DSSA Report

1. DSSA Report

2. Executive Summary

3. Background, Charter and Scope

3.1. Events

[Cheryl to develop 1st draft]

3.2. Charter, Scope and Approach

3.2.1. Charter

[insert highlights of charter, not the whole thing. Whole charter can go in Appendix]

3.2.2. Scope

[Introduce the various scope dimensions to the DSSA puzzle – scope of DNS, functional scope, organizational scope]

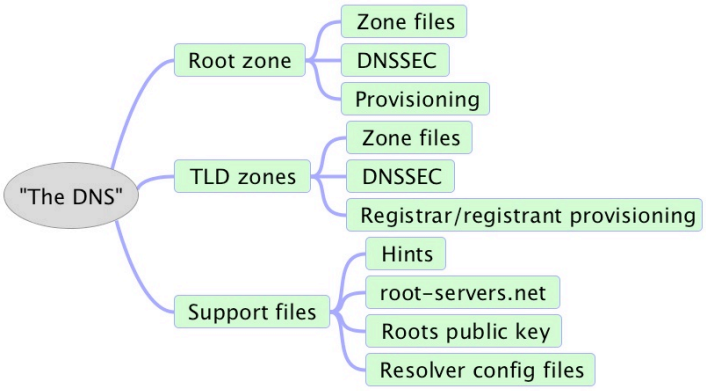
The DSSA had to refine and clarify its scope in three dimensions;

- the scope boundaries of "the DNS" (sometimes called "system boundaries"),
- the functional scope of the effort in the context of a much broader "Security Management" function (that has ICANN-specific elements and broader "DNS" components), and
- the organizational context of the effort (the DNS "ecosystem" and the Board DNS Risk Management Framework working group).

3.2.2.1. Scope of "the DNS" used by the DSSA working group

The DSSA charter states that the working group is to review: "The actual level, frequency and severity of threats to the DNS" but leaves the definition of "the DNS" up to the working group to define. However the charter offers the following additional guidance. "The DSSA-WG should limit its activities to considering issues at the root and top level domains within the framework of ICANN's coordinating role in managing Internet naming and numbering resources as stated in its Mission and in its Bylaws."

The working group arrived at the following definition of "The DNS" for the purposes of this analysis. It needs to be emphasized that this definition is primarily aimed at structuring the work to be done within the limits set by the charter. Broader use of this definition of "the DNS" within the community should be undertaken with caution.



"The DNS" includes:

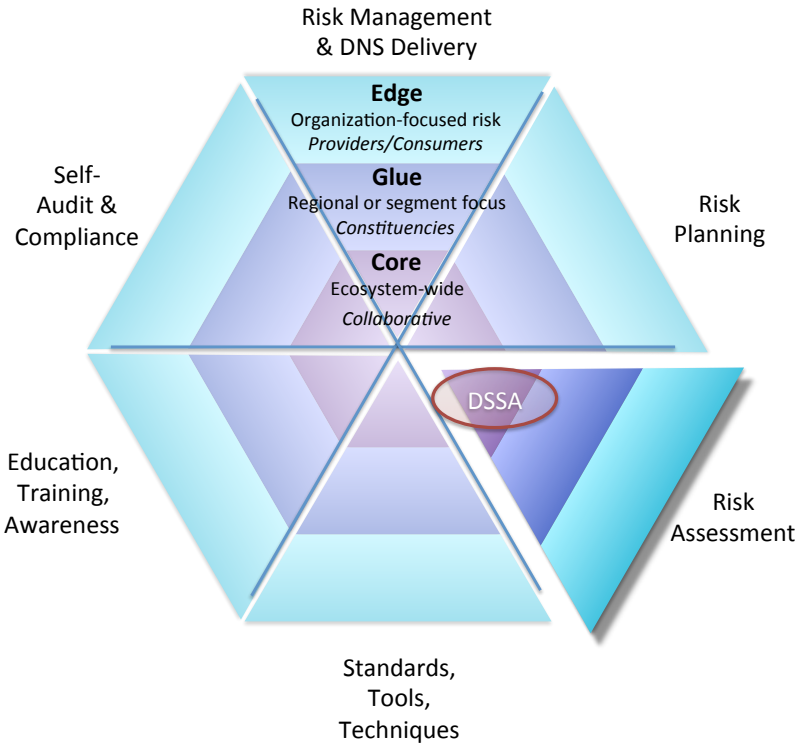
- The Root zone (zone files, DNSSEC and provisioning)
- Top-level domain zones (zone files, DNSSEC and provisioning)
- Support files (e.g. hints, root-servers.net, roots public key, resolver configuration files

Out of scope of this analysis

- 2nd-level zones and lower
- WHOIS
- Zone file access
- Data escrow
- Bulk data access

