DNS Security and Stability Analysis Working Group (DSSA)

DSSA Update

Toronto – October, 2012

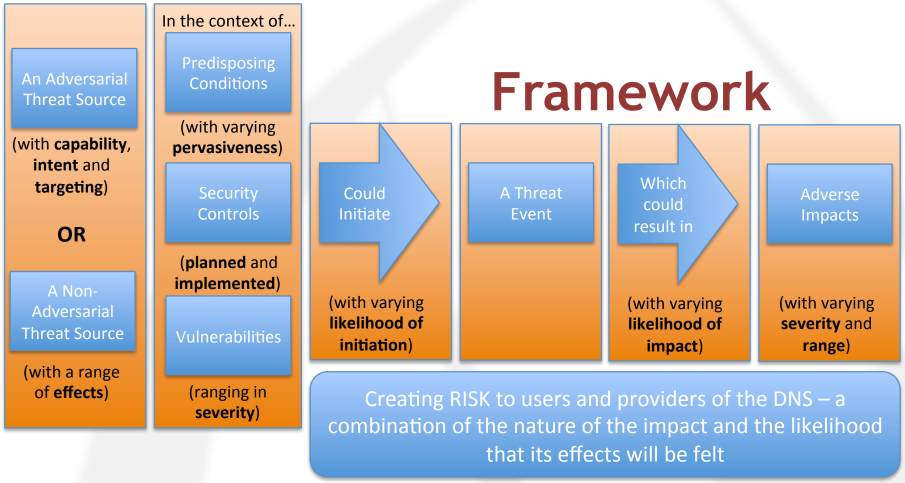
DSSA

DNS Security and Stability Analysis working group

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

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

Framework



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

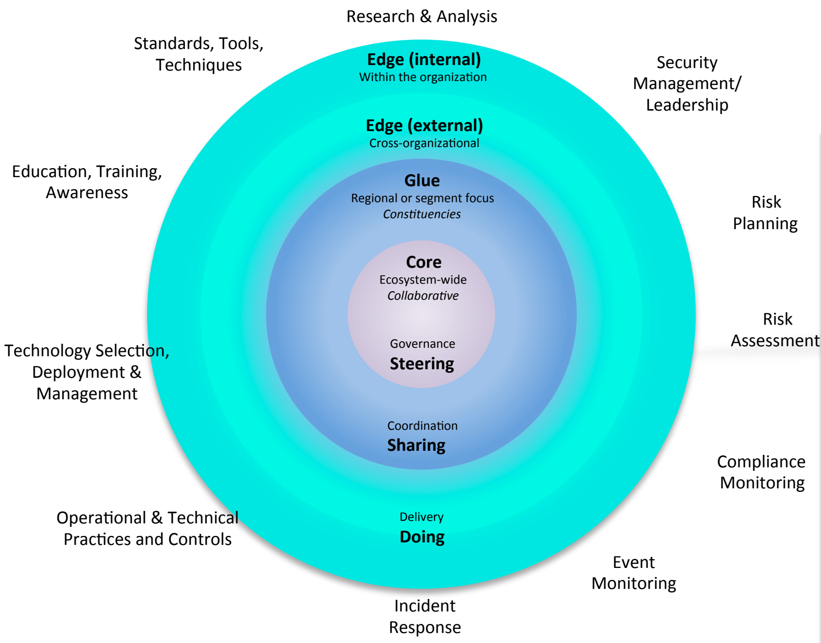
(with varying **likelihood of impact**)

