

#	Review	Time	Recommendation	Board Action	Sub-group	End-user Interest	Priority (1-max/3-min)
1	MSM		Prioritization of the Work				
2	MSM		Precision in scoping the work				
3	MSM		Costs				
4	MSM		Representativeness + Inclusiveness				
5	MSM		Consensus				
6	MSM		Terms				
7	MSM		Recruitment + Demographics				
8	MSM		Complexity				
9	MSM		Efficient use of Resources				
10	MSM		Culture + Trust + Silos				
11	MSM		Roles and Responsibilities + Holistic View of ICANN				
1	ATRT3		Assessment of Periodic (now Specific) and Organizational Reviews				2
2	ATRT3		Prioritization and Rationalization of Activities, Policies, and Recommendations				1
3	ATRT3		Accountability and Transparency Relating to Strategic and Operational Plans including Accountability Indicators				
4	ATRT3		Public Input				
5	ATRT3		Assessment of the Implementation of ATRT2 Recommendations				
1	CCTRT		Formalize and promote ongoing data collection	Adopted			
2	CCTRT		ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.	Adopted			
3	CCTRT		Include more detailed information on the subject matter of complaints in ICANN publicly available compliance reports. Specifically, more precise data on the subject matter of complaints, particularly: (1) the class/type of abuse; (2) the gTLD that is target of the abuse; (3) the safeguard that is at risk; (4) an indication of whether complaints relate to the protection of sensitive health or financial information; (5) what type of contractual breach is being complained of; and (6) resolution status of the complaints, including action details. These details would assist future review teams in their assessment of these safeguards.	Adopted			
4	CCTRT		Initiate engagement with relevant stakeholders to determine what best practices are being implemented to offer reasonable and appropriate security measures commensurate with the offering of services that involve the gathering of sensitive health and financial information. Such a discussion could include identifying what falls within the categories of "sensitive health and financial information" and what metrics could be used to measure compliance with this safeguard.	Adopted			
5	CCTRT		Expand and improve outreach into the Global South.	Adopted			

6	CCTR	The ICANN organization to coordinate the pro bono assistance program.	Adopted			
7	CCTR	The ICANN community should consider whether the costs related to defensive registration for the small number of brands registering a large number of domains can be reduced.	Forwarded to certain community groups for consideration			
8	CCTR	The GNSO should initiate a new Policy Development Process (PDP) to create a consistent privacy baseline across all registries, including to explicitly cover cases of privacy infringements such as sharing or selling personal data without a lawful basis, such as the consent of that person. The GNSO PDP should consider limiting the collection and processing of personal data within rules which are mandatory for all gTLD registries. It should also consider not allowing registries to share personal data with third parties without a lawful basis, such as the consent of that person or under circumstances defined by applicable law (e.g. upon requests of government agencies, IP lawyers, etc.). Also, it is necessary to be aware of emerging, applicable regulations related to the processing of the personal data. For clarification, this recommendation does not relate to issues involving WHOIS or registration directory services data.	Forwarded to certain community groups for consideration			
9	CCTR	Create incentives and/or eliminate current disincentives that encourage gTLD registries to meet user expectations regarding: (1) the relationship of content of a gTLD to its name; (2) restrictions as to who can register a domain name in certain gTLDs based upon implied messages of trust conveyed by the name of its gTLDs (particularly in sensitive or regulated industries) and (3) the safety and security of users' personal and sensitive information (including health and financial information). These incentives could relate to applicants who choose to make public interest commitments in their applications that relate to these expectations. Ensure that applicants for any subsequent rounds are aware of these public expectations by inserting information about the results of the ICANN surveys in the Applicant Guide Books	Forwarded to certain community groups for consideration			
10	CCTR	Further study the relationship between specific registry operators, registrars, and DNS Security Abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to be able to identify registries and registrars that need to come under greater scrutiny, investigation, and potential enforcement action by ICANN organization. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remedy problems identified, and define future ongoing data collection.	Forwarded to certain community groups for consideration			
11	CCTR	The next CCT should review the "Framework for Registry Operator to Respond to Security Threats" and assess whether the framework is a sufficiently clear and effective mechanism to mitigate abuse by providing for systemic and specified actions in response to security threats.	Forwarded to certain community groups for consideration			

12	CCTRT	<p>Assess whether mechanisms to report and handle complaints have led to more focused efforts to combat abuse by determining: (1) the volume of reports of illegal conduct in connection with the use of the TLD that registries receive from governmental and quasi-governmental agencies; (2) the volume of inquires that registries receive from the public related to malicious conduct in the TLD; (3) whether more efforts are needed to publicize contact points to report complaints that involve abuse or illegal behavior within a TLD; and (4) what actions registries have taken to respond to complaints of illegal or malicious conduct in connection with the use of the TLD. Such efforts could include surveys, focus groups, or community discussions. If these methods proved ineffective, consideration could be given to amending future standard Registry Agreements to require registries to more prominently disclose their abuse points of contact and provide more granular information to ICANN. Once this information is gathered, future review teams should consider recommendations for appropriate follow up measures.</p>	Forwarded to certain community groups for consideration			
13	CCTRT	<p>To the extent voluntary commitments are permitted in future gTLD application processes, all such commitments made by a gTLD applicant must state their intended goal and be submitted during the application process so that there is sufficient opportunity for community review and time to meet the deadlines for community and Limited Public Interest objections. Furthermore, such requirements should apply to the extent that voluntary commitments may be made after delegation. Such voluntary commitments, including existing voluntary PICs, should be made accessible in an organized, searchable online database to enhance data-driven policy development, community transparency, ICANN compliance, and the awareness of variables relevant to DNS abuse trends.</p>	Forwarded to certain community groups for consideration			
14	CCTRT	<p>Since the review team's initial draft recommendation, the PDP "Review of All Rights Protection Mechanisms in All gTLDs (RPM WG)" has started reviewing the Uniform Rapid Suspension system in detail and this is currently ongoing. Given this ongoing review, the CCT Review Team recommends that the RPM WG continues its review of the URS and also looks into the interoperability of the URS with the Uniform Domain Name Dispute Resolution Policy (UDRP). Given the current timeline, it would appear that the appropriate time to do so will be when the UDRP review is carried out by the PDP WG and at this time consideration be given to how it should interoperate with the UDRP. The review team has encountered a lack of data for complete analysis in many respects. The RPM PDP WG appears to also be encountering this issue and this may well prevent it drawing firm conclusions. If modifications are not easily identified, then the review team recommends continued monitoring until more data is collected and made available for a review at a later date.</p>	Forwarded to certain community groups for consideration			

