ID	Topic		Questions	ICANN Personnel	Date	Time	ICANN Personnel	Documents	Recommendations
1	Perform an assessment of ICANN's **Information Security Management** System.								
	1.1	***ISMS in general***							
	1.1.1		Does ICANN utilise a formal ISMS (Information Security Management System)?						
	1.1.2		Are the general ISMS objectives compatible mapped to the ICANN strategic plan and ICANN's identified enterprise risks?						
	1.1.3		Is there a formal training plan in place to ensure all staff are aware of the policies and operating procedures of the ISMS?						
	1.2	***Leadership and responsibilities***							
	1.2.1		Are the general ISMS objectives compatible with the strategic direction of ICANN?						
	1.2.2		Does Information Security Policy exist with objectives or framework for setting objectives?						
	1.2.3		Is Information Security Policy communicated within the company?						
	1.2.4		Are roles and responsibilities for information security assigned and communicated?						
	1.2.5		Is there a formal training plan in place to ensure all staff are aware of the policies and operating procedures of the ISMS?						
	1.3	***Resources, competence, awareness, and communication***							
	1.3.1		Are adequate resources provided for all the elements of ISMS?						
	1.3.2		Are required competences defined, trainings performed, and records of competences maintained?						
	1.3.3		Is the personnel aware of Information security policy, of their role, and consequences of not complying with the rules?						
	1.3.4		Does the process for communication related to information security exist, including the responsibilities and what to communicate?						
	1.3.5		Does the process for managing documents and records exist, including who reviews and approves documents, where and how they are published, stored and protected?						
	1.3.6		Are documents of external origin controlled?						
	1.3.7		Are all relevant employees and contractors being trained to perform their security duties, and do the awareness programs exist?						
	1.4	***Access control***							
	1.4.1		Does policy for physical access to hardware and equipment exists?						
	1.4.2		Does policy for Logical access control to protect data and software from unauthorised access and misuse exists?						
	1.5	***Physical and environmental security***							
	1.5.1		Is there physical methods to control access to information processing facilities?						
	1.5.2		Is there protecton of equipment from security and environmental threats and hazards?						
	1.5.3		Does equipment facilities have continuous power supply?						
	1.6	***Operational security***							
	1.6.1		Are Operational Procedures and Responsibilities established across organization?						
	1.6.2		Does Operational Procedures and Responsibilities comply with security policy?						
	1.6.3		Is there protection from malicious software?						
	1.6.4		Is there dokumented Backup procedure?						
	1.6.5		Are the rules been established for use of mobile devices and removable media?						
	1.7	***System acquisition, development and maintenance***							

ID		Topic	Questions	ICANN Personnel	Date	Time	ICANN Personnel	Documents	Recommendations
	1.7.1		Are there security requirements that new applications or all enhancements to existing systems must meet?						
	1.7.2		Are there security controls for aplication development or aquisition?						
	1.7.3		Does formal procedure to control changes to information systems exist?						
	1.7.4		Is there a policy on the use of cryptography?						
	1.8	***Supplier relationships***							
	1.8.1		Is the policy on how to treat the risks related to suppliers and partners documented?						
	1.8.2		Are suppliers regularly monitored for compliance with the security requirements, and audited if appropriate?						
	1.8.3		Do the agreements with suppliers include security requirements for ensuring the reliable delivery of services?						
2	Perform a comprehensive assessment of ICANN's **Business Continuity Management** System.								
	2.1	***Business Continuity Objectives and Plans***							
	2.1.1		Is there a documented Corporate (organization) BCM Strategy that has been signed-off by top management?						
	2.1.2		Does the organization have a documented business continuity operational planning and control process?						
	2.2	***Operational planning and control***							
	2.2.1		Have the operating procedures for IT processes been documented?						
	2.2.2		Is installation of software strictly controlled; do procedures exist for that purpose?						
	2.2.3		Is it clearly defined who should be in contact with which authorities?						
	2.2.4		Is it clearly defined who should be in contact with special interest groups or professional associations?						
	2.2.5		Are information security rules included in every project?						
	2.2.6		Are audits of production systems planned and executed in such a way that they minimize the risk of disruption?						
	2.3	***Business Continuity Strategies***							
	2.3.1		Is there a documented Corporate (organization) BCM Strategy that has been signed-off by top management?						
	2.4	***Prioritized Activity Recovery Strategy***							
	2.4.1		Have the Recovery Time Objective (RTO) for each prioritised activity been identified and agreed?						
	2.4.2		Has the organization identified the dependencies and resources needed to maintain, restore, resume and/or recover each of its prioritised activities to an acceptable level of functionality and performance (MBCO)?						