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

Context



Research & Analysis

Standards, Tools, Techniques

Security Management/ Leadership

Education, Training, Awareness

Risk Planning

Risk Assessment

Technology Selection, Deployment & Management

Compliance Monitoring

Operational & Technical Practices and Controls

Event Monitoring

Incident Response

Edge (internal)
Within the organization

Edge (external)
Cross-organizational

Glue
Regional or segment focus
Constituencies

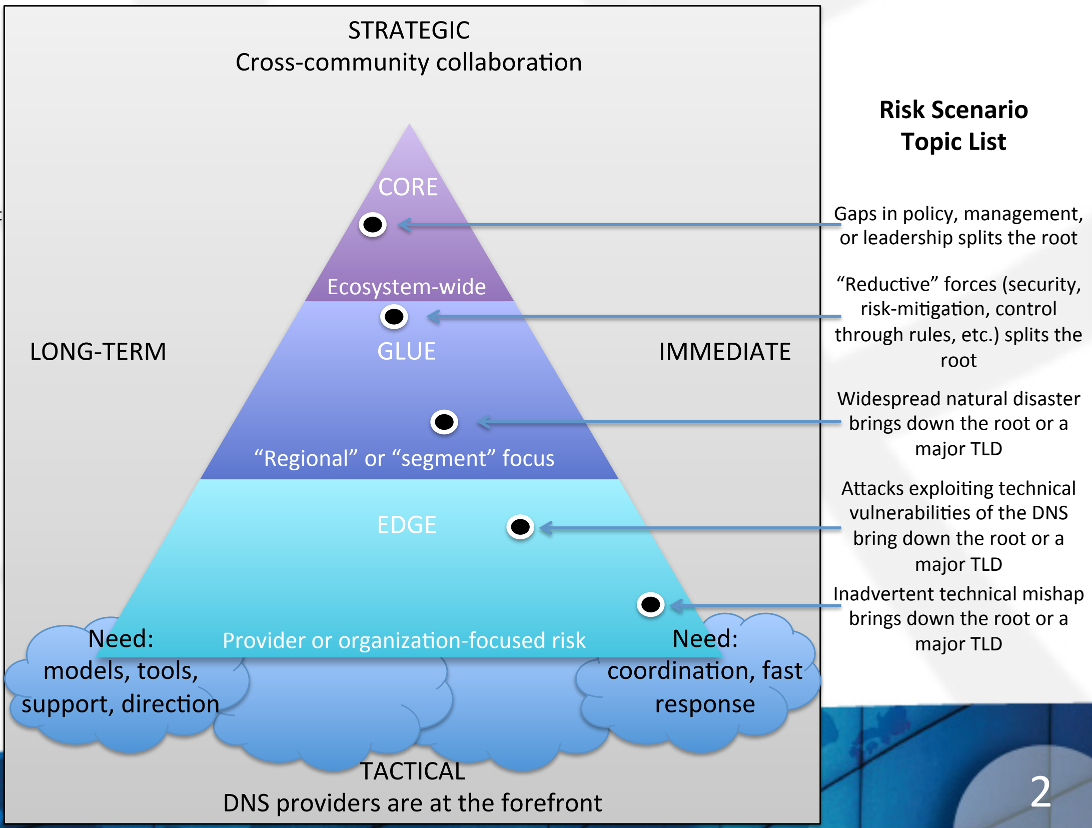
Core
Ecosystem-wide
Collaborative

Governance
Steering

Coordination
Sharing

Delivery
Doing

Scenarios



STRATEGIC
Cross-community collaboration

LONG-TERM

IMMEDIATE

CORE

Ecosystem-wide

GLUE

"Regional" or "segment" focus

EDGE

Provider or organization-focused risk

Need: models, tools, support, direction

Need: coordination, fast response

TACTICAL
DNS providers are at the forefront

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

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

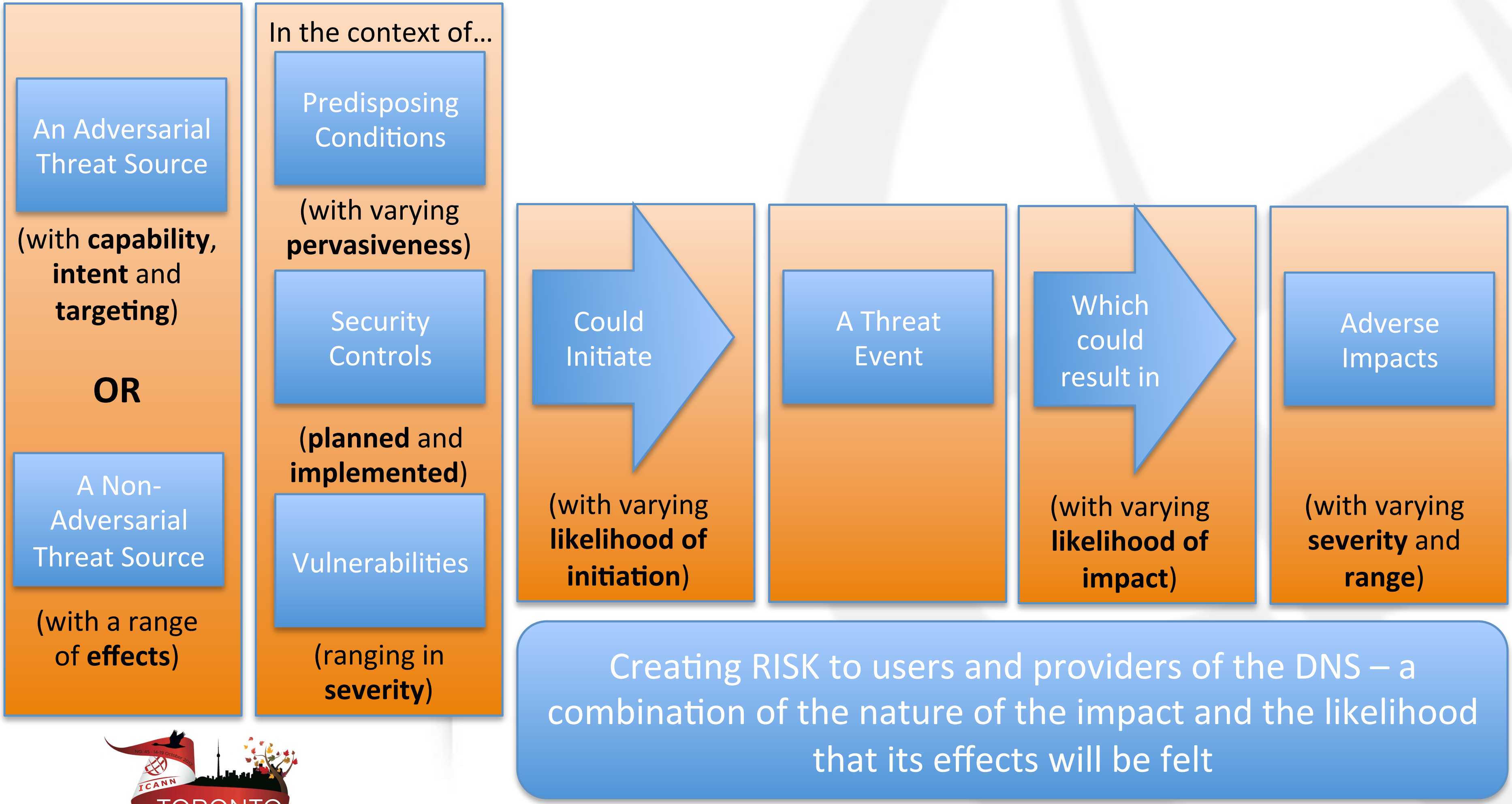
Since Prague:

