Charter

Better understand the security and stability of the global domain name system (DNS).

- The actual level, frequency and severity of threats to the DNS;
- The current efforts and activities to mitigate these threats to the DNS; and
- The gaps (if any) in the current security response to DNS issues.

Events

- DSSA Phase I “Go Fast”
- DSSA Phase II “Go Deep”
- Board DNS Risk Management Framework

Options

1. Consider the Final Report Phase 1 as the Final Report as envisioned in the charter of the DSSA WG, section 2.4. This will result in closure of the WG.
2. The ALAC, ccNSO, GNSO and NRO all decide that DSSA WG should continue its work.
   - In that case, the DSSA believes that the current charter needs to be updated, as it does not reflect either (a) the current environment, nor (b) the working method and scope of activities of the DSSA as agreed with the SO's and AC's.

Recommendation and Rationale

Recommendations:

- Accept the final report
- Disseminate to the membership of each of the participating SO's and AC's for their consideration and implementation.
  - The DSSA believes that there is substantial value in the Phase 1 Report as it outlines a shared mechanism to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested stakeholders.

Considerations for Option 2

- Refresh the volunteer pool
- Manage divergence with DNS Risk Management Framework
- Monitor and coordinate parallel efforts

DSSA

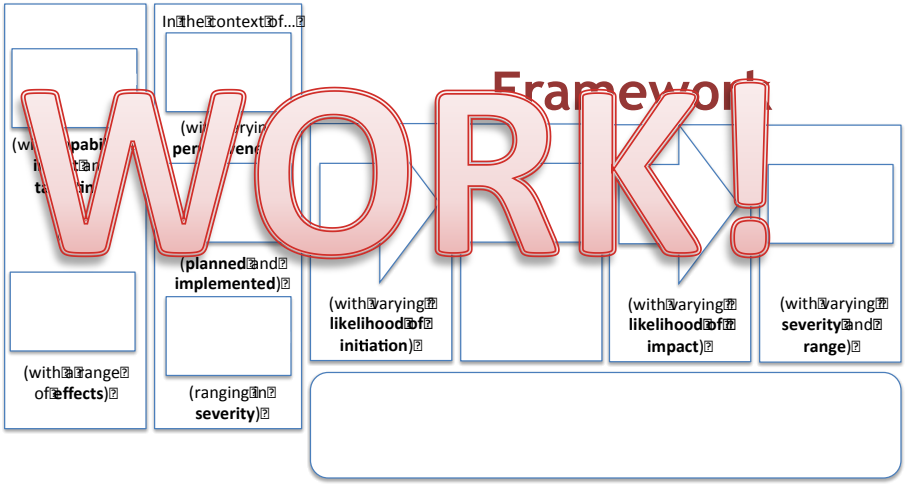
DNS Securit[illegible]nd Stabili[illegible] An[illegible]sis [illegible]orking gr[illegible]

Thursday, 1[illegible]ctob[illegible]11:1[illegible]arb[illegible]

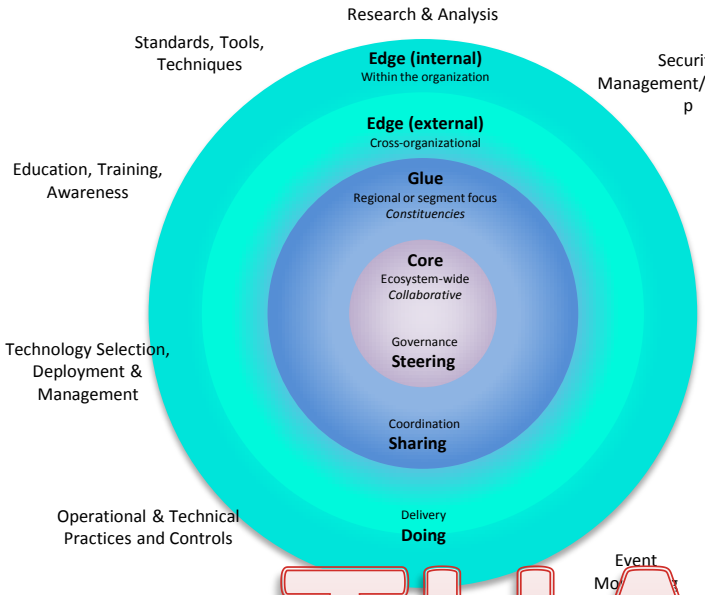
Details: htt[illegible]toron[illegible]5.i[illegible]n.[illegible]noa[illegible]4225

GREAT WORK!

Framework



Context



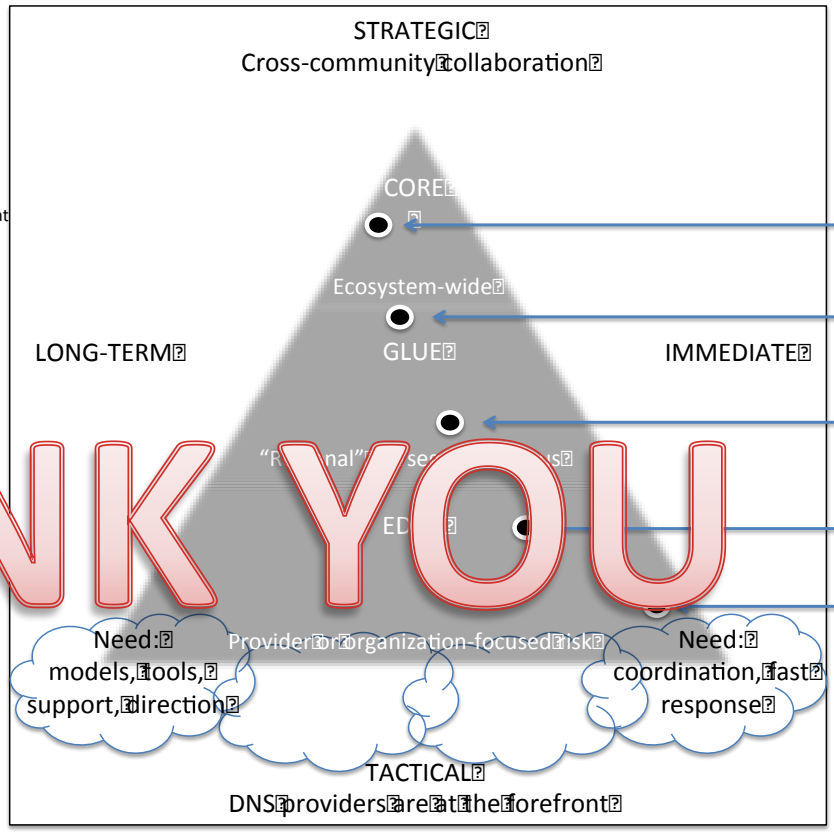
Risk Planning

Risk Assessment

Compliance Monitoring

Event

Scenarios



Risk Scenario Topic List

- Gaps in policy, management, or leadership splits the root
- "Reductive" forces (security, risk-mitigation, control through rules, etc.) splits the root
- Widespread natural disaster brings down the root or a major TLD
- Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD
- Inadvertent technical mishap brings down the root or a major TLD

THANK YOU