# 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

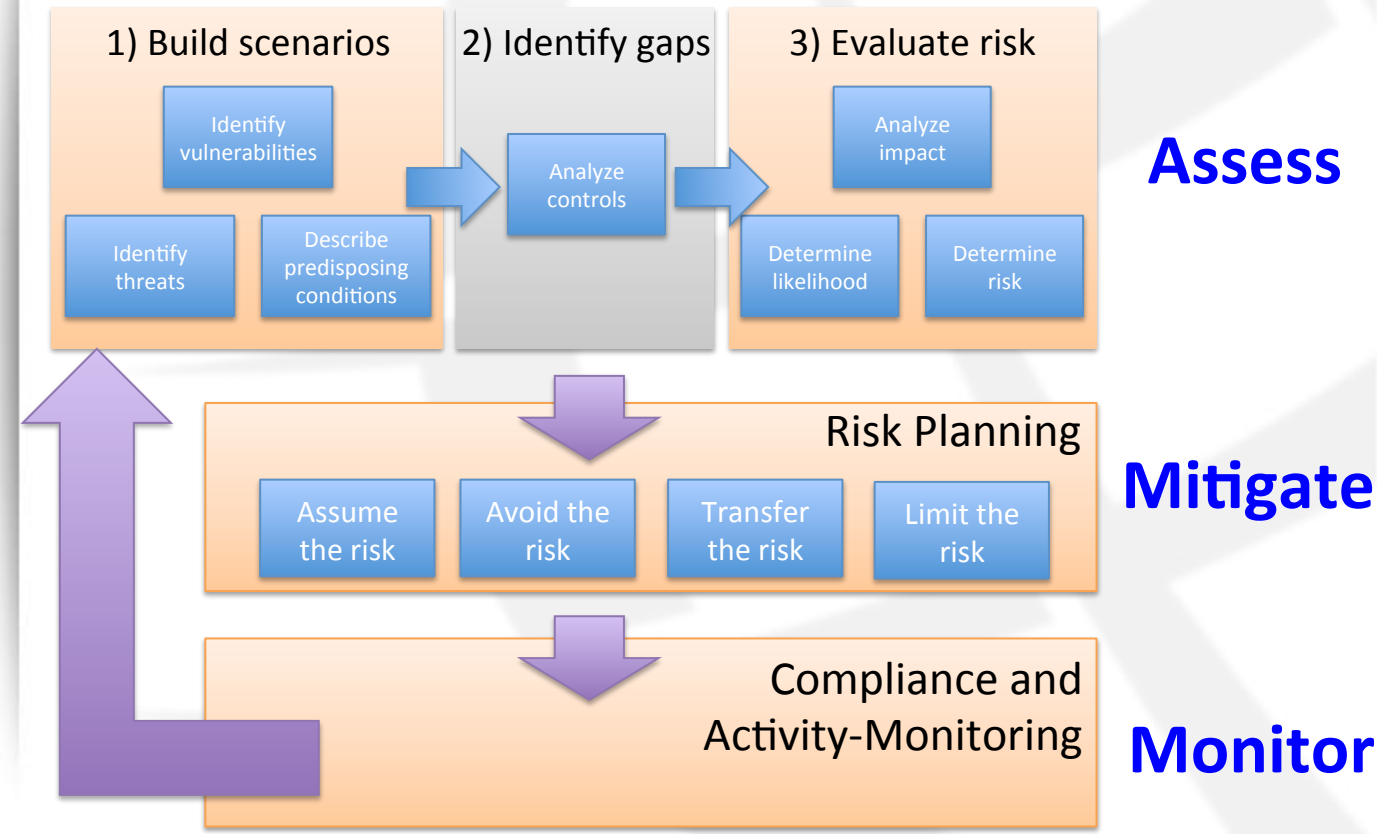
# The DSSA will:

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

# Scope: DSSA & DNRMF

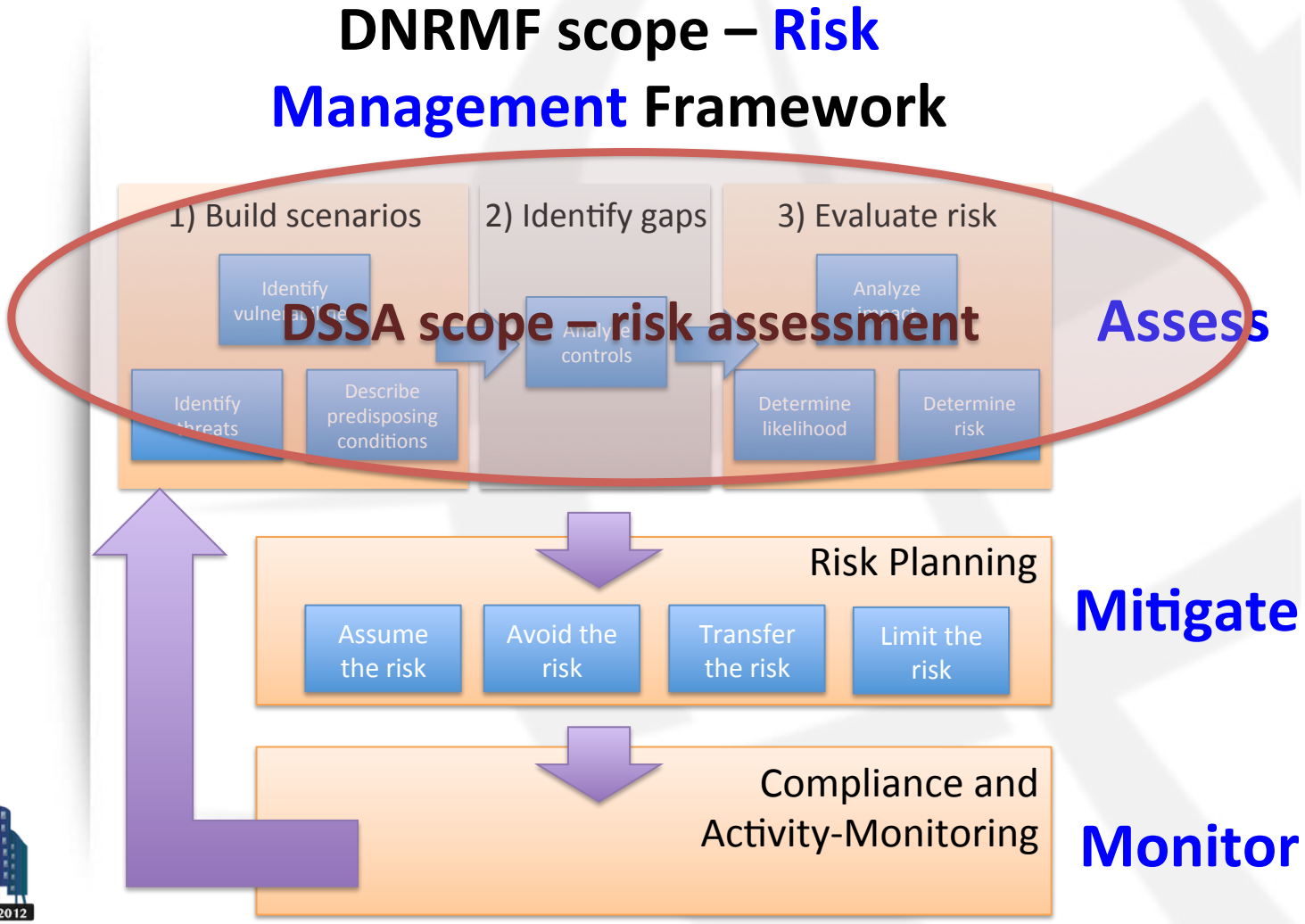
The Board DNS Risk Management Framework working group