- 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

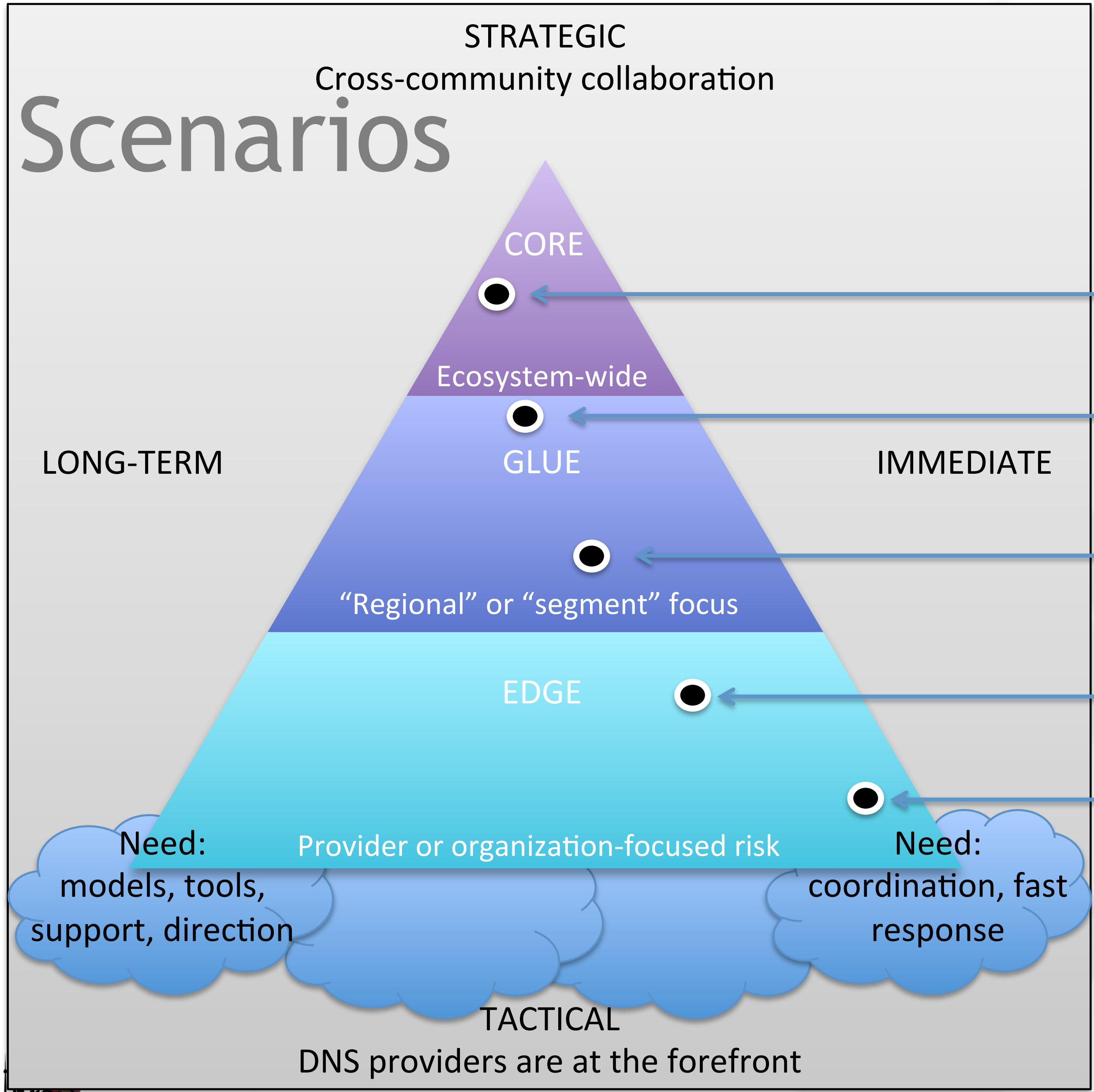
(with varying **likelihood of impact**)