	2.5	***Resource Recovery Strategy***							
	2.5.1		Is there a documented Resource Recovery Strategy for critical business activities and their dependencies that has been signed off by top management?						
	2.5.2		Is the strategy based upon and consistent with the resource recovery requirements identified within the current BIA in respect of the organization's prioritised activities their support services and dependencies recovery profile?						
	2.5.3		Have the resource requirements to implement the business continuity strategies been identified and provided?						
	2.6	***BC Procedures - Incident Response Structure***							
	2.6.1		Does organization have an Emergency Management/Evacuation Plan?						
	2.6.2		Does the organization have an incident management structure, procedures and arrangements that provide overall control of the response to a disruptive incident?						

ID	Topic		Questions	ICANN Personnel	Date	Time	ICANN Personnel	Documents	Recommendations
	2.6.3		Does the organization have a documented Corporate Crisis Management Plan (CCMP)?						
	2.6.4		Does the organization have predefined Incident Management Team(s) for co-ordinating and/or managing differing types of incident e.g. business, technical service delivery, site, building, corporate?						
	2.7	***Business Continuity Plans (BCP)***							
	2.7.1		Does the organization have documented business continuity plans in respect of each of the organization's prioritised activities and their dependencies?						
	2.7.2		Does each plan identify roles and teams that have the necessary seniority, authority, capability and competence to take control and manage the incident and communicate with stakeholders?						
	2.7.3		Has each plan and its component parts been successfully tested and/or invoked at least once within the last 12 months to ensure they can achieve its aim and objectives within the required timescales?						
	2.7.4		Does each plan contain predefined task checklists that includes mandatory and discretionary tasks together with individuals/roles/teams responsible for their completion and a process for tracking there completion within an allocated timeframe ?						
	2.7.5		Is there a documented and funded maintenance cycle and programme for the plan and its component parts to ensure it remains appropriate (fit for purpose), plausible and capable of meeting its objectives and required outcomes?						
	2.8	***Evaluation of Business Continuity Procedures***							
	2.8.1		Does the organization conduct performance evaluations of its business continuity procedures, arrangements and capabilities in order to verify their continued suitability, adequacy and effectiveness?						
	2.8.2		Is a post incident review undertaken in the event of an incident that disrupts the organization's prioritised activities or requires an incident response?						
3	Perform a comprehensive assessment of ICANN's **Risk Management Methodology** and Framework.								
	3.1	***Risk Assessment Process, Risk Acceptance Criteria and Criteria for Risk Assessment***							
	3.1.1		Is there an information risk assessment process documented, including the risk acceptance criteria and criteria for risk assessment?						
	3.1.2		Are the risks identified, their owners, likelihood, consequences, and the level of risk; are these results documented?						
	3.2	***Risk Management and Risk Treatment***							
	3.2.1		Is the risk treatment process documented, including the risk treatment options?						
	3.2.2		Does Risk treatment plan define who is responsible for implementation of which control, with which resources, what are the deadlines, and what is the evaluation method?						
4	Perform an assessment how effectively ICANN has implemented its **Security Incident Management** and response processes to reduce (pro-active and reactive) the probability of DNS-related incidents.								
