DNS Security and Stability Analysis Working Group (DSSA)

DSSA Update

Prague – June, 2012

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

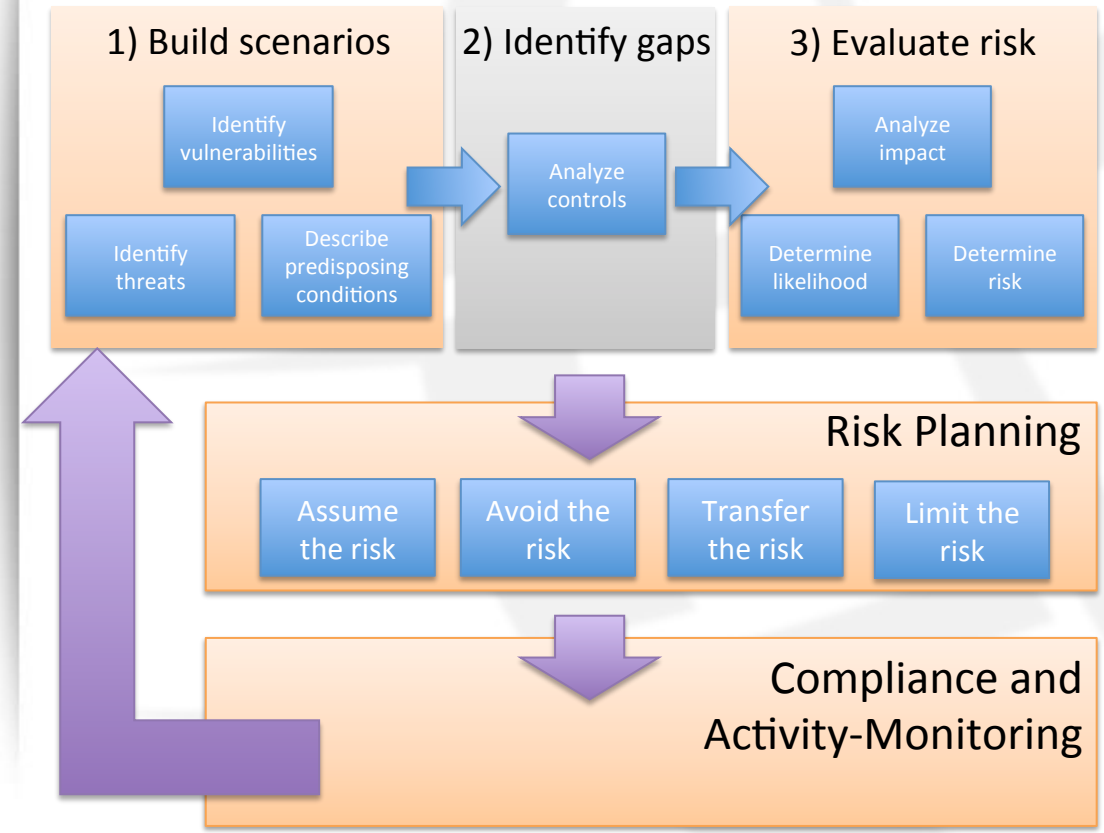
The DSSA will:

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

Scope: DSSA & DNRMF

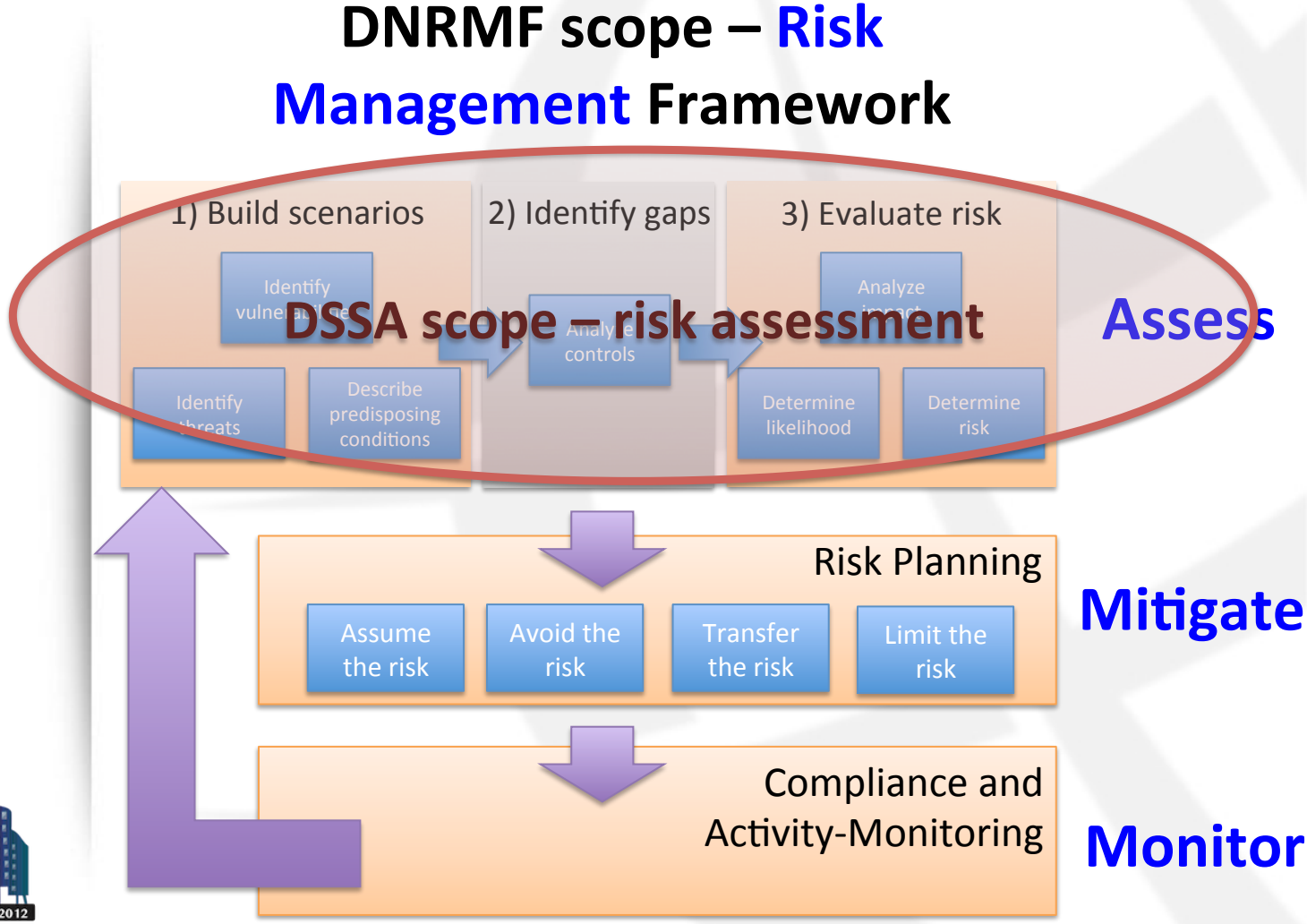
The Board DNS Risk Management Framework working group

DNRMF scope – Risk Management Framework



Scope: DSSA & DNRMF

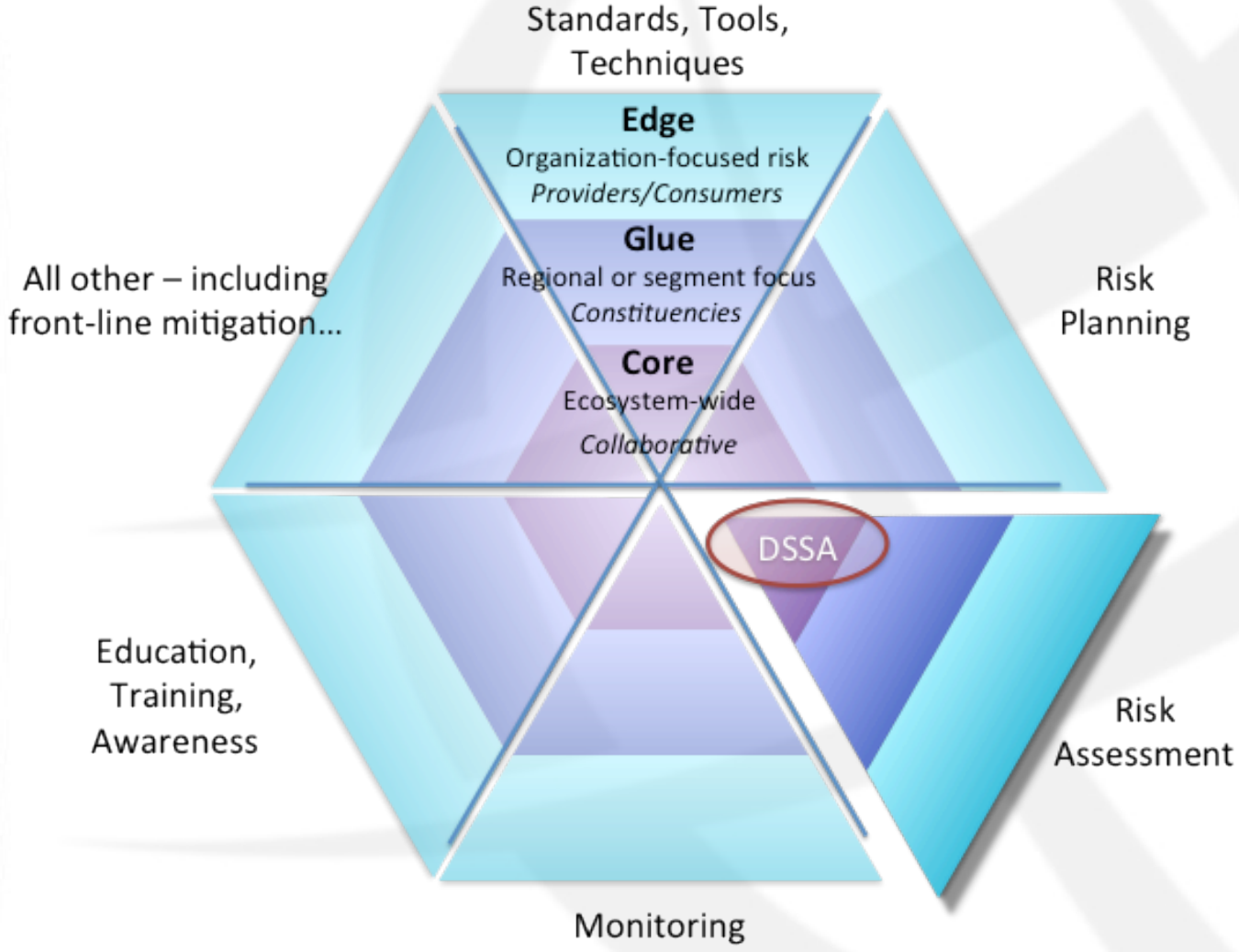
The DSSA is focusing on a subset of that framework



Scope: DSSA in a broader context

DSSA is a part of a much larger SSR ecosystem that includes:

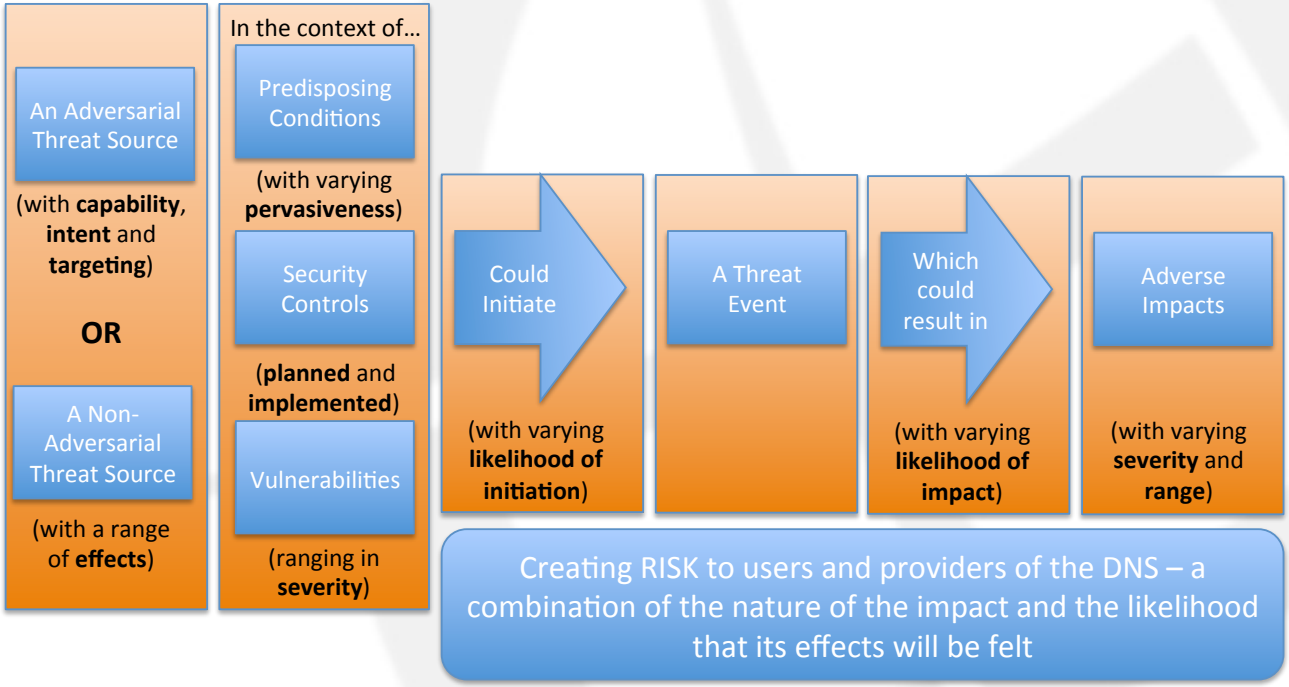
- Backend registry providers
- ccTLD registries
- CERTs
- DNRMF
- DNS-OARC
- ENISA
- FIRST
- gTLD registries
- IANA
- ICANN Security Team
- ICANN SOs and ACs
- IETF
- ISOC
- Network Operator Groups
- NRO
- RSAC
- SSAC
- SSR-RT
- And ???