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


STRATEGIC
Cross-community collaboration
CORE
Ecosystem-wide
GLUE
"Regional" or "segment" focus
EDGE
Provider or organization-focused risk
LONG-TERM
IMMEDIATE
Need:
models, tools,
support, direction
Need:
coordination, fast
response
TACTICAL
DNS providers are at the forefront

Risk Scenario Topic List

Gaps in policy, management, or leadership splits the root

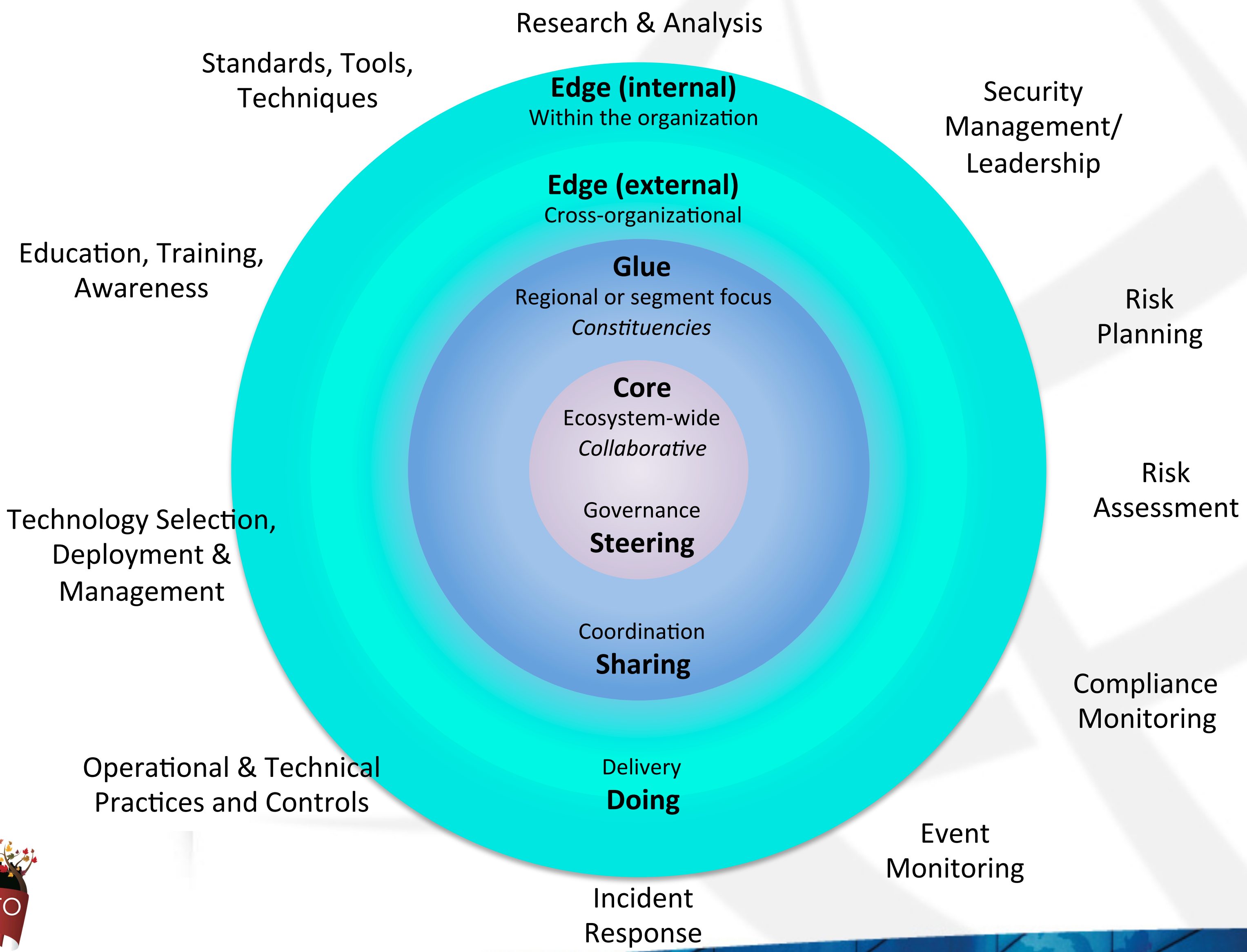
"Reductive" forces (security, risk-mitigation, control through rules, etc.) splits the root