## DNRMF scope – Risk Management Framework



# Scope: DSSA & DNRMF

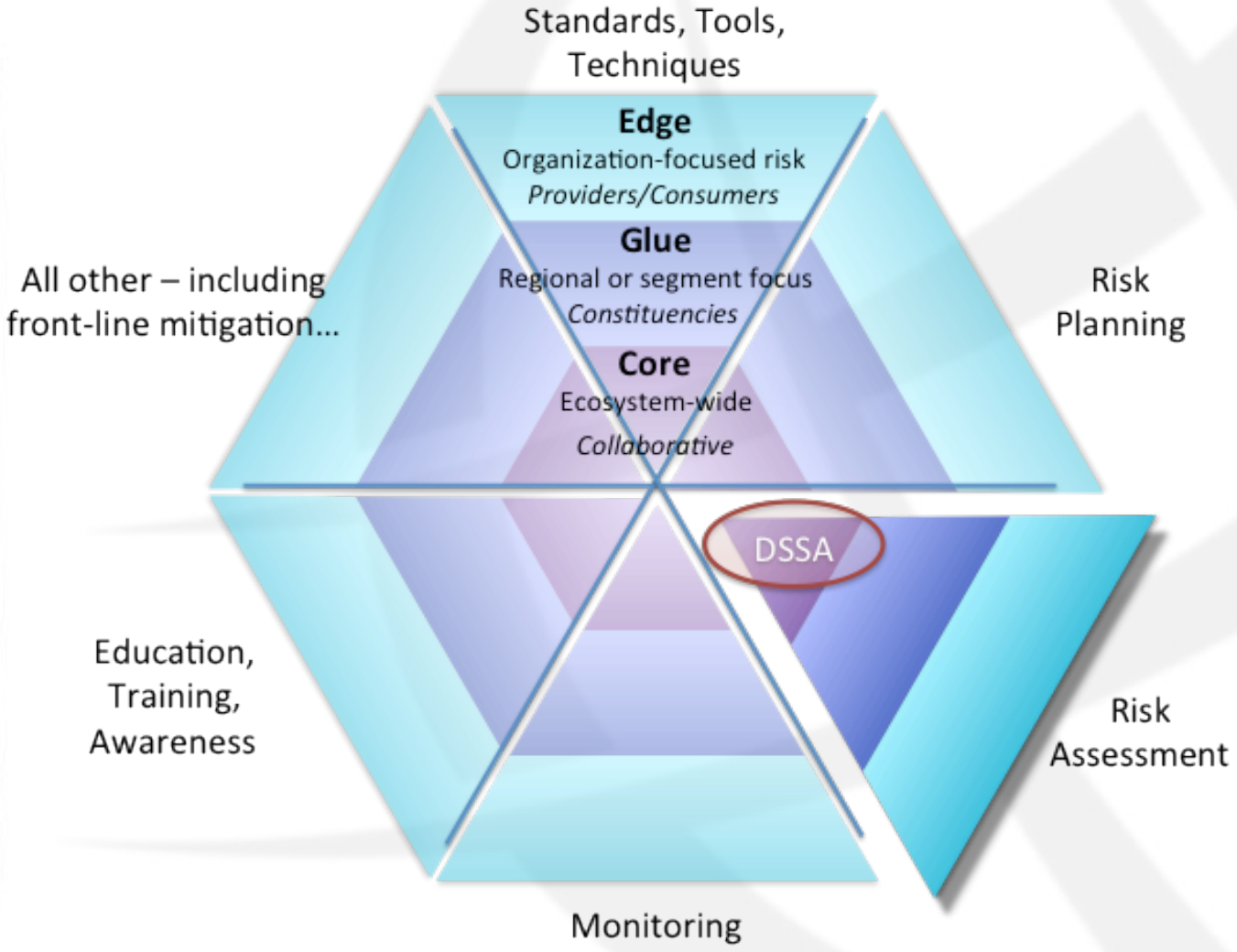
The DSSA is focusing on a subset of that framework



# Scope: DSSA in a broader context

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

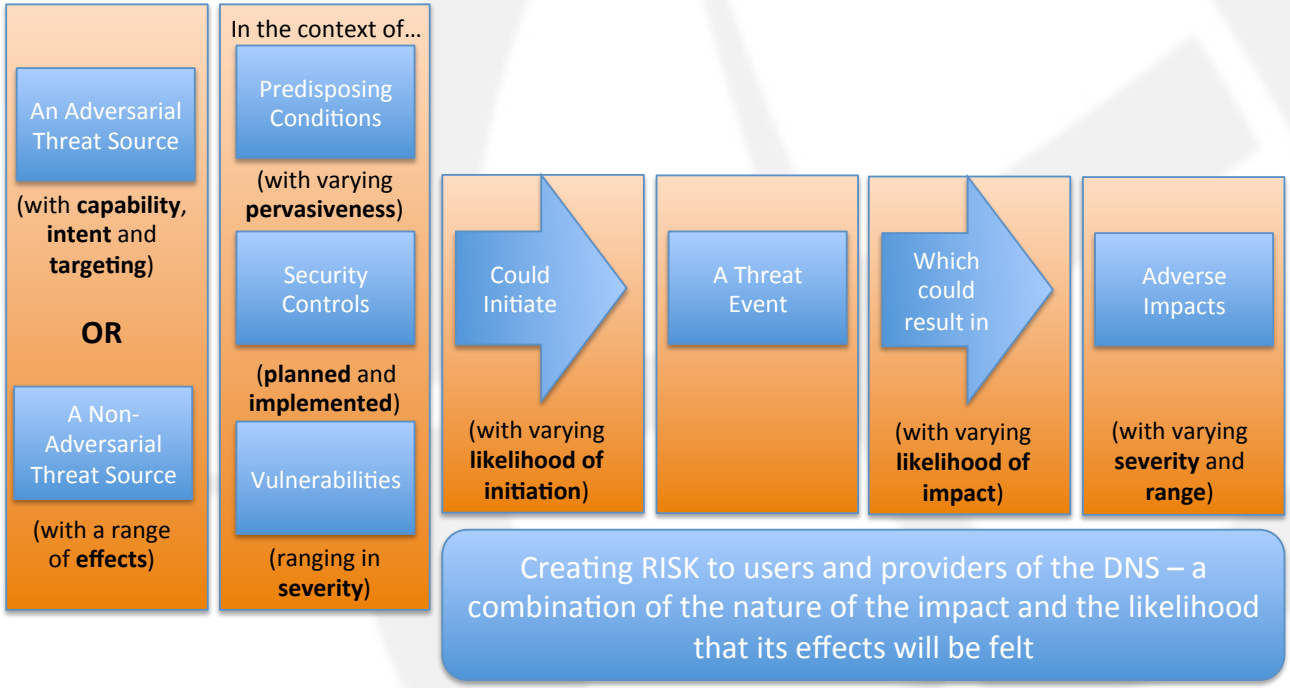
- Backend registry providers
- ccTLD registries
- CERTs
- DNRMF
- DNS-OARC
- ENISA
- FIRST
- gTLD registries
- IANA
- ICANN Security Team
- ICANN SOs and ACs
- IETF
- ISOC
- Network Operator Groups
- NRO
- RSAC
- SSAC
- SSR-RT
- And ???



# “Compound Sentence” Risk Assessment Framework

**Based on NIST 800-30 standard**

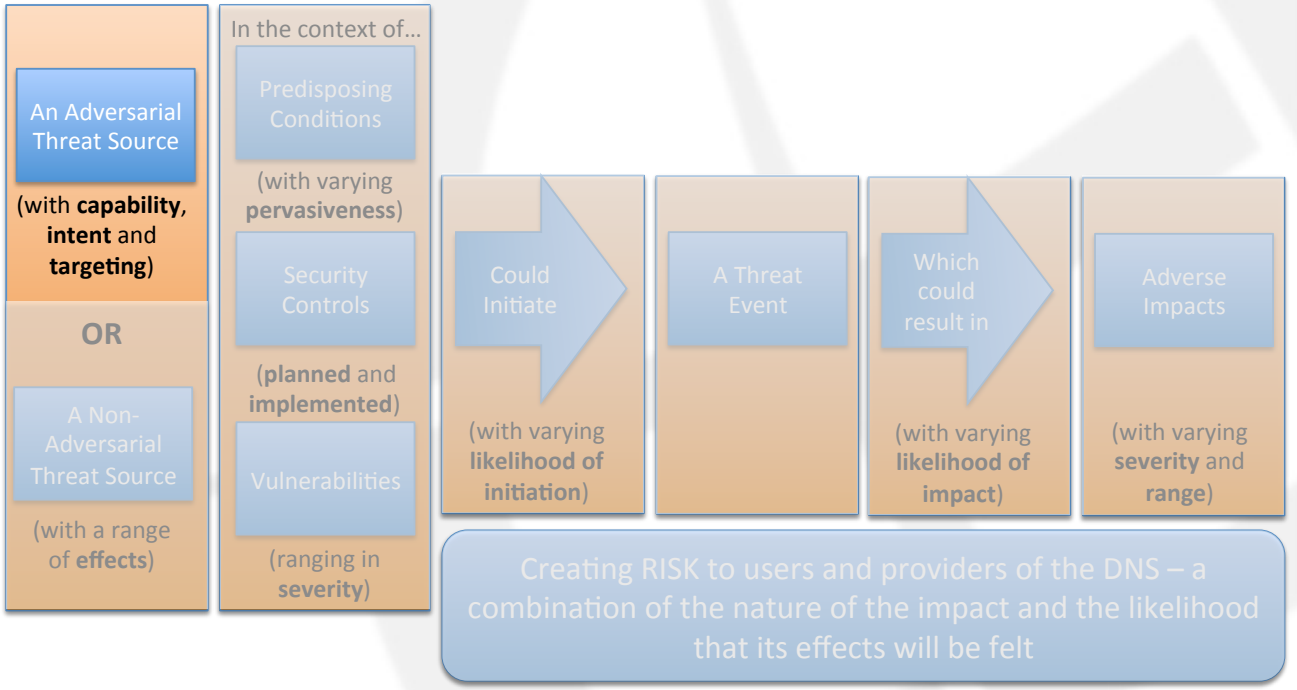
**Tailored to meet unique ICANN requirements**



