1. Perform a assessment of ICANN's **Information Security Management** System. This includes, but is not limited to the following domains:

- Leadership, roles, and responsibilities
- Resources, competence, awareness, and communication
- Access control and Cryptography
- Physical and environmental security
- Operational security
- System acquisition, development and maintenance
- Supplier relationships

- Questions & Answers from LA meeting: https://community.icann.org/display/SSR/Workstream+%232+-+ICANN+SSR?preview=/66071173/102144852/ICANN%20SSR%20Questions%20%26%20Answers%20%20-%20WIKI%20TABLE%20-%2024%20Jan%202019.xlsx (rows 11 - 16)
- ICANN SSR LA Meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 1 and top of p2)
- Day 1 & Day 2 transcripts here:
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604250/ssr2-09oct17-en.pdf
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

Follow up:

- More information is needed which areas/departments (or roles) in the organization are responsible for what: CIO vs COO vs CTO (Sr. Director Security & Network Engineering, VP Security Operations, CSSRO) and how they interact between them.

  Remark: Following implemented recommendation from SSR1 (24) as example Office of the Chief Technology Officer (OCTO)

- Are there any changes in the organization regarding security management since October 2017?

Comments:

Q: Is there a reason why ICANN does not use more industry-standard, certifiable and auditable processes, per SSR1 recommendation 9, instead of custom processes?

A: The ICANN org uses a suite of continuous improvement frameworks to drive improvement across the organization. This includes the use of audit and certification frameworks for Engineering and IT, and IANA functions, and EFQM as a holistic framework for assessing and improving the whole organisation.

- More information on these frameworks are needed - in particular: are the topics within ISM are covered by these frameworks and/or standards? ICANN should follow an organisational information security management standard like ISO/IEC 27001 or NIST 800-xx to be sure to cover all relevant topics related to an information management security system

Q: Expanding away from just IANA.org, there is a lot of “critical operations stuff”, the GDD portal and some of the other supporting infrastructure. Is that managed just as a general ICANN service or is attention given to the supporting infrastructure that sits around the root zone maintenance? And is that just handled as a general ICANN IT service?

A: Root zone administration is handled with the same care as all ICANN critical infrastructure, redundant systems, site failover, quick restore as well as enforcement of application security best practices. We can’t speak to the RZM (Root Zone Maintainer as that function is handled by Verisign). As for the GDD portal itself, that is a service hosted by Salesforce.

- More information on these best practices are needed. IMHO ICANN is still responsible for the RZM or other relevant supporting infrastructure. How does ICANN ensure that InfSec requirements are "communicated" to contractors? (reporting, controlling, auditing of contractors, etc.)

2. Perform a assessment of ICANN's **Business Continuity Management** System. This includes, but is not limited to the following domains:

- Business Continuity Objectives and Plans
- Operational planning and control
- Business Continuity Strategies
- Prioritized Activity Recovery Strategy
- Resource Recovery Strategy
- BC Procedures - Incident Response Structure
- Business Continuity Plans (BCP)
- Evaluation of Business Continuity Procedures

- ICANN SSR LA meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 1)
- Day 1 & Day 2 transcripts here:
    - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604250/ssr2-09oct17-en.pdf
    - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

Comments:

Q: Do business continuity testing tabletop exercises for PTI occur at a more regular frequency and to a deeper level than the standard for the rest of ICANN?

A: Historically, dedicated continuity exercises have been conducted for the root zone management component of the IANA functions with our root management partners. In addition, the ICANN org has conducted exercises for the shared IT systems and services that support the IANA functions. Since the creation of PTI we have not had a dedicated PTI-specific continuity exercise. We seek to develop a plan to conduct future exercises once we restore a full complement of staff following recent personnel changes.

- Recommendation: Develop a plan to conduct future exercises and practice them in a frequently manner.

Follow up questions:

- More information is needed who is responsible in the organization for BC in general?
- Additional information/discussion needed focused on how business continuity affects operational, compliance, and root zone security.
- Heard about significant work within ICANN but not much reporting on disaster preparedness and operational recovery planning. More information is needed. □
- Is there a need for adoption of a formal framework for security contingency planning (for instance, from NIST or ISO)? I think fact-finding is needed with a particular focus on disaster management and recovery for those systems that have a clear impact on the Internet’s public identifiers.
- What is the frequency of DR testing?
- Depth of testing of DR needs to be elaborated on (Table top vs power trip).
- Impact analysis done after PTI separation to asses needed for update to BC plans?
- Document boundaries and processes that have inter-org dependencies and relate back to BC plan

As an example: IANA Full-Scale Business Continuity Exercise Conducted 19 January 2010 (https://www.icann.org/en/system/files/files/iana-business-continuity-exercise-aar-23feb10-en.pdf)

Have the recommendations in the report been implemented? If so, how?