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

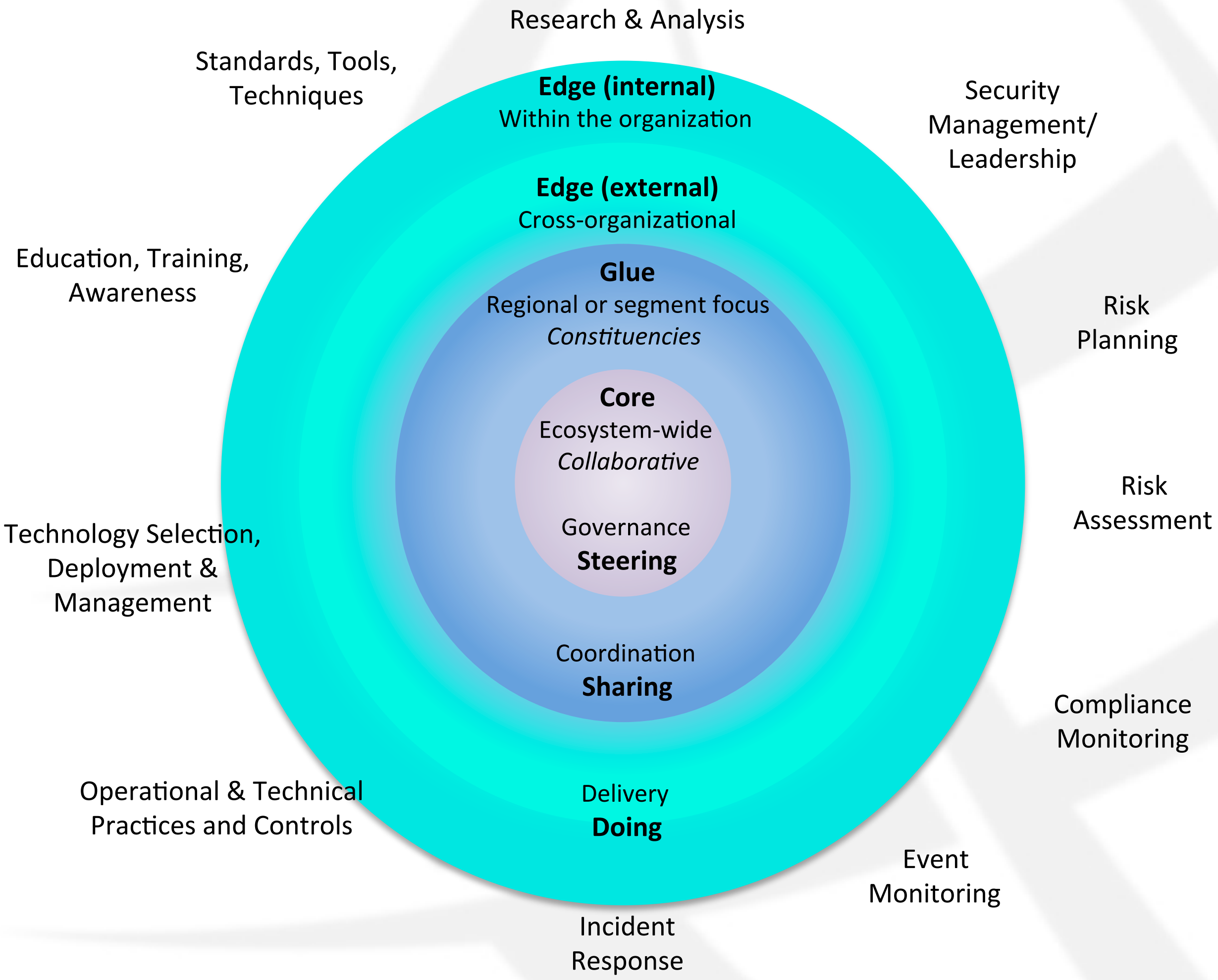
Roles and context



TORONTO

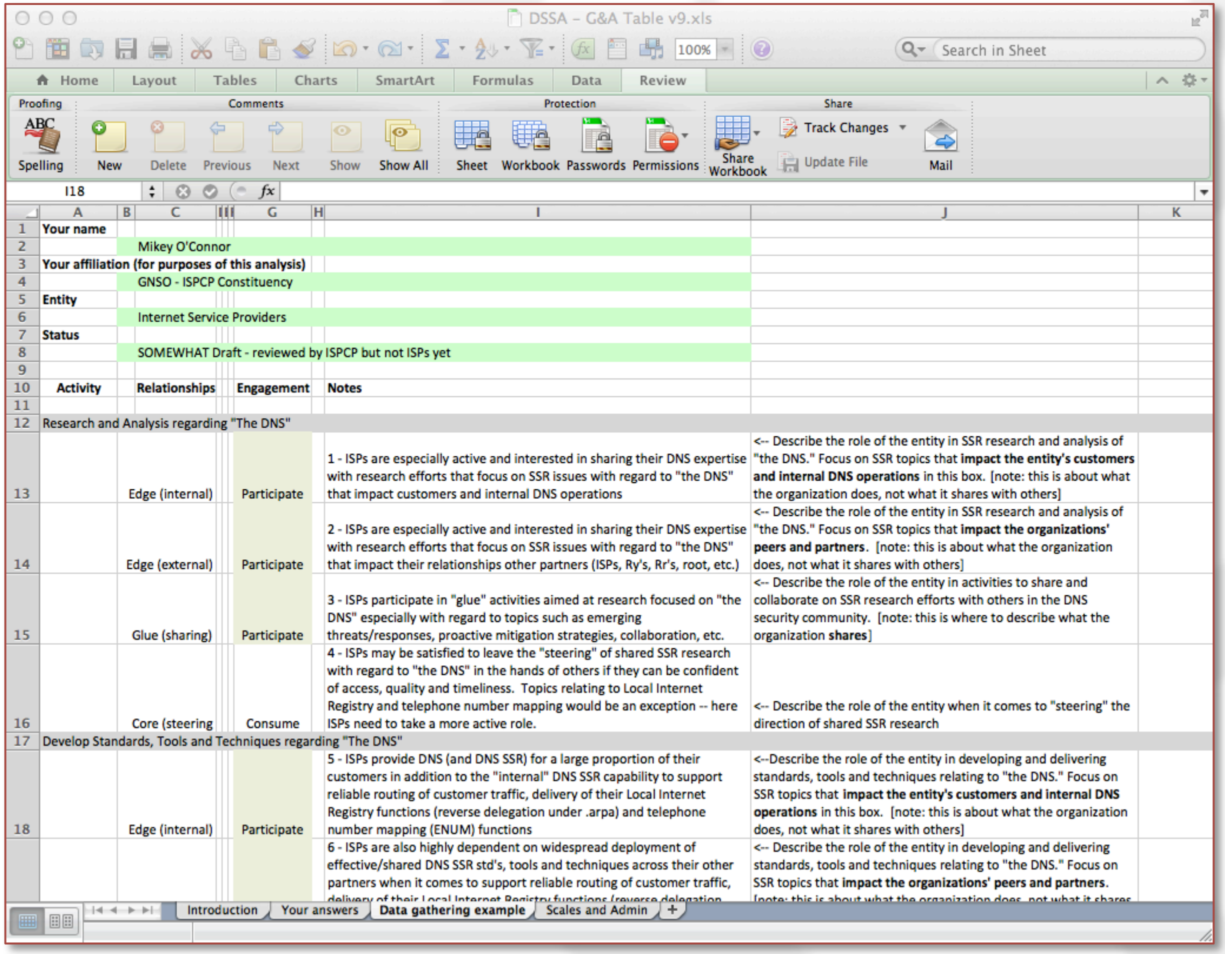
Question: Who is doing what?

