

DNS Security and Stability Analysis Working Group (DSSA)

DSSA Update

Toronto – October, 2012



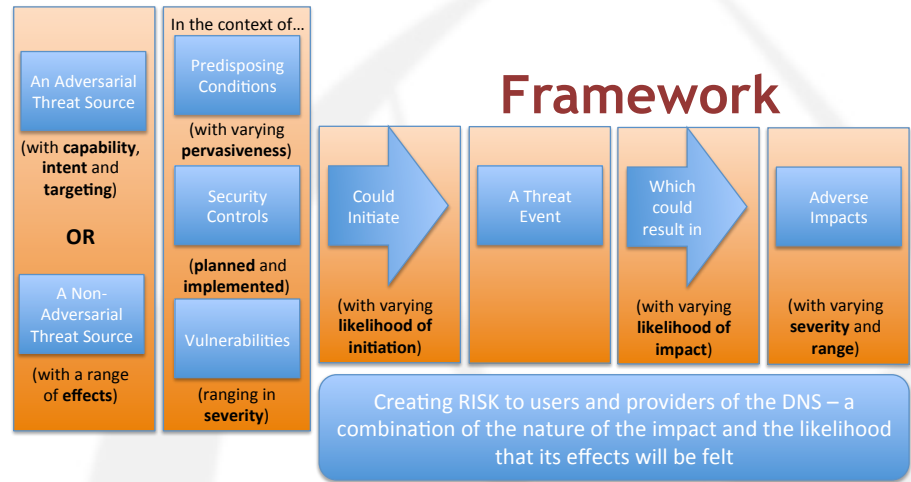
DSSA

DNS Security and Stability Analysis working group

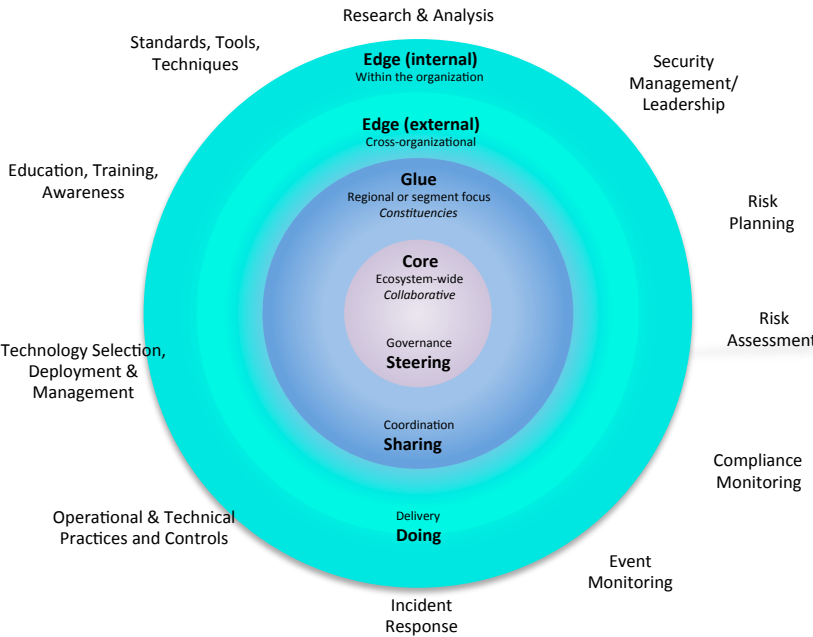
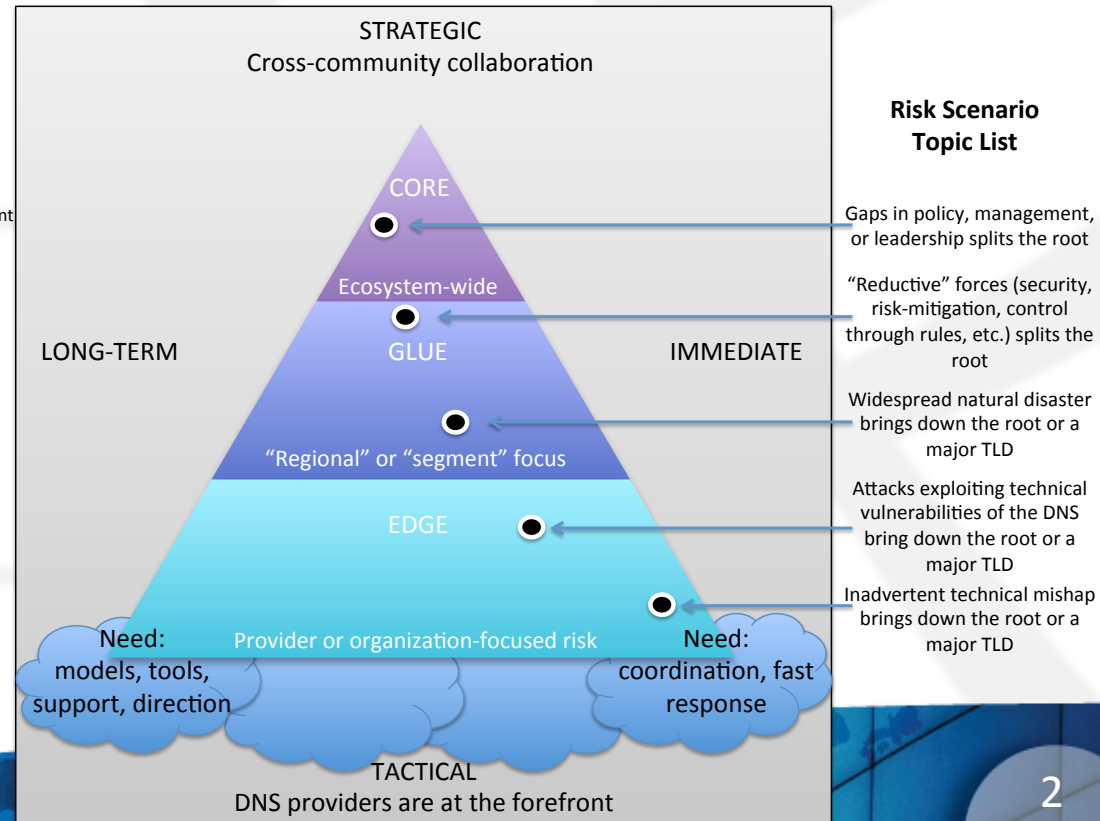
Thursday, 18-October: 11:15-12:45 Harbour C

Details: <http://toronto45.icann.org/node/34225>

Context



Scenarios



Background

At their meetings during the ICANN Brussels meeting the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs)...

acknowledged the need for a better understanding of the security and stability of the global domain name system (DNS).

This is considered to be of **common interest** to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably **undertaken in a collaborative effort**.



The DSSA has:

- Established a cross-constituency working group
- Clarified the scope of the effort
- Developed a protocol to handle confidential information
- Built a risk-assessment framework
- Developed risk scenarios
- Documented this work in a report



Since Prague:

- Refined and consolidated
- Launched public-comment cycle

Still to come (if needed)

- Refine the methodology
- Introduce the framework to a broader audience
- Complete the risk assessment



Methodology

An Adversarial Threat Source

(with **capability, intent** and **targeting**)

OR

A Non-Adversarial Threat Source

(with a range of **effects**)

In the context of...

Predisposing Conditions

(with varying **pervasiveness**)

Security Controls

(**planned** and **implemented**)

Vulnerabilities

(ranging in **severity**)

Could Initiate

(with varying **likelihood of initiation**)

A Threat Event

Which could result in

(with varying **likelihood of impact**)

