	Recommendation	RrSG Comment
0	**General Comment**	It is not clear how the recommendations below will be carried out. While some recommendations are directed to the ICANN Board or ICANN Org (and within their remit, e.g. audit of Compliance or staffing), many of the recommendations would need to to go through the PDP process to avoid having ICANN org creating policy. Those recommendations that include policy elements should be referred to the GNSO Council for further action.
1	**Complete the implementation of all relevant SSR1 recommendations**	The RrSG agrees with this recommendation.
2	**SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications** 2.1. ICANN org should establish a road map of its industry-standard security audits and certification activities that are being undertaken, including milestone dates for obtaining each certification and noting areas of continuous improvement. 2.2. 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. 2.3. ICANN org should also provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies 2.4. ICANN org should implement an Information Security Management System and undergo a third-party audit. 2.5. In order to reap the benefits of a certification and audit regimen, ICANN org should be audited and certified by a third party along the lines of industry security standards and should assess certification options with commonly accepted international standards (e.g., ITIL, ISO 27001, SSAE-18) for its operational responsibilities.	It makes sense for ICANN Org to be certified for key critical certifications like ISO 27001 and 27701. Such certifications will advance ICANN Org as an organization in terms of data protection and system security. Contracted parties will also benefit if ICANN ORG has certification like ISO 27001 and 27701 regarding their accountability towards compliance with laws or if they use such certifications themselves. ICANN Org management, the CEO, and the ICANN Board most fully support such certifications. The ICANN Board should adopt an accountability oversight mechanism for the Board members.

	Recommendation	RrSG Comment
3	**SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures** 3.1. ICANN org should address security issues clearly, publicly (with consideration for operational security, e.g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties. 3.2. ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs. 3.3. ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org. 3.4. ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community- agreed process and include anonymized metrics.	The RrSG doubts that such methods can be applied on a global level without discriminating against certain regions and/or creating high costs for specific contracted parties in certain areas. Modification of the contracts and agreements should not go through a consensus document process. The output from such consensus documents can be considered during arrangements negotiations like any other discussion points during such negotiations.
4	**SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs** 4.1. Where possible (contractually) and reasonable in terms of effort (i.e., over 10% of the activity described in the budget line item), ICANN should be more transparent with the budget for parts of ICANN org related to implementing the Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs.	The RrSG supports this recommendation

	Recommendation	RrSG Comment
5	**SSR1 Recommendation 27 - Risk Management** 5.1. ICANN's Risk Management Framework should be centralized and strategically coordinated. 5.2. ICANN org should clearly articulate their risk framework and strategically align the framework against the requirements and objectives of the organization, describing relevant measures of success and how ICANN org will assess these measures. 5.3. ICANN should make information pertaining to risk management centrally available to the community. This information should be regularly updated to reflect the current threat landscape (at least annually).	The RrSG supports this recommendation, which should build upon ICANN Org existing risk management structure.
6	**Create a Position Responsible for Both Strategic and Tactical Security and Risk Management** 6.1. ICANN org should create a position responsible for both strategic and tactical security and risk management across the internal security domain of the organization, as well as the external global identifier system. 6.2. ICANN org should hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions. 6.3. This position should manage ICANN org's Security Functionand oversee the interactions of staff in all relevant areas that impact security. 6.4. The position should also provide regular reports to ICANN's Board and community. 6.5. This position would act as a pathfinder and problem-solver who would strategize and execute multi-faceted programs to achieve substantial improvements. 6.6. Additionally, this role should take part in all security-relevant contractual negotiations (e.g., supply chains for hardware and software and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.	The RrSG agrees that there should be a position responsible for strategic and tactical security and risk management; it is not clear why this does not already exist. If the fucntion does not already exist, it seems to be a function that fits within the OCTO remit, and so should be part of that team. The RrSG does not consider this specific recommendation as one that requires a PDP; this is something that ICANN Org and the Board can do directly.