- 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

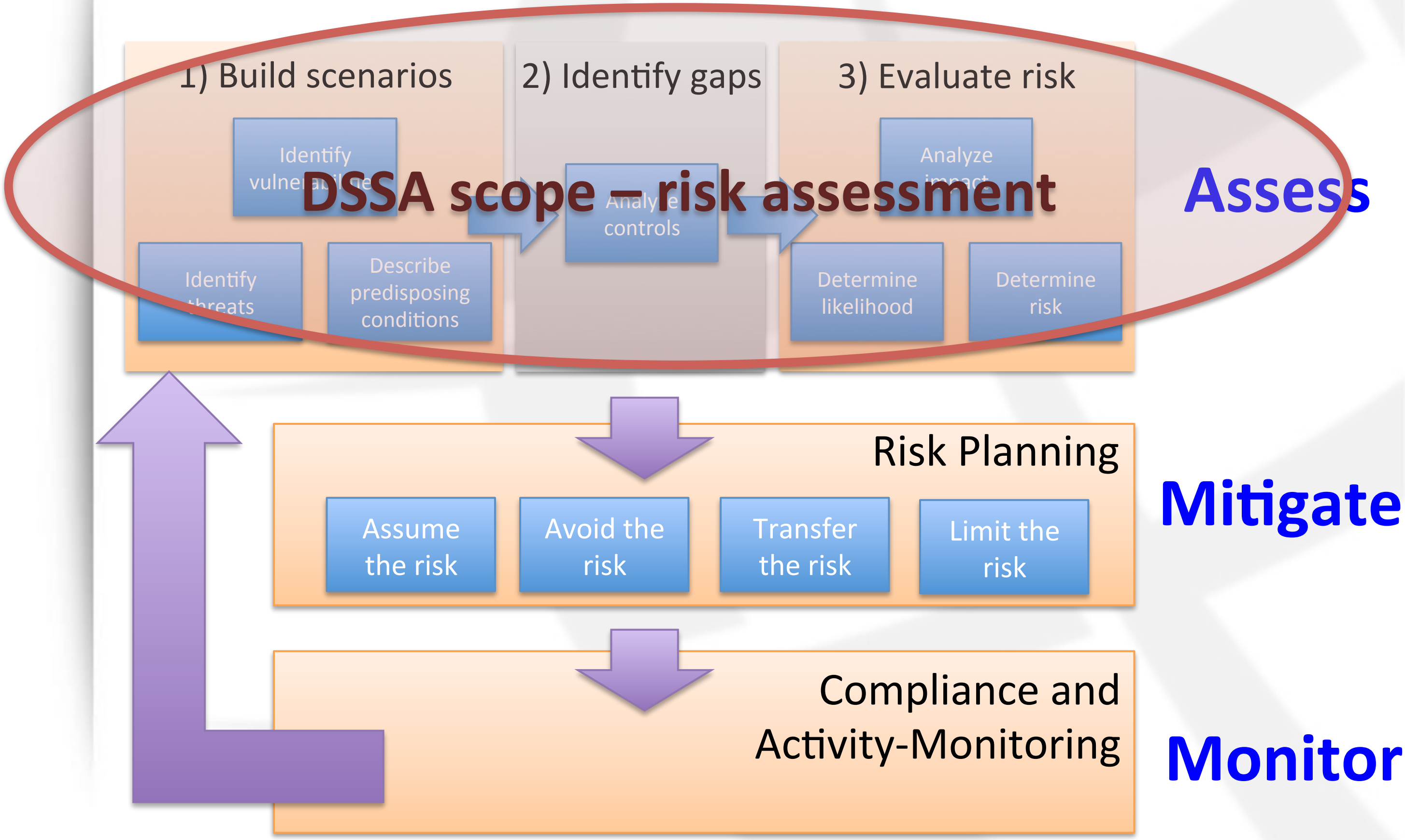
Goal: complete the map of DNS SSR functions and participants for our report – and provide a foundation for a "gaps and overlaps" analysis



