

ISSR2 15 May 2017 Topics Review

#	Topic	Mapping	Bylaws Association	Additional Notes
1	Complete the assessment of the implementation of SSR1 recommendations, the impact of the implementation, how the post implementation is being managed and what implications for the SSR2 review. YES	SSR1		
2	Scope of ICANN's SSR responsibilities: action zone, influence zone, coordination zone YES	ICANN Security		
3	Effectiveness of ICANN's SSR framework, SSR Plan and its implementation YES	ICANN Security		
4	1. Physical security requirements in place and enforcement of minimum security specification for DNSSEC key storage Facility KAB - YES	ICANN Security		
5	Level of compliance requirement for registrars agreements KAB - YES	ICANN Security		
6	SLAM and performance indicators KAB - YES	ICANN Security		
7	With regards to SSR1, implementation of Rec 7, 10, 11 and 27, to see to what extent the current OCTO research feeds into the risk management	SSR1		

10	DNSSec (progress, Key roll over) ET - YES	DNS Security		
11	Domain name abuse mitigation as it affects SSR issues	DNS Security		More info on ICANN's specific role is needed
12	ICANN's role in helping to mitigate DDoS ET - Needs clarification 1. Operational 2. Other (Lroot, zone ICANN is resp for, domain name contractual obligations/compliance, security training,	ICANN Security		
13	Universal acceptance: Can identifiers be consumed by clients ET - YES -IDNs and new gTLDs -Platforms, approaches, and status	DNS Security		
14	Measures and metrics (incorporate in all topics and subteams) - -What are, and how can the community measure the relevant DNS abuses -The evidence base: DNS health index and abuse data. What the evidence tells us; access to information (risks and benefits) ET - CLARIFY	ICANN Security		
15	ICANN's internal security, stability and resiliency operations: ET - YES -Allocation of resources and priority within the organisation (includes	ICANN Security		

	<p>budget and staffing) -Outreach and public information role (training, vulnerability disclosure, system attack mitigation etc) -Risk management, compliance with relevant frameworks.</p>			
16	<p>White-hat operations - What are the white-hat operations that are taken in ICANN space that may need exceptional handling (gratis for registering sink-holes, etc.) (can this be included in improving security of unique identifiers/threat mitigation?)</p>	ICANN Security		
17	<p>Proactive measures (Advisories, Technical alerts) yes</p>	DNS Security		
18				
19				
20	<p>The sub team will be responsible for reviewing the completeness and effectiveness of ICANNs internal security processes and the effectiveness of the ICANN security framework BK -YES</p>	ICANN Security		

21	<p>Due to ICANN's orientation to ISO/IEC 27001 (and ISO 22301? - BCMS) I would recommend to provide a gap-analysis to the normative requirements of the management part and Annex A of the ISO standard based on the SoA (Scope). BK -YES</p>	ICANN Security		
22	<p>Perform interviews and review descriptions and evidence of: BK - YES</p> <ul style="list-style-type: none"> * ISMS / BCMS Scope * Information security policy * Information risk assessment and risk treatment processes * Information security objectives * Information security roles and responsibilities * ISMS internal audit program and results of conducted audits * Operational planning and control documents * Evidence of top management reviews of the ISMS <p style="text-align: center;">Various others from the Annex A like rules for acceptable use of assets, access control policy, operating procedures, confidentiality or</p>	ICANN Security		<p>Gap assessment only.</p> <p>Note 22 & 23 & 24 & 25 & 26 connected</p>

	<p>non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, etc. BK</p> <p>Categorize and prioritize the outcome of the analysis - BK -</p>			
23	<p>Various others from the Annex A like rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, etc. BK</p> <p>(linked to previous item)</p>	ICANN Security		Gap assessment only
24	<p>Categorize and prioritize the outcome of the analysis - BK - (linked to previous item)</p>	ICANN Security		Linked to previous item
25	<p>Develop a short-, medium- and long-term schedule to implement different controls in accordance to the requirements - BK -</p>	ICANN Security		Linked to previous item

26	Define a set of metrics to measure the effectiveness of the implementation - BK - CLARIFY	SSR1 - ICANN Security		Linked to previous item
27	Analyze policies and procedures that are essential to ICANN identifier systems activities ZK - YES	ICANN Security		
28	Analyze the possibilities for faster exchange of information on methods of abuse of Internet unique identifiers and recommendations for mitigation - ZK - YES	ORPHAN		
29	Analyze universal accessibility and resolution of unique identifiers systems ZK - YES	DNS Security		
30	Analyze ICANN internal procedures essential for SSR of the organization and global operations - ZK - YES	ICANN Security		
31	Business continuity planning JG - YES	ICANN Security		
32	Business continuity plan for new IANA functions operator JG - YES	IANA		C7.3 replacement
33	Security Framework JG -	ICANN Security		