# “Compound Sentence” Risk Assessment Framework

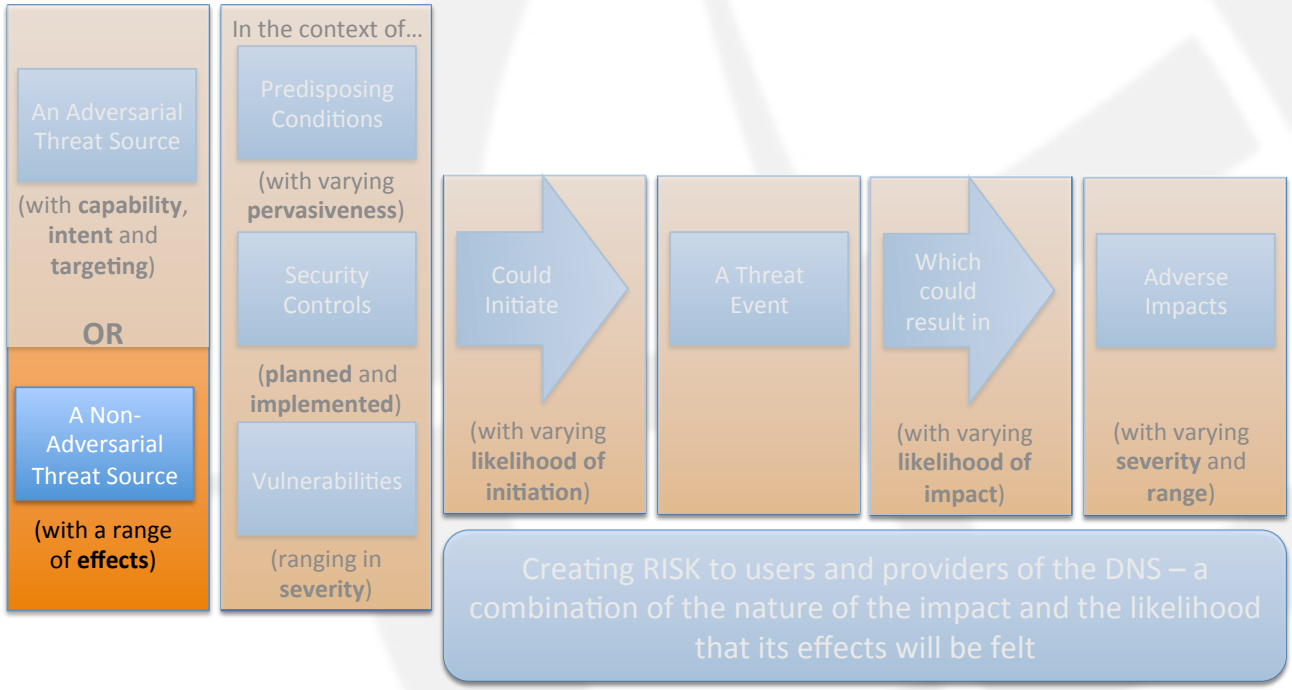
**An adversarial threat-source (with capability, intent and targeting),**

**OR…**



# “Compound Sentence” Risk Assessment Framework

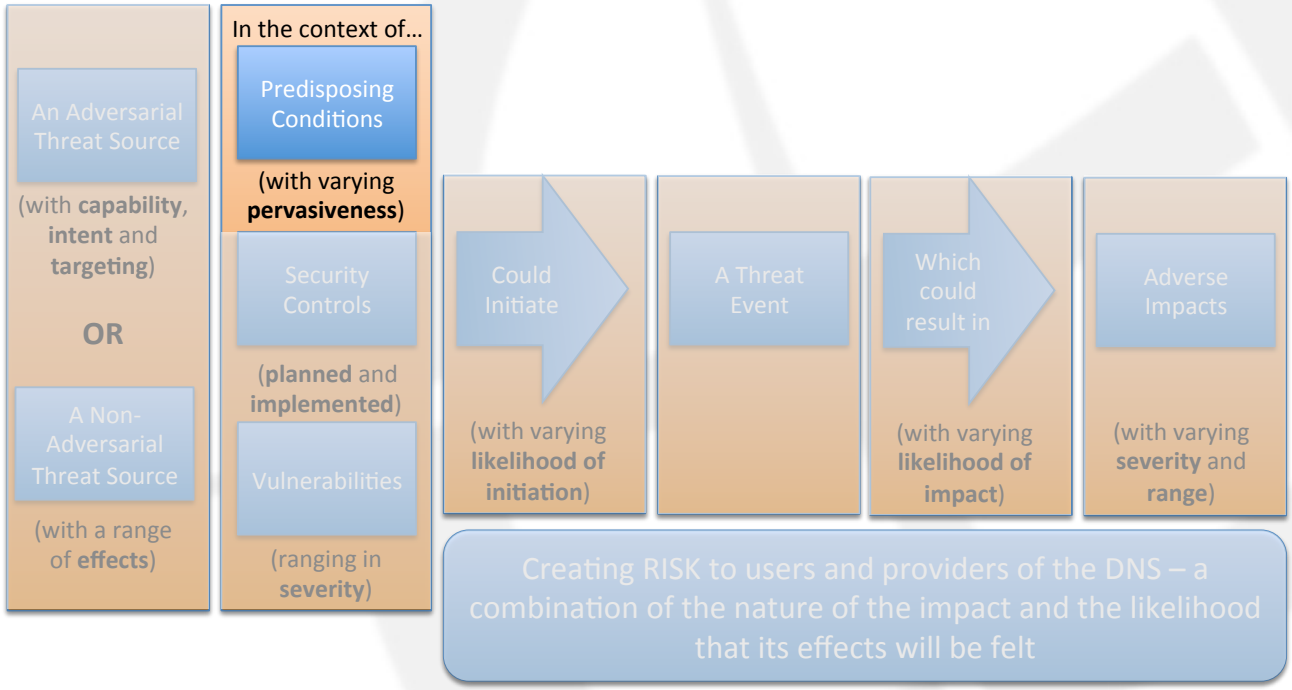
**A non-adversarial threat-source (with a range of effects)…**



# “Compound Sentence” Risk Assessment Framework

**In the context of:**

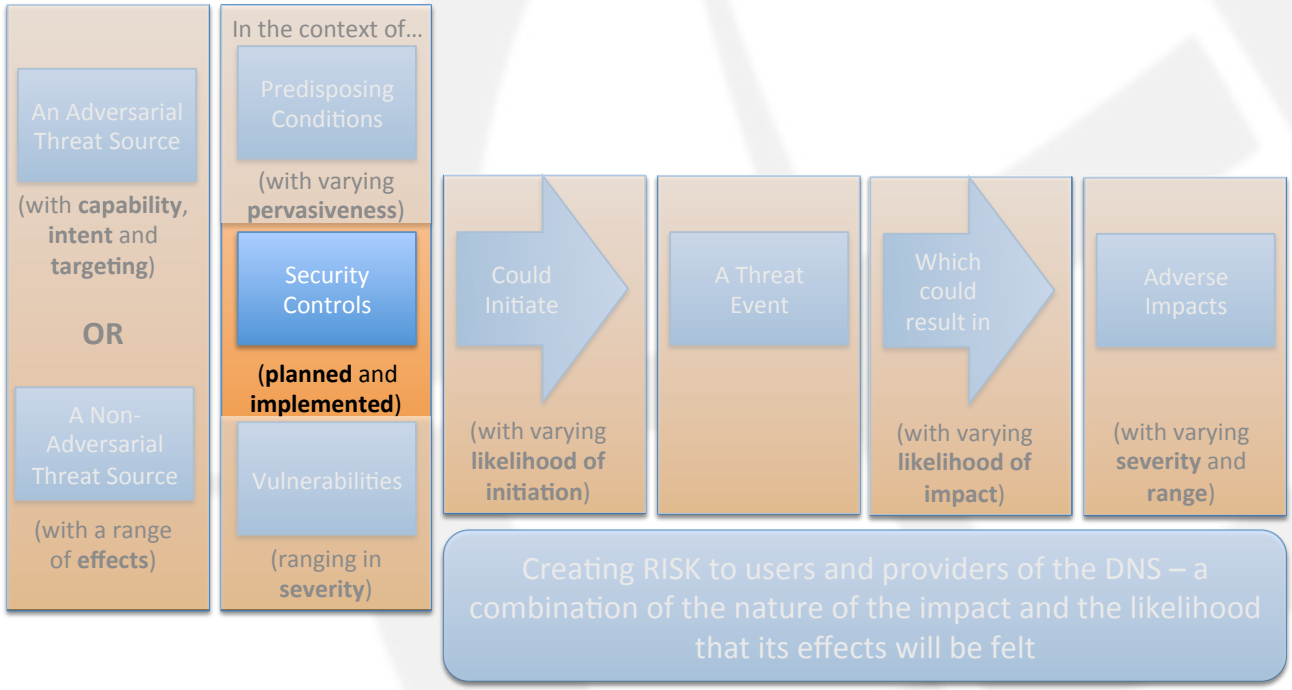
**Predisposing conditions (with varying pervasiveness)…**