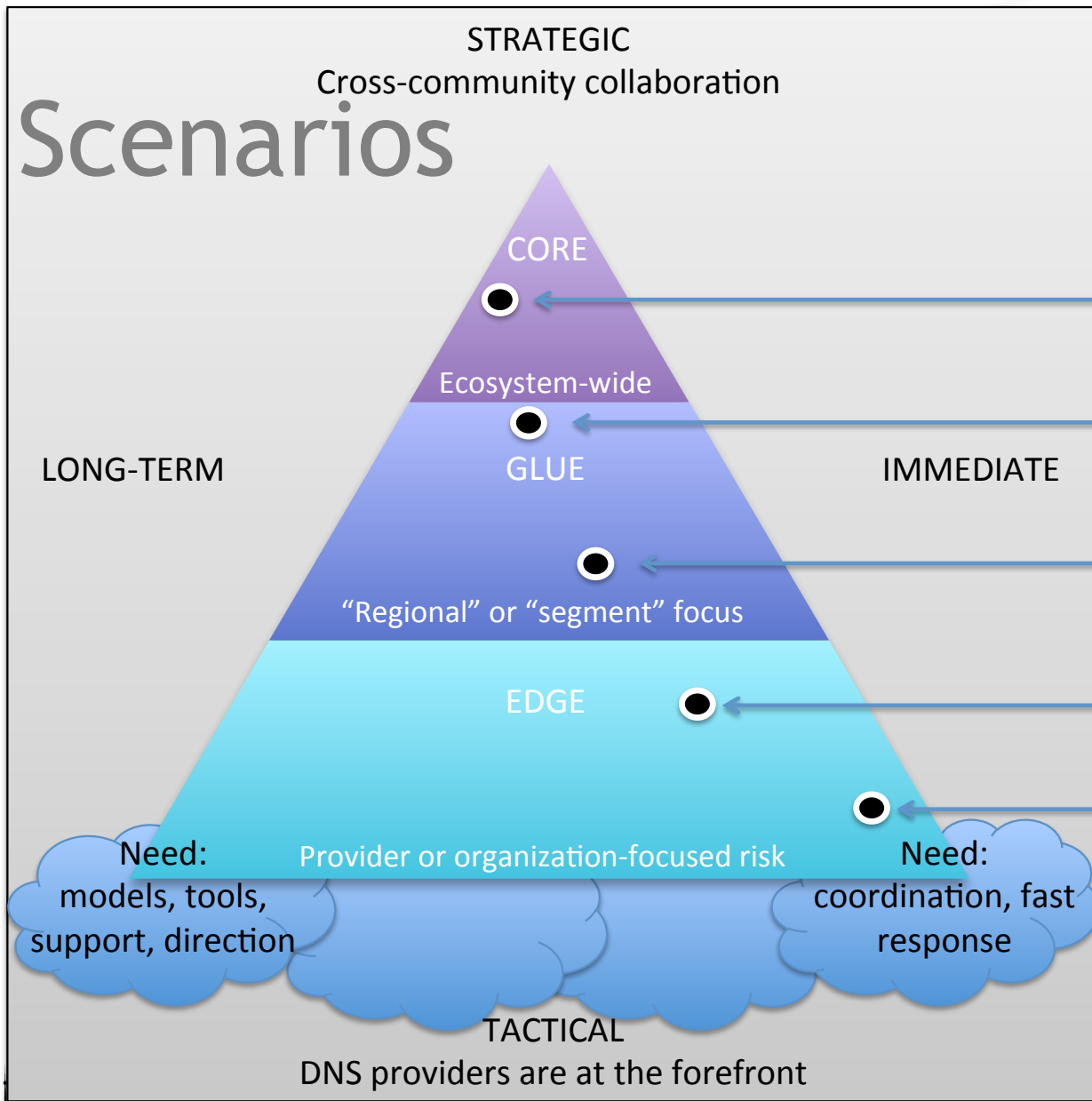
Adverse Impacts

(with varying **severity and range**)

Creating RISK to users and providers of the DNS – a combination of the nature of the impact and the likelihood that its effects will be felt



