN org's program dedicated to DNS security threats mitigation. This information will inform the Board's decision on next steps. The Board notes, however, that beyond the interdependencies related to the extensive community and ICANN org efforts around DNS security threats, there may be additional challenges associated with implementation of some of these recommendations that the Board would require to be addressed before determining if these recommendations can be approved.

allow independent verification of methodology behind blocklisting. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		
12.3: ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		
12.4: ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		
13.1: ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all gTLDs; the participation of each ccTLD would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting (13.1 - 13.2):** This recommendation can be considered implemented when ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members. This recommendation can be considered complete when the portal is up and running. This recommendation can be considered effective when contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints.	
13.2: ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.		

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

SSR2 designated priority: High **SSR2 designated owner:** ICANN org		
14.2: To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2):** SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time. ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.	The Board directs the ICANN President and CEO, or his designee(s) to regard the measures of success as defined by the SSR2 Review Team for Recommendations 14 and 15, and evaluate how this recommendation, along with other recommendations that pertain to DNS security threats, should be considered in a coordinated way, including through the ICANN org program dedicated to DNS security threats mitigation and ongoing projects such as the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project, and Domain Abuse Activity Reporting System (DAAR). . This information will inform the Board's decision on next steps.
17.1: ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which Controlled Interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the	**SSR2-defined measures of success for Recommendation 17: Measuring Name Collisions (17.1 - 17.2):** This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption	The Board notes that Recommendation 17.1 has dependencies on the SSAC NCAP. The output of the NCAP studies will inform the Board's decision on next steps. The Board noted such overlap in its comments on the SSR2 Review Team draft report, and encouraged the SSR2 Review Team to consider how its recommendations may be consolidated into or passed through to ongoing work.

appropriate handling of sensitive data and security threats. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	mechanism is successful. The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios.	
18.1: ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 18: Informing Policy Debates (18.1 - 18.3):** This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences. This recommendation can be considered effective when the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.	While the Board agrees that there is merit to ICANN org performing an evaluation to ensure that it is tracking at an appropriate level to the work that ICANN does, the Board notes that many academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials. In this manner, Recommendations 18.1 - 18.3 imply unbounded work. The Board would like to better understand the community's views as to if ICANN org should expend additional resources on this activity, in light of current existing work. The Board directs the ICANN President and CEO, or his designee(s), to perform an evaluation of its tracking efforts already underway and provide this to the Board to ensure that ICANN org is tracking at an appropriate level to the work that ICANN does. Further, the Board directs the ICANN President and CEO, or his designee(s) to engage the community to understand if ICANN org should expend additional resources on this activity, in light of current existing work. This information will inform the Board's decision on next steps.
18.2: ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org		
18.3: ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org		
20.1: ICANN org should establish a formal procedure, supported by a	**SSR2-defined measures of success for Recommendation**	The Board expects that this recommendation would require significant

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021

See Related Board Resolutions and Rationale for more details

formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for public comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**20: Formal Procedures for Key Rollovers (20.1 - 20.2):** This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process. This recommendation can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable.	resources to implement, while the cost versus benefit is not clear. Further, the Board notes that this recommendation has dependencies on research work that has not yet been conducted, such as algorithm rolls. The Board notes that alternative solutions, such as a process that contains evaluation checkpoints that allow circumstances to be evaluated and provide for potential course correction, may be more appropriate. In light of these considerations, the Board requires further information, including from community engagement as appropriate, in order to take dispositive action on this recommendation. The Board directs the ICANN President and CEO, or his designee(s) to gather further information, including via community engagement and engagement with the SSR2 Implementation Shepherds as appropriate on this recommendation. This information will inform the Board's decision on next steps.
24.1: ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised, and publish the results. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (24.1 - 24.2):** This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.	The Board notes that some elements of this recommendation are not clear. For example, it is not clear if the SSR2 Review Team's intent is for ICANN org conduct Emergency Back-end Registry Operator (EBERO) testing on "live" gTLDs with registrations. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board determines to be pending, likely to be rejected unless additional information shows implementation is feasible		
6.1: ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs**.** **SSR2 designated priority:** High	**SSR2-defined measures of success for Recommendation 6: SSR Vulnerability Disclosure and Transparency (6.1 - 6.2):** This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting. These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.	The Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding (MOUs)". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

SSR2 designated owner: ICANN org		matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
6.2: ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.		The Board notes there are three components of this recommendation, which each have different considerations. While ICANN org already does some of the things called for within the recommendation as ICANN org noted in its comments on the SSR2 Review Team draft report, the recommendation's focus on disclosure appears difficult or nearly impossible to implement. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation and the possible process to implement it with the relevant parties. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
7.4: ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5):** This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.	The Board does not have enough information to consider resource implications of implementing this recommendation versus the expected benefit. The Board notes that in its comment on the SSR2 Review Team draft report, ICANN org asked the SSR2 Review Team to provide clear justification as to why it believes the benefits of a third disaster recovery site justifies the costs of such a site. While the recommendation states that the new site could replace "either the Los Angeles or Culpeper sites", the requested cost/benefit information is not provided in the SSR2 Review Team Final Report. Further, the Board notes Section 4.2 of the Internet Assigned Numbers Authority (IANA) Naming Function Contract that prohibits IANA operations outside of the United States, and as such, the Board understands that implementation of this recommendation as written is not currently feasible for some portions of the IANA functions. These restrictions could be removed through contract amendments if there were a desire to do so from the ICANN community, which would require community consultation and discussion. The Board directs the ICANN President

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

		and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand elements of this recommendation that are not feasible as written, or are not clear, including if the SSR2 Review Team considered the benefit versus cost considerations. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps, which may include wider community consultation.
9.2: ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community.	The Board notes that ICANN org does not have authority to require validation beyond what is in the Registry Agreement and Registrar Accreditation Agreement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, including the authority the SSR2 Review Team understood that ICANN org's Contractual Compliance team has to carry out the recommended actions. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
16.2: ICANN org should create specialized groups within the contract compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems). **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SR2-defined measures of success for Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3):** This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.	The Board is not clear as to what is meant by "facilitate law enforcement needs" and how that is relevant to the role of ICANN org's Contractual Compliance team. As written, ICANN org does not have the authority to do this. Further, the intent of the recommendation is not clear, specifically why the SSR2 Review Team understands the existing subject matter experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation. The Board understands that ICANN org's Contractual Compliance team has subject matter experts in the areas listed to the extent that they are necessary for contract enforcement. For other matters and as necessary, ICANN org's Contractual Compliance members can refer to ICANN org's Chief Data Protection Officer for guidance regarding the specific areas listed. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role. The Board directs the ICANN President and CEO, or his designee(s), to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, as well as other

Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolutions and Rationale for more details

		elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
16.3: ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		The Board noted in its comment on the SSR2 Review Team draft report, ICANN org does not specifically require registrars to have "privacy policies." ICANN org's Contractual Compliance team cannot audit something that is not an ICANN contractual requirement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.