	Recommendation	RrSG Comment
7	**Further Develop a Security Risk Management Framework** 7.1. ICANN org should clearly articulate their Security Risk Management Framework and ensure that it aligns strategically against the requirements and objectives of the organization. 7.2. ICANN org should describe relevant measures of success and how these measures are to be assessed. The SSR2 RT described the foundation of this in detail in the additionalfeedback regarding SSR1's Recommendation 9 (see 'SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications' earlier in this report). 7.3. ICANN org should: 7.3.1. Adopt and implement ISO 31000 "Risk Management" and validate and certify their implementation with appropriate independent audits.4 Risk management efforts should feed into Business Continuity and Disaster Recovery Plans and Provisions. 7.3.2. Regularly update a register of security risks and use that register to prioritize and guide the activities of the ICANN org. ICANN org should report on updates of their methodology and updates to the register of security risks. Findings should feed into BC/DR and the Information Security Management System (ISMS). 7.3.3. Name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role as descr	This recommendation seems redundant with recommendation 2. Audits and an ISMS are part of the ISO certification, so this level of detail seems excessive. Everything in this recommendation is something that ICANN should do for recommendation 2.
8	**Establish a Business Continuity Plan Based on ISO 22301** 8.1. ICANN org should establish a Business Continuity Plan for all the systems owned by, or under the purview of ICANN org,based on ISO 22301 "Business Continuity Management."5 8.2. ICANN should identify the importance of functional, acceptable timelines for BC and DR based on the urgency of restoring full functionality. 8.3. For Public Technical Identifiers (PTI) operations (IANA functions, including all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management), ICANN org should develop a shared approach to service continuity in close cooperation with the Root Server System Advisory Committee (RSSAC) and the root server operators. 8.4. ICANN org should publish evidence (e.g., a summary) of their Business Continuity Plans and Provisions. An external auditor should be engaged to verify compliance aspects of the implementation of the resulting business continuity plans.	With the exception of 8.3, this recommendation seems redundant with recommendation 2, which would require ICANN do to this for ISO certification. The RrSG supports recommendation 8.3.

	Recommendation	RrSG Comment
9	**Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented** 9.1. ICANN org should ensure that the DR plan for PTI operations (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 Guidelines for information and communication technology readiness for business continuity. ICANN org should develop this plan in close cooperation with RSSAC and the root server operators. 9.2. ICANN org should also establish a DR Plan for all the systems owned by or under the purview of ICANN org, again in line with	This recommendation seems redundant with recommendation 2, which would require ICANN do to this for ISO certification.
10	**Improve the Framework to Define and Measure Registrar & Registry Compliance** 10.1. Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review.6,7 10.2. Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics. 10.3. Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident). 10.4. Further, the ICANN Board should take responsibility for bringing the EPDP8 to closure and passing and implementing a WHOIS policy in the year after this report is published.	In general, this recommendation is for policy and should go through the ICANN policy process. Regarding the sub recommendations: 10.1 - This is already covered by ICANN- Compliance metrics on complaints, Compliance audit, Whois ARS, monitoring by GDD tech team, etc 10.2 - This is something Compliance already does. A review team, with limited understanding of the operation and structure, should defer to Compliance to determine how it will best allocate resources. 10.3 - It is the position of the RrSG that contract negotiations do not originate from review teams or working groups. That is reserved for ICANN Org, and the RrSG/RySG. 10.4 - It is not for a review team to determine the pace of the PDPs or IRTs. There can be unexected issues that arise (as during the implementation of EPDP Phase 1), and it is better for ICANN to develop and implement policy properly rather than rushing to meet an artificial deadline.