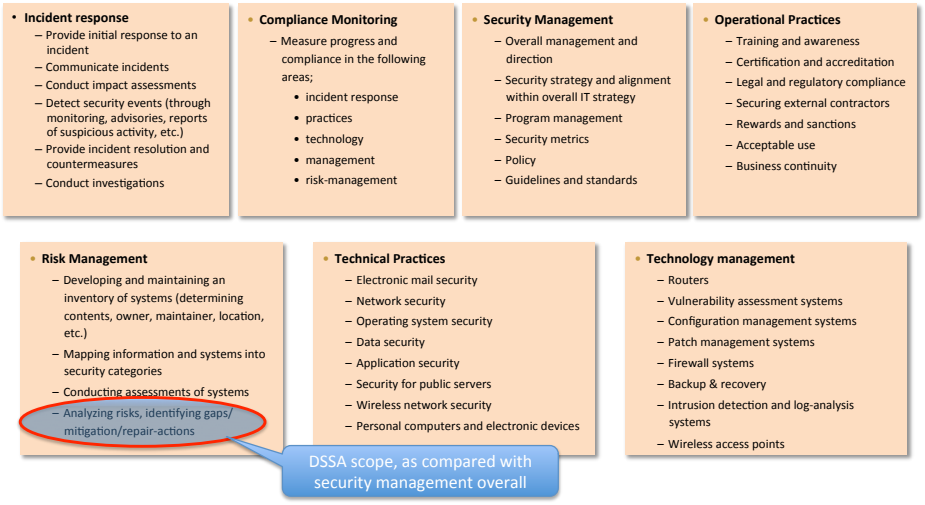
3.2.2.2. DSSA scope – functional context

[develop introduction to the SSR-RT discussion about scope]



The DSSA describes its relationship to the broader DNS security "ecosystem" in two dimensions – it's relationship with day-to-day front-line DNS-delivery and security management (the "core" to "edge" relationship in the diagram above) and the functional scope of its effort (the "spokes" or pie-slices of that same diagram).

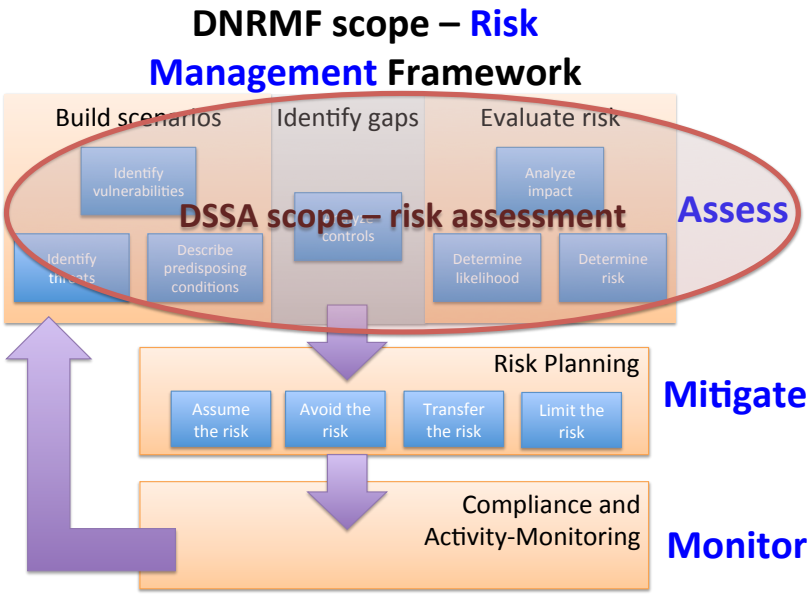
The following diagram attempts to highlight just how narrow the role of the DSSA is when compared to the range of activities addressed by a traditional "Security Management" function in a technical systems organization.



[include a discussion of the "multiple-organization puzzler – all these security-management models are designed for a single organization rather than a collaborative/ecosystem like what we're addressing]

3.2.2.3. DSSA scope – organizational context

3.2.2.3.1. Relationship to the Board DNS Risk Management Framework Working Group



> "The ICANN Board has asked (2011.03.18.07) the Board Governance Committee to recommend to the Board a working group to oversee the development of a risk management framework and system for the DNS as it pertains to ICANN's role as defined in the ICANN Bylaws.
> The purpose of the **DNS Risk Management Framework WG** (DNRMF WG) is to develop goals and milestones towards the implementation of a DNS security risk management framework for Internet naming and address allocation services, accompanied by defined timelines and budgetary implications. Further, the DNRMF WG will oversee the creation of an initial assessment which will serve as a baseline for the task."

[highlight the distinction between "risk assessment" (which is what we're charted to do) and "risk management" (which is a broader topic which includes, but is not limited to, risk assessment)]

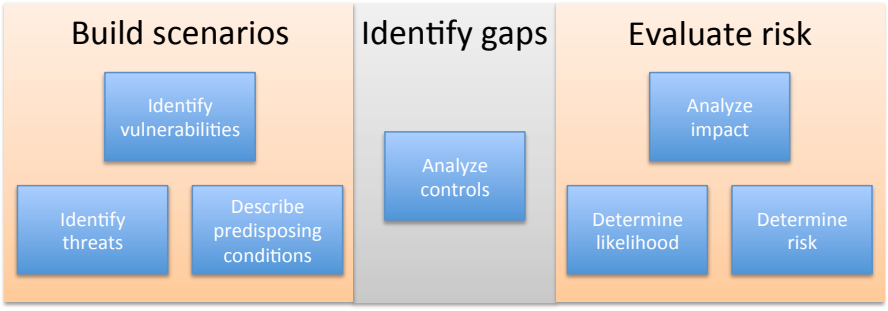
[also note that our charter is to **do** a risk-assessment – the DNRMF charter is to develop goals and milestones to establish a risk-management framework, and oversee a baseline analysis. Scope is broader in two dimensions – the function is broader and the analysis is broader (although DSSA work may contribute to the assessment piece of that broader baseline effort).]