“Compound Sentence” Risk Assessment Framework

Based on NIST 800-30 standard

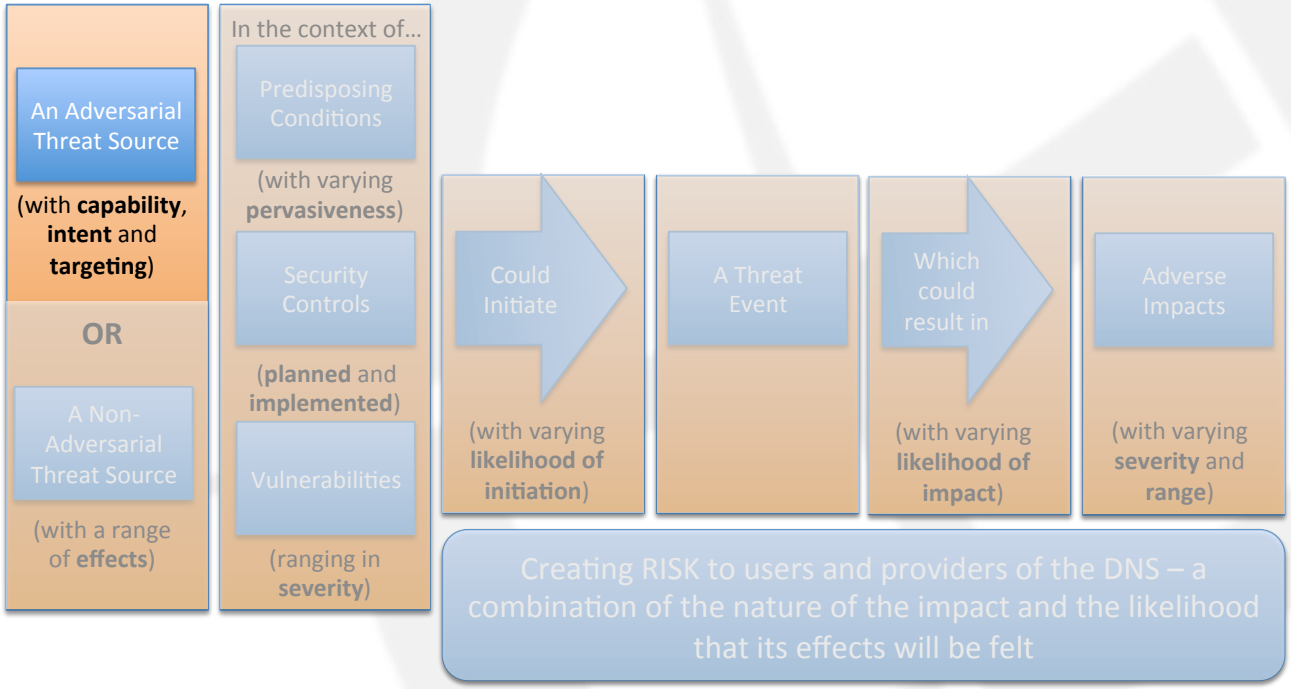
Tailored to meet unique ICANN requirements



“Compound Sentence” Risk Assessment Framework

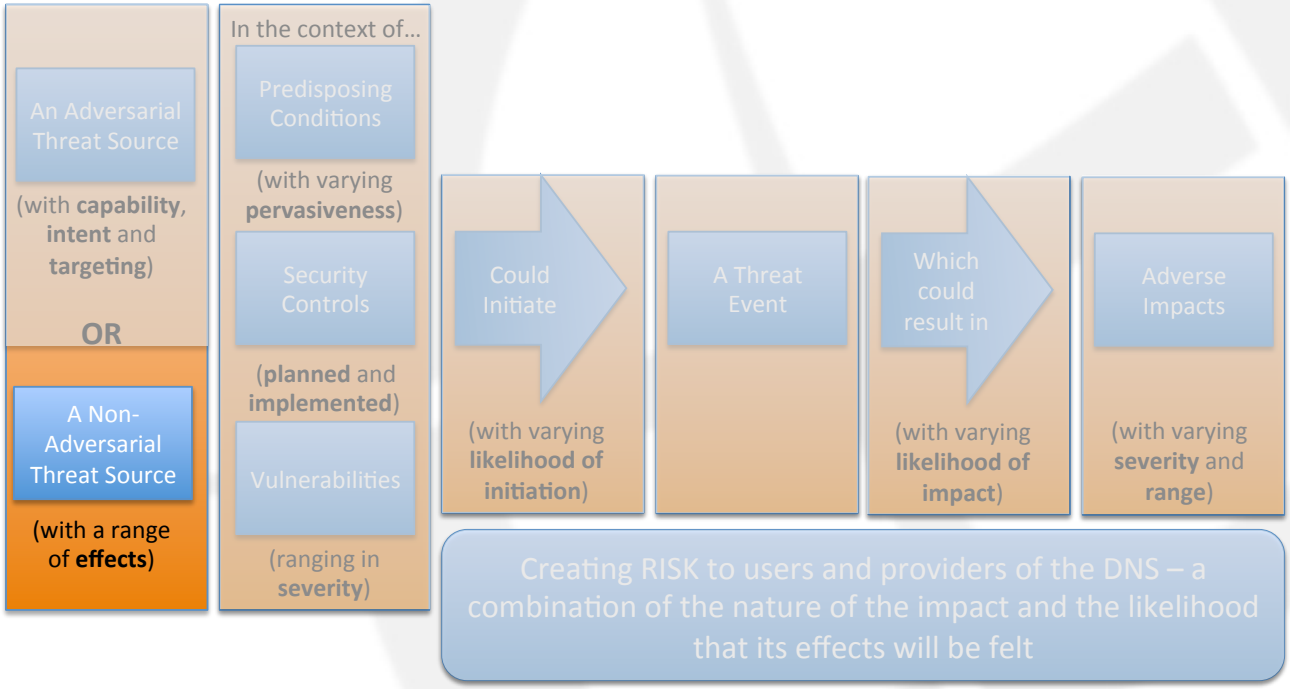
An adversarial threat-source (with capability, intent and targeting),

OR…



“Compound Sentence” Risk Assessment Framework

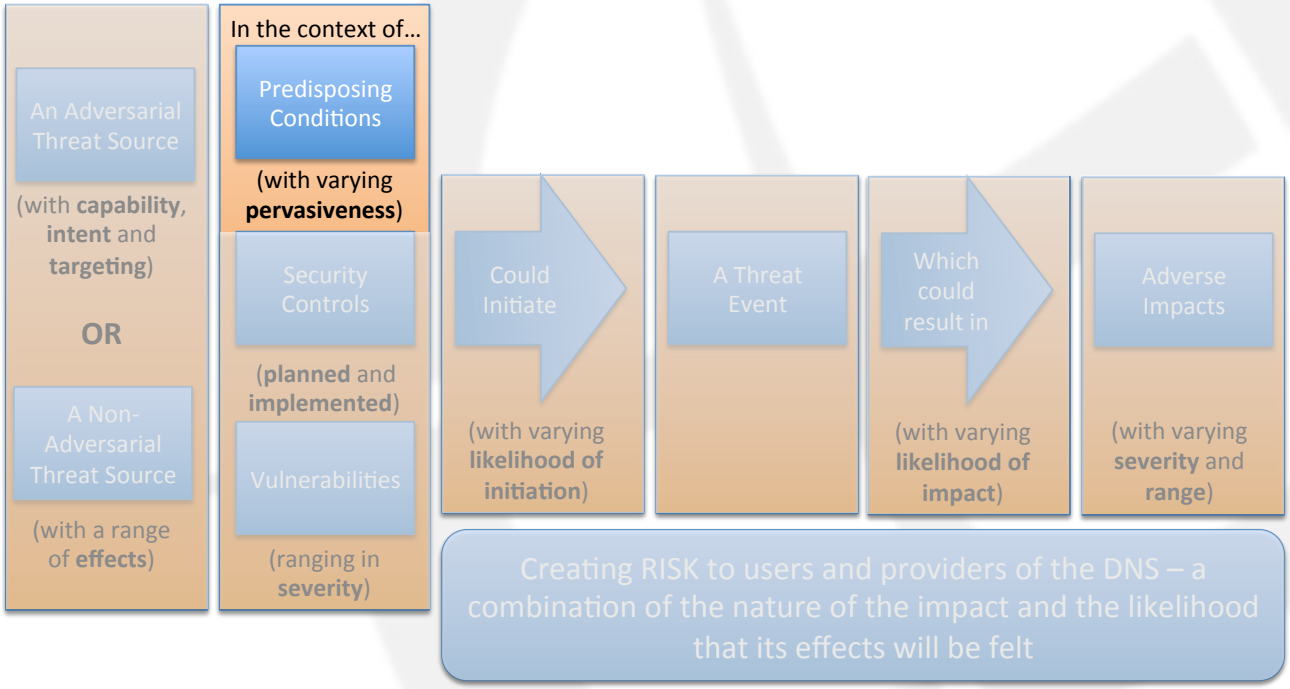
A non-adversarial threat-source (with a range of effects)…



“Compound Sentence” Risk Assessment Framework

In the context of:

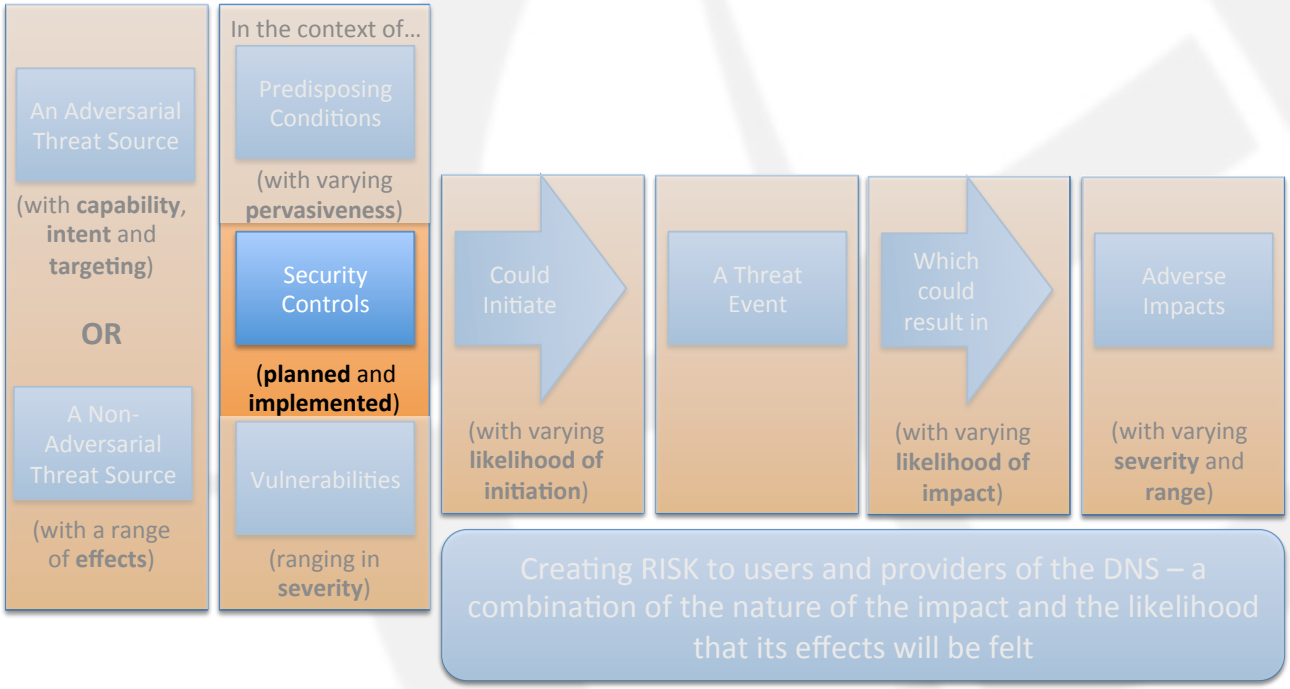
Predisposing conditions (with varying pervasiveness)…