	Recommendation	RrSG Comment
11	**Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions** 11.1. ICANN Board should drive efforts that minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties and implementation plans. 11.2. ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay9. 11.3. ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of “security threat”—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique10 and for Specification 1111), and addressed in international conventions such as the Convention on Cybercrime and its related “Explanatory Notes” 12 —to use in conjunction with ICANN org’s DNS Abuse definition.13 11.4. The ICANN Board should entrust SSAC and PSWG to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime.	The RrSG has concerns about this recommendation. The ICANN community is currently engaged in abuse and threat activities, as are the contracted parties. The definition of abuse and threats can be difficult to define broadly, which is perhaps indicitive why there is not a definition that satisfies the review team. It is essential that contracted parties, which have undertanding of implications of these activities, be involved in the process (rather than the ICANN board engaging only security-related community members).
12	**Create Legal and Appropriate Access Mechanisms to WHOIS Data** 12.1. The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement. 12.2. The ICANN Board should take responsibility for, and ensure ICANN org comes to immediate closure on, implementation of the Temporary Specification for gTLD Registration Data.	Regarding recommendation 12.1, this is currently being addressed by EPDP Phase 2, and should not be subject to another PDP. For recommendation 12.2, as indicated previously, there is a pending IRT that is dealing with complex issues. The IRT should be allowed to proceed at its current pace to ensure quality outcome (rather than rushing to meet an artificial deadline).

	Recommendation	RrSG Comment
13	**Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program** 13.1. The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse. 13.1.1. ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology. 13.1.2. ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items “daar” and “daar-summarized” of the ODI Data Asset Inventory14 for immediate community access. 13.1.3. ICANN org should publish reports that include machine- readable formats of the data, in addition to the graphical data in current reports. 13.1.4. ICANN org should provide assistance to the Board and all constituencies, stakeholder groups and advisory committees in DAAR Interpretation, including assistance in the identification of policy and advisory activities that would enhance domain name abuse prevention and mitigation.	Regarding recommendation 13.1, this data is already being published elsewhere. It is outside of ICANN's scope to aggregate and republish this data. It is also not clear that DAAR is incomplete or ineffective, so additional information is needed to know how the cost for these additional resources outweighs any benefit. Regarding recommendation 13.1.1, commercial entities already publish such data. Some of these reports include flawed, incomplete, or false positive information, so it is should not form the basis for ICANN to "name and shame" contracted parties. There are existing compliance activities to address registrars or registries that may not be complying with the RAA or RA. The recommendation does not mention the benefits and or possible issues such publication could create. This recommendation should be subject to community consideration before further action. For recommendation 13.1.2, it is not clear what source data DAAR entails, and whether the sources have been vetted by contracted parties and the broader ICANN community. The recommendation is not very clear what source data for DAAR entails. This data is likely published elsewhere, and it is not ICANN's remit to provide a "clearinghouse" for information that can be obtained elsewhere. If recommendation 13.1.3 is referencing DAAR, then again, these feeds are already available.
14	**Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse** 14.1. ICANN org should collect, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.	The RrSG notes that this was already recommended by CCT. The ICANN board deferred implementing and stated "questions raised regarding the value of the data" (see https://www.icann.org/en/system/files/files/resolutions-final-cct-recs-scorecard-01mar19-en.pdf). It is not clear what will be accomplished by collecting this information. There are extensive reports already that tie low cost, or free registrations to abuse activity (which are havens for abusive domains, along with low cost hosting). Additionally, ICANN is likely not in a position to determine a full picture due to the large and varying promotional pricing, or prices set by resellers of registrars, or for registrars that do not provide this information publicly. This could be a massive undertaking which might not produce useful information.