15	CCTRT	<p>A cost-benefit analysis and review of the Trademark Clearinghouse (TMCH) and its scope should be carried out to provide quantifiable information on the costs and benefits associated with the present state of the TMCH services and thus to allow for an effective policy review.⁴⁰ Since our initial draft recommendation, the RPM PDP has started reviewing the TMCH in detail and ICANN has appointed Analysis Group to develop and conduct the survey(s) to assess the use and effectiveness of the Sunrise and Trademark Claims RPMs. Provided that the RPM PDP has sufficient data from this survey or other surveys and is able to draw firm conclusions, the CCT Review Team does not consider that an additional review is necessary. However, the CCT Review Team reiterates its recommendation for a cost-benefit analysis to be carried out if such analysis can enable objective conclusions to be drawn. Such cost-benefit analysis should include but not necessarily be limited to looking at cost to brand owners, cost to registries, and cost to registrars of operating with the TMCH now and going forward and look at the interplay with premium pricing.</p>	Forwarded to certain community groups for consideration			
16	CCTRT	Set objectives/metrics for applications from the Global South.	Forwarded to certain community groups for consideration			
17	CCTRT	Revisit the Applicant Support Program.	Forwarded to certain community groups for consideration			
18	CCTRT	As required by the October 2016 Bylaws, Governmental Advisory Committee (GAC) consensus advice to the Board regarding gTLDs should also be clearly enunciated, actionable, and accompanied by a rationale, permitting the Board to determine how to apply that advice. ICANN should provide a template to the GAC for advice related to specific TLDs, in order to provide a structure that includes all of these elements. In addition to providing a template, the Applicant Guidebook (AGB) should clarify the process and timelines by which GAC advice is expected for individual TLDs.	Forwarded to certain community groups for consideration			
19	CCTRT	A thorough review of the procedures and objectives for community-based applications should be carried out and improvements made to address and correct the concerns raised before a new gTLD application process is launched. Revisions or adjustments should be clearly reflected in an updated version of the 2012 AGB.	Forwarded to certain community groups for consideration			
20	CCTRT	The New gTLD Subsequent Procedures PDP should consider adopting new policies to avoid the potential for inconsistent results in string confusion objections. In particular, the PDP should consider the following possibilities: 1. Determining through the initial string similarity review process that singular and plural versions of the same gTLD string should not be delegated. 2. Avoiding disparities in similar disputes by ensuring that all similar cases of plural versus singular strings are examined by the same expert panelist. 3. Introducing a post-dispute resolution panel review mechanism.	Forwarded to certain community groups for consideration			

21	CCTRT	Collect wholesale pricing for legacy gTLDs.	Pending			
22	CCTRT	Collect transactional pricing for the gTLD marketplace	Pending			
23	CCTRT	Collect retail pricing for the domain marketplace	Pending			
24	CCTRT	Collect secondary market data	Pending			
25	CCTRT	Partner with mechanisms and entities involved with the collection of TLD data. As feasible, collect TLD registration number data per TLD and registrar at a country-by-country level in order to perform analysis based on the same methods used in the Latin American and Caribbean DNS Marketplace (LAC) Study.	Pending			
26	CCTRT	Collect domain usage data to better understand the implications of parked domains	Pending			
27	CCTRT	Conduct periodic surveys of registrants that gathers both objective and subjective information with a goal of creating more concrete and actionable information.	Pending			
28	CCTRT	Conduct periodic end-user consumer surveys. Future review teams should work with survey experts to conceive more behavioral measures of consumer trust that gather both objective and subjective data with a goal toward generating more concrete and actionable information.	Pending			
29	CCTRT	ICANN should collect data in conjunction with its related data collection activities on the impact of restrictions on who can buy domains within certain new gTLDs (registration restrictions) to help regularly determine and report: 1. Whether consumers and registrants are aware that certain new gTLDs have registration restrictions; 2. Compare consumer trust levels between new gTLDs with varying degrees of registration restrictions; 3. Determine whether the lower abuse rates associated with gTLDs that impose stricter registration policies identified in the Statistical Analysis of DNS Abuse in gTLDs Study continue to be present within new gTLDs that impose registration restrictions as compared with new gTLDs that do not 4. Assess the costs and benefits of registration restrictions to contracted parties and the public (to include impacts on competition and consumer choice) and; 5. Determine whether and how such registration restrictions are enforced or challenged.	Pending			
30	CCTRT	Consider directing ICANN organization, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in consideration of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements to provide incentives, including financial incentives for registries, especially open registries, to adopt proactive anti-abuse measures.	Pending			