“Compound Sentence” Risk Assessment Framework

… Security controls (both planned and implemented),

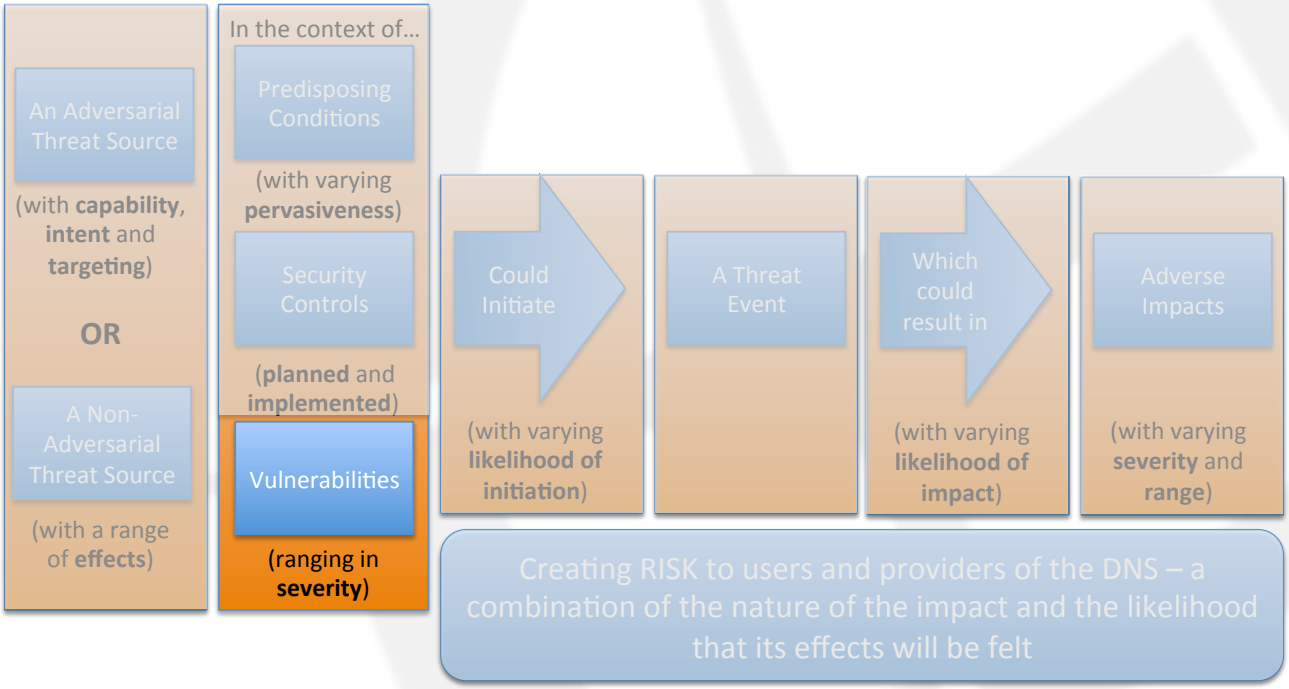
and…



“Compound Sentence” Risk Assessment Framework

…

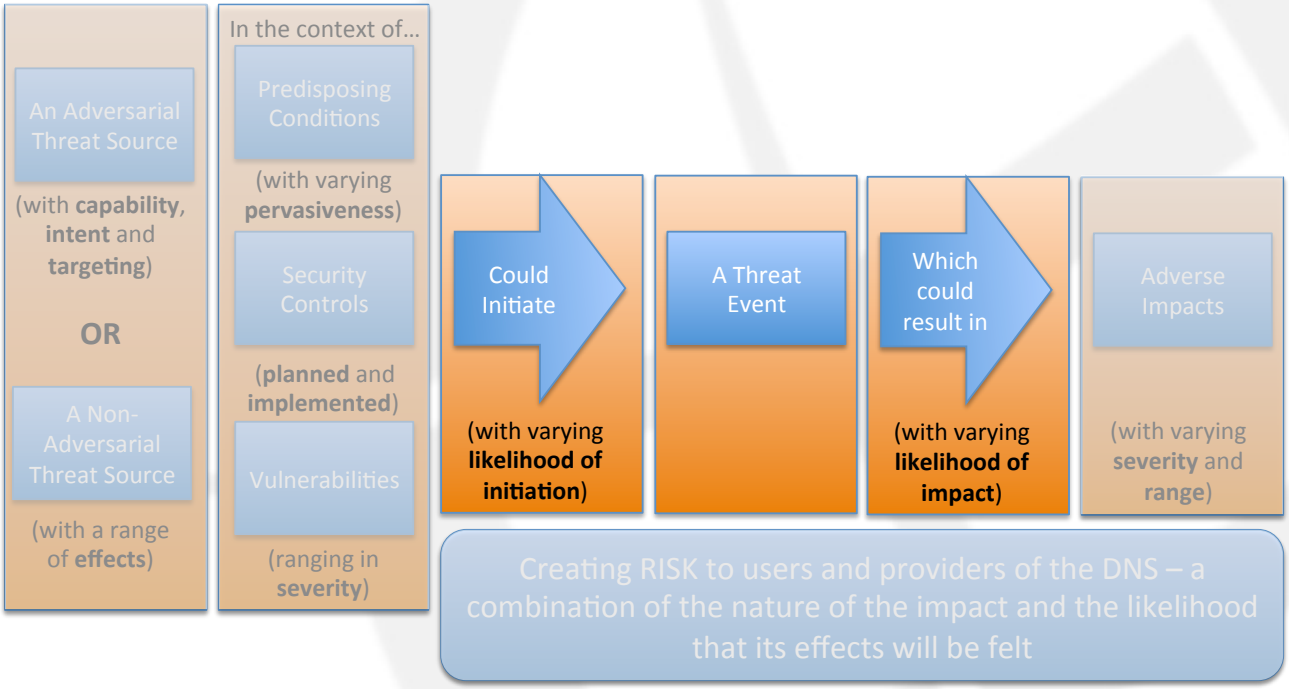
Vulnerabilities (that range in severity)…



“Compound Sentence” Risk Assessment Framework

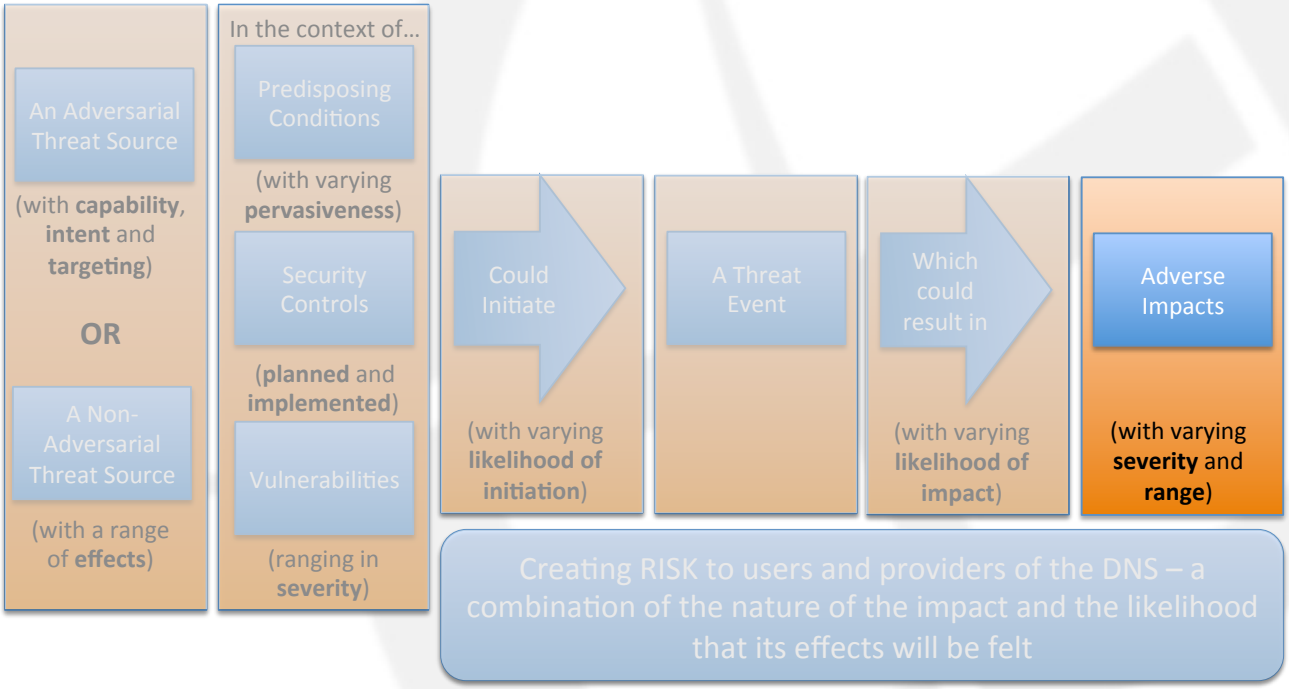
… Could initiate (with varying likelihood of initiation)

a Threat Event which (with varying likelihood of impact) could result in…



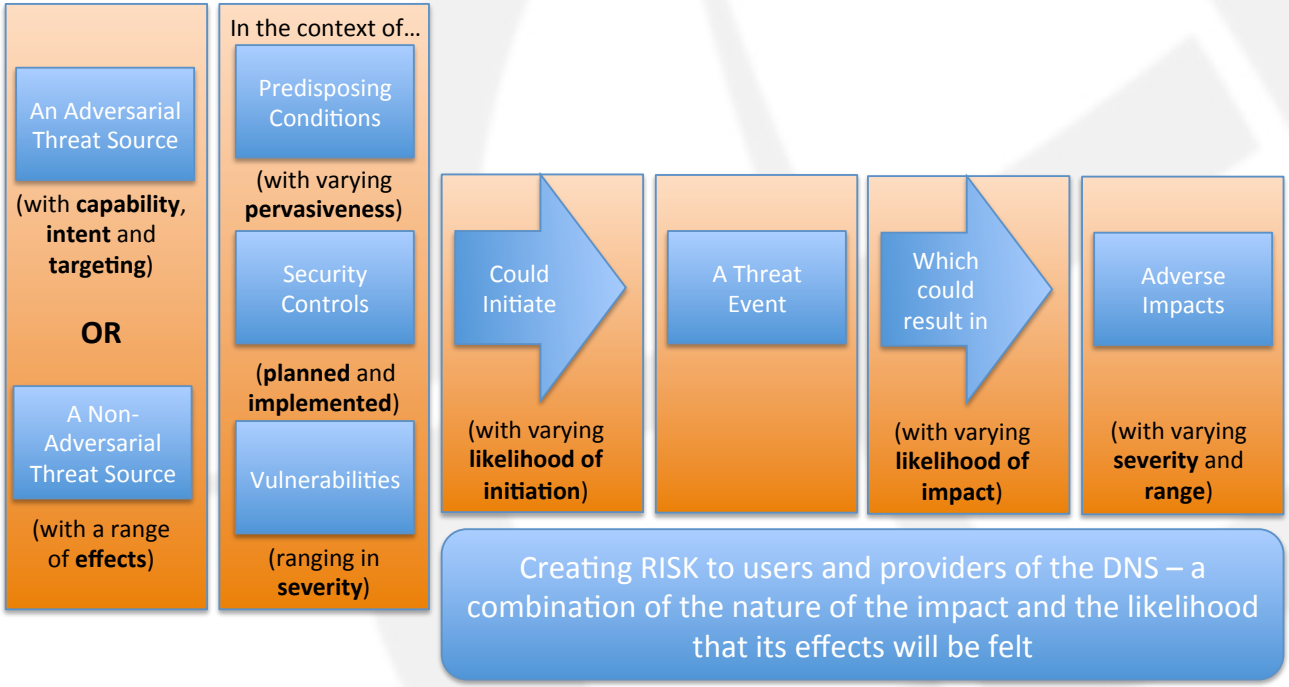
“Compound Sentence” Risk Assessment Framework

Adverse impacts (with varying severity and range)...

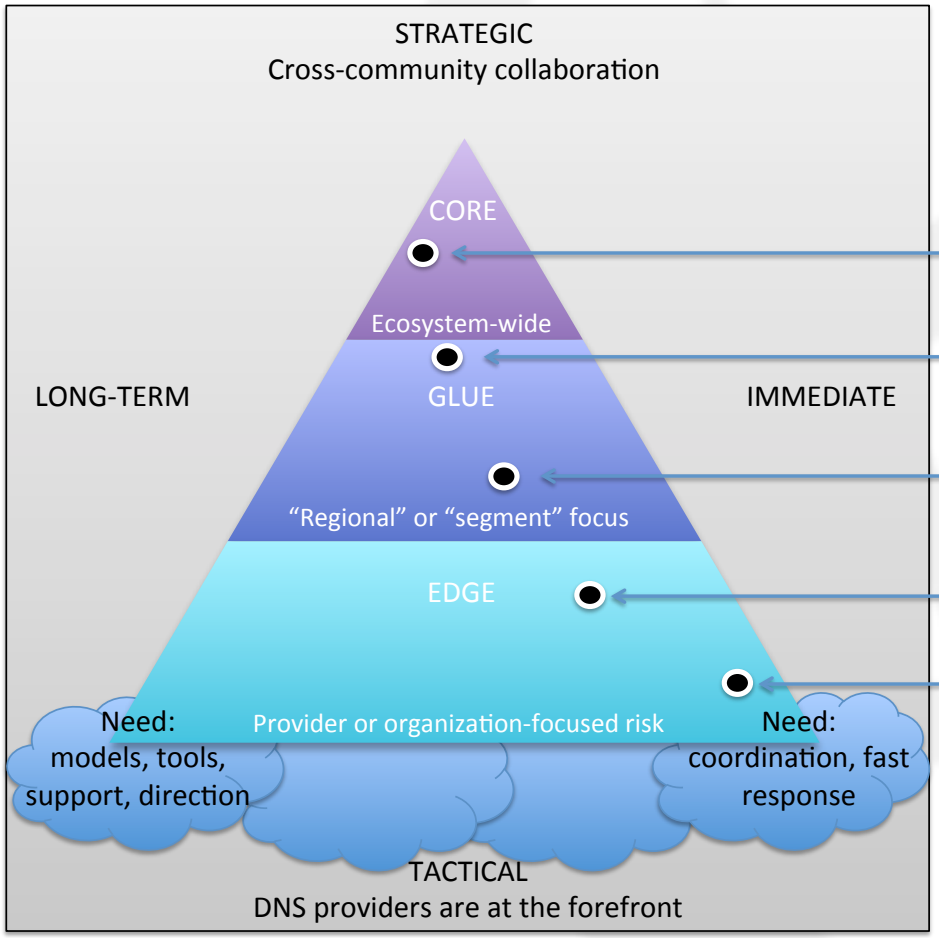


“Compound Sentence” Risk Assessment Framework

All of which combined create 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.