# “Compound Sentence” Risk Assessment Framework

**… Security controls (both planned and implemented),**

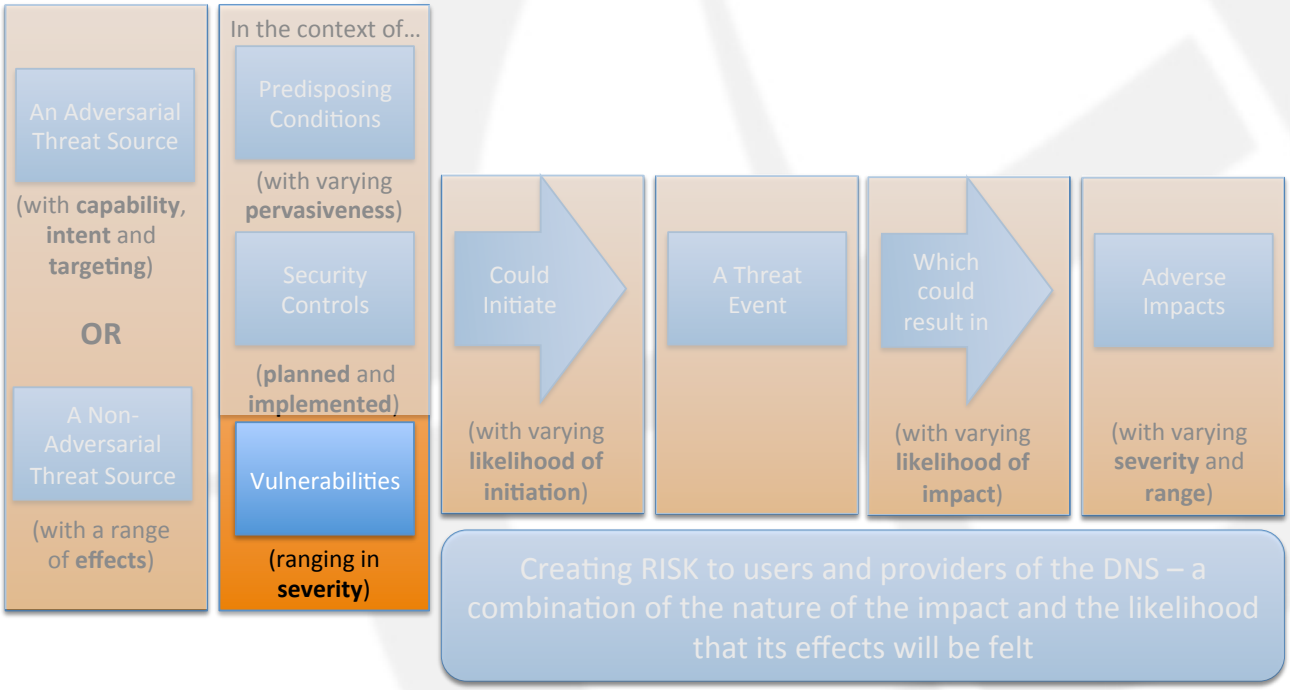
**and…**



# “Compound Sentence” Risk Assessment Framework

…

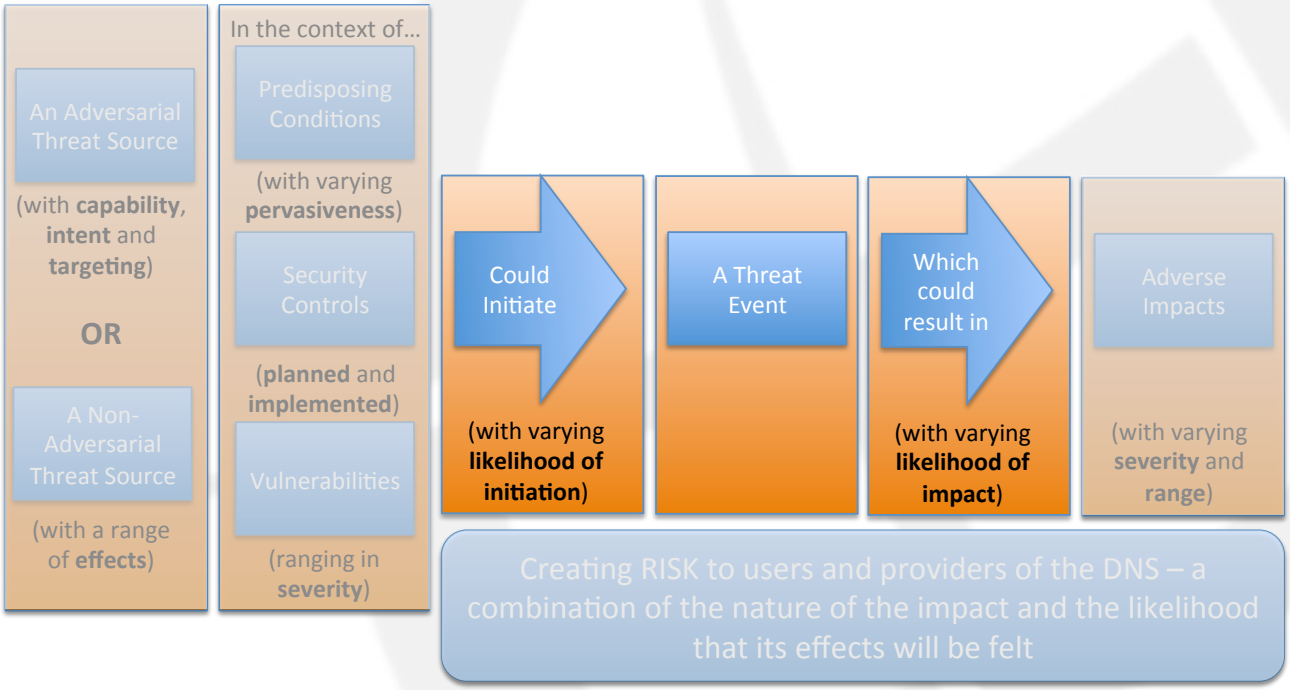
**Vulnerabilities (that range in severity)…**



# “Compound Sentence” Risk Assessment Framework

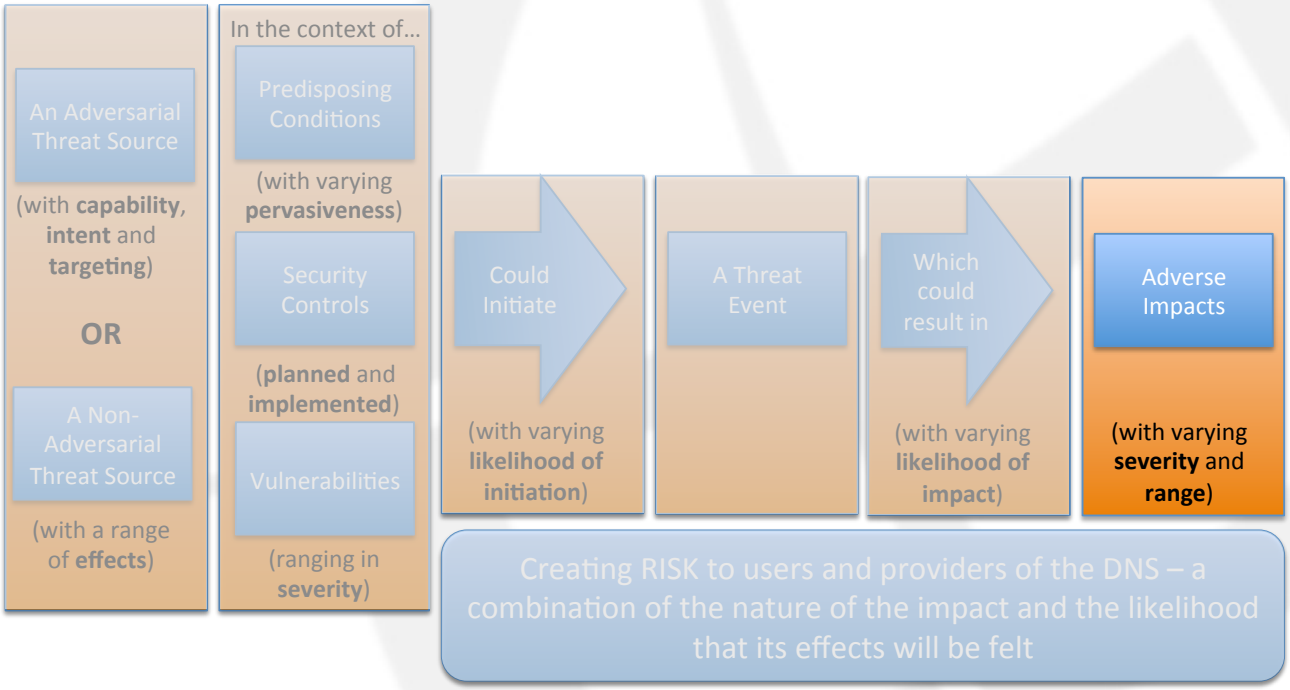
**… Could initiate (with varying likelihood of initiation)**

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



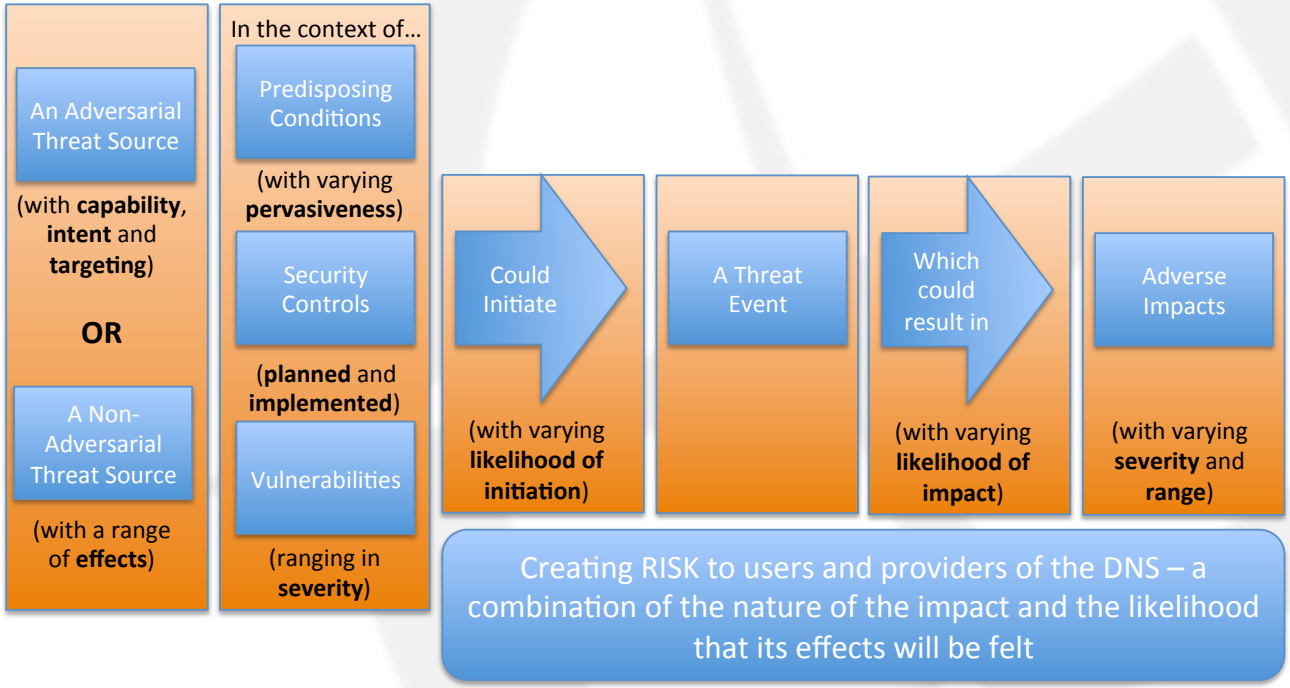
# “Compound Sentence” Risk Assessment Framework

