REC	ORIGINAL RECOMMENDATION	RECOMMENDATIONS CONSOLIDATED	RATIONALE	RESPONSIBILITY & TIMING
21	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 and the volume of inquires that registries receive from the public related to malicious conduct in the TLD and (2) 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 registry operators to provide this information to ICANN. Once this information is gathered, future review teams should consider recommendations for appropriate follow-up measures	*Provide continuous capability to assess the efficacy of the safeguards against DNS abuse in service of maintaing the security, stability, resiliency of the DNS via rigourous enforcement of the requirement in contract to provide mechanisms to report abuse, an obligation of the registry operator to act to mitigate abuse via formal processes and known mechanisms, record and curate data sufficient to identify complainants, classify complaints and make meaningful attempts to share data and information on volume of complaints, results from mitigation activities and any changes in either process or mechanisms informed by analyzing the data and information recorded and curated.*	The recommendation is intended to solve the documented and pervasively reported case of lack of data for a robust analytic approach to determine level of DNS abuse . The reasons given were the apparent confusion locating points of contact for reporting abuse by consumers, the reporting mechanisms and, whether ICANN had sufficient investment in abuse mitigation outcomes. The consensus was there were sufficient tools to record abuse but the enforcement mechanisms or the will to enforce was inadequate or missing. No new policy developments are anticipated to achieve improved outcomes.	ICANN Organisation No change in time; Pre-requisite **PRIORITTY: HIGH**
22	Assess whether more efforts are needed to publicize contact points where complaints that involve abuse or illegal behavior within a TLD should be directed. 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) what type of law violation is being complained of and (2) an indication of whether complaints relate to the protection of sensitive health or financial information, would assist future review teams in their assessment of these safeguards.	*Specifically and per Specification 11 of the Base Registry Agreement 2013, the ICANN organisation shall encourage a code of best practice by, among other things, ensuring that the abuse complaint point of contact is pervasively and clearly publicized, that a single report format for complaints and their disposition be applied to all registries and in fulfilling the obligations consistent with contract compliance.* *ICANN would mandate that specific abuse data is captured and curated so that it (1) Enables determination of the volume of abuse reports categorised by source of complaints, especially governments, quasi-government agencies and endusers (2) Response actions by registries (3) The awareness of the general public and complainants to both abuse reports and registry operator response*	In the main, the negative comments associated with each recommendation from the Public Commnets was that the definition of 'abuse' is inconsistent and a fear ICANN could be led to take positions outside its narrow remit. This consolidation is predicated on a clarified and fixed meaning of abuse. Abuse is defined as any act that broadly undermines "*the openness, interoperability, resilience, security and/or stability of the DNS* ". To avoid the argument about the definition of the DNS, we contextualize its meaning by reference and direct connection to our understanding of ICANN's mission as per byelaws; Section 1.1: Mission. We cement the approach by reprising the SSAC's definitions of the terms: " *Security - The capacity to protect and prevent misuse of Internet unique identifiers.* *Stability - The capacity to ensure that the Identifier System operates as expected and that users of unique identifiers have confidence that the system operates as expected.* *Resiliency - The capacity of the Identifier System to effectively withstand, tolerate and survive malicious attacks and other disruptive events without disruption or cessation of service." See SSAC Review*	
23		*Finally, the ICANN organisation is obliged to collect, curate and disseminate, as applicable, abuse data and information collected and managed by the registries and, from time to time, seek consumer feedback to gauge the effectivess of all measures.*		