Findings: 5 Broad 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

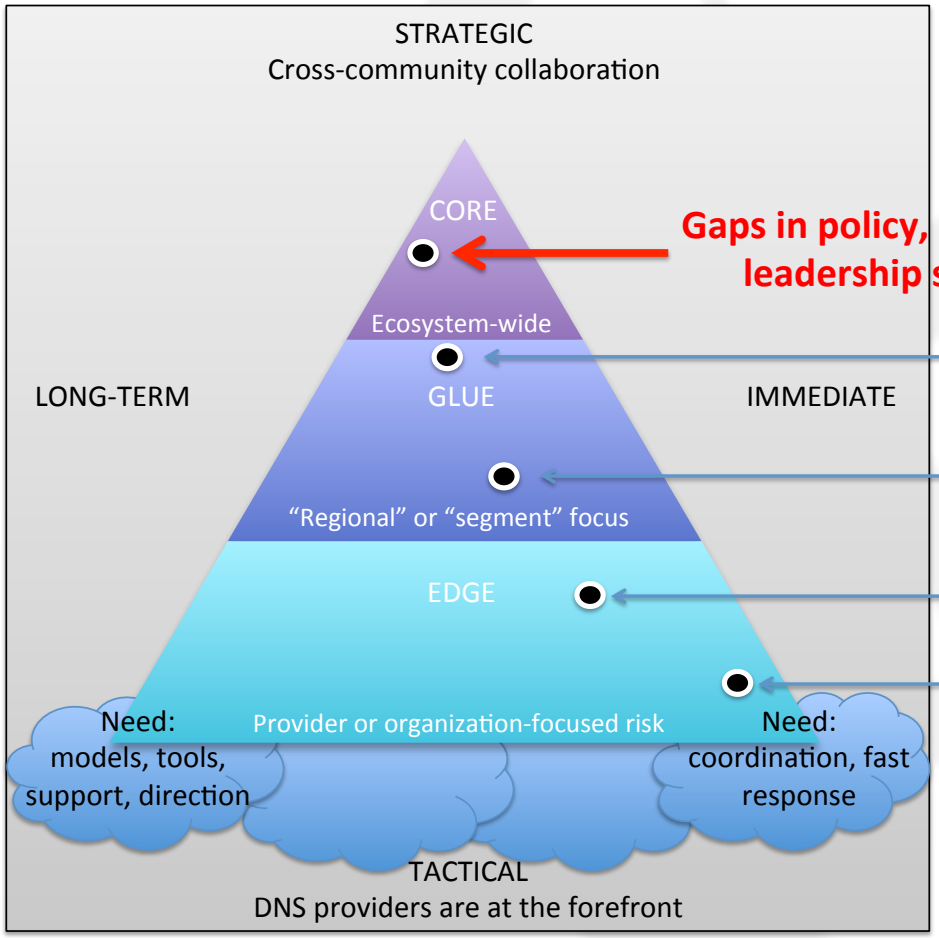
Widespread natural disaster brings down the root or a major TLD