Risk Scenarios

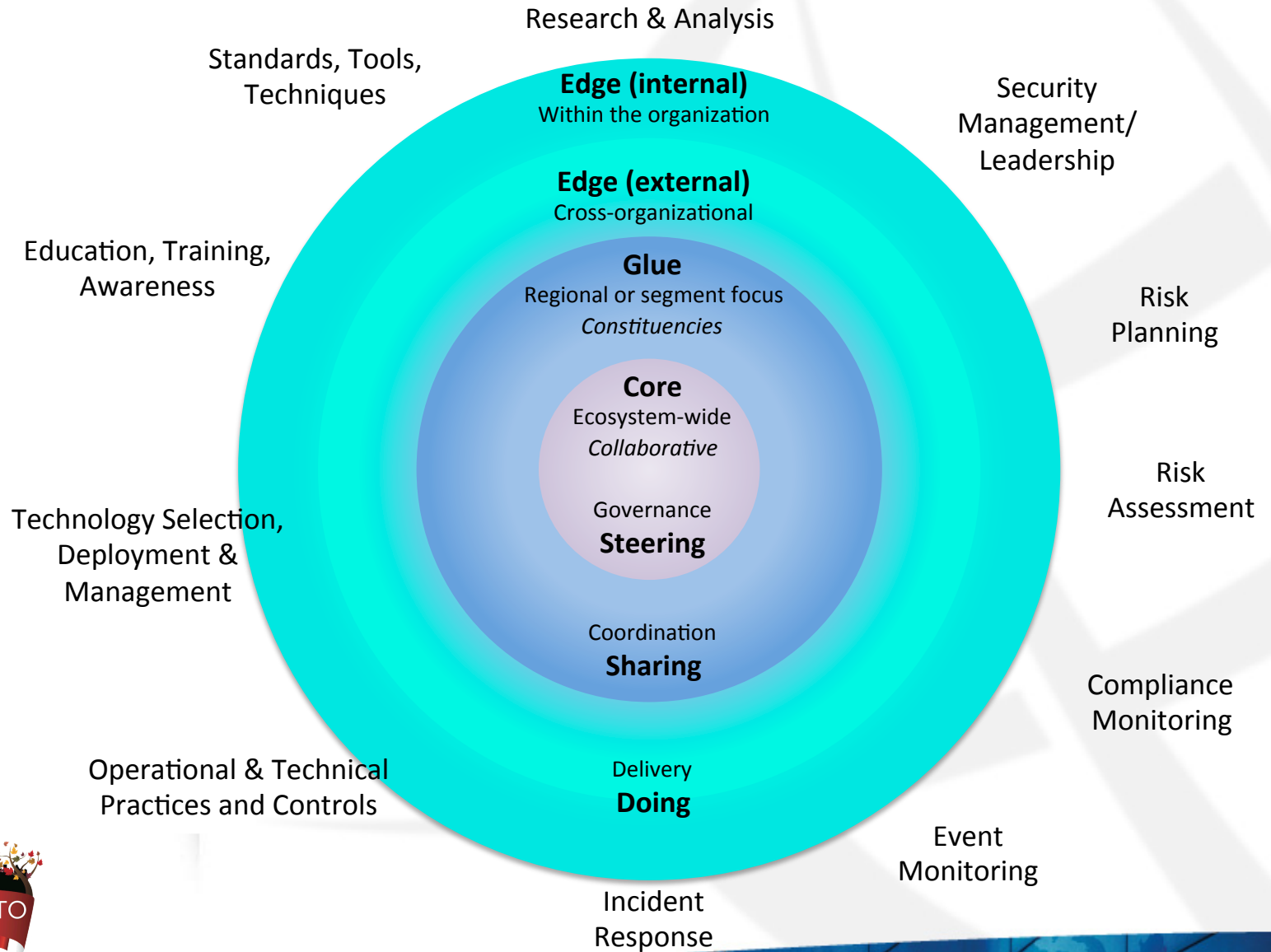


Risk Scenario Topic List

- 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

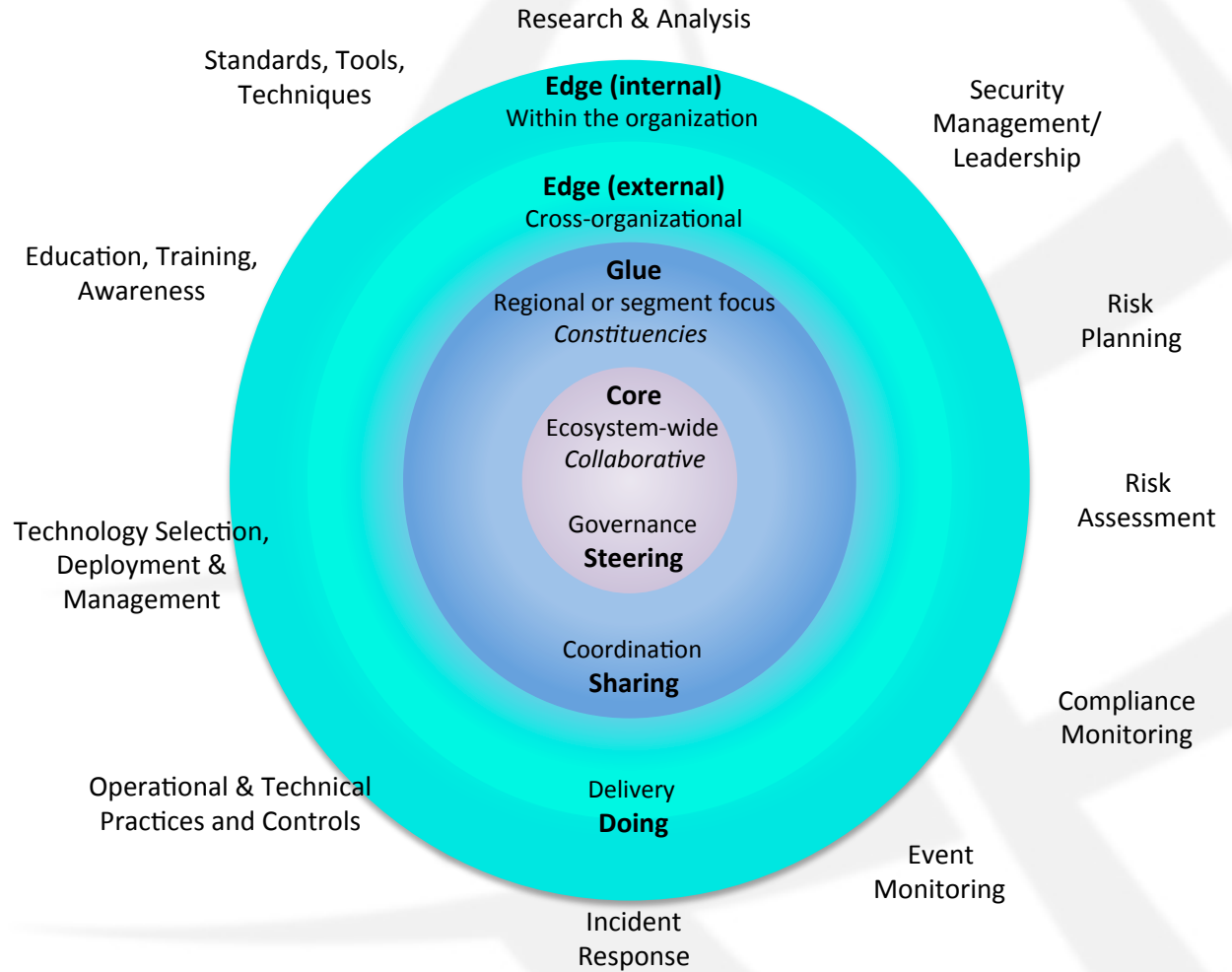


Roles and context



Question: Who is doing what?

- Backend registry providers
- ccTLD registries
- CERTs
- DNRMF
- DNS-OARC
- ENISA
- FIRST
- gTLD registries
- IANA
- ICANN
- Security Team
- ICANN SOs and ACs
- IETF
- ISOC
- ISPs
- Network Operator Groups
- NRO
- RSAC
- SSAC
- And ????