	YES			
34	Incident response planning JG - YES	ICANN Security		
35	Coordinated Vulnerability Disclosure Process - JG - YES	ICANN Security		
36	Assess ICANNs ability to respond to strategic threats to the unique identifiers it coordinates.YES	ICANN Security		
37	Vetting process for EBERO operators - JG - YES	ICANN Security		
38	ICANN processes around vetting registry operators - Nick Shorey observer - YES	ICANN Security		
39	Assess DNS threat landscape, domain abuse, and mitigation relevant to ICANN's role - Yes	DNS Security		
40	Risk Assessment and Management relevant to SSR NA - Yes	SSR1		
41	Corporate Data Security and/or Business Systems NA - Yes	ICANN Security		
42				
43	What is the scope of ICANN's threat modeling? BRAINSTORMING - YES	ICANN Security		
44				
45	How effective it is ICANN risk management? BRAINSTORMING - YES	ICANN Security		

46				
47	If I how ICANNs security efforts related to the DNS? BRAINSTORMING - YES	ICANN Security		
48	How ICANN measures the effectiveness as security efforts? BRAINSTORMING - YES	ICANN Security		
49	What are ICANN’s security efforts? (x2) BRAINSTORMING - YES	ICANN Security		
50	What are the benchmarks and good practices for successful security efforts? Yes (note duplicates)	ORPHAN		
51				
52				
53	Review ICANN security procedures. BRAINSTORMING - YES	ICANN Security		
54	What are the indicators for “successful” implementations and intended effects? BRAINSTORMING - YES	SSR1		
55				note about SO/AC recommendations on security including R/SSAC?
56	What are the changes to ICANN SSR with the IANA transition? BRAINSTORMING -	IANA		Combine w/ other IANA/PTI items

	CLARIFY			
57				
58	What are the key performance indicators BRAINSTORMING - YES	SSR1		
59	How can we measure “the extent” of ICANN’s success in implementing security efforts? BRAINSTORMING - YES	ORPHAN		
60				
61				
62				
63	How do we assess “Future challenges to security and stability a DNS?” BRAINSTORMING - YES	Future Threats		
64	What are the actual and potential challenges and threats? BRAINSTORMING - YES	DNS Security		
65				
66				
67	How do we get an understanding of what SSR1 recommendations have been implemented? BRAINSTORMING - YES	SSR1		
68				
69				
70	Which extent of SSR1 recommendations implemented?	SSR1		

	BRAINSTORMING - YES			
71				
72	What are the indicators the SSR2 would want to use to measure “success” of security efforts? BRAINSTORMING - YES	Other		
73	How are we distinguishing operational stability and security from measures that stem from compliance issues? Yes	ICANN Security		
74				
75				
76	Collect input from the community on how ICANN should improve on SSR BRAINSTORMING - YES	Other		
77	Explore forecasting research on the Internet unique identifiers. Yes	Future Threats		
78				
79				
80	What does “interoperable security processes” mean BRAINSTORMING - YES	ICANN Security		
81	What has been, or could be, the impact of the evolution and the number and types of devices in the DNS? Yes	Future Threats		
82				
83	Which portion of the	DNS Security		

	Internet systems of unique identifiers does ICANN not coordinate? BRAINSTORMING - YES			
84				
85				
86				
87				
88	What is the current state of ICANN and disaster and operational recovery planning? BRAINSTORMING - YES	ICANN Security		
89				
90				
91				
92				
93				
94				
95				
96				
97				
98				
99				
100				
101				
102				
103				

104				
105				
106				
107	What is the appropriate security contingency planning framework? BRAINSTORMING - YES	ICANN Security		
108				
109				
110	What is ICANN doing in the area of interoperable security STDs to monitor? (ITHI) BRAINSTORMING - YES	ICANN Security		
111	How the end-user feel secure, reliable, instable	ORPHAN		Note: avoid duplication of CCT research
112				
113				
114				
115				
116				
117				
118				
119	How does ICANN compliance impact SSR? BRAINSTORMING - YES	SSR1		
120	What are the SSR issues with new	DNS Security		