	4.1	***Security Incident Management Process***							
	4.1.1		Are procedures and responsibilities for managing incidents clearly defined?						
	4.1.2		Are all information security events reported in a timely manner?						

ID		Topic	Questions	ICANN Personnel	Date	Time	ICANN Personnel	Documents	Recommendations
	4.1.3		Are employees and contractors reporting on security weaknesses?						
	4.1.4		Are all security events assessed and classified?						
	4.1.5		Are procedures on how to respond to incidents documented?						
	4.1.6		Are security incidents analyzed in order to gain knowledge on how to prevent them?						
	4.1.7		Do procedures exist which define how to collect evidence that will be acceptable during the legal process?						
	4.2	***Security Incident Response Process relating to a global incident (DNS-related)***							
	4.2.1		Does ICANN have a documented incident response plan, with processes and resources identified						
	4.2.2		Does ICANN maintain contracts with third parties to potentially assist in major incident responses						
	4.2.3		Is this incident response plan tested on a periodic basis?						
	4.2.4		Does ICANN have a vulnerability management process?						
	4.2.5		Does ICANN have a vulnerability disclosure policy?						
	4.3	***ICANN operational responsibilities (L-Root)***							
	4.3.1		Are there technical and operational requirements for hosting L-Root node?						
	4.3.2								
	4.3.3		Is there a backup procedure for obtaining a zone file?						
5	Perform a comprehensive assessment of internal security, stability and resiliency of **ICANN's operation processes and services** .								
	5.1	***Global Domain Division Operations (GDD Operations)***							
	5.2	***Centralized Zone Data Service (CZDS)***							
	5.3	***SLA Monitoring System (SLAM)***							
	5.4	***Statistical Analysis of DNS Abuse in gTLDs (SADAG)***							
	5.5	***Domain Abuse Activity Reporting (DAAR)***							
6	Perform an assessment how effectively ICANN has implemented its processes around vetting registry operators and services concerning the New gTLD Delegation and Transition process.								
	6.1	***New gTLD Registry Agreement (Registry Operator)***							
	6.1.1		Is there relevant metrics for reviewing of the impact of the New gTLD Program on the security and stability of the root system						
	6.1.2		Does ICANN assess the impact of the addition of the new gTLDs in order to determine what steps, if any, should be undertaken as a prerequisite to adding more TLDs to the root system?						

ID		Topic	Questions	ICANN Personnel	Date	Time	ICANN Personnel	Documents	Recommendations
	6.1.3		How ICANN identify steps that should be undertaken by the community going forward to assess the state of the root system on an ongoing basis						
	6.2	***Back-End Registry Operator (BERO)***							
	6.2.1		Are there basic security standards and criteria that should be fulfilled by back-end registry operators in pre-delegation process?						
	6.2.2		What steps will ICANN take in the cases when BERO has serious security and stability issues?						
	6.2.3		How long it will take to determine that one of the Critical Functions is performing below a defined threshold?						
	6.2.4		Is there relevant metrics for revieving BERO performance?						
	6.3	***Emergency Back-End Registry Operator (EBERO)***							
	6.3.1		Is there a prosess for determining that one of the Critical Functions (DNS, DNSSEC, Whois, SRS/EPP, Data Escrow) is performing below a defined emergency threshold.						
	6.3.2		Is there procedure for seamless transition to EBERO? Is this procedure tested?						
	6.3.3		Is there relevant metrics for reviewing EBERO performance?						
	6.4	***Registry Data Escrow (RyDE) - Data Escrow Agent (DEA)***							
	6.4.1		Is there a prosess for determining that Data Escrow Agents fulfils operational and security requirements?						
	6.4.2		Is there procedure for verifying and testing data escrow service?						
	6.4.3		Is there procedure for Escrow Agent change?						
7	Perform an assessment how effectively ICANN has implemented its processes to ensure compliance regarding **REGISTRAR agreement** and the consensus policies.								
	7.1	***WHOIS Accuracy Reporting System (ARS)***							
	7.2	***WHOIS Accuracy Program Specification (WAPS)***							
	7.3	***Expired Domain Deletion Policy (EDDP), Expired Registration Recovery Policy (ERRP):***							
	7.4	***Uniform Domain Name Dispute Resolution Policy (UDRP):***							
	7.5	***Registrar Data Escrow (RDE)***							
	7.6	***Abuse Reports***							
	7.7	***Transfer Policy***							