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

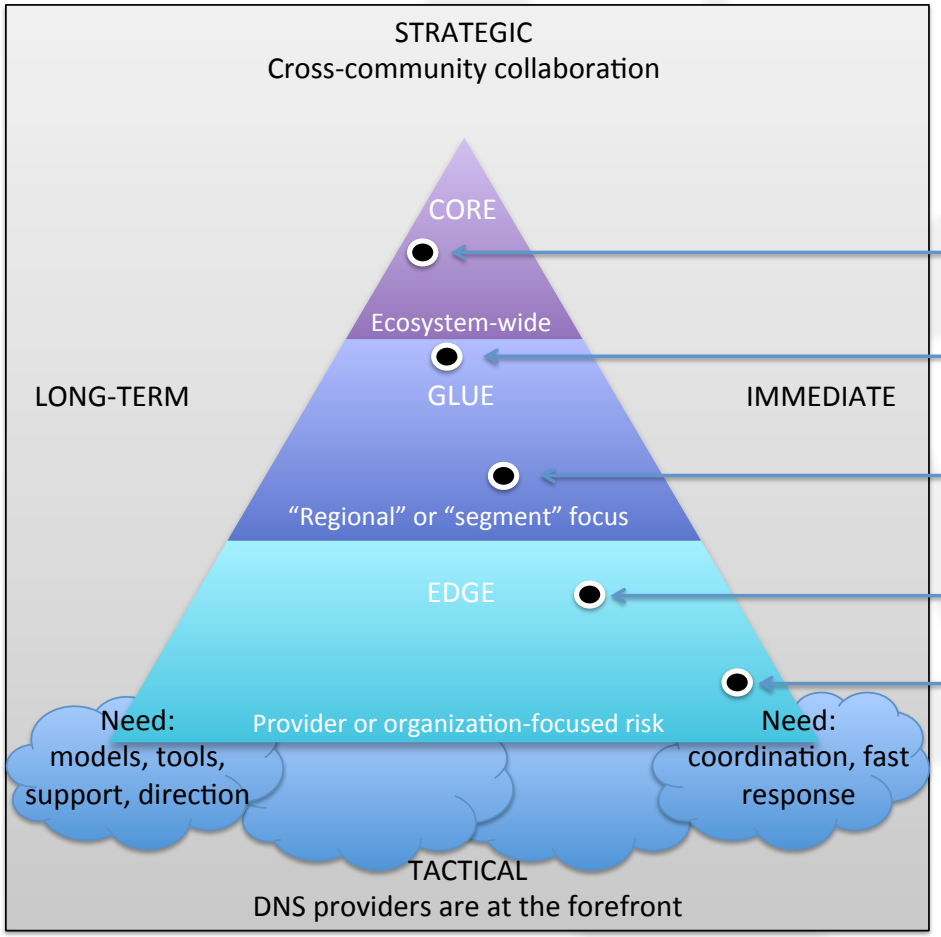


# “Compound Sentence” Risk Assessment Framework

**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.**

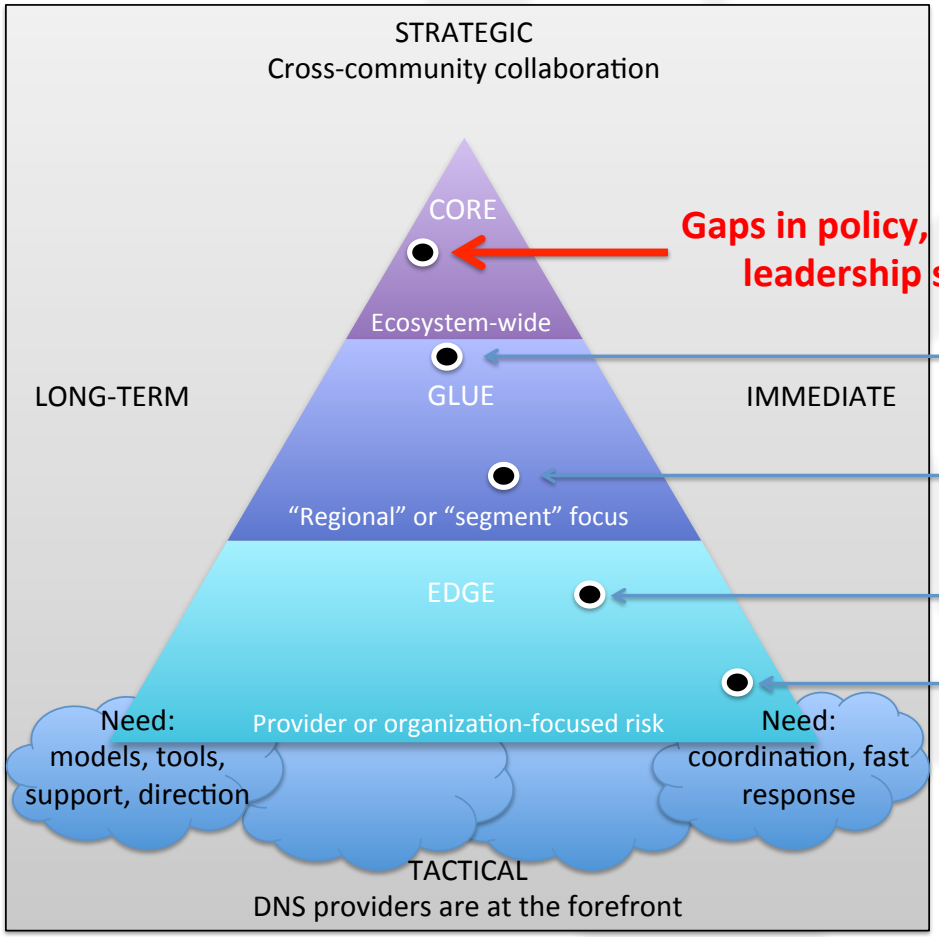


# Findings: 5 Broad Risk Scenarios



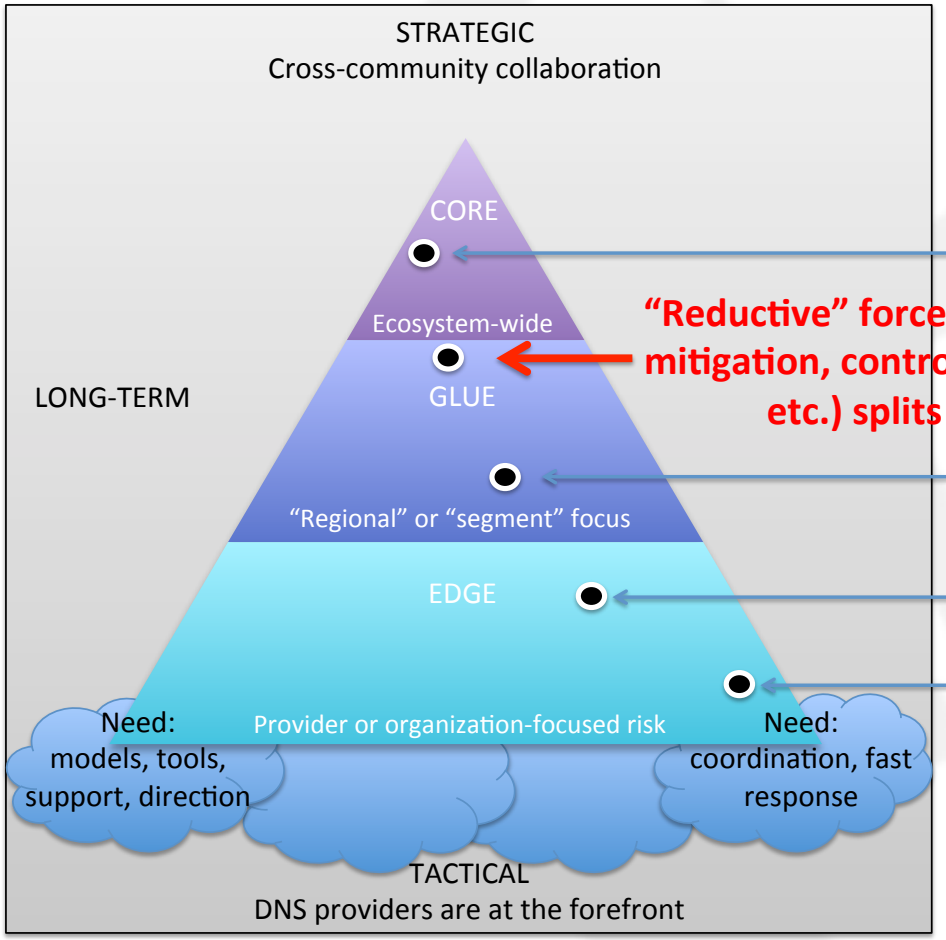
# Findings: 5 Broad Risk Scenarios

**Gaps in policy, management or leadership splits the root**



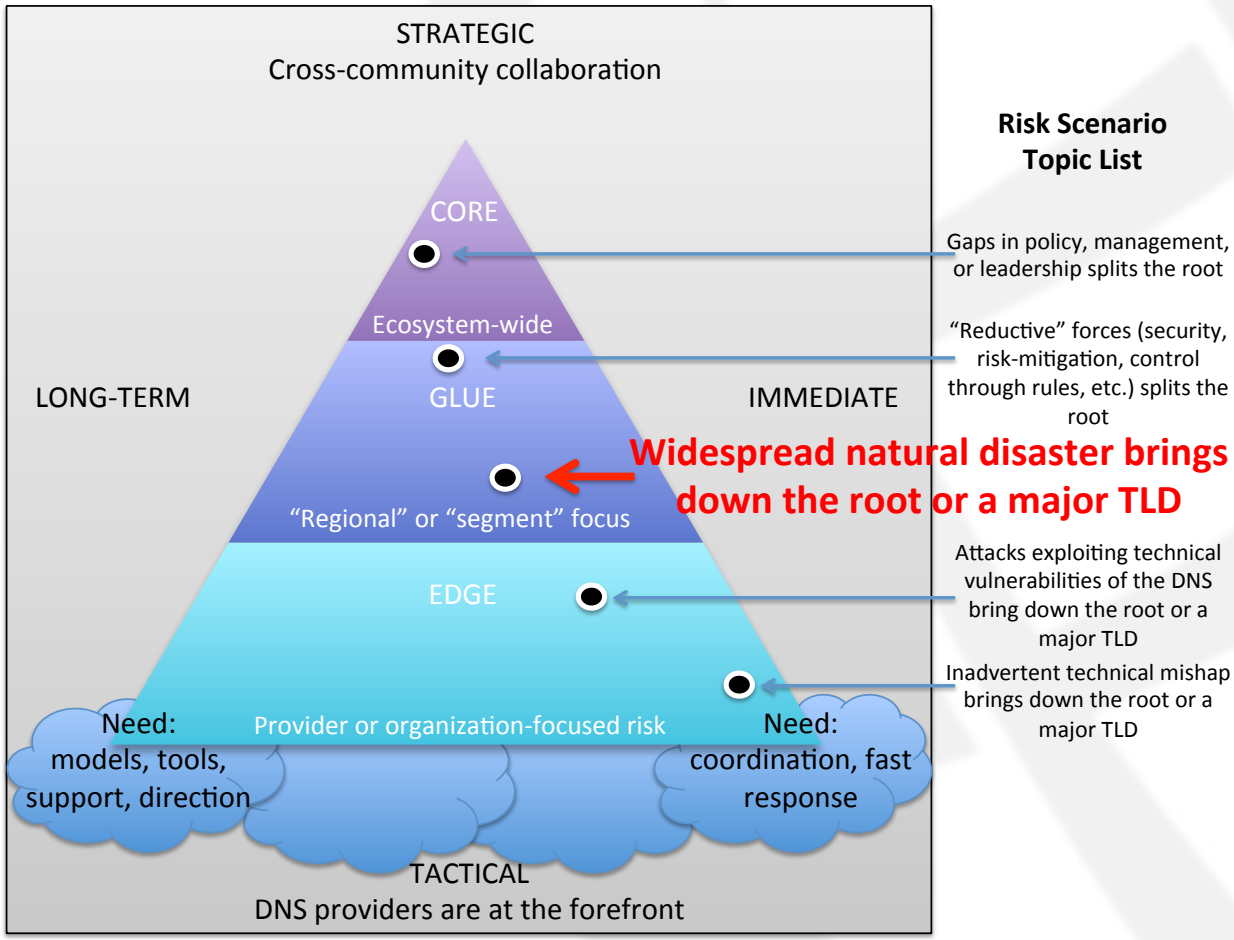
