OWNERS: **Calvin (lead), Carlos, Laureen**

Refer to Laureen's Model Issue Paper -
https://docs.google.com/document/d/1rswTUNmvB_Lkt2RDwU2OuNx13pptdP_TpgCZ3V77UBk/edit?usp=sharing

CCT-RT DISCUSSION PAPER WORKSHEET

HIGH LEVEL QUESTION: Have the safeguards been fully implemented? *[Calvin/Carlos to focus on technical safeguards].*

OWNER: Calvin Browne

SUB-QUESTIONS:

1. Have the Technical safeguards applicable to all new gTLDs been fully implemented?
    a. Have registry operators been technically vetted.
    b. Has DNSSEC been deployed (and monitored).
    c. Has Wild-carding been prevented.
    d. Has orphan glue been appropriately managed.
    e. Has Thick WHOIS been implemented.
    f. Has centralised access to zone file data been implemented.
    g. Expedited Registry Security Request (ERSR) Process.
    h. Voluntary framework for high-security zones/High security top level domain-draft program development.

FINDINGS: Most Technical safeguards applicable to new gTLDs have been implemented via contract provisions in the standard Registry and Registrar Agreements required for all new gTLDs. Additionally, before delegation can take place, passing of Pre-Delegation Testing (PDT) is mandatory for all nGTLDs. Whether the safeguards as implemented have been effective, or have been effectively enforced are separate questions.

1.
    a. As a requirement in the application process, all nGTLD applicants had to provide a full description of technical back end services, even where subcontracted. This was a first cut at ensuring technical competence. These provided technical descriptions were evaluated at application time. It would make little sense to audit registry operators against these initial applications on an on-going basis as technical requirements change. Additionally, all applicants were required to pass Pre-Delegation Testing (PDT). PDT included comprehensive technical checks of EPP, Name Server setup, DNSSEC etc. Passing of these tests was an absolute requirement in order to get Delegation of a domain.

    b. DNSSEC is an absolute contractual requirement. Additionally, DNSSEC is actively monitored and compliance notices raised if and when checks fail. See ICANN Registry

agreement (https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm) specification 6, clause 1.3.

c. Wild-carding is absolutely prevented by contract. Given the nature of wild-carding, it is not possible to monitor this on an ongoing basis, but given the nature of wild-carding, it stands to reason that a registry deploying wild-carding would quickly be found out. See ICANN Registry agreement specification 6, clause 2.2.

d. It is a Contractual requirement for the registry to remove orphan glue, when presented of evidence of such glue used in malicious conduct. See ICANN Registry agreement specification 6, clause 4.1. Anecdotally, some registries have implemented registration policies that make this a non-issue with orphan glue records being technically prevented by registration policies.

e. Thick WHOIS is an absolute contractual requirement. Additionally, ICANN compliance monitor this on an active basis, for both reachability and format. See ICANN Registry agreement specification 10, Section 4. Accuracy of WHOIS is a different matter and a different process applies to this. See http://whois.icann.org/en/whoisars. ~~See ICANN Registry agreement specification 10, Section 4.~~

f. Again, it is a contractual requirement that a registry makes their zone files available. ICANN has implemented Centralized Zone Data Service (https://czds.icann.org/en) in order for registries to comply with this. See ICANN Registry agreement specification 4, section 2.1.

g. The ERSR process https://www.icann.org/resources/pages/ersr-2012-02-25-en "has been developed to provide a process for gTLD registries who inform ICANN of a present or imminent security incident (hereinafter referred to as "Incident") to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident". ~~[need to see if and if so, how many times this has been activated]~~As of 5th October 2016 it had never been invoked for a nGTLD (source email Brian Aitchison)

h. These two concepts appear to be two ideas raised in the formation of the nGLTD program that appear not to have progressed to implementation. They appear to be a voluntary idea for a type of nGTLD that would require extra security/authentication for registration purposes. Neither concept appears to have moved from a draft idea. [do we want to explore this further – idea appears stillborn due to lack of consensus/difficulty to agree on implementation]

CAUSES:

Don't quite understand this – but let me take a stab:

Technical safeguards have been reduced to contractual compliance issues by being incorporated into the Registry agreement. They are actively monitored and reported on.

PRIORITY TO ADDRESS: Low priority – The technical requirements are documented in the Registry agreement.

RECOMMENDATIONS:

1. Consider the effectiveness of the monitoring of the safeguards.

2. Consider cost benefit relationship of the safeguards.
3. Consider if the WHOIS Accuracy Reporting System might point to effectiveness of the thick WHOIS requirement.

REVIEW:

Aside from the reviews recommended by the non-technical safeguards document;

1. Contractual compliance metrics (https://features.icann.org/compliance) could be reviewed for relevancy.