3. Perform a assessment of ICANN's **Risk Management Methodology** and Framework. This includes, but is not limited to the following processes:

- Documented Risk Assessment Process

- Risk Management and Risk Treatment
- Risk Acceptance Criteria and Criteria for Risk Assessment?

- Questions & Answers from LA meeting: https://community.icann.org/display/SSR/Workstream+%232+-+ICANN+SSR?preview=/66071173/102144852/ICANN%20SSR%20Questions%20%26%20Answers%20%20-%20WIKI%20TABLE%20-%2024%20Jan%202019.xlsx (rows 2-4)
- ICANN SSR LA Meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 1 items b,c,d and top of page 2)
- Day 1 & Day 2 transcripts here:
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604250/ssr2-09oct17-en.pdf
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

- As of Oct 2017, ICANN did not follow formal information security audit frameworks such as ISO 27001. Is that still the case?
- Are there any plans to adopt a formal framework? If so, please give details of the framework, timeline for implementation and budget allocated.
- Please provide documentation (links/perma-links) about your business continuity and risk management processes.
- Is James Caulfield still the person responsible for risk and business continuity management?
- There is a Board Risk Committee which meets at least twice a year, and considers the risk register. Is this still the case? The Committee organises an interactive risk workshop at least once a year, is that still the case? Please give dates of meetings since 2016, along with attendees and agendas.
- Please confirm that the risk register is updated on an ongoing basis, and give evidence of these updates.
- Relevant managers are responsible for declaring a disaster. Is this still the case?

4. Perform an how effectively ICANN has implemented its **Security Incident Management and Response Processes** to reduce (pro-active and reactive) the probability of DNS-related incidents. This includes, but is not limited to the following processes:

- Security Incident Management Process
- Security Incident Response Process relating to a global, IANA incident (DNS-related)
- ICANN operational responsibilities (L-Root)

- Questions & Answers from LA meeting: https://community.icann.org/display/SSR/Workstream+%232+-+ICANN+SSR?preview=/66071173/102144852/ICANN%20SSR%20Questions%20%26%20Answers%20%20-%20WIKI%20TABLE%20-%2024%20Jan%202019.xlsx (rows 18-21)
- ICANN SSR LA Meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 4 and the last page)
- Day 1 & Day 2 transcripts here:

    - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/7160,4250/ssr2-09oct17-en.pdf
    - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

Comments:

Row 18: Vulnerability disclosure PDF dates back to 2013.

https://www.icann.org/news/blog/transparency-of-security-efforts-in-icann
https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf
https://www.icann.org/news/blog/ciio-perspectives-icann-s-incident-response-protocol

ICANN has engaged HackerOne to run their Vulnerability Disclosure Policy (VDP) and Bug Bounty Program (BBP). However it appears the onboarding and deployment of such program is still in progress and not complete.
https://www.icann.org/vulnerabilities
https://hackerone.com/icann

What is the timeline for completing, implementing and public launch of the VDP and BBP?
Is there resourcing or budget reasons for the delay?

Are reports on incidents required? How are they released, and on what schedule?

Note: Compliance reports are necessary to have community review.

Why have there been no obvious updates since 2013, is the process as outlined in the PDF still followed?

Row 19: Segmentation

ICANN Org employs network segmentation strategies designed to reduce the risk of pivoting activity by an attacker.

Are these segmentation strategies implemented now, how are they implemented?

Administrative access to critical services (particularly those managed by IANA) have restrictions beyond internal network access.

What are those restrictions, and are they on the same network (topology, in detail -- diagram)?

Periodic network penetration testing is conducted by independent service providers against ICANN Org network defenses, simulating attacks from both outside the network and attempted lateral movement from within the network.

Are industry best practices followed? Please report and link to which ones.

Are penetration testers being rotated on a regular basis? If there is evidence relating to these processes, please provide a link? Is there version control, is there a permanent link?