# Findings: 5 Broad Risk Scenarios

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



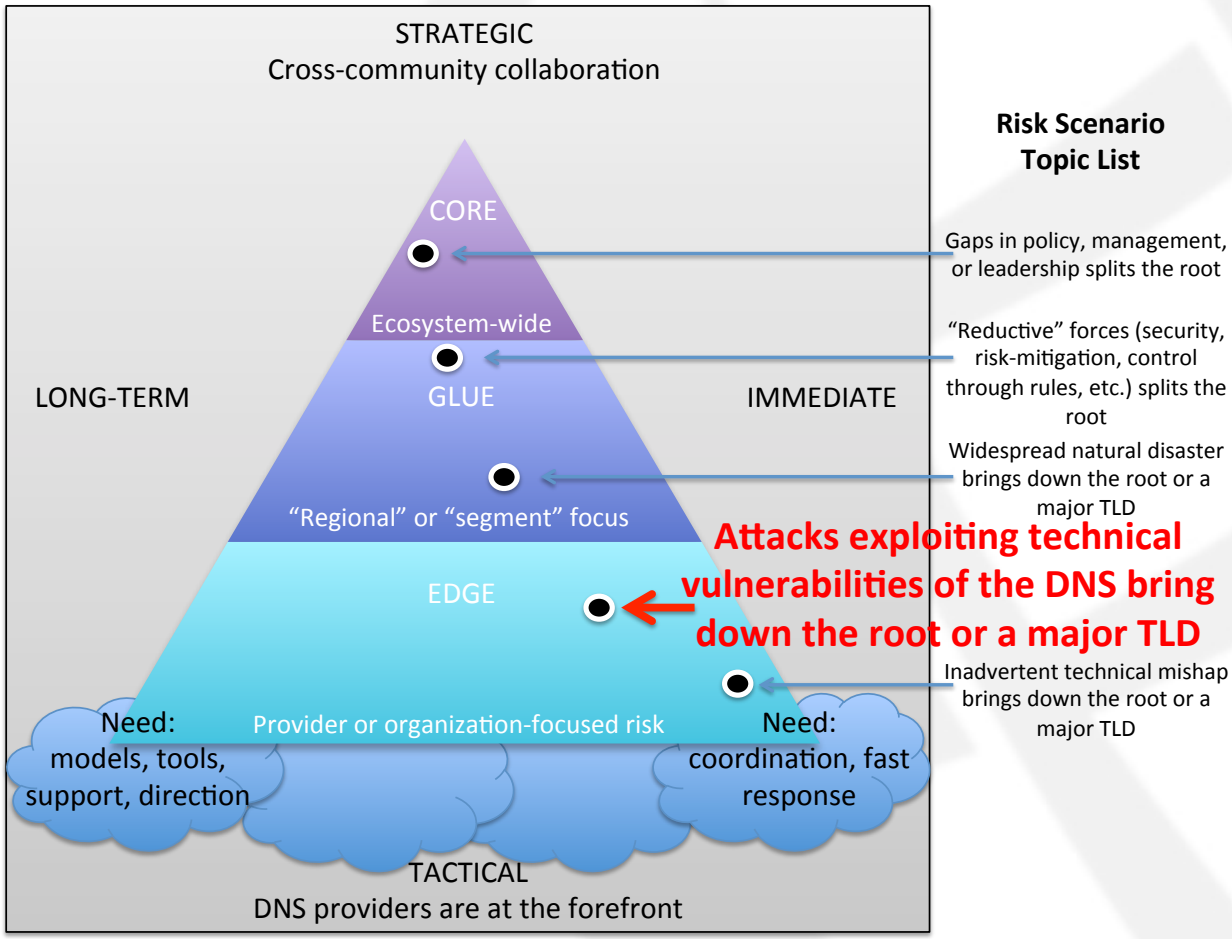
# Findings: 5 Broad Risk Scenarios

**Widespread natural disaster brings down the root or a major TLD**



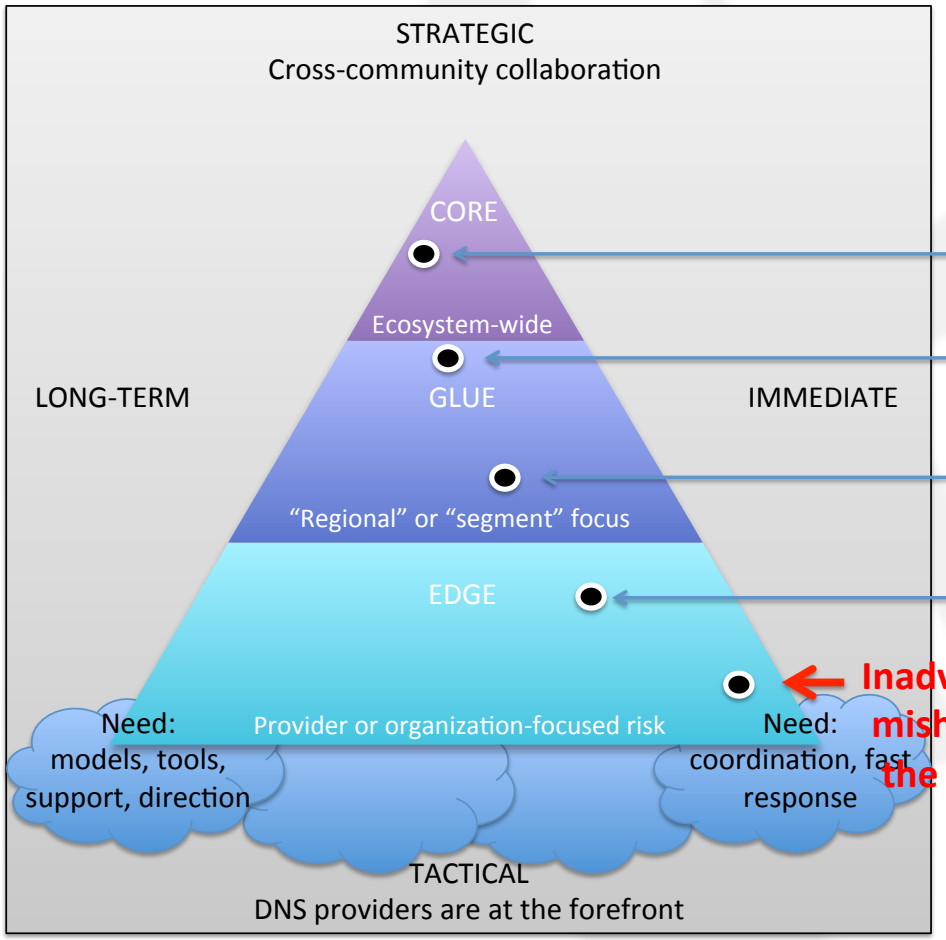
# Findings: 5 Broad Risk Scenarios

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



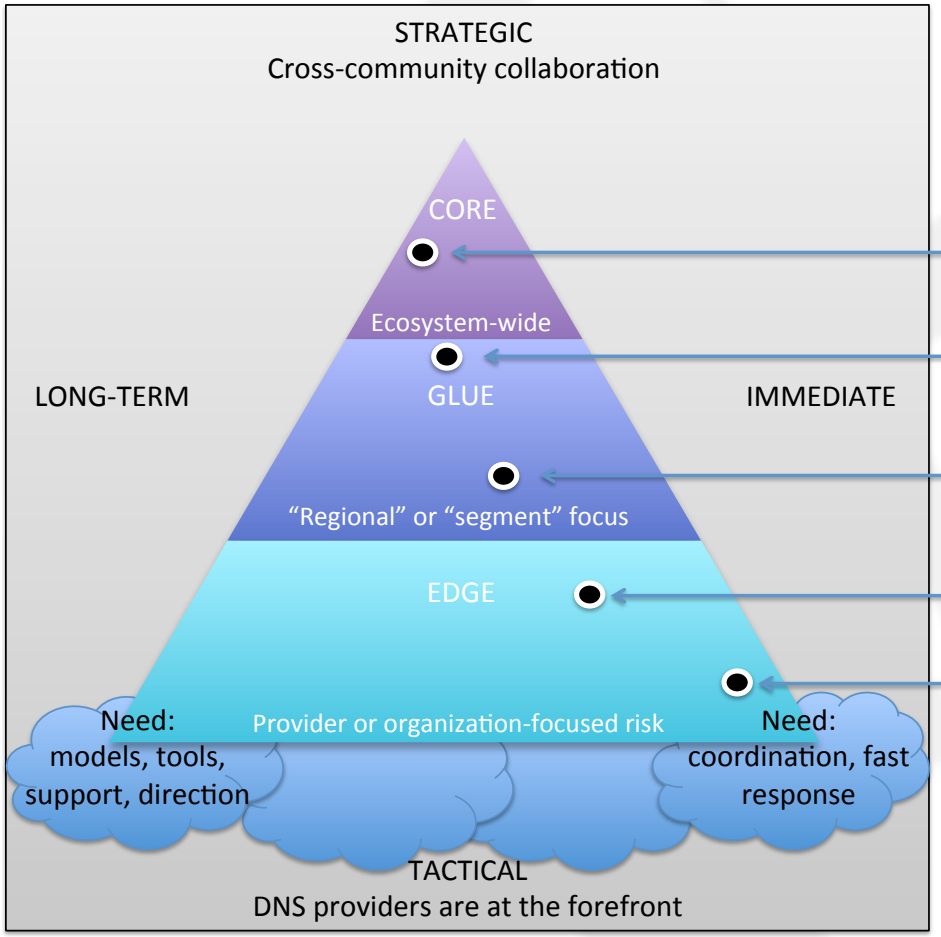