31	CCTRT	<p>ICANN Org should, in its discussions with registrars and registries, negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse. With a view to implementing this recommendation as early as possible, and provided this can be done, then this could be brought into effect by a contractual amendment through the bilateral review of the Agreements. In particular, ICANN should establish thresholds of abuse at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements. If the community determines that ICANN org itself is ill-suited or unable to enforce such provisions, a DNS Abuse Dispute Resolution Policy (DADRP) should be considered as an additional means to enforce policies and deter against DNS Security Abuse. Furthermore, defining and identifying DNS Security Abuse is inherently complex and would benefit from analysis by the community, and thus we specifically recommend that the ICANN Board prioritize and support community work in this area to enhance safeguards and trust due to the negative impact of DNS Security Abuse on consumers and other users of the Internet.</p>	Pending			
32	CCTRT	<p>Further study the relationship between specific registry operators, registrars, and DNS Security Abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to be able to identify registries and registrars that need to come under greater scrutiny, investigation, and potential enforcement action by ICANN organization. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remedy problems identified, and define future ongoing data collection.</p>	Pending			
33	CCTRT	<p>In order for the upcoming WHOIS Review Team to determine whether additional steps are needed to improve WHOIS accuracy, and whether to proceed with the identity phase of the Accuracy Reporting System (ARS) project, ICANN should gather data to assess whether a significant percentage of WHOISrelated complaints applicable to new gTLDs relate to the accuracy of the identity of the registrant.³⁰ This should include analysis of WHOIS accuracy complaints received by ICANN Contractual Compliance to identify the subject matter of the complaints (e.g., complaints about syntax, operability, or identity). The volume of these complaints between legacy gTLDs and new gTLDs should also be compared. ICANN should also identify other potential data sources of WHOIS complaints beyond those that are contractually required (including but not limited to complaints received directly by registrars, registries, ISPs, etc.) and attempt to obtain anonymized data from these sources. Future CCT Reviews may then also use these data.</p>	Pending			

34	CCTRT	<p>Assess whether mechanisms to report and handle complaints have led to more focused efforts to combat abuse by determining: (1) the volume of reports of illegal conduct in connection with the use of the TLD that registries receive from governmental and quasi-governmental agencies; (2) the volume of inquires that registries receive from the public related to malicious conduct in the TLD; (3) whether more efforts are needed to publicize contact points to report complaints that involve abuse or illegal behavior within a TLD; and (4) what actions registries have taken to respond to complaints of illegal or malicious conduct in connection with the use of the TLD. Such efforts could include surveys, focus groups, or community discussions. If these methods proved ineffective, consideration could be given to amending future standard Registry Agreements to require registries to more prominently disclose their abuse points of contact and provide more granular information to ICANN. Once this information is gathered, future review teams should consider recommendations for appropriate follow up measures.</p>	Pending			
35	CCTRT	<p>ICANN should gather data on new gTLDs operating in highly-regulated sectors to include the following elements: - A survey to determine: 1) the steps registry operators are taking to establish working relationships with relevant government or industry bodies; and 2) the volume of complaints received by registrants from government and regulatory bodies and their standard practices to respond to those complaints. - A review of a sample of domain websites within the highly-regulated sector category to assess whether contact information to file complaints is sufficiently easy to find. - An inquiry to ICANN Contractual Compliance and registrars/resellers of highly regulated domains seeking sufficiently detailed information to determine the volume and the subject matter of complaints regarding domains in highly regulated industries. - An inquiry to registry operators to obtain data to compare rates of abuse between those highly-regulated gTLDs that have voluntarily agreed to verify and validate credentials to those highly-regulated gTLDs that have not. - An audit to assess whether restrictions regarding possessing necessary credentials are being enforced by auditing registrars and resellers offering the highly-regulated TLDs (i.e., can an individual or entity without the proper credentials buy a highly-regulated domain?). To the extent that current ICANN data collection initiatives and compliance audits could contribute to these efforts, we recommend that ICANN assess the most efficient way to proceed to avoid duplication of effort and leverage current work.</p>	Pending			
36	CCTRT	<p>a. Determine whether ICANN Contractual Compliance should report on a quarterly basis whether it has received complaints for a registry operator's failure to comply with either the safeguard related to gTLDs with inherent governmental functions or the safeguard related to cyberbullying. b. Survey registries to determine: 1) whether they receive complaints related to cyberbullying and misrepresenting a governmental affiliation; and 2) how they enforce these safeguards.</p>	Pending			

37	CCTRT	A study to ascertain the impact of the New gTLD Program on the costs required to protect trademarks in the expanded DNS space should be repeated at regular intervals to see the evolution over time of those costs. The CCT Review Team recommends that the next study be completed within 18 months after issuance of the CCT Final Report, and that subsequent studies be repeated every 18 to 24 months. The CCT Review Team acknowledges that the Nielsen survey of INTA members in 2017 intended to provide such guidance yielded a lower response rate than anticipated. We recommend a more user friendly and perhaps shorter survey to help ensure a higher and more statistically significant response rate.	Pending			
1	WS2	SO/AC/Groups should agree that the following seven key elements of diversity should be used as a common starting point for all diversity considerations within ICANN: Age, Gender, Physical disability, Diverse skills, Stakeholder group or constituency, language, Geographical regional representation	Adopted	Diversity		
2	WS2	Each SO/AC/Group should identify which elements of diversity are mandated in their charters or ICANN Bylaws and any other elements that are relevant and applicable to each of its levels including leadership (Diversity Criteria) and publish the results of the exercise on their official websites.	Adopted	Diversity		
3	WS2	Each SO/AC/Group, supported by ICANN staff, should undertake an initial assessment of their diversity for all of their structures including leadership based on their Diversity Criteria and publish the results on their official website	Adopted	Diversity		
4	WS2	Each SO/AC/Group should use the information from their initial assessment to define and publish on their official website their Diversity Criteria objectives and strategies for achieving these, as well as a timeline for doing so.	Adopted	Diversity		
5	WS2	Each SO/AC/Group, supported by ICANN staff, should undertake a regular update of their diversity assessment against their Diversity Criteria and objectives at all levels including leadership. Ideally this update should be carried out annually but not less than every three years. They should publish the results on their official website and use this information to review and update their objectives, strategies, and timelines.	Adopted	Diversity		
6	WS2	ICANN staff should provide support and tools for the SO/AC/Groups to assist them in assessing their diversity in an appropriate manner. ICANN should also identify staff or community resources that can assist SO/ACs or other components of the community with diversity-related activities and strategies.	Adopted	Diversity		
7	WS2	ICANN staff should support SO/AC/Groups in developing and publishing a process for dealing with diversity-related complaints and issues.	Adopted	Diversity		