[we needed to select and tailor a risk-assessment methodology in order to complete our work, which may prove to be a useful contribution to the broader risk-management work of the DNRMF – but it should not be considered preemptive.]

3.2.3. Analysis approach

The working group has tailored NIST methodologies (800-30 risk-assessment and NIST 800-53a controls-assessment) into a series of "compound-sentence" risk scenarios to define the starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.

While not a part of its charter, the working group needed to define a risk assessment framework in order to complete its work. That framework, documented in a later section of this report and detailed in the Appendix, may be information that more specialized teams (and other organizations) can use in the future to develop additional scenarios or analyze already-identified scenarios in more depth.



See [section ___] for a detailed description of the methods that were selected, refined and used by the working group to structure this process.

4. Findings

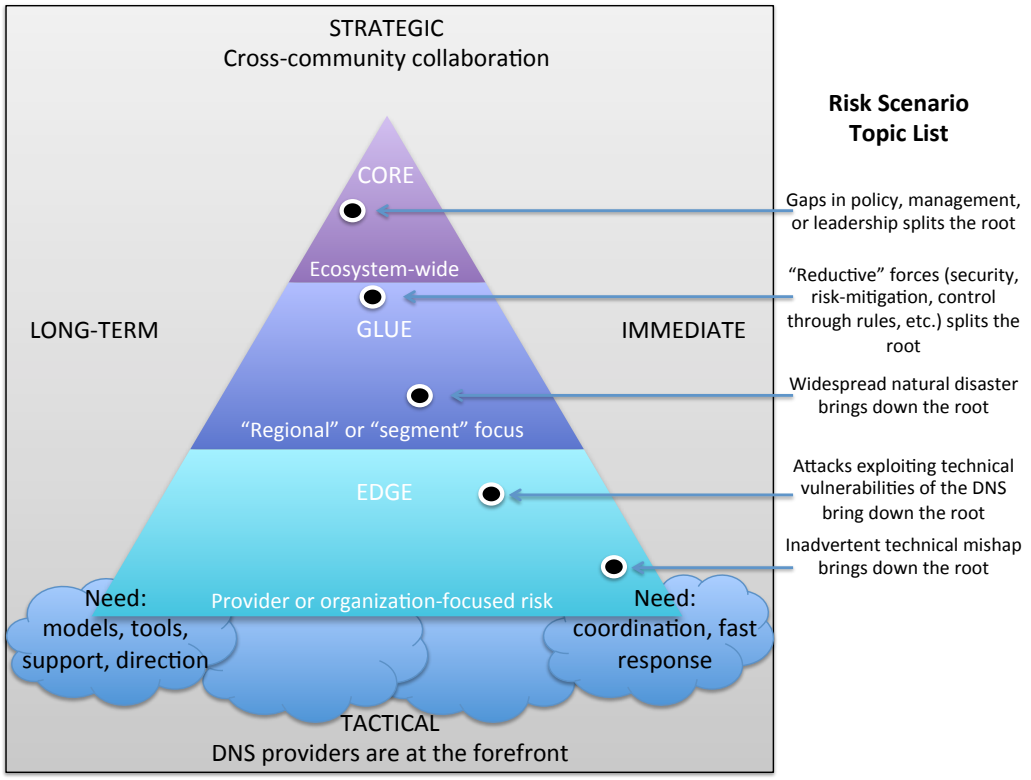
4.1. Overview

[Things to highlight

The assessment of "risk" depends on your point of view; one size does not fit all organizations in the DNS-providing ecosystem. Thus, one of the most helpful deliverables of the DSSA may well be a risk-assessment framework and methodology that can be readily understood and used by a variety of organizations to assess DNS risk from their own unique perspective.

Describe the difference between this "go fast" phase report and the "go deep" report(s) that follow. We focused on pushing the "process" deliverables, along with the assessment of "interesting areas for further study," out in this phase.]

4.2. Actual level, frequency and severity of threats to the DNS, plus current efforts and activities to mitigate these.



The working group has developed five broad risk scenarios that will be used to structure the deeper analysis in the next phase of its work. These are listed here, and presented in detail in Appendix [___].

Adversarial risk scenarios

- Gaps in Policy, Management, Leadership Issues Lead to Splitting the Root
- "Reductive" Forces (Security, Risk-mitigation, Control through rules, etc.) Lead to Splitting the Root
- Attacks Exploiting Technical Vulnerabilities of the DNS

Non-Adversarial Risk Scenarios

- Impacts of Natural Disasters
- Inadvertent Technical Mishaps

The DSSA is very interested in community reaction to these scenarios and especially interested in identifying scenarios that have been overlooked.