# Findings: 5 Broad Risk Scenarios

**Inadvertent technical mishap brings down the root or a major TLD**



# Next phase

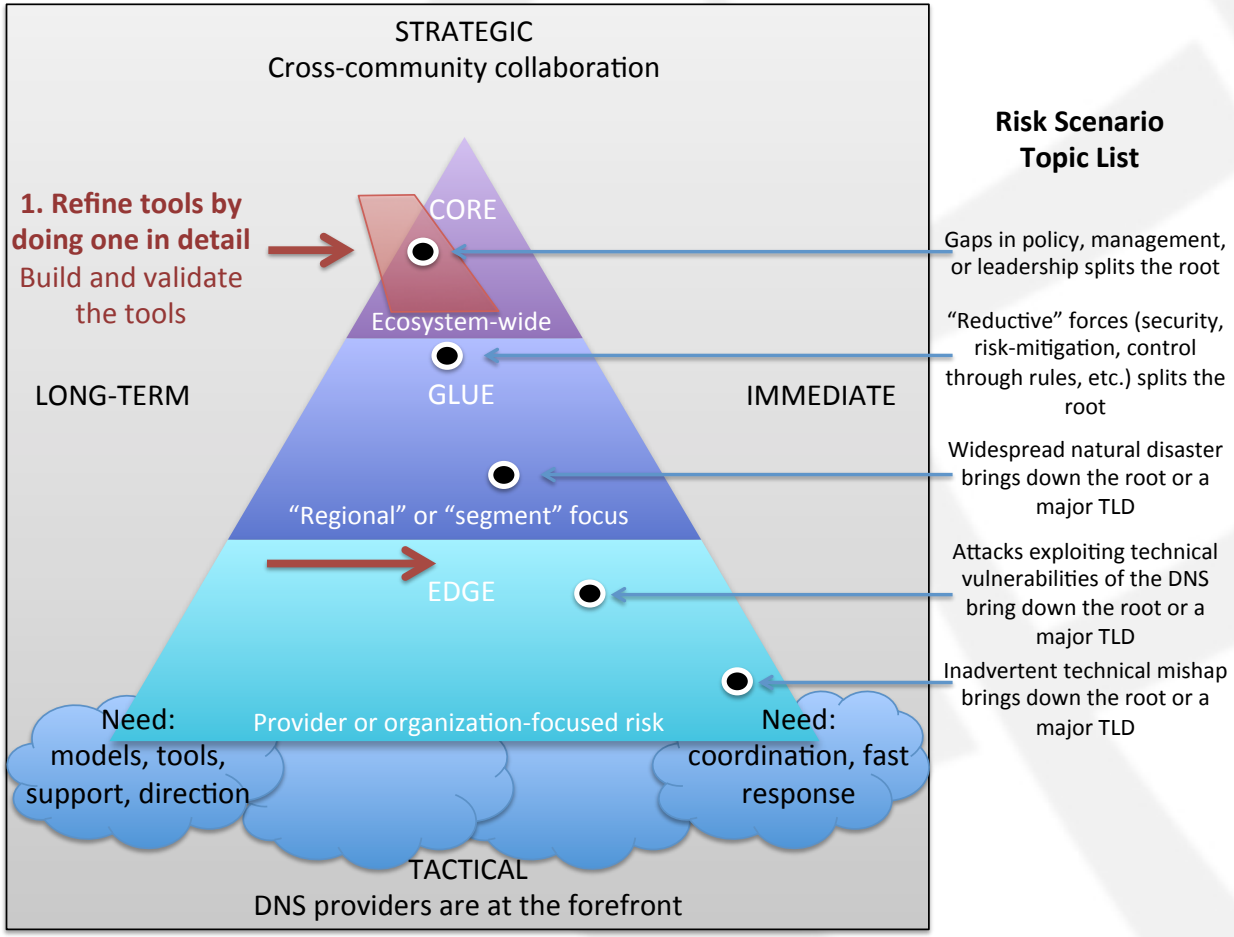
**"Go deep" into the risk topics**



# Next phase

**"Go deep" into the risk topics**

**Refine by doing**

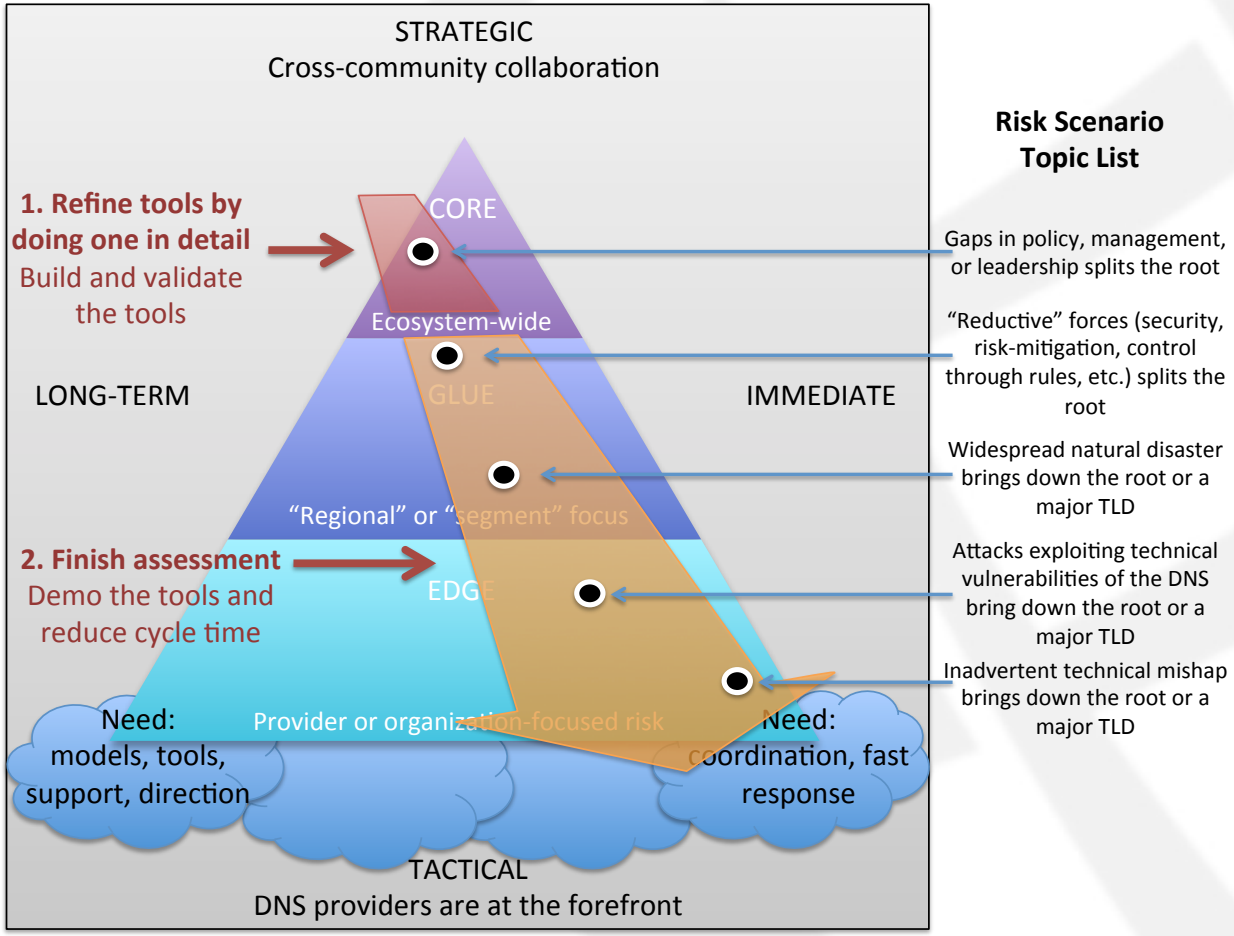


# Next phase

**"Go deep" into the risk topics**

**Refine by doing**

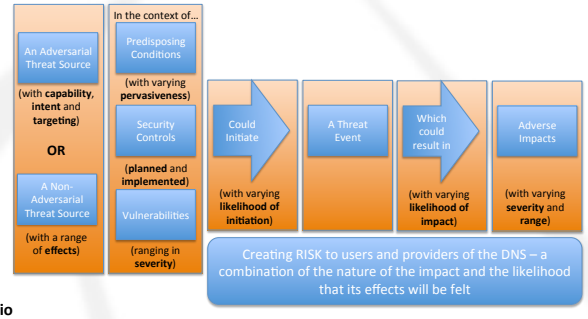