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

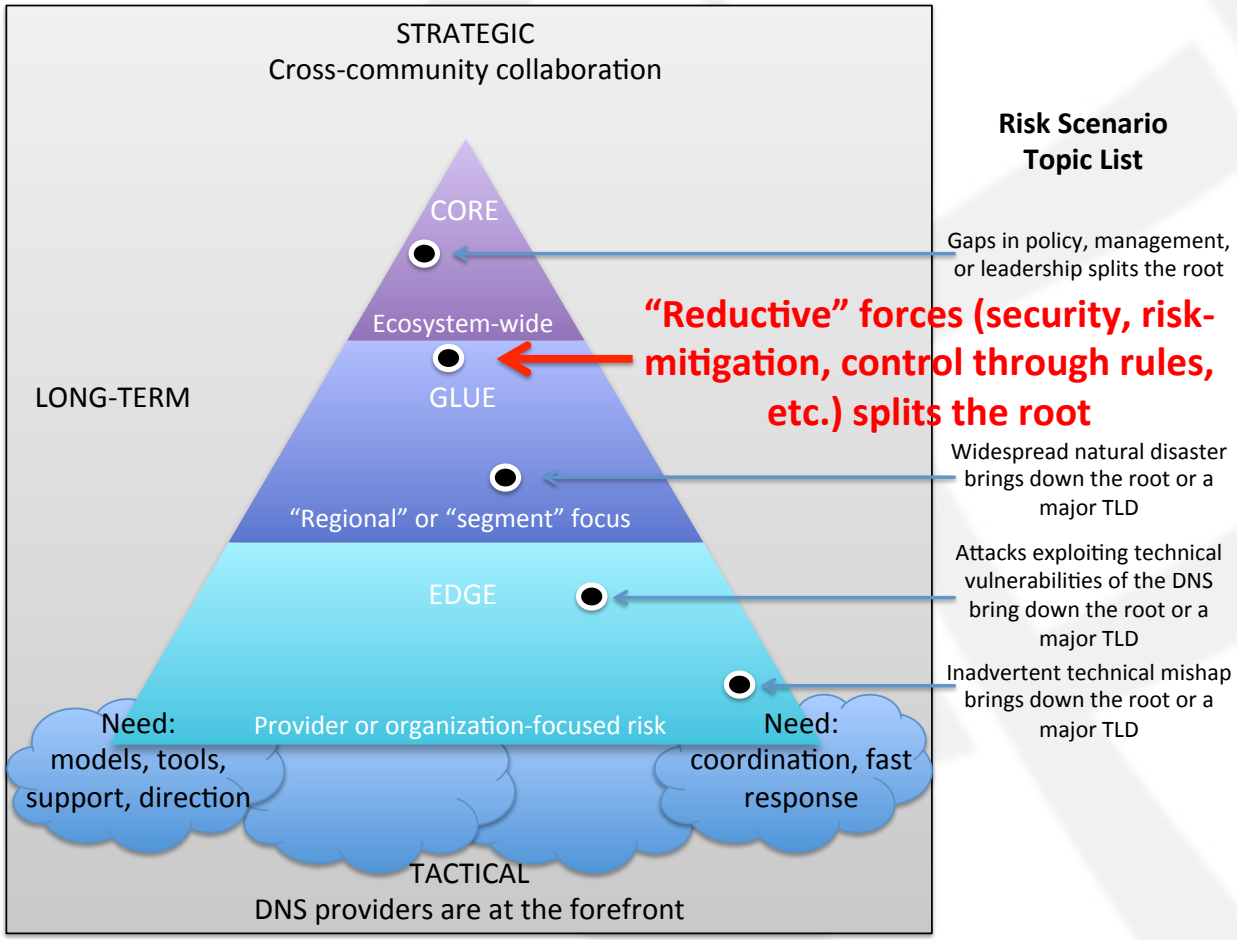
Findings: 5 Broad Risk Scenarios

Gaps in policy, management or leadership splits the root



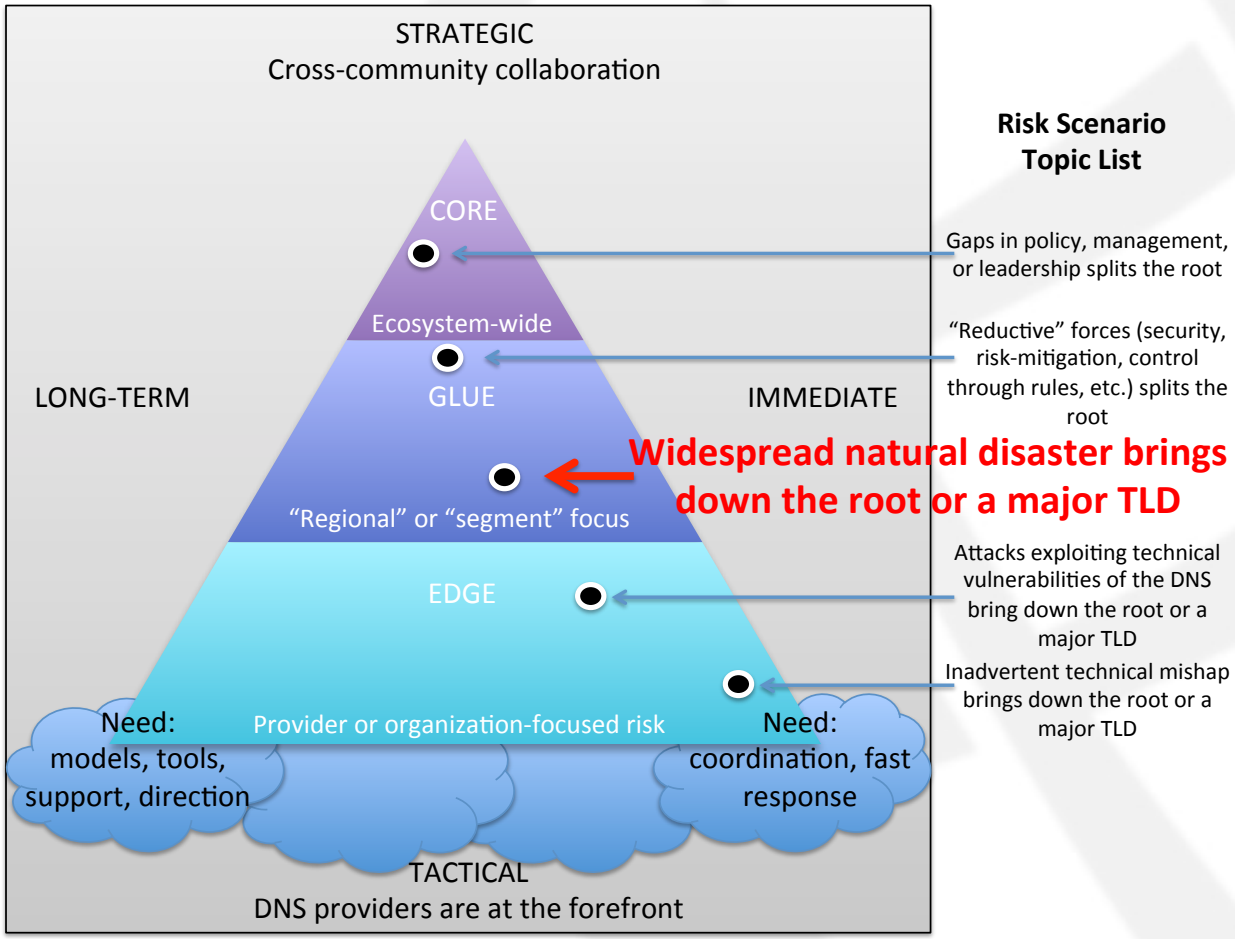
Findings: 5 Broad Risk Scenarios

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



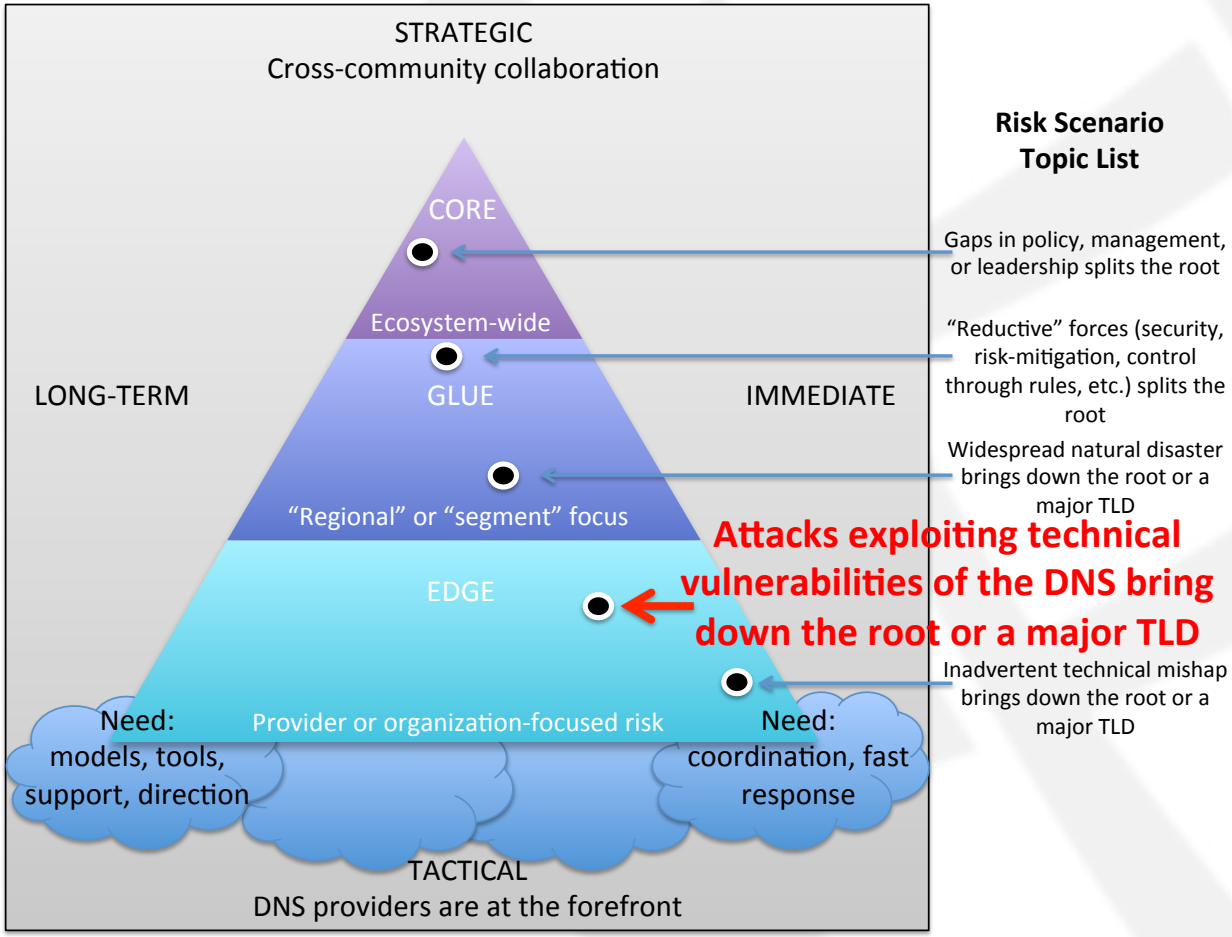
Findings: 5 Broad Risk Scenarios

Widespread natural disaster brings down the root or a major TLD



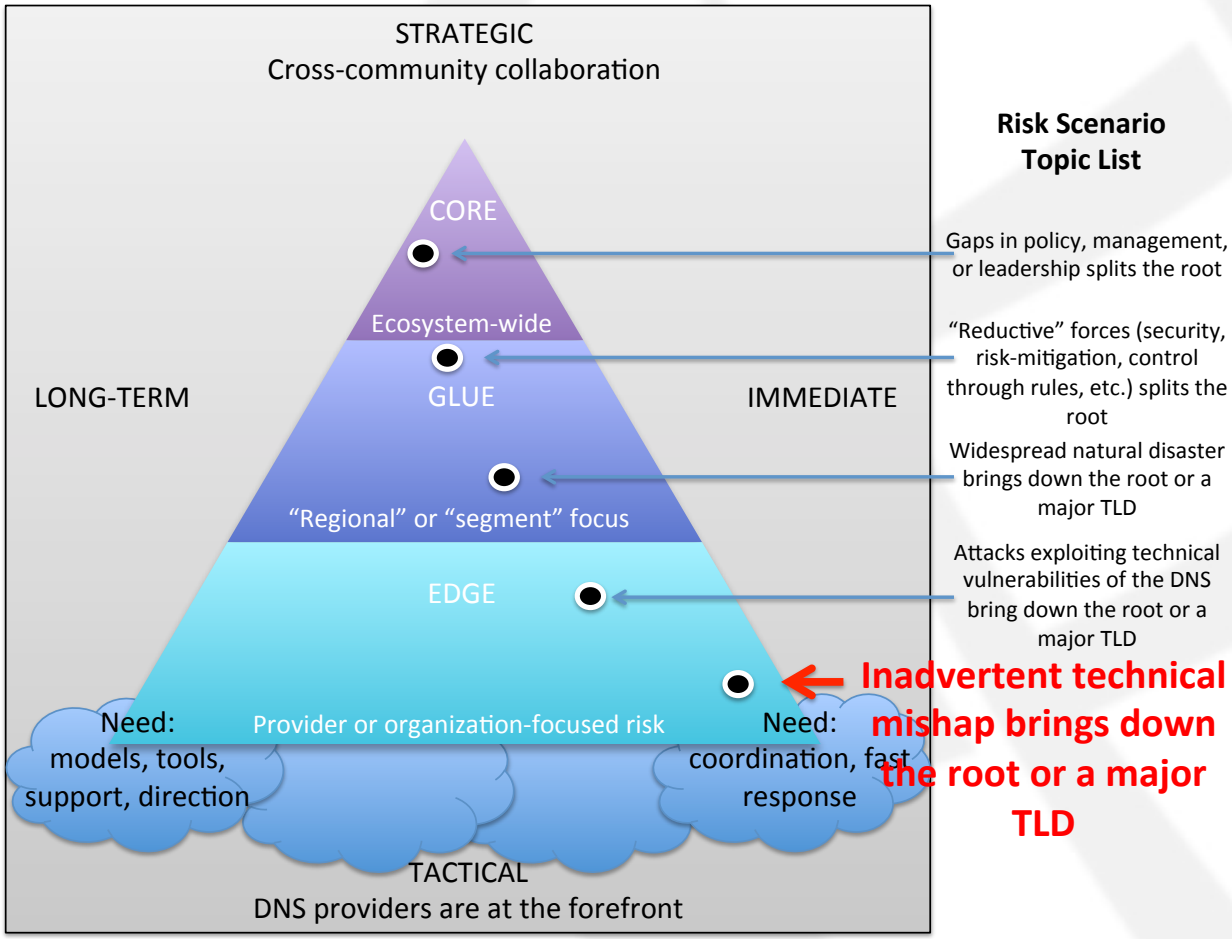
Findings: 5 Broad Risk Scenarios

Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD



Findings: 5 Broad Risk Scenarios

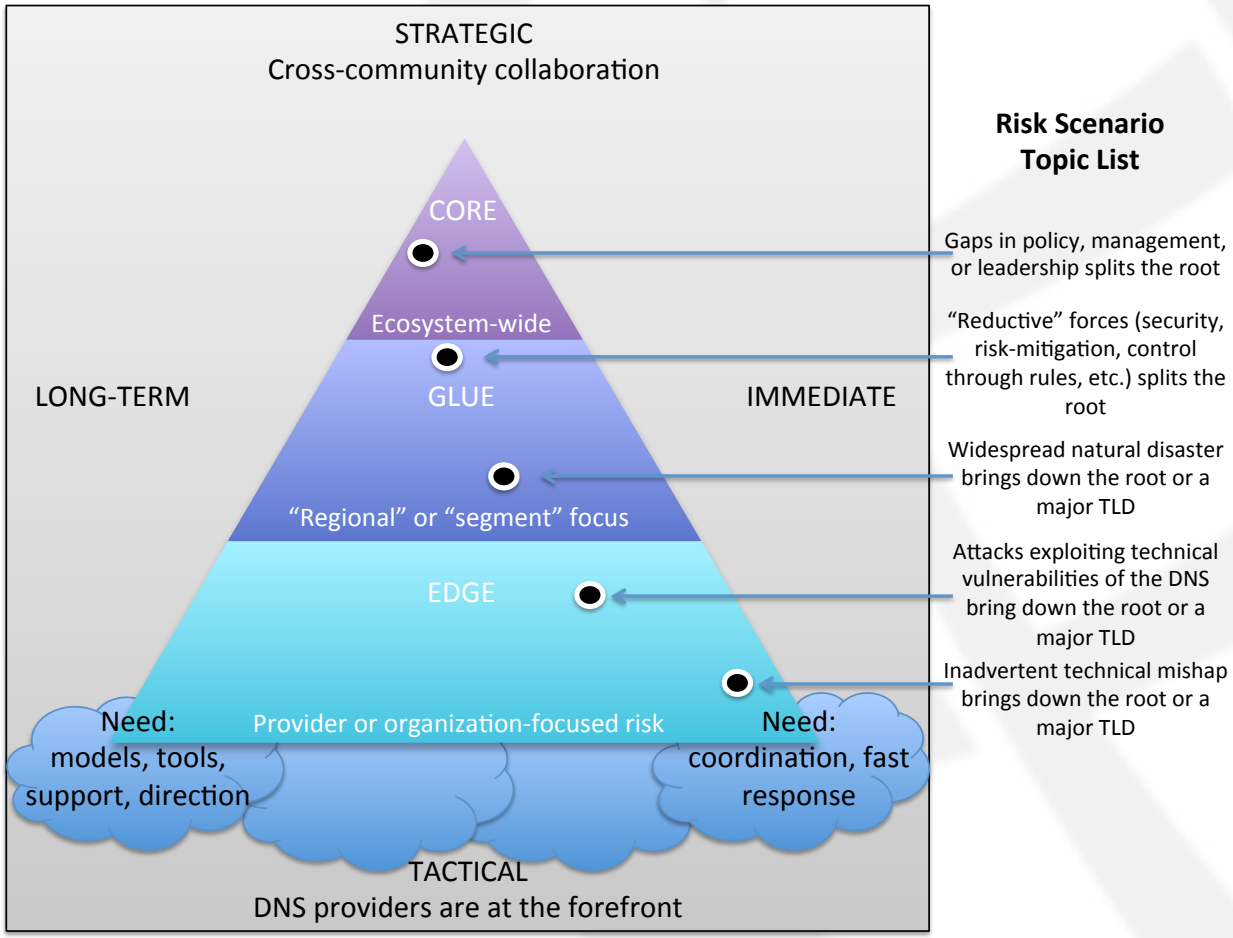
Inadvertent technical mishap brings down the root or a major TLD



Findings: 5 Broad Risk Scenarios

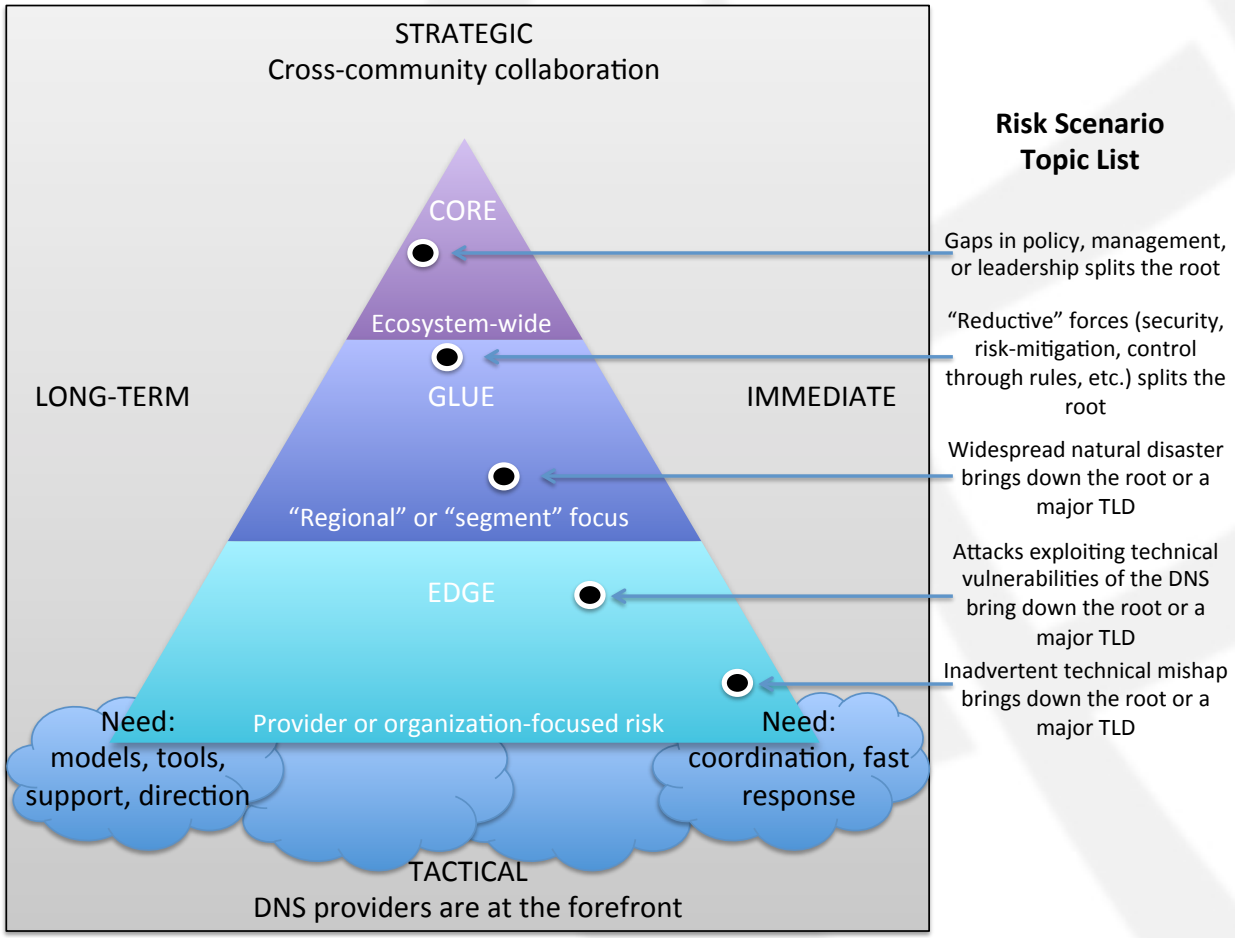
Question: Have we missed an important topic?