These scenarios outline the shape of the analysis that the DSSA will do next. We view this as the preliminary topic-list and will "go deep" in defining and assessing these scenarios in the next phase of our work.

We are especially interested in hearing from the community as to whether we have <u>missed</u> any major risk-scenarios. Please read this section with that request in mind and consider forwarding your suggestions to the DSSA directly.

If you are concerned that simply describing a particularly embarrassing scenario might reveal confidential information about you or your organization, [Paul Vixie] has volunteered to act as an intermediary to enter into a confidentiality agreement with you and "anonymize" your suggestion. Contact information for the DSSA [and Paul] is contained in the Appendix.

4.3. Current efforts and activities to mitigate these threats to the DNS

[Much of this may have to wait until next phase – when we go deep]

[Need to build this into the risk-assessment framework – perhaps in addition to the "sources of information" column on the worksheet for now]

[May be able to draw on the lists from the SSR Framework]

[May be difficult to build a "unified" view of all of the activity –due to the number of different organizations involved, because much of that work is confidential, because it is rapidly evolving]

> [We may want to come up with several perspectives on this section of the report – root-server operators, gTLD operators, ccTLD operators and ICANN.]
>
> [Coordinated and accessible view vs "unified" view – closer to the actual intent]

4.4. Gaps in current response to DNS issues

Pay special attention to the "Controls" portion of the analysis -- missing or inadequate managerial, operational or technical controls should be highlighted

[Much of this may have to wait until next phase -- when we go deep]

[May find a number of organizational-response topics in SSR-RT report]

Take note of the different perspectives and situations that various DNS providers experience with regard to risk, resources and responses. Our charter implies that the DSSA is supposed to develop a unified view of "threats to the DNS." In fact, this may be very difficult (and perhaps counterproductive) to do. [Coordinated and accessible view vs "unified" view – closer to the actual intent]

Root server operators, TLD providers vary rather dramatically in a number of dimensions (e.g. resources, reach, etc.). The DSSA is arriving at the conclusion that one size may not fit all, and that assessment mechanisms may need to be developed that take this diversity into account.

[We may want to introduce the goal of arriving at several perspectives on this section of the report – root-server operators, gTLD operators, ccTLD operators and ICANN.]

4.5. Possible additional risk mitigation activities that would assist in closing those gaps

- Ongoing roles and responsibilities
- Risk assessment methodology
- Clarify responsibilities and accountability between ICANN and others in the security community

[draw on SSR-RT report for some more ideas – here's a starter-list from their report]

> RECOMMENDATION 1: ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement.
>
> RECOMMENDATION 3: ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN community in order to provide a single focal point for understanding the interdependencies between organizations.
>
> RECOMMENDATION 4: ICANN should use the definition of its SSR relationships to encourage broad engagement on SSR matters using this to create an effective and coordinated SSR approach.
>
> RECOMMENDATION 12: ICANN should support the development and implementation of SSR-related best practices through contracts, agreements, MOUs and other mechanisms.
>
> RECOMMENDATION 13: ICANN should encourage all Supporting Organizations to develop and publish SSR- related best practices for their members.
>
> RECOMMENDATION 15: ICANN should publish information about DNS threats and mitigation strategies as a resource for the broader Internet community.
>
> RECOMMENDATION 16: ICANN should continue its outreach efforts to expand community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.
>
> RECOMMENDATION 14: ICANN should ensure that its SSR related outreach activities continuously evolve to remain relevant, timely and appropriate. Feedback from the community should provide a mechanism to review and increase this relevance.
>
> RECOMMENDATION 23: ICANN must provide appropriate resources for SSR-related working groups and advisory committees, consistent with the demands place upon them. ICANN also must ensure decisions reached by working groups and advisory committees are reached in an objective manner that is free from external or internal pressure.

5. Approach to the work, this phase and in the future

5.1. Approach Hybrid go fast, then go deep

[Describe "gofast" vs "godeep"]

Go back to the AC/SOs at the end of the first pass for instruction on what to do in the next phase (build a proposal for next-phase towards the end of this one)

Come up with a good name for the report -- preliminary/summary/phase-1/??

5.2. During this "go fast" iteration

5.2.1. Methods – rationale, selection, risk model and tailoring

[replace these details with a summary here – move the details of the selection and rationale into an appendix]

5.2.1.1. Rationale

Using a predefined methodology will save time and improve our work product

- Consistent terminology
- Shared model
- Structured work
- Sample deliverables

Reviewed several dozen alternatives -- We selected this one because it's:

- Available at no cost
- Actively supported and maintained
- Widely known and endorsed in the community
- Reusable elsewhere in ICANN

5.2.1.2. Selection

Methods evaluated

- A&K Analysis - ISO 17799
- Austrian IT Security Handbook
- BSI - IT-Grundschutz
- EBIOS - ISO 17799
- Hazard Analysis -- Critical Control Point (HACCP)
- HITRUST Common Security Framework
- ISAMM
- ISO/IEC 13335-2 (27005)
- ISO/IEC 17799
- ISO 27000 series
- ISO 31000 series
- Marion
- NIST 800-30
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