The results are used to prioritize network security Improvements.

Can you provide details on how these findings feed into improvements? Are there any reports on this? Is there version control, is there a permanent link?

Row 20: ANSWER MISSING; Still relevant
Row 21: ANSWER MISSING; Still relevant

- Security Incident Management Process (ICANN internal)

Is there periodic reporting? How are incidents reported on? Is there version control, is there a permanent link?

Are there formal procedures for SIMP at ICANN, can you provide a document that outlines them? Is there version control, is there a permanent link?

Were there only incidents in 2017, nothing available about 2018 for example? Has an updated report been published?

Where is the "single page" you mentioned 15 months ago (see transcript) about the SIMP process? Is there a permanent link?

Where is that policy that was said to be updated 15 months ago (see transcript)? Is there version control, is there a permanent link?

- From LA transcript: "SAMUEL SUH: *Right now, it's kind of scattered. You have to search. But I think within the next couple of weeks, we'll be reporting on all incidents on a single page." Need to get updated policy.*
- *FYI: https://www.icann.org/vulnerabilities*
-

- Security Incident Response Process relating to a global, IANA incident (DNS-related)

How is this being done, is there a structure and process? Is there version control, is there a permanent link?

Is there periodic reporting, if so, where? Is there version control, is there a permanent link?

- ICANN operational responsibilities (L-Root)

What are the processes to secure L-Root, are they being published? As it is the "best practice" case, this appears sensible. Is there version control, is there a permanent link?

Is there periodic reporting on security incidents - if so, where? Is there version control, is there a permanent link?

What are the processes to coordinate with the other root server administrators; are these available publicly?

RECOMMENDATION:
Real management level audit needed (ISO etc). Audit by professional compliance party, e.g. big four -- need to defend on reputation.(acknowledge audits occurring in IANA/PTI space and that this audit applies to other ICANN functions)

Which certifications is ICANN pursuing for the organisation and staff?

Which certifications and compliance frameworks has ICANN completed?

Who are ICANN's auditors, what audits are completed regularly?

5. Perform a assessment of internal security, stability and resiliency of **ICANN's operation processes and services**. This includes, but is not limited to the following scope:

- Global Domain Division Operations (GDD Operations)
- Centralized Zone Data Service (CZDS)
- SLA Monitoring System (SLAM)
- Statistical Analysis of DNS Abuse in gTLDs (SADAG)
- Domain Abuse Activity Reporting (DAAR)

- Questions & Answers from LA meeting: https://community.icann.org/display/SSR/Workstream+%232+-+ICANN+SSR?preview=/66071173/102144852/ICANN%20SSR%20Questions%20%26%20Answers%20%20-%20WIKI%20TABLE%20-%2024%20Jan%202019.xlsx (rows 10, 22)
- ICANN SSR LA Meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 2,3 4)
- Day 1 & Day 2 transcripts here:
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604250/ssr2-09oct17-en.pdf
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

Comments:

Reporting, Row 10

There are two things conflated here. One is the cost of curating and validating the the data. This is the major cost and is covered by ICANN's budget transparency. The other is the cost of then *defining which of the curated data we can publish and presenting that to the public. It is ICANN's intention to publish as much data that our licensing allows via ODI. This cost is not yet certain as we have not finalized the possible output but it is likely to be minimal.*

This was reported on 15 months ago, what is the cost?

What curated data is now considered publishable? Is there documentation with version control, is there a permanent link?

Compliance, Row 22

Contractual Compliance has a standard Approach and Process (https://www.icann.org/resources/pages/approach-processes-2012-02-25-en) that applies across the registrar, registry and audit program. Contractual Compliance monitors complaints to identify patterns and systemic issues of noncompliance within and across the complaint types and the contracted parties.This effort is useful in identifying trends of issues and most importantly in identifying opportunities to conduct outreach or additional proactive monitoring. For example, based on trends identified by Contractual Compliance (including review of WHOIS inaccuracy complaints submitted by the public and generated as a result of the WHOIS ARS), Contractual Compliance launched a WHOIS Inquiry effort in 2016 that focused on registrars in China and Korea. These inquiries focused on issues with the 2013 RAA WHOIS Accuracy Specification Program (WAPS) requirements. These efforts continued for registrars in China, United States and other regions. Please refer to the annual update published at this link: https://www.icann.org/en/system/files/files/annual-2016-31jan17-en.pdf . Outreach efforts are ongoing; please refer to Outreach page (https://www.icann.org/resources/compliance-reporting-performance) for more information.