**Finish assessment**

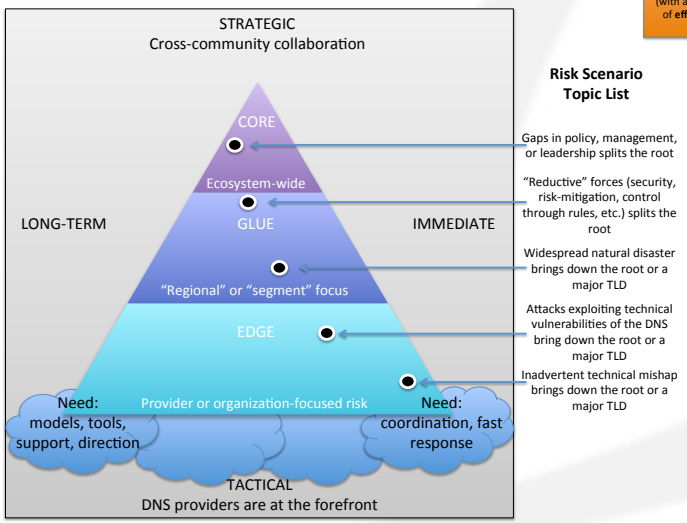


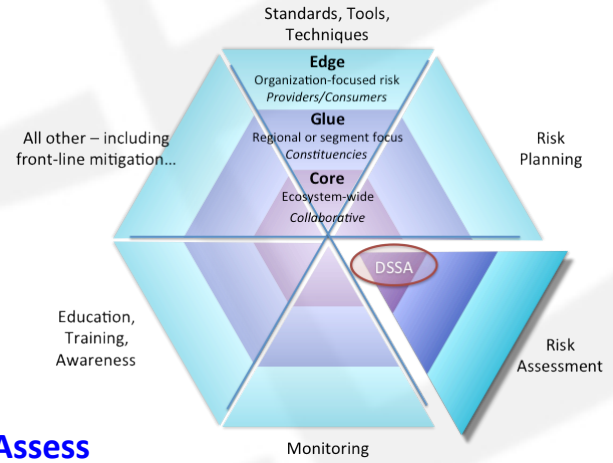
# Questions?

## Are we on the right track?

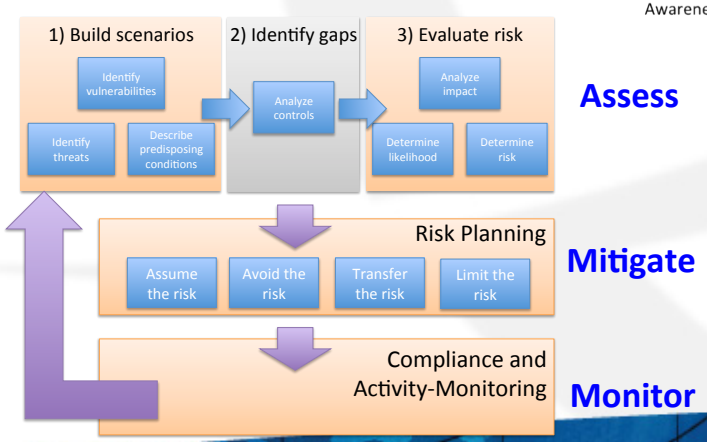
## Have we missed something important?



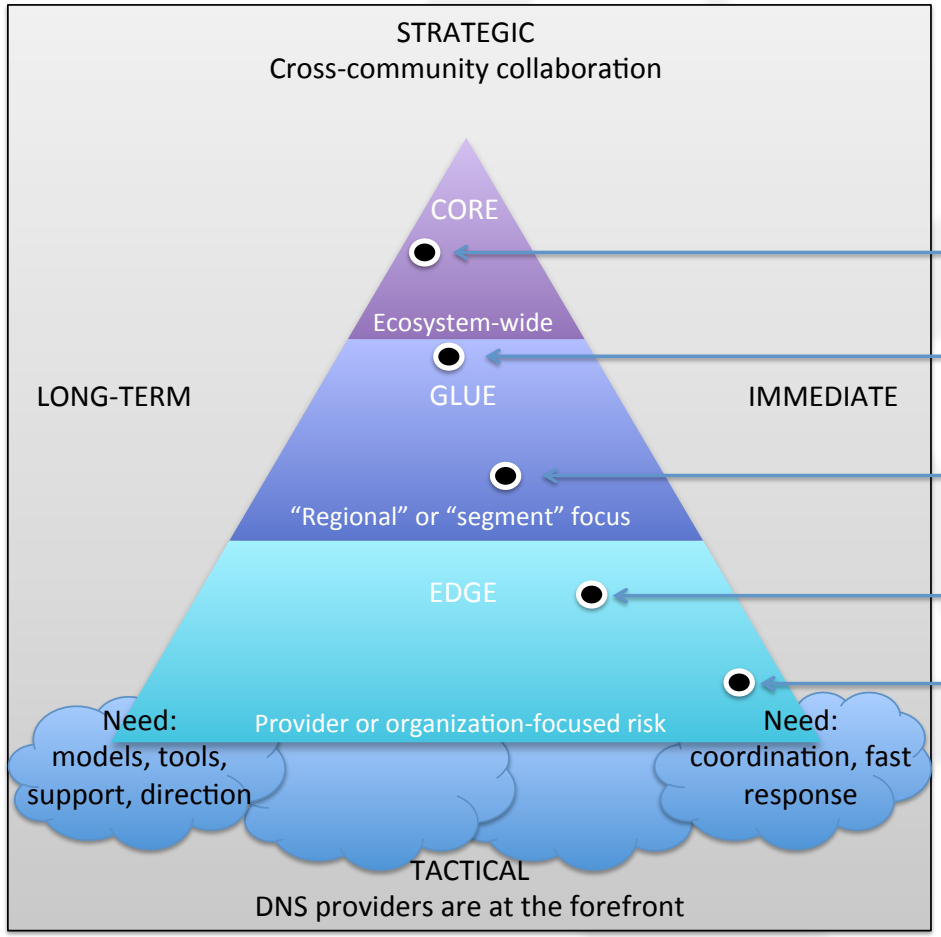

**DNRMF scope – Risk Management Framework**



# 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)**




**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