8	WS2	<p>ICANN staff should support the capture, analysis, and communication of diversity information, seeking external expertise if needed, in the following ways:</p> <p>1.8.1. Create a Diversity section on the ICANN website.</p> <p>1.8.2. Gather and maintain all relevant diversity information in one place.</p> <p>1.8.3. Produce an Annual Diversity Report for ICANN based on all the annual information and provide a global analysis of trends and summarize SO/AC/Groups recommendations for improvement, where appropriate. This should also include some form of reporting on diversity complaints.</p> <p>1.8.4. Include diversity information derived from the Annual Diversity Report in ICANN's Annual Report.</p>	Adopted	Diversity		
9	WS2	<p>2.1 Recommendations for guidelines with respect to Petitions for removal:</p> <p>2.1.1 May for any reason; and</p> <p>2.1.2 Must:</p> <p>2.1.2.1 Be believed by the Indemnified Party to be true.</p> <p>2.1.2.2 Be in writing.</p> <p>2.1.2.3 Contain sufficient detail to verify facts; if verifiable facts are asserted.</p> <p>2.1.2.4 Supply supporting evidence if available/applicable.</p> <p>2.1.2.5 Include references to applicable by-laws and/or procedures if the assertion is that a specific by-law or procedure has been breached.</p> <p>2.1.2.6 Be respectful and professional in tone.</p>	Adopted	ICANN Board of Directors		
10	WS2	<p>Recommendations for guidelines with respect to procedures for consideration of board removal notices by SO/ACs to include:</p> <p>2.2.1 Reasonable time frames for investigation by SO/AC councils or the equivalent decision-making structures if the SO/AC deems that an investigation is required.</p> <p>2.2.2 Period of review by the entire membership of the SO/AC provided the SO/AC organizational structure customarily provides review for individual members; otherwise, period of review by those empowered to represent the SO/AC in decisions of this nature.</p> <p>2.2.3 Consistent and transparent 40 voting method for accepting or rejecting a petition; such voting maybe be by the entire membership or those empowered to represent the SO/AC in decisions of this nature.</p> <p>2.2.4 Documentation of the community process and how decisions are reached.</p>	Adopted	ICANN Board of Directors		

11	WS2	<p>Standalone Recommendations</p> <p>In addition to the proposed guidelines which are intended to trigger the indemnity under ICANN Bylaws Article 20, Section 20.2, two other recommendations were developed that may be helpful to the community as standalone items</p> <p>2.3.1 A standard framework be developed and used to raise the issue of Board removal to the respective body – either the specific SO/AC who appointed the member or the Decisional Participant in the case of a NomCom appointee. The framework would be in the context of developing a broader framework for implementing community powers and entering into the discussions contemplated by WS1. This framework could be developed by a new group specifically formed for that purpose.</p> <p>2.3.2 Implement the guidelines as a community best practice to apply to all discussions even if not covered by the indemnities contemplated under Article 20. There may be discussions around rejecting a budget or rejecting a proposed standard Bylaw that would benefit from a good faith process. The guidelines for engaging discussions around Board removal could be adopted as a universal standard given that they are broad enough to encompass any discussion.</p>	Adopted	ICANN Board of Directors		
12	WS2	<p>The CCWG-Accountability WS2 recommends the adoption of the Framework of Interpretation it developed for the ICANN Bylaws dealing with Human Rights, which can be found in Annex 3.</p>	Adopted	Human Rights		
13	WS2	<p>Recommendations Relating to OFAC Sanctions and Related Sanctions Issues The Subgroup considered issues relating to government sanctions, particularly41 U.S. government sanctions administered by the Office of Foreign Asset Control (OFAC). OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals.</p>	Adopted	Jurisdiction		
14	WS2	<p>Recommendations relating to Choice of Law and Choice of Venue Provisions in ICANN Agreements</p> <p>This sub-group considered how the absence of a choice of law provision in the base RA, the absence of a choice of law provision in the standard RAA, and the contents of the choice of venue provision in RAs could impact ICANN’s accountability. These are standard-form contracts that are not typically negotiated; changes are now determined through an amendment procedure (e.g. Art. 7.6 of the RA).</p> <p>The sub-group understands that it cannot require ICANN to make amendments to the RA or the RAA. Rather, this recommendation suggests possible changes to the RA and RAA for study and consideration by ICANN the organization, the GNSO, and the contracted parties.</p> <p>The RA and RAA do not contain choice of law provisions. The governing law is thus undetermined, until determined by a judge or arbitrator or by agreement of the parties.</p>	Adopted	Jurisdiction		
15	WS2	<p>The Ombuds Office should have a more strategic focus.</p>	Adopted	ICANN Office of Ombuds		