5.2.2. Risk assessment framework

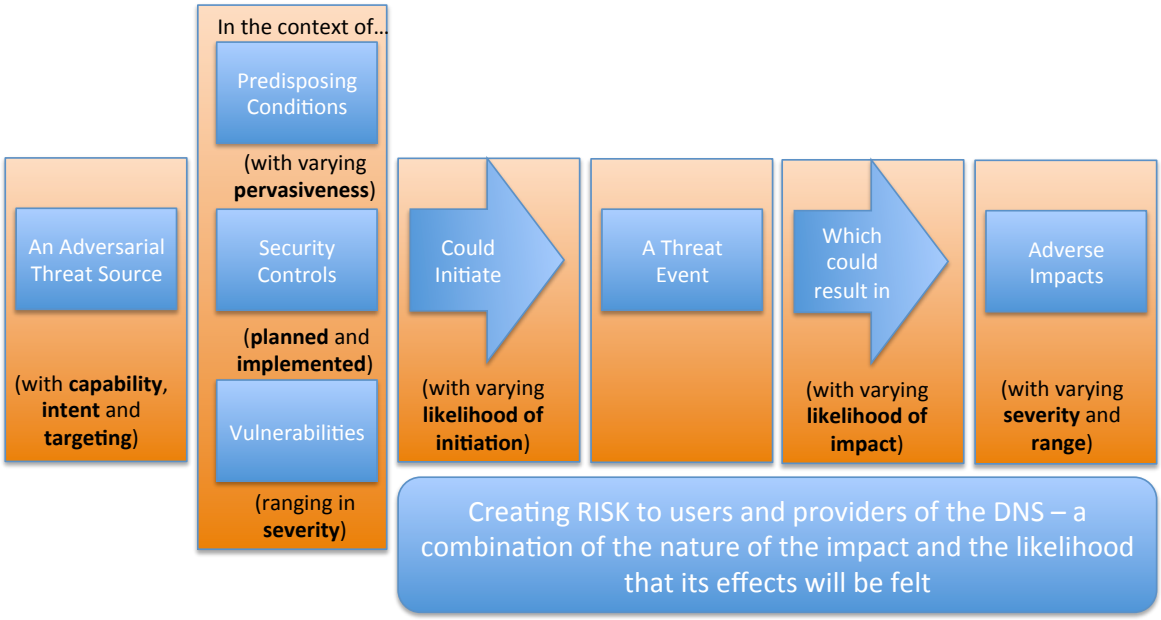
The DSSA developed its risk scenarios by composing "compound sentences" based on a tailored version of the NIST 800-30 risk framework. This section describes the three broad "adversarial" scenarios; the following section describes two more "non-adversarial" scenarios.

The difference between adversarial and non-adversarial risk scenarios is in the treatment of "threat-sources."

Adversarial threat-sources are analyzed along three scales – their capability, their intent and how narrowly they are targeting the DNS. Examples of adversarial threat-sources include nation-states, rogue elements, organized crime and so on.

Examples of non-adversarial threat sources include a range of sources that is broader than adversarial threat-sources, but they are only evaluated with a "range of effect" scale since their actions are not intentional.

Reading the words in the following diagram from left to right results in the compound sentence that was used to formulate adversarial risk scenarios.



This framework has also been published as an Excel worksheet and is available to the community on the DSSA wiki. Here is a link to the page where all of the risk scenario worksheets (templates and completed worksheets) are archived.

https://community.icann.org/display/AW/Risk+Scenario+worksheets

We strongly encourage members of the community to explore the (very rich) details of the risk-management framework by downloading this worksheet. A more traditional narrative version of the framework is published in Appendix [___] but most readers have found the worksheet to be much easier to understand and use.

5.2.2.1. Introduce the risk models - relationships between risk factors (aka "compound sentences") [pull longer definition from methodology]

5.2.2.2. Adversarial Risk Model [insert the picture of adversarial risk model (based on the one in the update slide deck, but redrawn in MS format)]

An ADVERSARIAL THREAT SOURCE (with a range of capability, intent and targeting)...

In the context of...

VULNERABILITIES (ranging in severity),

PREDISPOSING CONDITIONS (with varying pervasiveness)

SECURITY CONTROLS (planned and implemented),

could INITIATE (with varying likelihood) a THREAT EVENT,

that could result in ADVERSE IMPACTS (which have RISK, which is in turn a combination of the nature of the impact and the likelihood that its effects will be felt)

5.2.2.3. Non-Adversarial Risk Model [Insert a picture of non-adversarial risk model (build out, based on the adversarial one -- pretty similar, just fewer threat-sources)

A NON-ADVERSARIAL THREAT SOURCE (with a range of effects)...

In the context of...