	Recommendation	RrSG Comment
15	**Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse** 15.1. ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach.15 15.2. ICANN org should introduce a contract clause that wouldsupport contract termination in the case of “a pattern and practice” of abuse (as in section 5.5.2.4 “TERM,TERMINATION AND DISPUTE RESOLUTION” of the 2013Registrar Accreditation Agreement)16. 15.3. In order to support the review of these contract changes, ICANN org should: 15.3.1. Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms. 15.3.2. Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes. 15.3.3. Attract and collaborate with ccTLDs and the ccNSO to help address DNS abuse and security threats in ccTLDs. 15.3.4. The ICANN Board, community, and org should work with the ccNSO to advance data tracking and reporting, assess DNS abuse and security threats in ccTLDs, and develop a ccNSO plan to support ccTLDs in further mitigating DNS abuse and security threats. 15.3.5. Immediately instantiate a requirement for the RDAP services of contracted parties to white-list ICANN org address space and establish a process for vetting other entities that RDAP services of contracted parties will whitelist for non-rate-limited access. 15.4. In the longer term, ICANN Board should request that the GNSO initiate the process to adopt new policies and agreements with Contracted Parties that measurably improve mitigation of DNS abuse and security threats, including changes to RDAP and registrant information, incentives for contracted parties for abuse/security threat mitigation, establishment of a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders.	It is the position of the RrSG that contract negotiations should originate through ICANN, the RrSG, and the RySG, rather than a review team. Any recommendations for changes to the RAA or RA are out of scope. For recommendation 15.3.1, this is most likely not possible because it would violate fundamental rights of data subjects. Furthermore, the correlation between registration data and the effectiveness of actual threat mitigation is unknown. Regarding recommendation 15.3.2, such research is already possible under many data protection laws. However, current ICANN community processes do not comply with these laws, and as such, the RrSG recommends that the ICANN community focus on how research in a manner that complies with existing laws (rather than making proposals that might violate those laws). The RrSG notes that ICANN OCTO has mentioned several times it does not need access to registrant data for research purposes. For recommendation 15.4, the RrSG supports the use of the GNSO to develop ICANN policy.

	Recommendation	RrSG Comment
16	**Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats** 16.1. ICANN org should incentivize the mitigation of abuse and security threats making the following changes to contracts: 16.1.1. Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount). 16.1.2. Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold. 16.1.3. Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant. 16.1.4. Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered). 16.2. Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers, and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse [citation to be added] and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.	While this recommendation appears to be a good start, it must be subject to a PDP to determine if incentives are a good mechanism to address security threats. As for incentives, they are usually subject to abuse itself and or gaming (and bad actors will figure out a way around it). For recommendation 16.1.1 and 16.1.3, how will ICANN offset the discount (which will result in a lower revenue for ICANN)? Recommendation 16.1.2 will be difficult to implement in light of privacy laws. There are also questions, such as how can registrars verify registrants, what will prevent bad registrars from faking the verification, and does verification mean lower abuse? It is not clear how recommendation 16.1.4 can be tracked. As with other parts of this recommendation, it is subject to gaming/abuse. It could also lead to a new version of frontrunning (e.g. register a domain, track traffic for 25 days, then suspend for "abuse" to get money back if the domain is not generating sufficient parking page revenue or a malicious campaign ends). Recommendation 16.2 is outside of ICANN's remit, and the source of funding for this is not clear (e.g. what would ICANN cancel to pay for this).
17	**Establish a Central Abuse Report Portal** 17.1. 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 inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.	It is not clear what are the "relevant parties" in this recommendation. If only registrars and registries, then such a system will likely cost more than any perceived benefit. If it is intended that it would be all inclusive (e.g. P/P providers, hosting providers, etc), it would be outside of ICANN's scope.