What are the other regions referred to in the answer?

Can you report on your methodology for the ICANN Contractual Compliance Performance Reports? Is there documentation with version control, is there a permanent link?

How are indicators chosen, and how do you account for regional differences (e.g. number of registries in different regions)? Is there documentation with version control, is there a permanent link?

Is there a compliance function in GDD?
For example, is there contractual enforcement if access to data is denied?

- Centralized Zone Data Service (CZDS)

See other section

- SLA Monitoring System (SLAM)

See other section

- Statistical Analysis of DNS Abuse in gTLDs (SADAG)

Is there regular abuse reporting? Is there documentation with version control, is there a permanent link?

What is ICANN's methodology for analysing and presenting data, as well as reporting? Is there documentation with version control, is there a permanent link?

- Domain Abuse Activity Reporting (DAAR)

Is ICANN providing validated data to the community on abuse and contractual compliance? What is ICANN doing to foster a community of researchers and other parties who are dealing with these issues?

What steps are taken to provide this crucial information? What methodology is ICANN following? Is there documentation with version control, is there a permanent link?

Is there any enforcement activity based on DAAR reports? Is there documentation about such action, is there a permanent link?

Recommendation:
ICANN should provide or foster regular studies of different forms of abuse (phishing, spam, targeted attacks)

ICANN should take steps to make DAAR and other abuse-related data public by changing contracts accordingly or "re-architecting" a DAAR system that only relies on publishable data.

Relevant refs with recommendations in them:
https://www.icann.org/en/system/files/files/sac-103-en.pdf

https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf

FYI: Sources of abuse data: SADAG report (ICANN paid for), SpamHaus, SURBL, Norm's Secure Domain Foundation, CleanMX, and others…

SSAC (SAC 103 pg. 12 addresses abuse data). Lots of other ICANN groups have been requesting abuse data from ICANN for years. Also see https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf clause in RAA: 3(b) Registry will periodically conduct a technical analysis to assess whether domains are being used to perpetrate security threats (pharming, phishing, malware, and botnets) and provide records of such analysis to ICANN upon request.

(is any of that done?)

6. Perform an how effectively ICANN has implemented its **processes around vetting registry operators and services concerning the New gTLD Delegation and Transition process**. This includes, but is not limited to the following scope:

- New gTLD Registry Agreement (Registry Operator)
- Back-End Registry Operator (BERO)
- Emergency Back-End Registry Operator (EBERO)
- Registry Data Escrow (RyDE) - Data Escrow Agent (DEA)

- Questions & Answers from LA meeting: https://community.icann.org/display/SSR/Workstream+%232+-+ICANN+SSR?preview=/66071173/102144852/ICANN%20SSR%20Questions%20%26%20Answers%20%20-%20WIKI%20TABLE%20-%2024%20Jan%202019.xlsx (rows 5-9)

Notes from LA breakout team.

Row 6: https://schd.ws/hosted_files/icann60abudhabi2017/08/7%20EBERO%20Arias.pdf
Since the testing in the Fall of 2017, have the issues raised been addressed? If so, is there a re-test scheduled or been held and are the results available?

Row 7: https://www.icann.org/en/system/files/files/mosapi-specification-26nov18-en.pdf. https://www.icann.org/resources/pages/mosapi-specification-2019-01-03-en This appears to be done.

Row 8: Complete.
https://schd.ws/hosted_files/icann60abudhabi2017/08/7%20EBERO%20Arias.pdf

Row 9: Has the Root Cause Analysis been conducted? If so, is there a reference to the report?