Approach: a data-gathering worksheet

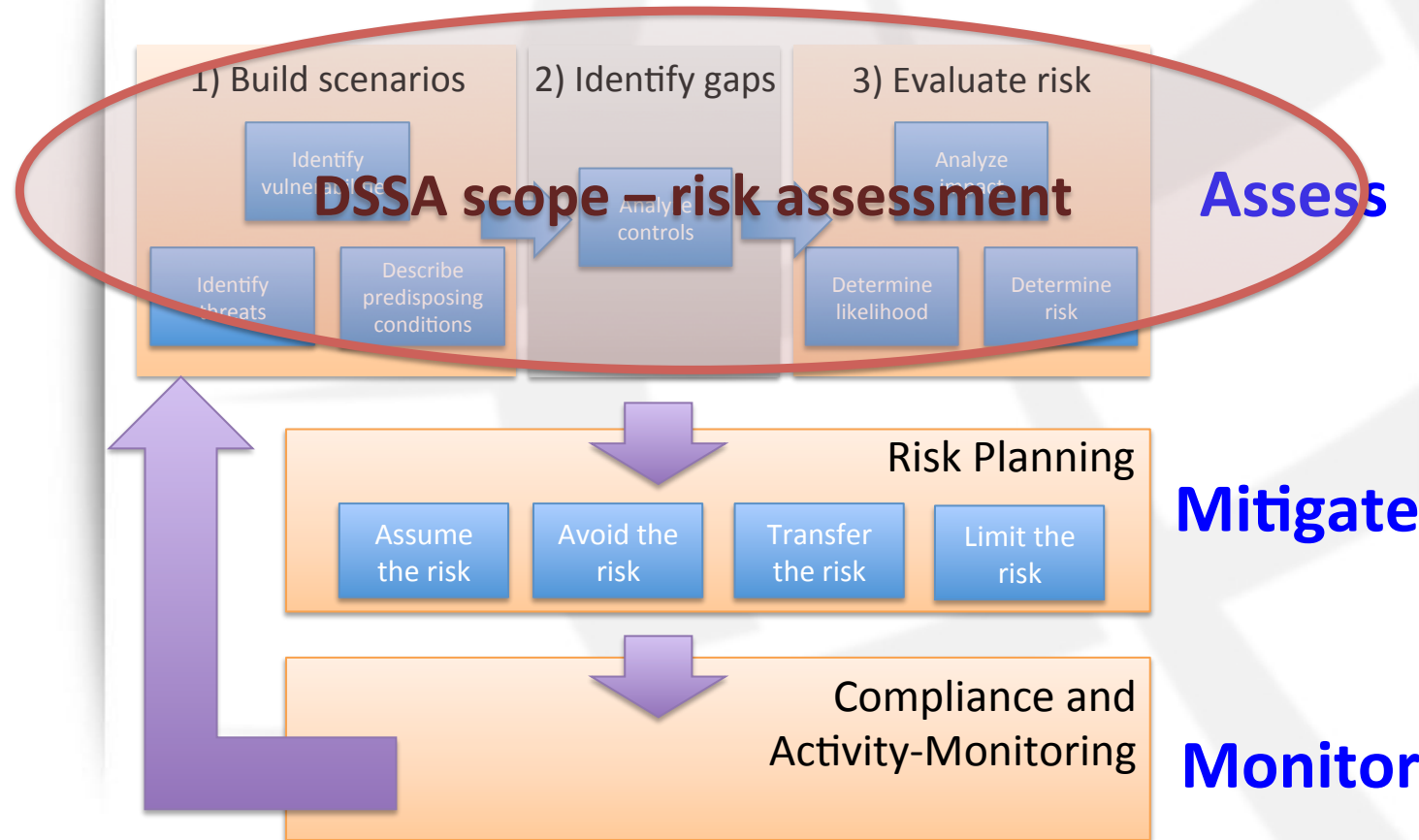
Goal: complete the map of DNS SSR functions and participants for our report - and provide a foundation for a “gaps and overlaps” analysis