	A	B	C	G	I	J
1	**Your name**					
2			Mikey O'Connor			
3	**Your affiliation (for purposes of this analysis)**					
4			GNSO - ISPCP Constituency			
5	**Entity**					
6			Internet Service Providers			
7	**Status**					
8			SOMEWHAT Draft - reviewed by ISPCP but not ISPs yet			
9						
10	**Activity**		**Relationships**	**Engagement**	**Notes**	
11						
12	Research and Analysis regarding "The DNS"					
13			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	<-- Describe the role of the entity in SSR research and analysis of "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]
14			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, Rr's, root, etc.)	<-- Describe the role of the entity in SSR research and analysis of "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 with others]
15			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.	<-- Describe the role of the entity in activities to share and collaborate on SSR research efforts with others in the DNS security community. [note: this is where to describe what the organization **shares**]
16			Core (steering	Consume	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.	<-- 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"					
18			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	<--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]
					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 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



1) Build scenarios

2) Identify gaps

3) Evaluate risk

Identify vulnerabilities

Analyze controls

Analyze impact

Identify threats

Describe predisposing conditions

Determine likelihood

Determine risk

DSSA scope – risk assessment

Assess

Risk Planning

Assume the risk

Avoid the risk

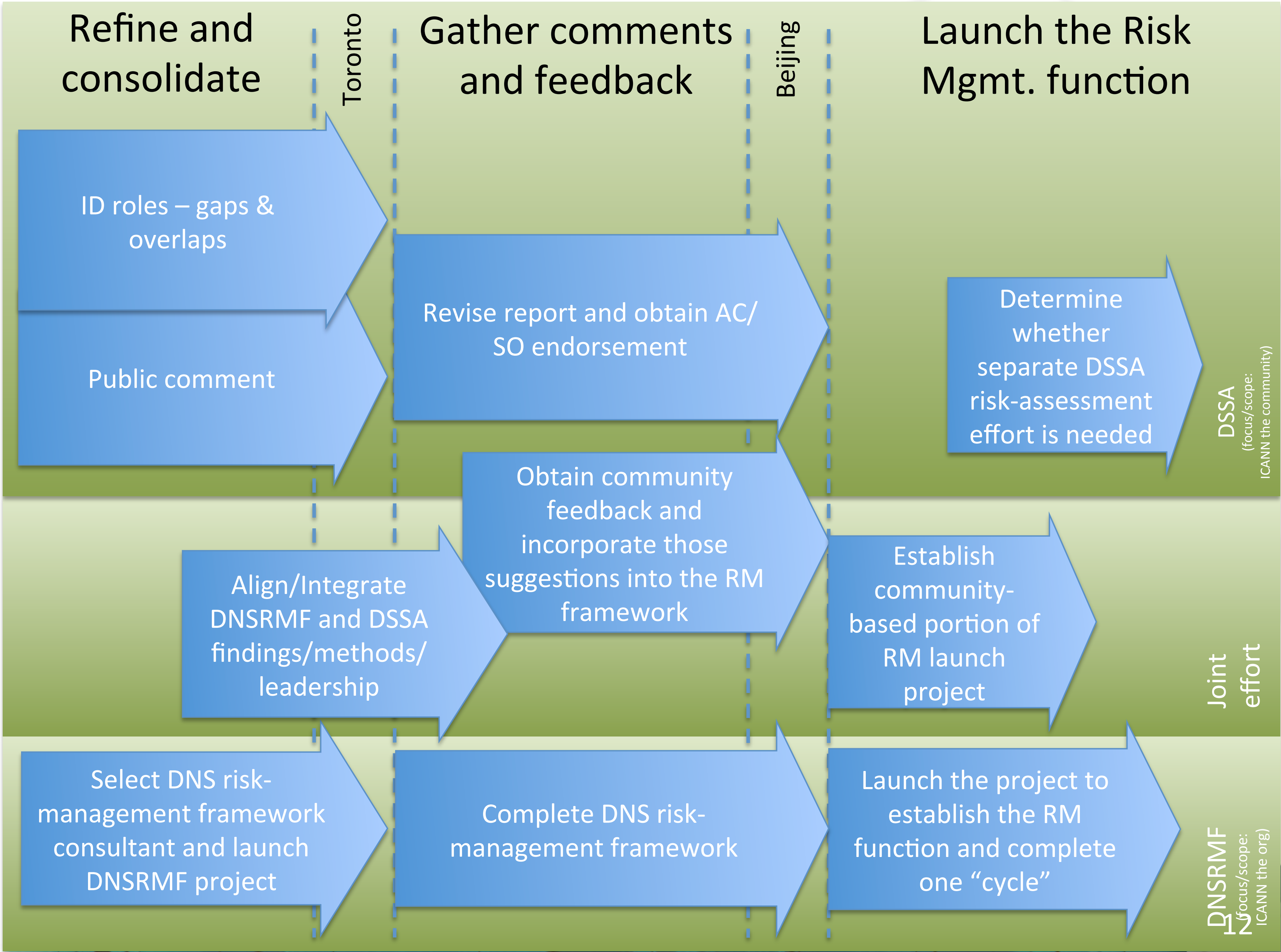
Transfer the risk

Limit the risk

Mitigate

Compliance and Activity-Monitoring

Monitor



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

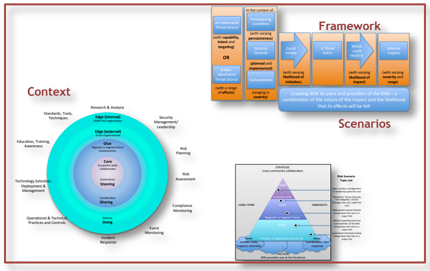
Select DNS risk-management framework consultant and launch DNSRMF project

Complete DNS risk-management framework

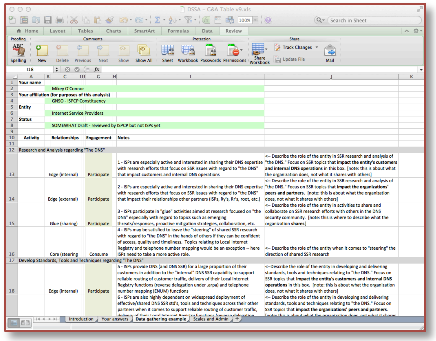
Launch the project to establish the RM function and complete one “cycle”

DNSRMF (focus/scope: ICANN the org)

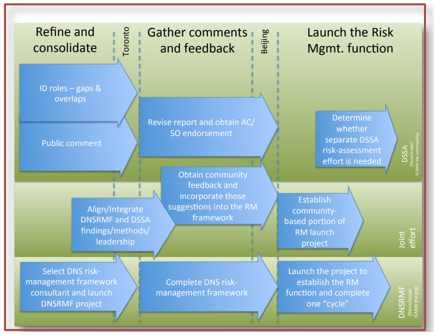
How you can help



Framework
In the context of...
An Adversarial Threat Source
(with capability, intent and targeting)
OR
A Non-Adversarial Threat Source
(with a range of effects)
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