- ICANN SSR LA Meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 3 and page 5)
- Day 1 & Day 2 transcripts here:
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604250/ssr2-09oct17-en.pdf
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

(Boban) Suggest ongoing testing and collaboration between ICANN & Registry operators & Escrow agents and improvements/best practices

Questions around security of data and breaches

7. Perform an assessment how effectively ICANN has implemented its **processes to ensure compliance regarding registrar agreements and the consensus policies**. This includes, but is not limited to the following scope:

- WHOIS Accuracy Reporting System (ARS)
- WHOIS Accuracy Program Specification (WAPS)
- Expired Domain Deletion Policy (EDDP), Expired Registration Recovery Policy (ERRP):
- Uniform Domain Name Dispute Resolution Policy (UDRP):
- Registrar Data Escrow (RDE)
- Abuse Reports
- Transfer Policy

- Questions & Answers from LA meeting: https://community.icann.org/display/SSR/Workstream+%232+-+ICANN+SSR?preview=/66071173/102144852/ICANN%20SSR%20Questions%20%26%20Answers%20%20-%20WIKI%20TABLE%20-%2024%20Jan%202019.xlsx (rows 17, 22-38)

Notes from LA breakout team.

Row 17: Denise and Norm to write-up description of the current contractual compliance process and procedures for whois accuracy and assessment and recommendation. To be reviewed by the full team. Cross- where reference the CCT report where applicable.

Row 22: Beta testing is currently underway (Jan 2019) for new CZDS portal and API. Does this also impact submission of zones? Review after release of new CZDS.

Row 23/24: Read/review relevant section from CCT report. We need an update on the plans and improvements made to contractual compliance wrt WHOIS.

Row 25/26: Need an update on whois changes/plans following the interim changes to whois invoked as a response to GDPR.

- ICANN SSR LA Meeting report: https://docs.google.com/document/d/1aiwB9VjxXNhOqGmaIeHiGIr1zM4uus0B2chUmk3m8p4/edit (page 3)
- Day 1 & Day 2 transcripts here:
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604250/ssr2-09oct17-en.pdf
  - https://community.icann.org/pages/viewpage.action?pageId=69277737&preview=/69277737/71604251/SSR2%20-%20ICANN%20SSR%20-%20F2F%20LA%20Meeting%20-%2010OCT17%20-%20Day%202.pdf

Additional Questions

IANA and impact of ICANN Org's systems on the DNS

- Is there are separate risk management framework (including risk register and business continuity plan) for the PTI?
- IANA (PTI) systems (both IT and operational) continue to be dependent on ICANN. When PTI staff login in the morning, they are on the ICANN secured network, correct? Is this still the case? Note: may want to address this off the public list/wiki)
- Within risk classification or scoring, there is no multiplier for potential impact on the internet's system of unique identifiers. Is this still the case?

Contractual compliance, EBERO and SLA Monitoring

- ICANN was not monitoring EPP. Is this still the case?
- As of Oct 2017, no action had been taken in relation to 32 RSPs which have reached emergency thresholds in 2017. Is this correct? Please provide updates on action taken (if any) in relation to RSPs that have reached emergency thresholds before and since October 2017.
- In your experience, are the emergence thresholds fit for purpose? If not, are there any plans to revisit them with the community?
- Francisco referred to internal procedures to deal with SLA monitoring cases that require follow up, please provide SSR2 with a copy?
- To what extent are the EBERO processes part of ICANN's risk management framework?
- What is the status of the registry service provider certification program? Is ICANN Org recommending any changes? What is the status of this issue within the Subsequent Procedures PDP?
- To what extent have the relationships or contracts with EBERO providers been updated to take into account the changing security landscapes, information security requirements?

OCTO, open data initiative, and GDPR

- Specifically, to what extent and how has the work of OCTO and Compliance been affected by the coming into force of GDPR? Please provide details.
- Is OCTO going to provide public information on DAAR and its findings and how much will that cost?
- To what extent are there correlations between certain types of contracted party business models and certain types of abuse? Please provide details
- Is there a plan to make the information from DAAR actionable by registries and registrars? Please provide details.
- Is there a plan to continue research on the abuse of and possible safeguards in the DNS, and in particular with reference to New gTLDs, following the report on DNS abuse (commissioned by CCT Review Team)?

Security incidents, vulnerabilities and breaches

- Please provide details of any and all security breaches that have occurred since the period of the last SSR Review, including what remediation action and changes of system have been put in place following such breaches.

Outreach & Capacity Building

- Please provide details on outreach or other efforts, and training, to inform or improve uptake among new gTLD registries, legacy gTLDs and ccTLDs, for DNSSEC and DNS operations.
- Do you provide such specific training (not high level info session) at ICANN and other related industry events?
- Please provide a progress report on the planned webpage with current information on common challenges for RSPs, and suggested mitigation actions/proactive measures?