16	WS2	<p>The Ombuds office should include procedures that:</p> <p>5.2.1 Distinguish between different categories of complaints and explains how each will be handled.</p> <p>5.2.2 Set out the kinds of matters where the Ombuds will usually not intervene – and where these matters are likely to be referred to another channel (with the complainant's permission)</p> <p>5.2.3 Provides illustrative examples to deepen understanding of the Ombuds' approach.</p>	Adopted	ICANN Office of Ombuds		
17	WS2	<p>Once ICANN has agreed to a revised configuration for the Office of the Ombuds, a plan should be developed for a soft relaunch of the function, which should incorporate action to emphasize the importance of the Ombuds function by all relevant parts of ICANN, including:</p> <p>Board CEO Community Groups Complaints Officer</p>	Adopted	ICANN Office of Ombuds		
18	WS2	<p>All relevant parts of ICANN should be required (should include the corporation, the Board and committees, and anybody or group with democratic or delegated authority) to respond within 90 days (or 120 days with reason) to a formal request or report from the Office of the Ombudsman. The response should indicate the substantive response along with reasons. Should the responding party not be able to meet the 120-day limit due to exceptional circumstances, that party can apply to the IOO to seek an additional extension prior to the expiration of the original 90-day delay. The application should be in writing, stating the nature of the exception and the expected time required to respond. The IOO will respond to such requests within a week.</p>	Adopted	ICANN Office of Ombuds		
19	WS2	<p>The ICANN Office of the Ombuds should establish timelines for its own handling of complaints and report against these on a quarterly and annual basis.</p>	Adopted	ICANN Office of Ombuds		
20	WS2	<p>The Office of the Ombuds should be configured so that it has formal mediation training and experience within its capabilities.</p>	Adopted	ICANN Office of Ombuds		
21	WS2	<p>Ideally, the Office of the Ombuds should be configured so that it has gender and, if possible, other forms of diversity within its staff resources. (The primary objective of this recommendation is to ensure that the Community has choices as to whom in the IOO they can bring their complaints to and feel more comfortable doing so.)</p>	Adopted	ICANN Office of Ombuds		

22	WS2	<p>ICANN should establish an Ombuds Advisory Panel:</p> <p>5.8.1 Made up of five members to act as advisers, supporters, and wise counsel for the Ombuds and should be made up of a minimum of at least two members with Ombudsman experience and the remainder with extensive ICANN experience.</p> <p>5.8.2 The Panel should be responsible for:</p> <p>5.8.2.1 Contributing to the selection process for new Ombuds, which would meet the various requirements of the Board and Community, including diversity.</p> <p>5.8.2.2 Recommending candidates for the position of Ombuds to the Board.</p> <p>5.8.2.3 Recommending terms of probation to the Board for new Ombuds.</p> <p>5.8.2.4 Recommend to the Board firing an Ombuds for cause.</p> <p>5.8.2.5 Contribute to an external evaluation of the IOO every five years.</p> <p>5.8.2.6 Making recommendations regarding any potential involvement of the IOO in non-complaint work based on the criteria listed in Recommendation 11.</p> <p>5.8.3 The Panel cannot be considered as being part of the Ombuds Office and cannot be considered additional Ombuds, but rather external advisors to the office.</p> <p>5.8.4 Any such advisory panel would require the Ombuds to maintain its confidentiality engagements per the Bylaws.</p>	Adopted	ICANN Office of Ombuds		
23	WS2	<p>The Ombuds employment contracts should be revised to strengthen independence by allowing for a:</p> <p>5.9.1 Five-year fixed term (including a 12-month probationary period) and permitting only one extension of up to three years (the extension should be subject to a community-based feedback mechanism to the Advisory Panel covering Ombuds performance over the previous years).</p> <p>5.9.2 The Ombuds should only be able to be terminated with cause.</p>	Adopted	ICANN Office of Ombuds		
24	WS2	<p>The Ombuds should have as part of their annual business plan, a communications plan – including the formal annual report – publishing reports on activity, collecting and publishing statistics and complaint trend information, collecting user satisfaction information, and publicizing systemic improvements arising from the Ombuds' work.</p>	Adopted	ICANN Office of Ombuds		
25	WS2	<p>The following points should be considered and clarified publicly when looking at the Ombuds' involvement in any non-complaints work:</p> <p>Whether there is unique value that the Ombuds can add through the proposed role or function?</p> <p>Whether the proposed reporting/accountability arrangements may compromise perceived independence?</p> <p>Whether the workload of the proposed role/function would limit the Ombuds ability to prioritize their complaints-related work?</p> <p>Whether any Ombuds' involvement with the design of new or revised policy or process, meets the requirement of not, in any way, creating a "stamp of approval"?</p> <p>Whether the proposed Ombuds input may be seen as a "short-cut" or substituting for full stakeholder consultation?</p>	Adopted	ICANN Office of Ombuds		