Scenarios
Context
Research & Analysis
Standards, Tools, Techniques
Security Management/ Leadership
Education, Training, Awareness
Risk Planning
Risk Assessment
Technology Selection, Deployment & Management
Compliance Monitoring
Operational & Technical Practices and Controls
Event Monitoring
Incident Response
Edge (internal)
Within the organization
Edge (external)
Cross-organizational
Glue
Regional or segment focus
Constituencies
Core
Ecosystem-wide
Collaborative
Governance
Steering
Coordination
Sharing
Delivery
Doing
STRATEGIC
Cross-community collaboration
LONG-TERM
IMMEDIATE
CORE
Ecosystem-wide
GLUE
"Regional" or "segment" focus
EDGE
Provider or organization-focused risk
Need: models, tools, support, direction
Need: coordination, fast response
TACTICAL
DNS providers are at the forefront
Risk Scenario Topic List



	A	C	G	I	J
1	**Your name**				
2		Mikey O'Connor			
3	**Your affiliation (for purposes of this analysis)**				
4		GNSO - ISPCP Constituency			
5	**Entity**				
6		Internet Service Providers			
7	**Status**				
8		SOMEWHAT Draft - reviewed by ISPCP but not ISPs yet			
9					
10	**Activity**	**Relationships**	**Engagement**	**Notes**	
11					
12	Research and Analysis regarding "The DNS"				
13		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	<-- Describe the role of the entity in SSR research and analysis of "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]
14		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, Rr's, root, etc.)	<-- Describe the role of the entity in SSR research and analysis of "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 with others]
15		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.	<-- Describe the role of the entity in activities to share and collaborate on SSR research efforts with others in the DNS security community. [note: this is where to describe what the organization **shares**]
16		Core (steering	Consume	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.	<-- 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"				
18		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	<--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]
				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,	<-- 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**.



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)

- Comment on our Phase I report
- Fill out one of our "Gaps & Overlaps" worksheets
- Comment on our plans going forward

https://community.icann.org/**x/4AB5**