Preliminary Recommendation #15 - Audits

The EPDP Team expects that the appropriate auditing processes and procedures are put in place to ensure appropriate monitoring and compliance with the requirements outlined in these recommendations.

As part of any audit, the auditor MUST be subject to reasonable confidentiality obligations with respect to proprietary processes and personal information disclosed during the audit.

More specifically:

Audits of the Accrediting Authority

If ICANN outsources the accreditation authority function to a qualified third party, the accrediting authority MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the accreditation authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new accreditation authority must be identified or created.

Any audit of the accreditation authority shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data, and other information requested.

As part of such audits, the accreditation authority shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches, noting that in such an extreme case, requirements for other entities involved in SSAD may be temporarily lifted until a confirmed breach has been addressed.

Audits of Identity Provider(s)

Identity Providers MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the Identity Provider be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new Identity Provider must be identified.

Any audit of an Identity Provider shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the Identity Provider shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

Audits of Accredited Entities/Individuals

Appropriate mechanisms must be developed in the implementation phase to ensure accredited entities' and individuals' compliance with the policy requirements as defined in the accreditation preliminary recommendation. These could include, for example, audits triggered by complaints, random audits, or audits in response to a self-certification or self-assessment. Should the accredited entity or individual be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure the matter should be referred back to the Accreditation Authority for action.

Any audit of accredited entities/individuals shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the accredited entity/individual shall, in a timely manner, provide to the auditor all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

Audits of Entity disclosing the data / Contracted Parties

The EPDP Team will further consider these requirements once the EPDP Team has decided on the roles and responsibilities of the different parties in the SSAD.

NOTE: Depending on the ultimate SSAD model the EPDP Team recommends, there may be other relevant parties that would be subject to auditing. This will be revisited when the ultimate SSAD model is recommended.