	Recommendation	RrSG Comment
18	**Ensure that the ICANN Compliance Activities are Neutral and Effective** 18.1. ICANN org should have compliance activities audited externally and hold them to a high standard. 18.2. The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes. 18.3. The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.	Regarding recommendation 18.1, the RrSG supports that ICANN Compliance should be subject to outside audit. For recommendation 18.2, the RrSG notes that these obligations exist in the RAA and Compliance already monitors it. For recommendation 18.3, ICANN Compliance already does this (see https://features.icann.org/compliance/dashboard/report-list).
19	**Update Handling of Abusive Naming** 19.1. ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable. 19.2. When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices. 19.3. ICANN org should publish the number of abusive naming complaints made at the portal in a form that allows independent third parties to analyze, mitigate, and prevent harm from the use of such domain names. 19.4. ICANN org should update the current "Guidelines for the Implementation of IDNs" [citation to be added] to include a section on names containing trademarks, TLD-chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.	Recommendation 19.1 is something that is already shared among commercial and community-driven threat exchanges and are used by many companies for their endpoint protection. It is not for ICANN to aggregate and provide these services for free (as some of them are available for purchase). Recommendation 19.2 is not clear. If a misleading domain names become abusive, then it will be listed in the feeds DAAR uses automatically. For recommendation 19.3, such data needs to be curated and require a Traffic Light Protocol for sharing such information. Furthermore, this requires a clear definition of what is misleading and what can lead to abuse. Recommendation 19.4 should originate from a PDP rather than a review team. Additionally, it is not the place of a review team to initiate RAA or RA negotiation or changes.
20	**Complete Development of a DNS Regression Testing** 20.1. ICANN org should complete the development of a suite for DNS regression testing.17 20.2. ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained.	It is not clear how this recommendation will be paid for, and what the benefit is over other commercially available solutions.

	Recommendation	RrSG Comment
21	**Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers** 21.1. ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process. 21.2. ICANN org should establish a formal procedure, supported by a formal process modeling tool and language18 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, FSM) for public comment, and community feedback should be incorporated. 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 lessons learned can be used to adjust the process. 21.3. 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.	The RrSG does not have a position on this recommendation.
22	**Establish Baseline Security Practices for Root Server Operators and Operations** 22.1. ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSS governance model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best practices should include change management, verification procedures, and sanity check procedures. 22.2. ICANN org should also develop relevant KPIs to measure the implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs. 22.3. ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L- Root, and should encourage other RSOs to do the same. 22.4. ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.	The RrSG does not have a position on this recommendation.

	Recommendation	RrSG Comment
23	**Accelerate the Implementation of the New-Generation RZMS** 23.1. ICANN and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes. 23.2. ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.	The RrSG does not have a position on this recommendation.
24	**Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems** 24.1. ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over. 24.2. ICANN org should publish a directory of these services, data sets, and metrics on a single page on the ICANN org web site, such as under the Open Data Platform. 24.3. ICANN should publish annual and longitudinal summaries of this data, solicit public feedback on the summaries, and incorporate the feedback to improve future reports. 24.4. For both sets of KPIs, ICANN org should produce summaries over both the previous year and longitudinally, request and publish a summary of community feedback on each report and incorporate this feedback to improve follow-on reports.	If this recommendation is restricted to the ennumerated items in 24.1, then the RrSG supports this recommendation. If this recommendation is intended to include registrars and registries, then it is not acceptable. As indicated elsewhere, it is not ICANN's role to publicly score the "operational status" of contracted parties.

	Recommendation	RrSG Comment
25	**Ensure the Centralized Zone File Data Access is Consistently Available** 25.1. The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available, in a timely manner, and without unnecessary hurdles to requesters. 25.2. ICANN org should implement the four recommendations in SSAC 97:19 “Recommendation 1: The SSAC recommends that the ICANN Board suggest to ICANN Staff to consider revising the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. This could include an option allowing a registry operator to depart from the default on a per- subscriber basis, thereby forcing the chosen subscriber to reapply at the end of the current term. The CZDS should continue to provide registry operators the ability to explicitly terminate a problematic subscriber’s access at any time. Recommendation 2: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that in subsequent rounds of new gTLDs, the CZDS subscription agreement conform to the changes executed as a result of implementing Recommendation 1. Recommendation 3: The SSAC recommends that the ICANN Board suggest to ICANN Staff to seek ways to reduce the number of zone file access complaints, and seek ways to resolve complaints in a timely fashion. Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.	The RrSG requires additional information, as it is not clear what the concern this recommendation intends to address. Additionally, the term "other data" is very broad and should be narrowed.