NOTE: If you want to share embarrassing ideas, contact Paul Vixie (paul@vix.com)



Next phase

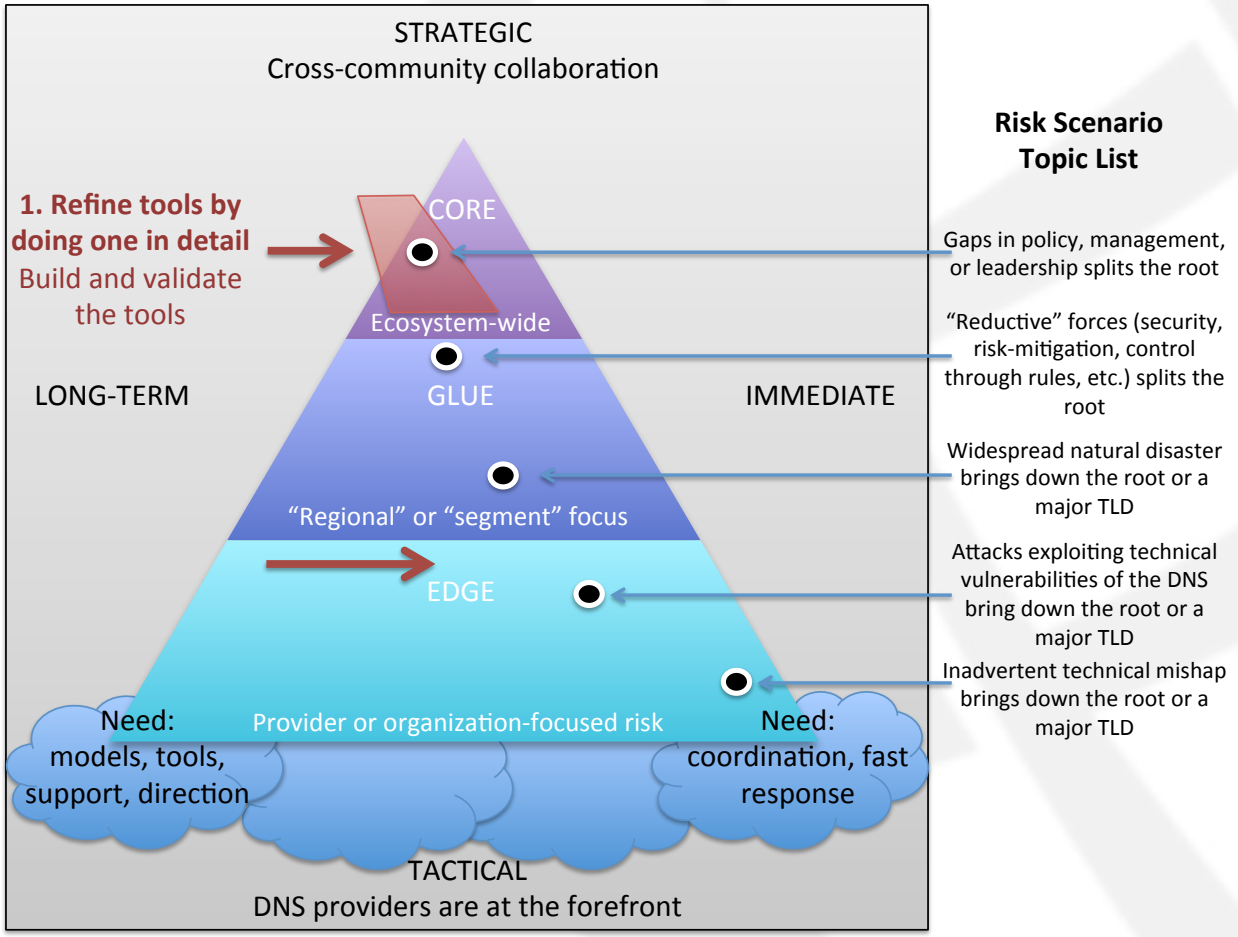
"Go deep" into the five risk topics



Next phase

"Go deep" into the five risk topics

Refine by doing

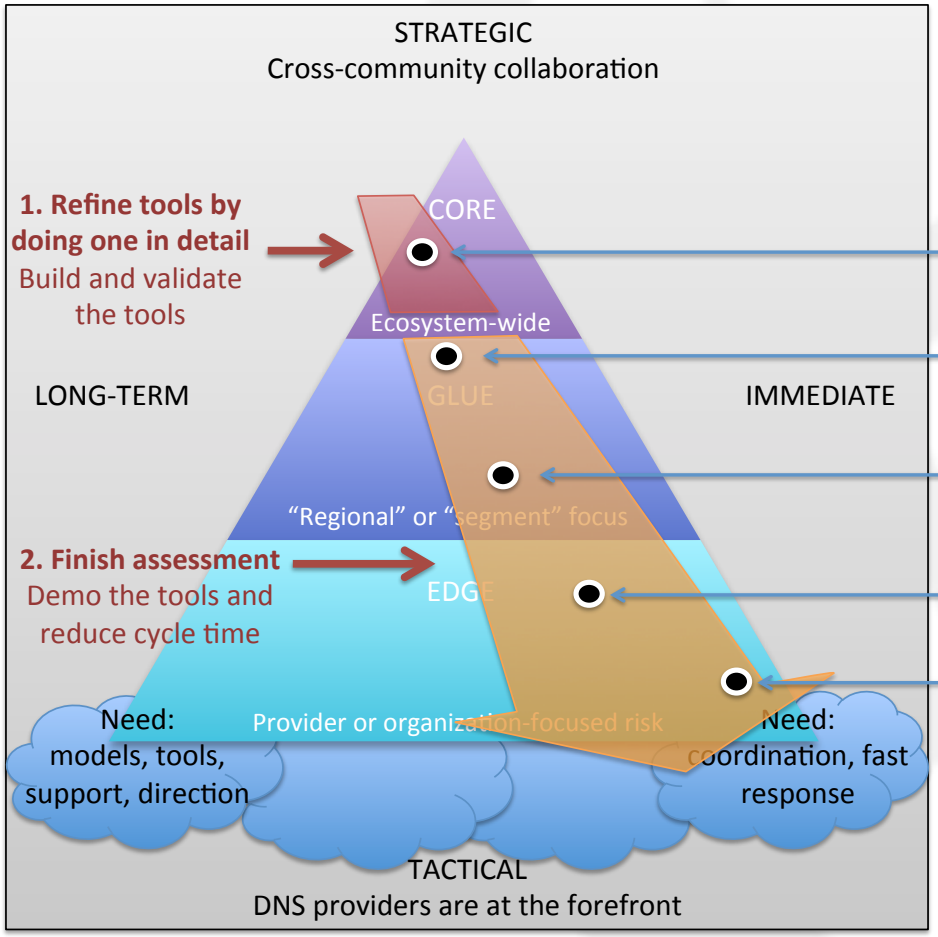


Next phase

"Go deep" into the five risk topics

Refine by doing

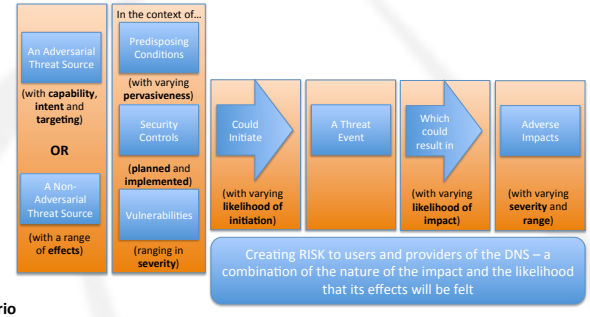
Finish assessment

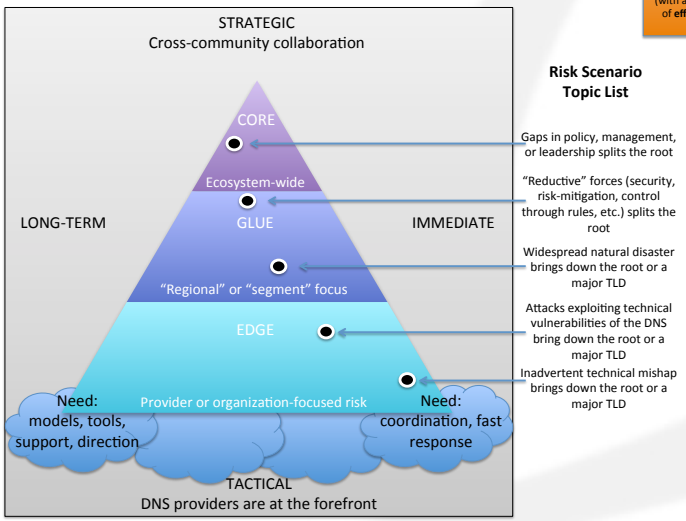


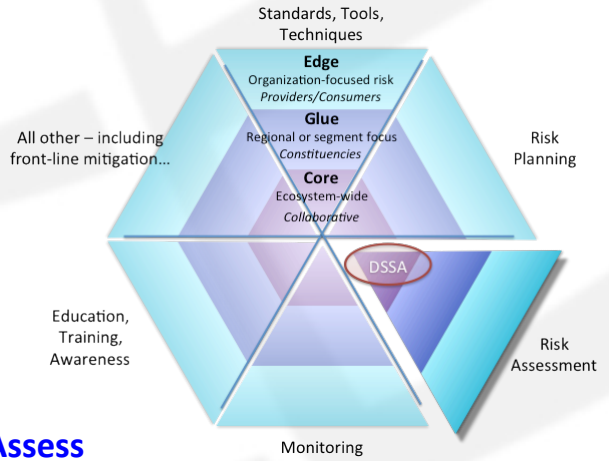
Questions?

Are we on the right track?

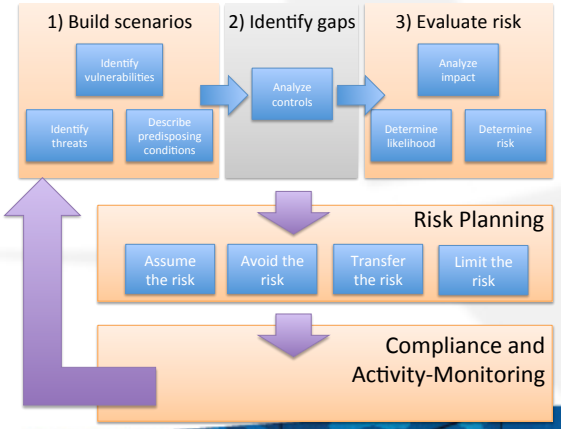
Have we missed something important?



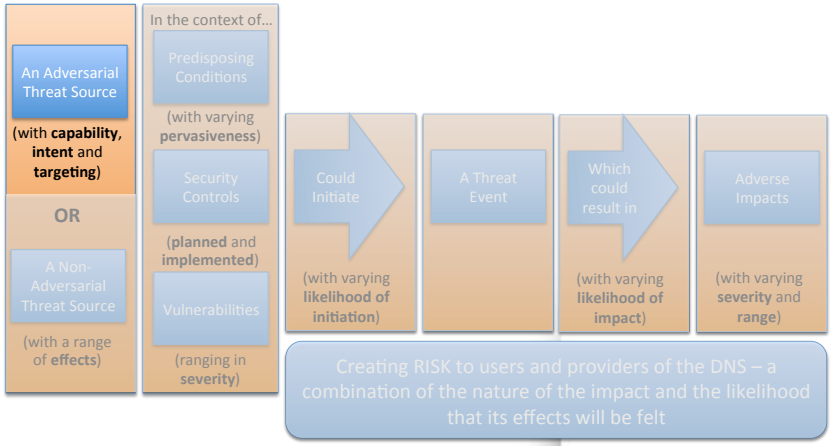




DNRMF scope – Risk Management Framework



Detailed slides follow…



Adversarial Threat Sources

- International governance/regulatory bodies
- Nation states
- Rogue elements
- Geo-political groups
- External parties and contractors
- Insiders
- Organized crime

Capability (Adversarial threat sources)

10 -- Very High -- The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.

8 -- High -- The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.

5 -- Moderate -- The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.

2 -- Low -- The adversary has limited resources, expertise, and opportunities to support a successful attack.

1 -- Very Low -- The adversary has very limited resources, expertise, and opportunities to support a successful attack

Targeting (Adversarial threat sources)

10 -- Very High -- The adversary analyzes information obtained via reconnaissance and attacks to persistently target the DNS, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.

8 -- High -- The adversary analyzes information obtained via reconnaissance to target persistently target the DNS, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.

5 -- Moderate -- The adversary analyzes publicly available information to persistently target specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.

2 -- Low -- The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.

1 -- Very Low -- The adversary may or may not target any specific organizations or classes of organizations.

Intent (Adversarial threat sources)

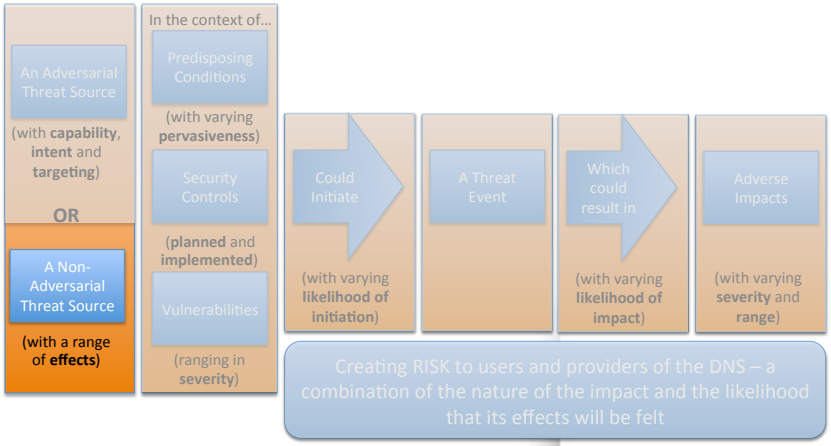
10 -- Very High -- The adversary seeks to undermine, severely impede, or destroy the DNS by exploiting a presence in an organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.