PREDISPOSING CONDITIONS (with varying pervasiveness)

SECURITY CONTROLS (planned and implemented), and

VULNERABILITIES (ranging in severity),

could INITIATE (with varying likelihood) a THREAT EVENT,

which could result in ADVERSE IMPACTS (which have RISK, which is a combination of the nature of the impact and the likelihood that its effects will be felt)

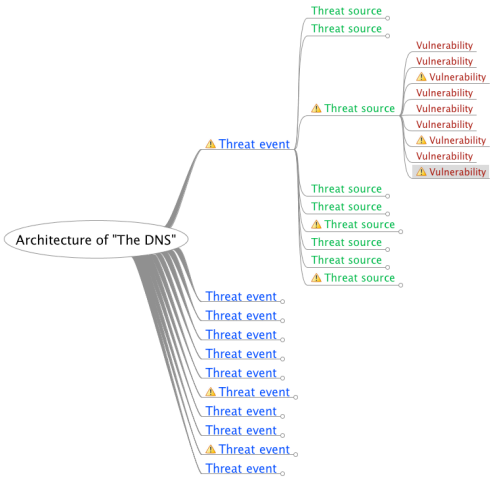
5.2.2.4. Risk Factor Definitions and Ranges [insert a combination of risk factor DEFINITIONS and RANGES - pull these from the latest version of the worksheet and/or the methodology]

- Threat events - what happens?
- Adverse impacts - what is the harm?
- Vulnerabilities – severe and widespread?
- Predisposing conditions – pervasive?
- Controls and mitigation – effective and deployed?
- Threat sources – how broad is range of impact, what are their capabilities, how strong is their intent, are they targeting the DNS?
- Initiation – what is the likelihood that a threat-event will happen?
- Risk - how bad is the impact and how likely is it that it will be felt?

5.2.2.5. Tailoring - how risk factors are combined to arrive at risk scenarios

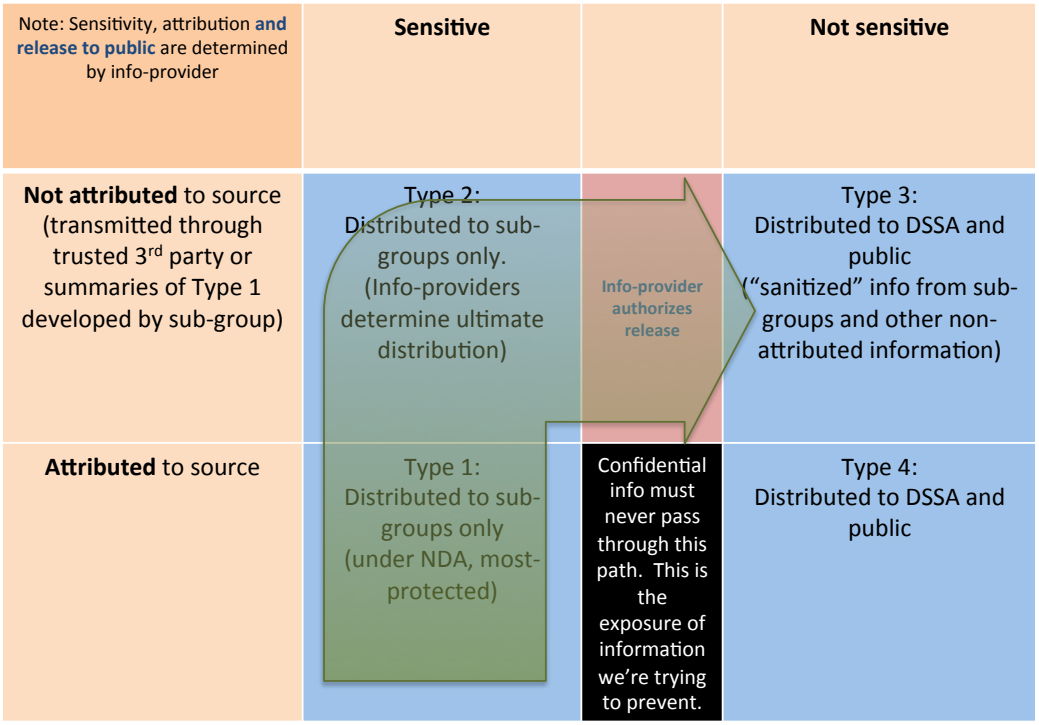
[discuss the process by which the DSSA created the first-pass scenarios in the report, also discuss the "does not scale" issue and our approach to solving it]

[the DSSA ran into difficulty when it tried to develop and evaluate an exhaustive list of scenarios based on the methodology, because the number of scenarios exploded with each successive "layer" of the analysis. It became clear that working through each permutation of the assessment framework would take too long.



5.2.3. Protocol for handling confidential information

[summarize and introduce it here, put the full text in an appendix]



5.3. Tentative approach for the next iteration

[Question for AC/SOs - one more iteration or ongoing effort?]