26	WS2	SO/AC/Groups should document their decision-making methods, indicating any presiding officers, decision-making bodies, and whether decisions are binding or nonbinding.	Adopted	SO/AC Accountability		
27	WS2	SO/AC/Groups should document their procedures for members to challenge the process used for an election or formal decision.	Adopted	SO/AC Accountability		
28	WS2	SO/AC/Groups should document their procedures for non-members to challenge decisions regarding their eligibility to become a member.	Adopted	SO/AC Accountability		
29	WS2	SO/AC/Groups should document unwritten procedures and customs that have been developed in the course of practice, and make them part of their procedural operation documents, charters, and/or bylaws.	Adopted	SO/AC Accountability		
30	WS2	Each year, SO/AC/Groups should publish a brief report on what they have done during the prior year to improve accountability, transparency, and participation, describe where they might have fallen short, and any plans for future improvements.	Adopted	SO/AC Accountability		
31	WS2	Each Empowered Community (EC) Decisional Participant should publicly disclose any decision it submits to the EC. Publication should include description of processes followed to reach the decision.	Adopted	SO/AC Accountability		
32	WS2	Links to SO/AC transparency and accountability (policies, procedures, and documented practices) should be available from ICANN's main website, under "accountability." ICANN staff would have the responsibility to maintain those links on the ICANN website.	Adopted	SO/AC Accountability		
33	WS2	Charter and operating guidelines should be published on a public webpage and updated whenever changes are made.	Adopted	SO/AC Accountability		
34	WS2	Members of the SO/AC/Group should be listed on a public webpage.	Adopted	SO/AC Accountability		
35	WS2	Officers of the SO/AC/Group should be listed on a public webpage.	Adopted	SO/AC Accountability		
36	WS2	Meetings and calls of SO/AC/Groups should normally be open to public observation. When a meeting is determined to be members-only, that should be explained publicly, giving specific reasons for holding a closed meeting.	Adopted	SO/AC Accountability		
37	WS2	Records of open meetings should be made publicly available. Records include notes, minutes, recordings, transcripts, and chat, as applicable.	Adopted	SO/AC Accountability		
38	WS2	Records of closed meetings should be made available to members, and may be made publicly available at the discretion of the AC/SO/Group. Records include notes, minutes, recordings, transcripts, and chat, as applicable.	Adopted	SO/AC Accountability		
39	WS2	Filed comments and correspondence with ICANN should be published and publicly available.	Adopted	SO/AC Accountability		
40	WS2	Rules of eligibility and criteria for membership should be clearly outlined in the bylaws or in operational procedures	Adopted	SO/AC Accountability		
41	WS2	Where membership must be applied for, the process of application and eligibility criteria should be publicly available	Adopted	SO/AC Accountability		

42	WS2	Where membership must be applied for, there should be a process of appeal when application for membership is rejected.	Adopted	SO/AC Accountability		
43	WS2	An SO/AC/Group that elects its officers should consider term limits.	Adopted	SO/AC Accountability		
44	WS2	A publicly visible mailing list should be in place.	Adopted	SO/AC Accountability		
45	WS2	if ICANN were to expand the list of languages that it supports, this support should also be made available to SO/AC/Groups.	Adopted	SO/AC Accountability		
46	WS2	A glossary for explaining acronyms used by SO/AC/Groups is recommended.	Adopted	SO/AC Accountability		
47	WS2	Each SO/AC/Group should publish newsletters or other communications that can help eligible non-members to understand the benefits and process of becoming a member.	Adopted	SO/AC Accountability		
48	WS2	Each SO/AC/Group should maintain a publicly accessible website/wiki page to advertise their outreach events and opportunities.	Adopted	SO/AC Accountability		
49	WS2	Each SO/AC/Group should create a committee (of appropriate size) to manage outreach programs to attract additional eligible members, particularly from parts of their targeted community that may not be adequately participating.	Adopted	SO/AC Accountability		
50	WS2	Outreach objectives and potential activities should be mentioned in SO/AC/Group bylaws, charter, or procedures.	Adopted	SO/AC Accountability		
51	WS2	Each SO/AC/Group should have a strategy for outreach to parts of their targeted community that may not be significantly participating at the time, while also seeking diversity within membership.	Adopted	SO/AC Accountability		
52	WS2	Each SO/AC/Group should review its policies and procedures at regular intervals and make changes to operational procedures and charter as indicated by the review.	Adopted	SO/AC Accountability		
53	WS2	Members of SO/AC/Groups should be involved in reviews of policies and procedures, and should approve any revisions.	Adopted	SO/AC Accountability		
54	WS2	Internal reviews of SO/AC/Group policies and procedures should not be prolonged for more than one year, and temporary measures should be considered if the review extends longer.	Adopted	SO/AC Accountability		
55	WS2	It is recommended that the Mutual Accountability Roundtable not be implemented.	Adopted	SO/AC Accountability		
56	WS2	The IRP should not be made applicable to activities of SO/AC/Groups. The appropriate mechanism for individuals to challenge an SO/AC action or inaction is through ICANN's Ombuds Office, whose bylaws and charter are adequate to handle such complaints.	Adopted	SO/AC Accountability		

57	WS2	<p>The ICANN organization should improve visibility and transparency of the organization's existing accountability mechanisms, by posting on icann.org in one dedicated area the following:</p> <p>7.1.1.1 Description of the organization's performance management system and process.</p> <p>7.1.1.2 Description of how departmental goals map to ICANN's strategic goals and objectives.</p> <p>7.1.1.3 Description of the Complaints Office and how it relates to the Ombuds Office.</p> <p>7.1.1.4 Organization policies shared with the CCWG-Accountability during the course of the WS2 work.</p> <p>7.1.1.5 ICANN Organization Delegations document.</p> <p>7.1.1.6 The roles descriptions included in this overall report.</p> <p>7.1.1.7 Expectations and guidelines regarding the development of staff reports for Public Comments, or staff response to Community correspondence.</p>	Adopted	SO/AC Accountability		
58	WS2	<p>The ICANN organization should also evaluate what other communication mechanisms should be utilized to further increase awareness and understanding of these existing and new accountability mechanisms</p>	Adopted	SO/AC Accountability		
59	WS2	<p>To address the lack of clearly defined, or broadly understood, mechanisms to address accountability concerns between community members and staff members regarding accountability or behavior: The ICANN organization should enhance existing accountability mechanisms to include: A regular information acquisition mechanism (which might include surveys, focus groups, reports from the Complaints Office) to allow the ICANN organization to better ascertain its overall performance and accountability to relevant stakeholders. Results of these evaluations should be made available to the Community.</p>	Adopted	Staff Accountability		