8 -- High -- The adversary seeks to undermine/impede critical aspects of the DNS, or place itself in a position to do so in the future, by maintaining a presence in an organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.

5 -- Moderate -- The adversary actively seeks to obtain or modify specific critical or sensitive DNS information or usurp/disrupt DNS cyber resources by establishing a foothold in an organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the DNS to achieve these ends.

2 -- Low -- The adversary seeks to obtain critical or sensitive DNS information or to usurp/disrupt DNS cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

1 -- Very Low -- The adversary seeks to usurp, disrupt, or deface DNS cyber resources, and does so without concern about attack detection/disclosure of tradecraft.



Non-Adversarial Threat Sources

Individual And Organizational Sources

- International governance/regulatory bodies
- Nation states
- Privileged users
- Key providers

Root-Related Sources

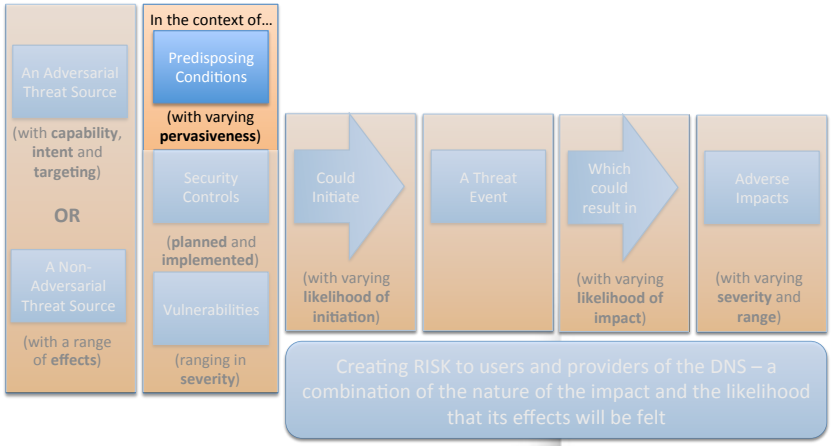
- Alternate DNS roots
- Root scaling (SAC 46)
- Intentional or accidental results of DNS blocking (SAC 50)

Infrastructure-Related Sources

- Widespread infrastructure failure
- Key hardware failure
- Earthquakes
- Hurricanes
- Tsunami
- Blackout/Energy Failure
- Snowstorm/blizzard/ice-storm

Range of effect (to DNS providers) (Non-adversarial threat sources)

10 -- sweeping, involving almost all DNS providers
8 -- extensive, involving most DNS providers (80%?)
5 --wide-ranging, involving a significant portion of DNS providers (30%?)
3 --limited, involving some DNS providers
1 -- minimal, involving few if any DNS providers



Predisposing Conditions

Managerial

- Legal standing (and relative youth) of ICANN
- Multi-stakeholder, consensus-based decision-making model
- Managerial vs. operational vs. technical security skills/focus/ resources
- Definitions of responsibility, accountability, authority between DNS providers
- Security project and program management skills/capacity
- Common ("inheritable") vs. hybrid vs. organization/system-specific controls
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities
- Contractual relationships between entities

Operational

- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches

Technical

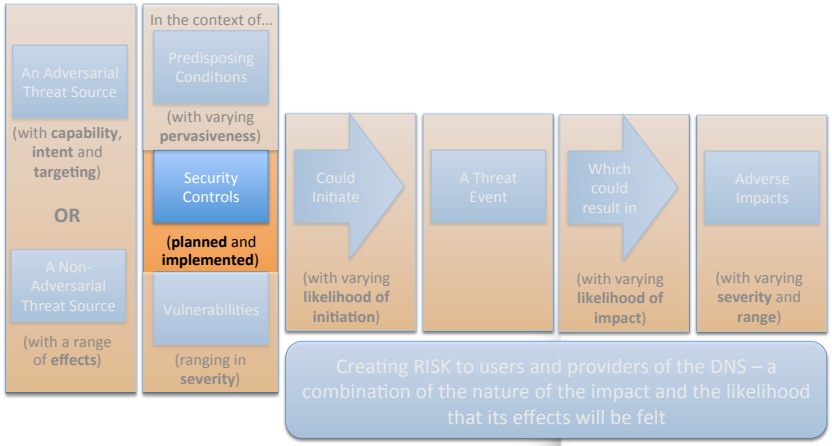
- Requirement for public access to DNS information
- Requirements for scaling

Pervasiveness Of Predisposing Conditions That Negatively Impact Risk

10 -- Very High -- Applies to all organizational missions/business functions
8 -- High -- Applies to most organizational missions/business functions
5 -- Moderate -- Applies to many organizational missions/ business functions
3 -- Low -- Applies to some organizational missions/business functions
1 -- Very Low -- Applies to few organizational missions/business functions

Pervasiveness Of Predisposing Conditions That Positively Impact Risk

.1 -- Very High -- Applies to all organizational missions/business functions
.3 -- High -- Applies to most organizational missions/business functions
.5 -- Moderate -- Applies to many organizational missions/ business functions
.8 -- Low -- Applies to some organizational missions/business functions
1 -- Very Low -- Applies to few organizational missions/business functions



Pervasiveness Of Controls

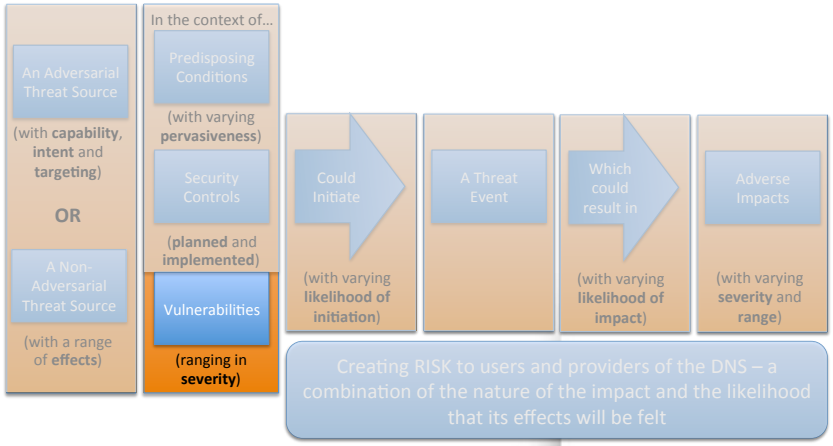
10 -- Controls are missing
8 -- Controls are acknowledged as needed
5 -- Controls are planned or being implemented
2 -- Controls are implemented
1 -- Controls are effective

Controls

Management Controls
- Security Assessment and Authorization
- Planning
- Risk Assessment
- System and Services Acquisition
- Program Management

Operational Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Personnel Security
- System and Information Integrity

Technical Controls
- Access Control
- Audit and Accountability
- Identification and Authentication
- System and Communications Protection



Vulnerability Severity

10 -- Very High -- Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.

8 -- High -- Relevant security control or other remediation is planned but not implemented.

5 -- Moderate -- Relevant security control or other remediation is partially implemented and somewhat effective.

2 -- Low -- Relevant security control or other remediation is fully implemented and somewhat effective.

1 -- Very Low -- Relevant security control or other remediation is fully implemented, assessed, and effective.

Vulnerabilities

Managerial

- Interventions from outside the process
- Poor inter-organizational communications
- External relationships/dependencies
- Inconsistent or incorrect decisions about relative priorities of core missions and business functions
- Lack of effective risk-management activities
- Vulnerabilities arising from missing or ineffective security controls
- Mission/business processes (e.g., poorly defined processes, or processes that are not risk-aware)
- Security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems)

Operational

- Infrastructure vulnerabilities
- Business continuity vulnerabilities
- Malicious or unintentional (erroneous) alteration of root or TLD DNS configuration information
- Inadequate training/awareness
- Inadequate incident-response

Technical (Under Discussion)

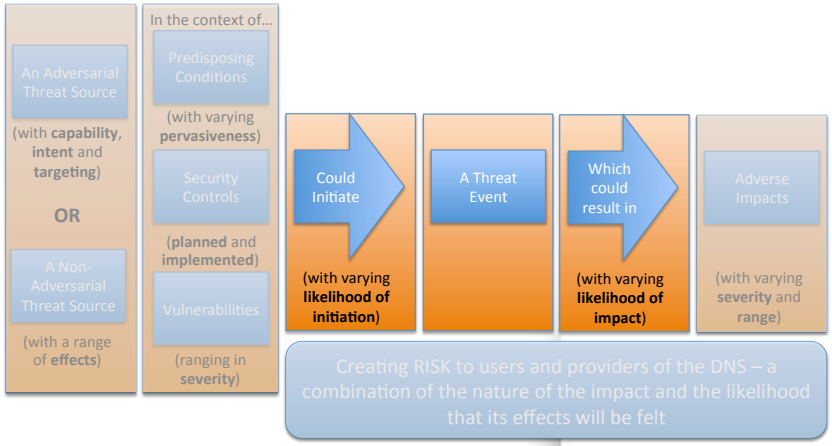
- IDN attacks (lookalike characters etc. for standard exploitation techniques)

Technical (System And Network)

- Recursive vs. authoritative nameserver attacks
- DDOS
- Email/spam

Technical (Identification And Authentication)

- Data poisoning (MITM, Cache)
- Name Chaining (RFC 3833)
- Betrayal by Trusted Server (RFC 3833)
- Authority or authentication compromise
- Packet Interception
- Man in the middle
- Eavesdropping combined with spoofed responses



Threat Events

Zone does not resolve or is not available
Zone is not correct or does not have integrity

Likelihood of initiation (by adversarial threat sources)

10 -- Very High -- Adversary is almost certain to initiate the threat-event
8 -- High -- Adversary is highly likely to initiate the threat event
5 -- Moderate -- Adversary is somewhat likely to initiate the threat event
2 -- Low -- Adversary is unlikely to initiate the threat event
0 -- Very Low -- Adversary is highly unlikely to initiate the threat event

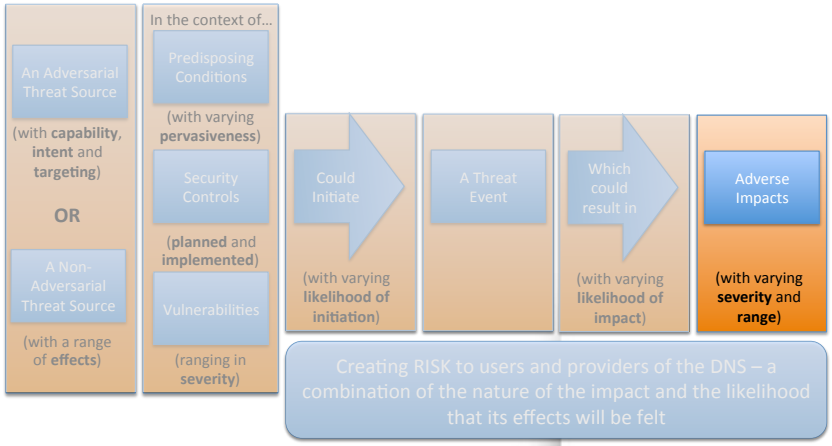
Likelihood of initiation (by non-adversarial threat sources)

10 -- Very high -- Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
8 -- High -- Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
5 -- Moderate -- Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
2 -- Low -- Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
0 -- Very Low -- Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

DSSA default va

Likelihood of impact

10 -- Very High -- If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
8 -- High -- If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
5 -- Moderate -- If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
2 -- Low -- If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
0 -- Very Low -- If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.



Severity

10 -- Very Severe -- The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the world. And in all cases there would be significant problems for registrants and users in the zone.

8 -- High -- The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the world.

5 -- Moderate -- The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the world.

2 -- Low -- The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the world.

0 -- Very Low -- The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the world.

Range of Impact

10 -- Very Broad -- The effects of the threat event are sweeping, involving almost all consumers of the DNS

8 -- Broad -- The effects of the threat event are extensive, involving most of the consumers of the DNS

5 -- Moderate -- The effects of the threat event are substantial, involving a significant portion of the consumers of the DNS

2 -- Low -- The effects of the threat event are limited, involving some consumers of the DNS but involving no critical resources.

0 -- The effects of the threat event are minimal or negligible, involving few if any consumers of the DNS and involving no critical resources. .

DSSA default value

Adverse Impacts

Harm To Nations And The World; E.G.

Damage to a critical infrastructure sector
Loss of government continuity of operations.
Relational harms.
Damage to trust relationships with other governments or with nongovernmental entities.
Damage to national reputation (and hence future or potential trust relationships).
Damage to current or future ability to achieve national objectives.

Harm To Individuals; E.G.

Identity theft (only applies to "loss of integrity" threat-event)
Loss of Personally Identifiable Information (only applies to "loss of integrity" threat-event)
Injury or loss of life
Damage to image or reputation.

Harm To Assets; E.G.