5.3.1. Issues

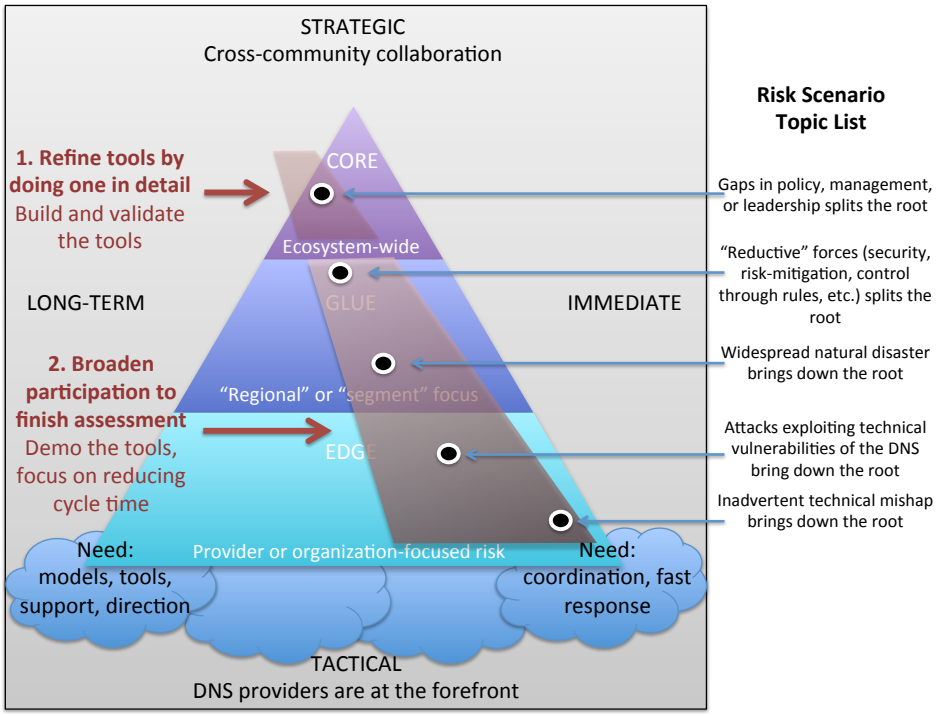
Scaling – many more people involved as we move outward from "core" to "edge"

Volunteer time/energy/attention – the group is already dwindling, it may be very difficult to sustain the effort

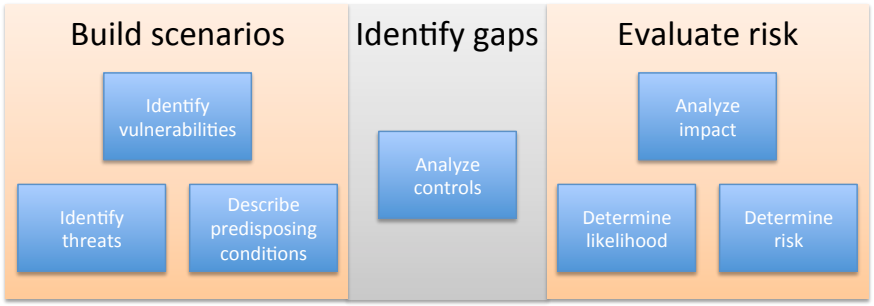
Information-gathering approach (maybe surveys based on pre-built scenario worksheets?)

Need – do the requirements that drove the formation of the DSSA still exist?

5.3.2. More scenarios, more depth, more independent work-teams



5.3.3. Work breakdown



[introduce it here, but move the actual detail of the methodology into an appendix – list tasks and summary descriptions here]

[highlight the goal – build and evaluate a risk-scenario in as little as an hour – so that the approach could be used by first-responders in addition to us more-contemplative type people]

Step 1 – Build Scenarios

Individual working-group members use risk-scenario worksheets to quickly brainstorm a series of related scenarios based on the broad risk topic under discussion.

TASK 1-1: Identify the threat sources of concern

TASK 1-2: Identify potential threat-event scenarios, the relevance to the DNS, and the threat sources that could initiate the events.

TASK 1-3: Identify vulnerabilities and predisposing conditions (which may increase or decrease risk) that affect the likelihood that threat events of concern result in adverse impacts to the organization.

TASK 1-4: Develop consolidated scenarios and prepare scenario-evaluation surveys for the next step of the analysis

TASK 1-5: Evaluate the process with an eye to reducing cycle time and ease of use for subsequent efforts

Step 2 – Identify gaps

The working-group uses a structured survey process to collectively evaluate each threat-scenario (threat-events, vulnerabilities and predisposing conditions) and then identify and evaluate gaps in security controls.

TASK 2-1: Characterize threat sources (capability, intent and targeting of adversarial threats, range of effect of non-adversarial threat sources) for each risk-scenario

TASK 2-2: Characterize vulnerabilities (by severity) and predisposing conditions (by pervasiveness) for each risk-scenario

TASK 2-3: Identify security controls that are the most relevant to addressing each risk-scenario

TASK 2-4: Characterize the current state of those security controls (by the degree to which they are implemented across the ecosystem) for each risk-scenario

TASK 2-5: Develop consolidated scenarios and prepare scenario-evaluation surveys for the next step of the analysis

TASK 2-6: Evaluate the process with an eye to reducing cycle time and ease of use for subsequent efforts

Step 3 – Evaluate risk

The working-group uses a structured survey process to collectively evaluate the risk of each threat-scenario

TASK 3-1: Assess the likelihood that each risk-scenario will be initiated, considering the characteristics of the threat sources that have been identified

TASK 3-2: Assess the likelihood that each risk-scenarios will result in adverse impacts to the DNS, considering: the vulnerabilities and predisposing conditions identified; and ecosystem susceptibility reflecting security controls planned or implemented to impede such events.