60	WS2	To address the lack of clearly defined, or broadly understood, mechanisms to address accountability concerns between community members and staff members regarding accountability or behavior: Consistent with common best practices in services organizations, standardize and publish guidelines for appropriate timeframes for acknowledging requests made by the community, and for responding with a resolution or updated timeframe for when a full response can be delivered. The ICANN organization should include language in the performance management guidelines for managers that recommends people managers of community-facing staff seek input from the appropriate community members during the organization's performance reviews. Identification of appropriate community members, frequency of outreach to solicit input, and how to incorporate positive and constructive feedback into the overall performance review should be at the discretion and judgement of the personnel manager, with appropriate guidance from HR as necessary. Such a feedback mechanism should be supplemental to the existing mechanisms available to the community to provide input on ICANN staff performance, including direct communication to specific staff member, their personnel managers, senior executive staff, Board Directors, and the Complaints Officer.	Adopted	Staff Accountability		
61	WS2	The ICANN Organization should work with the community to develop and publish service level targets and guidelines (similar to the Service Level Agreement for the IANA Numbering Services) that clearly define the services provided by ICANN to the community as well as the service level target for each service.	Adopted	Staff Accountability		
62	WS2	The caveat that the DIDP applies only to "operational activities" should be deleted.	Adopted	Transparency		
63	WS2	The DIDP should include a documentation rule whereby, if significant elements of a decision-making process take place orally, or otherwise without a lasting papertrail, the participants in that decision-making process should be required to document the substance of the conversation, and include it alongside other documentation related to this decision-making process.	Adopted	Transparency		
64	WS2	The DIDP should be expanded to include clearly defined procedures for lodging requests for information, including requirements that requesters should only have to provide the details necessary to identify and deliver the information.	Adopted	Transparency		
65	WS2	The DIDP should impose clear guidelines on ICANN for how to process requests, including delegating a specific employee or employees with the responsibility of responding to DIDP requests, including a commitment to provide reasonable assistance to requesters who need it, particularly where they are disabled or unable to identify adequately the information they are seeking.	Adopted	Transparency		

66	WS2	The DIDP should commit to complying with requesters' reasonable preferences regarding the form in which they wish to receive information under request (for example, if it is available as either a pdf or as a doc), if ICANN either already has that information available in the requested format, or can convert it to the requested format relatively easily.	Adopted	Transparency		
67	WS2	The DIDP should specify that requests should receive a response "as soon as reasonably possible" and should cap timeline extensions to an additional 30 days.	Adopted	Transparency		
68	WS2	The phrase "to the extent feasible, to reasonable requests" should be deleted from the provision on Responding to Information Requests	Adopted	Transparency		
69	WS2	In cases where information subject to request is already publicly available, ICANN staff should direct requesters, with as much specificity as possible, to where the information may be found. In other words, if the processing of a DIDP request reveals that the information has already been published, staff should include information about where this information may be found in their response to the requester.	Adopted	Transparency		
70	WS2	The exception for information "that relates in any way to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone" should be amended so that it only applies to information whose disclosure would be harmful to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone.	Adopted	Transparency		
71	WS2	The exception for "drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication" should be amended to clarify that this information should be disclosed unless it would be harmful to an ongoing deliberative or decision-making process.	Adopted	Transparency		
72	WS2	The exceptions for "trade secrets and commercial and financial information not publicly disclosed by ICANN" and for "confidential business information and/or internal policies and procedures" should be replaced with an exception for "material whose disclosure would materially harm ICANN's financial or business interests or the commercial interests of its stake-holders who have those interests."	Adopted	Transparency		
73	WS2	Where an exception is applied to protect a third party, the DIDP should include a mechanism for ICANN staff to contact this third party to assess whether they would consent to the disclosure.	Adopted	Transparency		
74	WS2	The exception for information requests which are "not reasonable, excessive or overly burdensome, not feasible, abusive or vexatious or made by a vexatious or querulous individual" should be amended so that either the Ombudsman or the Complaints Officer automatically reviews any decision to use this exception.	Adopted	Transparency		
75	WS2	The following sentence should be deleted: "Further, ICANN reserves the right to deny disclosure of information under conditions not designated above if ICANN determines that the harm in disclosing the information outweighs the public interest in disclosing the information."	Adopted	Transparency		

76	WS2	ICANN should consider future processes to expand transparency at ICANN Legal, including through clarification of how attorney-client privilege is invoked.	Adopted	Transparency		
77	WS2	Wherever possible, ICANN's contracts should either be proactively disclosed or available for request under the DIDP. The DIDP should allow ICANN to withhold information subject to a non-disclosure agreement; however, such agreements should only be entered into where the contracting party satisfies ICANN that it has a legitimate commercial reason for requesting the NDA, or where information contained therein would be subject to other exceptions within the DIDP (such as, for example, where the contract contains information whose disclosure would be harmful to the security and stability of the Internet)	Adopted	Transparency		
78	WS2	The DIDP should include a severability clause, whereby in cases where information under request includes material subject to an exception to disclosure, rather than refusing the request outright, the information should still be disclosed with the sensitive aspects severed, or redacted, if this is possible.	Adopted	Transparency		
79	WS2	Where an information request is refused, or the information is provided in a redacted or severed form, the DIDP should require that ICANN's response include the rationale underlying the decision, by reference to the specific exception(s) invoked, as well as information about appeal processes that are available	Adopted	Transparency		
80	WS2	The Ombudsman's mandate regarding transparency should be boosted to grant the office a stronger promotional role, including by integrating understanding of transparency and the DIDP into ICANN's broader outreach efforts, by publishing a list of the categories of information ICANN holds.	Adopted	Transparency		
81	WS2	Either the Ombudsman or the Complaints Officer should be tasked with carrying out reasonable monitoring and evaluation procedures, such as publishing the number of requests received, the proportion which were denied, in whole or in part, the average time taken to respond, and so on.	Adopted	Transparency		
82	WS2	ICANN should commit to reviewing the DIDP every five years.	Adopted	Transparency		
83	WS2	In the interest of providing the community greater clarity with regard to how ICANN engages government stakeholders and to ensure that the ICANN Community and, if necessary, the Empowered Community is fully aware of ICANN's interactions with governments, the CCWG-Accountability recommends that ICANN begin disclosing publicly the following (notwithstanding any contractual confidentiality provisions) on at least a yearly (but no more than quarterly) basis with regard to expenditures over \$20,000 per year devoted to "political activities," both in the U.S. and abroad:	Adopted	Transparency		
84	WS2	The DIDP exception for deliberative processes should not apply to any factual information, technical reports, or reports on the performance or effectiveness of a particular body or strategy, as well as any guideline or reasons for a decision which has already been taken or where the material has already been disclosed to a third party	Adopted	Transparency		