Damage to or of loss of information assets.
Loss of intellectual property (only applies to "loss of integrity" threat-event)
Damage to or loss of physical facilities.
Damage to or loss of information systems or networks.
Damage to or loss of information technology or equipment.
Damage to or loss of component parts or supplies.

Harm To Operations/Organizations; E.G.

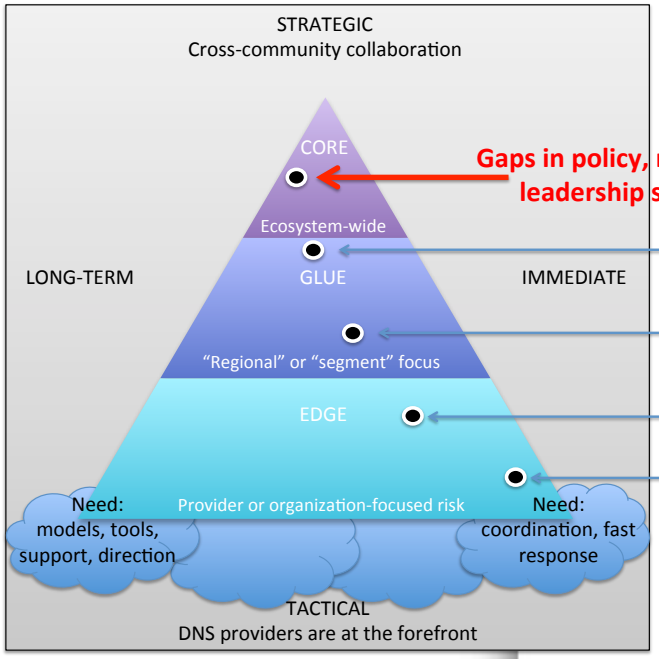
Inability to perform current missions/business functions.
- In a sufficiently timely manner.
- With sufficient confidence and/or correctness.
- Within planned resource constraints.

Inability, or limited ability, to perform missions/business functions in the future.
- Inability to restore missions/business functions.
- In a sufficiently timely manner.
- With sufficient confidence and/or correctness.
- Within planned resource constraints.

Harms (e.g., financial costs, sanctions) due to noncompliance.
- With applicable laws or regulations.
- With contractual requirements or other requirements in other binding agreements.

Direct financial costs.
Damage to trust relationships or reputation
- Damage to trust relationships.
- Damage to image or reputation (and hence future or potential trust relationships).

Relational harms



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

Threat Events

Zone does not resolve or is not available

Zone is incorrect or does not have integrity

Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Vulnerabilities

Managerial

- **Interventions from outside the process**
- **Poor inter-organizational communications**
- **External relationships/dependencies**
- **Inconsistent or incorrect decisions about relative priorities of core missions and business functions**
- **Lack of effective risk-management activities**
- **Mission/business processes (e.g., poorly defined processes, or processes that are not risk-aware)**

Threat Sources

- **Nation states**
- **Geo-political groups**
- **International governance/regulatory bodies**

Predisposing Conditions that increase risk

Managerial

- **Legal standing (and relative youth) of ICANN**
- **Definitions of responsibility, accountability, authority between DNS providers**

Operational

- **Diverse operational environments and approaches**

Missing or Insufficient Security Controls

Management Controls

- **Planning**
- **Risk Assessment**
- **Program Management**

Operational Controls

- **Awareness and Training**
- **Incident Response**

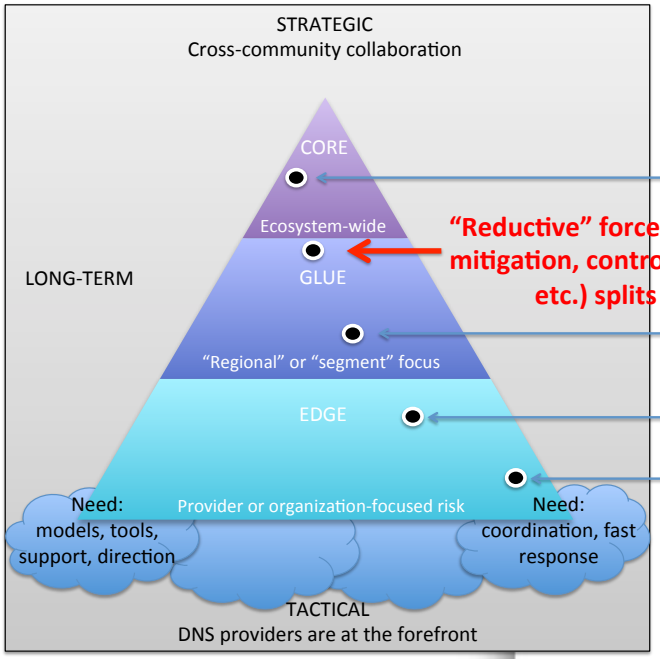
Predisposing Conditions The Reduce Risk

Managerial

- **Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities**
- **Contractual relationships between entities**

Operational

- **Diverse, distributed system architecture and deployment**
- **Culture of collaboration built on personal trust relationships**
- **Diverse operational environments and approaches**



Threat Events

Zone does not resolve or is not available

Zone is incorrect or does not have integrity

Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Vulnerabilities

Managerial

- **Interventions from outside the process**
- **Poor inter-organizational communications**
- **External relationships/dependencies**
- **Inconsistent or incorrect decisions about relative priorities of core missions and business functions**
- **Lack of effective risk-management activities**
- **Mission/business processes (e.g., poorly defined processes, or processes that are not risk-aware)**

Threat Sources

- External parties and contractors -- large content and network providers
- International governance/regulatory bodies

Predisposing Conditions That Increase Risk

Managerial

- **Legal standing (and relative youth) of ICANN**
- **Managerial vs. operational vs. technical security skills/focus/ resources**
- **Definitions of responsibility, accountability, authority between DNS providers**

Missing or Insufficient Security Controls

Management Controls

- **Planning**
- **Risk Assessment**
- **Program Management**

Operational Controls

- **Awareness and Training**

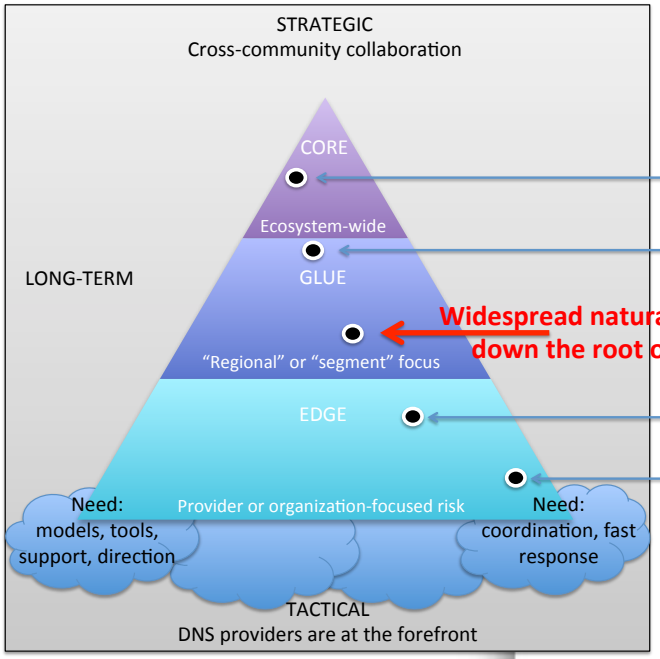
Predisposing Conditions That Reduce Risk

Managerial

- **Multi-stakeholder, consensus-based decision-making model**

Operational

- **Diverse, distributed system architecture and deployment**
- **Emphasis on resiliency and redundancy**
- **Culture of collaboration built on personal trust relationships**
- **Diverse operational environments and approaches**



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

Threat Events

Zone does not resolve or is not available

Zone is incorrect or does not have integrity

Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Vulnerabilities

Managerial

- **Poor inter-organizational communications**
- **Lack of effective risk-management activities**

Operational

- **Infrastructure vulnerabilities**
- **Business continuity vulnerabilities**

Non-Adversarial Threat Sources

Infrastructure-Related Sources

- **Widespread infrastructure failure**
- **Earthquakes**
- **Hurricanes**
- **Tsunami**
- **Blackout/Energy Failure**
- **Snowstorm/blizzard/ice-storm**

Predisposing Conditions That Increase Risk

Managerial

- **Contractual Relationships Between Entities**

Operational

- **Diverse operational environments and approaches**

Missing or Insufficient Security Controls

Management Controls

- **Risk Assessment**

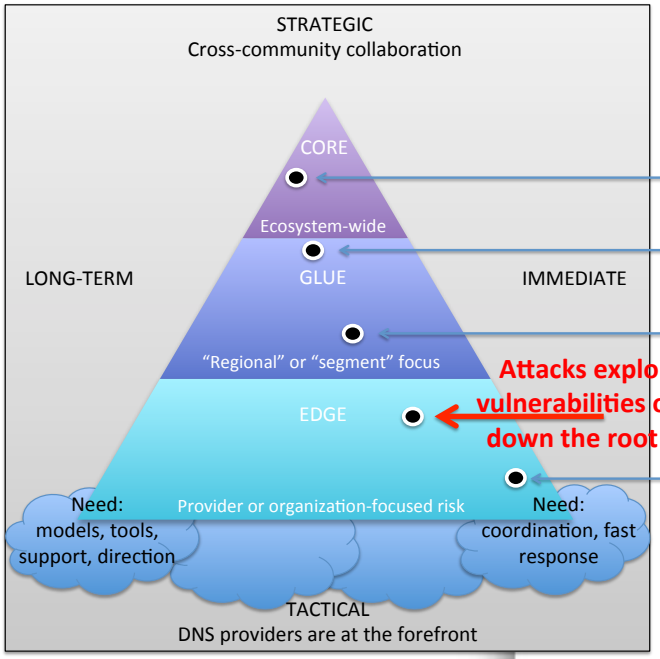
Operational Controls

- **Awareness and Training**
- **Configuration Management**
- **Contingency Planning**
- **Incident Response**
- **Physical and Environmental Protection**

Predisposing Conditions The Reduce Risk

Operational

- **Diverse, distributed system architecture and deployment**
- **Emphasis on resiliency and redundancy**
- **Culture of collaboration built on personal trust relationships**
- **Diverse operational environments and approaches**



Threat Events

Zone does not resolve or is not available

Zone is incorrect or does not have integrity

Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Vulnerabilities

Managerial

Security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems)

Operational

Infrastructure vulnerabilities

Inadequate training/awareness

Technical Vulnerabilities

Adversarial Threat Sources

Rogue elements

Insiders

Predisposing Conditions That Increase Risk

Managerial

Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities

Contractual relationships between entities

Operational

Culture of collaboration built on personal trust relationships

Diverse operational environments and approaches

Missing or Insufficient Security Controls

Management Controls

Security Assessment and Authorization

Operational Controls

Configuration Management

Incident Response

Technical Controls

Identification and Authentication

System and Communications Protection

Predisposing Conditions That Reduce Risk

Managerial

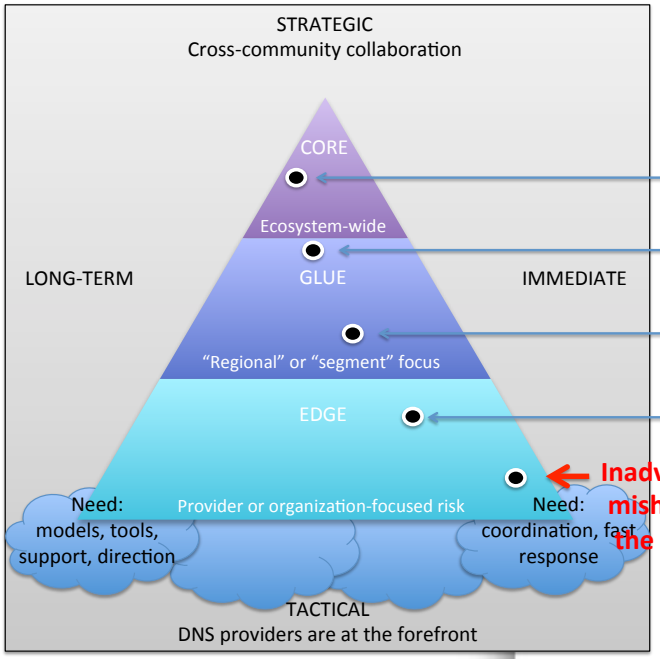
Managerial vs. operational vs. technical security skills/focus/resources

Contractual relationships between entities

Operational

Diverse, distributed system architecture and deployment

Emphasis on resiliency and redundancy



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

Threat Events

Zone does not resolve or is not available

Zone is incorrect or does not have integrity

Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Vulnerabilities

Managerial

Vulnerabilities arising from missing or ineffective security controls

Operational

Malicious or unintentional (erroneous) alteration of root or TLD DNS configuration information

Non-Adversarial Threat Sources

Infrastructure-Related Sources

Key hardware, software or process failure

Predisposing Conditions That Increase Risk

Operational

Chain of trust single point of failure

Technical

Reliance on immature or custom built DNSSEC technologies

Missing or Insufficient Security Controls

Operational Controls

Awareness and Training

Incident Response

System and Information Integrity

Predisposing Conditions That Reduce Risk

Managerial

Managerial vs. operational vs. technical security skills/focus/resources

Security project and program management skills/capacity

Operational

Emphasis on resiliency and redundancy

Diverse operational environments and approaches