	Recommendation	RrSG Comment
26	**Document, Improve, and Test the EBERO Processes** 26.1. ICANN org should publicly document the ERERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception. 26.2. Where possible, ICANN org should automate these processes and test them annually. 26.3. ICANN org should publicly conduct EBERO smoke-testing at predetermined intervals using a test plan coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results. 26.4. ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider.	The RrSG does not have a position on this recommendation.
27	**Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers** 27.1. PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security. 27.2. As 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.	The RrSG does not have a position on this recommendation.

	Recommendation	RrSG Comment
28	**Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution** 28.1. ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs. 28.2. ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By "independent," SSR2 RT means that ICANN org should ensurethat the SSAC Name Collision Analysis Project (NCAP) workparty research and report evaluation team's results need to bevetted by parties that are free of any financial interest in TLD expansion. 28.3. ICANN org should enable community reporting on instances of name collision. These reports should allow appropriate handling of sensitive data and security threats and should be rolled into community reporting metrics.	The RrSG does not have a position on this recommendation.

	Recommendation	RrSG Comment
29	**Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements** 29.1. ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS). 29.2. ICANN org's consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name. 29.3. ICANN org should: 29.3.1. Create specialized units within the contract compliance function that focus on 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 evolving RDAP framework. 29.3.2. Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.20 29.3.3. Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented. 29.3.4. Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches. 29.4. ICANN org's DPO should also be responsible for external DNS PII. The DPO should provide guidance to managers and stakeholders regarding responsibilities and procedures and monitor and report on relevant technical developments.	For recommendation 29.1, this appears to be outside of ICANN's remit. The RrSG needs additional information about recommendation 29.2, as it is not clear what problem or concern this addressing- those obligations already exist. For recommendation 29.3.1, it is the position of the RrSG that Compliance should be allowed to determine its structure and functions without community interference. If this recommendation is adopted, then Compliance would be subject to control by other areas of the ICANN community (and other structures within ICANN as well). Regarding recommendation 29.3.2, it is the understanding of the RrSG that ICANN already does this, with a focus on all laws that could impact the ICANN community. For recommendation 29.3.3, ICANN org should already do this, and this is already covered in the RAA and RA. For recommendation 29.3.4, ICANN Compliance already has an audit program. The RrSG need more information regarding recommendation 29.4 as it is not clear what "external DNS PII" refers to.

	Recommendation	RrSG Comment
30	**Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates** 30.1. 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 S&P, as well as the operational security conferences APWG, M3AAWG, and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior. 30.1.1. These reports should include 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. 30.1.2. These reports should also include recommendations for additional study to confirm peer-reviewed findings, a description of what data would be required to execute additional recommended studies, and how ICANN can offer to help broker access to such data, e.g., CZDS.	It is the understanding of the RrSG that ICANN attends a lot of these events already. It is not clear from the draft report how the expense of ensuring attendence and reporting will provide signficant benefit, or where ICANN will find the funding for this initiative. Additionally, it is the position of the RrSG that these forums, which have limited (if any) participation of contracted parties, should not be the source for changes to the RAA or RA. There are already existing structures within the ICANN community for the participants of these forums to participate in ICANN's multi-stakholder model, and this proposed recommendation would circumvent that process.
31	**Clarify the SSR Implications of DNS-over-HTTP** 31.1. ICANN org should commission an independent investigation(s) into the SSR-related implications of DoH deployment trends, as well as implications for the future role of IANA in the Internet ecosystem. The intended outcome is to ensure that all stakeholders have the opportunity to understand the SSR- related implications of these developments, and the range of alternatives (or lack thereof) various stakeholders have to influence the future.	As with many of the recommendations, this appears to be outside of ICANN's remit, the source of the funds is not clear, and the potential benefits are not defined.