Activity	Relationships	Engagement	Notes
12 Research and Analysis regarding "The DNS"			
	Edge (internal)	Participate	1 - ISPs are especially active and interested in sharing their DNS expertise with research efforts that focus on SSR issues with regard to "the DNS" that impact customers and internal DNS operations
	Edge (external)	Participate	2 - ISPs are especially active and interested in sharing their DNS expertise with research efforts that focus on SSR issues with regard to "the DNS" that impact their relationships other partners (ISPs, Ry's, R's, root, etc.)
	Glue (sharing)	Participate	3 - ISPs participate in "glue" activities aimed at research focused on "the DNS" especially with regard to topics such as emerging threats/responses, proactive mitigation strategies, collaboration, etc. 4 - ISPs may be satisfied to leave the "steering" of shared SSR research with regard to "the DNS" in the hands of others if they can be confident of access, quality and timeliness. Topics relating to Local Internet Registry and telephone number mapping would be an exception -- here ISPs need to take a more active role.
	Core (steering)	Consume	<<- Describe the role of the entity when it comes to "steering" the direction of shared SSR research
17 Develop Standards, Tools and Techniques regarding "The DNS"			
	Edge (internal)	Participate	5 - ISPs provide DNS (and DNS SSR) for a large proportion of their customers in addition to the "internal" DNS SSR capability to support reliable routing of customer traffic, delivery of their Local Internet Registry functions (reverse delegation under .arpa) and telephone number mapping (ENUM) functions 6 - ISPs are also highly dependent on widespread deployment of effective/shared DNS SSR std's, tools and techniques across their other partners when it comes to support reliable routing of customer traffic, delivery of their Local Internet Registry functions (reverse delegation
			<<- Describe the role of the entity in developing and delivering standards, tools and techniques relating to "the DNS." Focus on SSR topics that impact the entity's customers and internal DNS operations in this box. [note: this is about what the organization does, not what it shares with others] <<- Describe the role of the entity in developing and delivering standards, tools and techniques relating to "the DNS." Focus on SSR topics that impact the organizations' peers and partners . [note: this is about what the organization does, not what it shares



Approach: Coordinate DSSA and DNSRMF

DNRMF scope – Risk Management Framework



Refine and consolidate

Toronto

Gather comments and feedback

Beijing

Launch the Risk Mgmt. function

ID roles – gaps & overlaps

Public comment

Revise report and obtain AC/
SO endorsement

Determine whether
separate DSSA
risk-assessment
effort is needed

DSSA
(focus/scope:
ICANN the community)

Align/Integrate
DNSRMF and DSSA
findings/methods/
leadership

Obtain community
feedback and
incorporate those
suggestions into the RM
framework

Establish
community-
based portion of
RM launch
project

Joint
effort

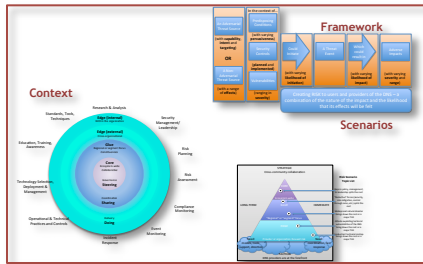
Select DNS risk-
management framework
consultant and launch
DNSRMF project

Complete DNS risk-
management framework

Launch the project to
establish the RM
function and complete
one “cycle”

DNSRMF
(focus/scope:
ICANN the org)

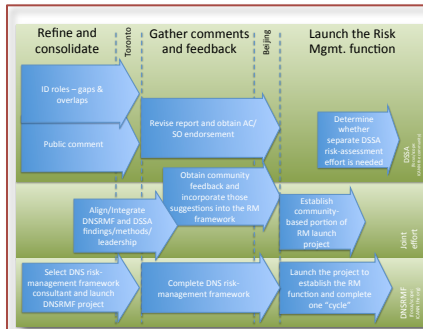
How you can help



- Comment on our Phase I report

The screenshot shows a spreadsheet with columns for 'ID Role', 'Activity', 'Relationship', 'Engagement', and 'Notes'. The rows contain detailed information about various ID roles and their associated activities and relationships. The 'Notes' column contains specific observations and recommendations for each role.

- Fill out one of our “Gaps & Overlaps” worksheets



- Comment on our plans going forward

<https://community.icann.org/x/4AB5>