85	WS2	The Bylaws should be revised so that material may only be removed from the minutes of Board meetings where it would be subject to a DIDP exception. Decisions to remove material from the minutes of Board meetings should be subject to IRP appeal.	Adopted	Transparency		
86	WS2	Where material is removed from the minutes of Board meetings, the default should be to allow for its release after a particular period of time, once the potential for harm has dissipated.	Adopted	Transparency		
87	WS2	The policy should be clearly posted as “Employee Hotline Policy and Procedures” on the ICANN public website under the “Who we Are” or “Accountability and Transparency” portions as soon as possible	Adopted	Transparency		
88	WS2	Related to the above, the term “whistleblower” should be included in introductory text explaining the policy so that an ICANN community member – who may not know that the policy is called a “Hotline Policy” – may easily locate it using “whistleblower” as the search term. For example: “The following outlines elements of ICANN’s Hotline Policy and Procedures. Some organizations refer to this as “whistleblower protections.”	Adopted	Transparency		
89	WS2	The definition of incidents reported should be broadened from “serious issues” to encourage the report of all issues and concerns related to behavior that may violate local laws and conflict with organizational standards of behavior. Furthermore, the policy should provide specific examples of such violations to guide a potential reporter.	Adopted	Transparency		
90	WS2	The definition of incidents reported should be broadened from “serious issues” to encourage the report of all issues and concerns related to behavior that may violate local laws and conflict with organizational standards of behavior. Furthermore, the policy should provide specific examples of such violations to guide a potential reporter.	Adopted	Transparency		
91	WS2	ICANN need to improve internal administration of the Hotline process by employing case management software to better enable tracking, documenting, reporting, and anticipating potential problem areas.	Adopted	Transparency		
92	WS2	ICANN should regularly provide employees with data about use of the Hotline, that details not only the frequency of use but also the types of incidents reported.	Adopted	Transparency		
93	WS2	ICANN should not prioritize receipt of reports as “urgent” and “non-urgent,” but treat every report as a priority warranting formal acknowledgment of receipt of a report within 48 hours at the latest.	Adopted	Transparency		
94	WS2	ICANN needs to more effectively address potential fear of retaliation against the reporter by stating unequivocally that alleged retaliation will be investigated with the same level of rigor as alleged wrongdoing. ICANN should also guarantee remedy for reporters who suffer from retaliation as well as clarify that good-faith reporting of suspected wrong-doing will be protected from liability.	Adopted	Transparency		
95	WS2	ICANN’s Hotline Policy and Procedures should undergo a third-party audit least every two years to help identify gaps and enable timely corrections. The audit, in turn, should be posted on the public website.	Adopted	Transparency		
1	SSR2	Complete the implementation of all relevant SSR1 recommendations	No action			

2	SSR2	Information Security Management Systems and Security Certifications: At the moment, it is unclear how ICANN org is approaching security certification and audit.	No action			
3	SSR2	SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	No action			
4	SSR2	Budget Transparency and Budgeting SSR in new gTLDs While SSR-related activities may be covered under various items within ICANN's annual budget, it is not clear how ICANN org allocates funds to specific SSR-related functions.	No action			
5	SSR2	Risk Management 5.1. ICANN org'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).	No action			
6	SSR2	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management The SSR2 RT considers it necessary to have an officer at the Executive C-Suite level to coordinate and strategically manage ICANN org's security and security risk activities and implement ICANN org's mission and strategic security objectives.	No action			
7	SSR2	Further Develop a Security Risk Management Framework	No action			
8	SSR2	Establish a Business Continuity Plan Based on ISO 22301	No action			
9	SSR2	Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	No action			
10	SSR2	Improve the Framework to Define and Measure Registrar & Registry Compliance	No action			
11	SSR2	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	No action			
12	SSR2	Create Legal and Appropriate Access Mechanisms to WHOIS Data	No action			
13	SSR2	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	No action			
14	SSR2	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	No action			
15	SSR2	Enhance Contracts with Registrars and Registries to Incentivize the Mitigation of DNS Abuse	No action			
16	SSR2	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats.	No action			
17	SSR2	Establish a Central Abuse Report Portal	No action			

18	SSR2	Ensure that the ICANN Compliance Activities are Neutral and Effective	No action			
19	SSR2	Update Handling of Abusive Naming	No action			
20	SSR2	Complete Development of the DNS Regression Test Suite	No action			
21	SSR2	Formal Procedures for Key Rollovers	No action			
22	SSR2	Baseline Security Practices	No action			
23	SSR2	Phased implementation of the new-generation RZMS	No action			
24	SSR2	Measurements For 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, 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 metrics on a single page on the icann.org web site, such as under the Open Data Platform.	No action			
25	SSR2	Zone File Data Access 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: “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.	No action			
26	SSR2	Document, Improve, and Test the EBERO Processes	No action			
27	SSR2	Algorithm Rollover	No action			
28	SSR2	Measuring Name Collisions	No action			

29	SSR2	Privacy and SSR Measurements	No action			
30	SSR2	Staying Informed and Informing Policy Debates	No action			
31	SSR2	Clarifying SSR Implications of DoH	No action			