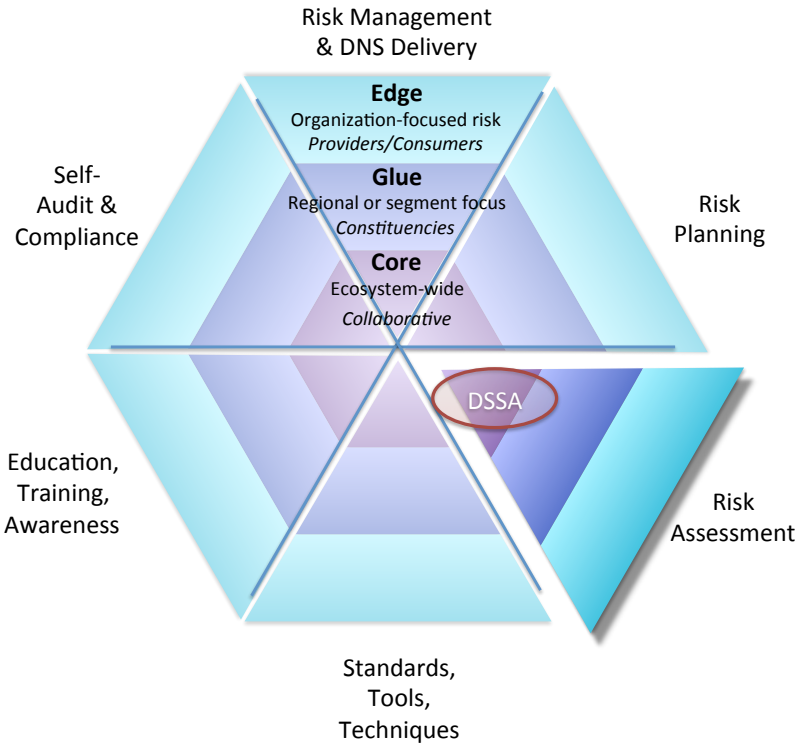
TASK 3-3: Determine the risk to the DNS from each risk-scenario considering the impact that would result from the events; and the likelihood of the events occurring.

TASK 3-4: Develop consolidated scenarios and publish overall risk-assessment

TASK 3-5: Evaluate the process with an eye to reducing cycle time and ease of use for subsequent efforts

5.3.4. Possible ongoing organization and approach

5.3.4.1. Introduction



[describe the possible value of some kind of "ongoing DSSA" organization]

[tie back to the "maintain risk assessment' portion of the methodology]

[questions include: who would do this, who could participate, etc?]

[the following is a first pass at that invention – we need to make this proposal really clear]

5.3.4.2. Purpose

To quickly and accurately assess the actual level and severity of existing and emerging threats to the DNS

To evolve/engage/empower a community of mutual trust and support to share ideas and resources

To provide tools, models and best practices that assist the diverse community of DNS providers assess their own situation in an effective and appropriate way

5.3.4.3. Principles

- Favor the edge -- Vest authority, perform functions, and use resources in the smallest or most local part that includes all relevant and affected parties.
- Open membership -- to any who subscribe to purpose and principles
- Self organize -- for any activity consistent with purpose and principles
- Decision-making -- representative of all, dominated by none -- consensus where possible
- Resolve conflict creatively
- Draw out, rather than compel, action
- Freely exchange information unless it's confidential or materially reduces competitive position

5.3.4.4. Participants

Individuals and organizations who see the purpose and principles as their own

Provide a recognizable "doorway" for participants to enter (and depart)

Is the current ICANN structure (AC/SOs) the best way to describe the "groupings" of participants? Are there any stakeholders missing?

Determine what interests have to be balanced in order to create an organization trusted by all

5.3.4.5. Organization

- Decentralized, self-organizing
- Diversity essential
- Blurring the rules of competition and cooperation
- Favor innovation, novelty, creativity and learning
- Build intellectual and social capital that can be shared

5.3.4.6. Edge-glue-middle relationship

5.3.4.6.1. Edge-middle continuum

- Center -- start with ICANN staff and volunteer SSR thought-leaders and tool-builders

- Glue -- Constituencies and related organizations
- Edge -- DNS providers/deliverers/consumers

5.3.4.6.2. Capability (spokes, pie-slices)

- risk assessment
- education, training, awareness
- standards, tools, techniques
- self-audit/compliance
- mission continuity
- DNS "delivery"

6. Appendices

6.1. Charter

6.2. Risk Scenarios

6.2.1. Adversarial risk scenarios

[insert "adversarial risk scenario" introduction here…]

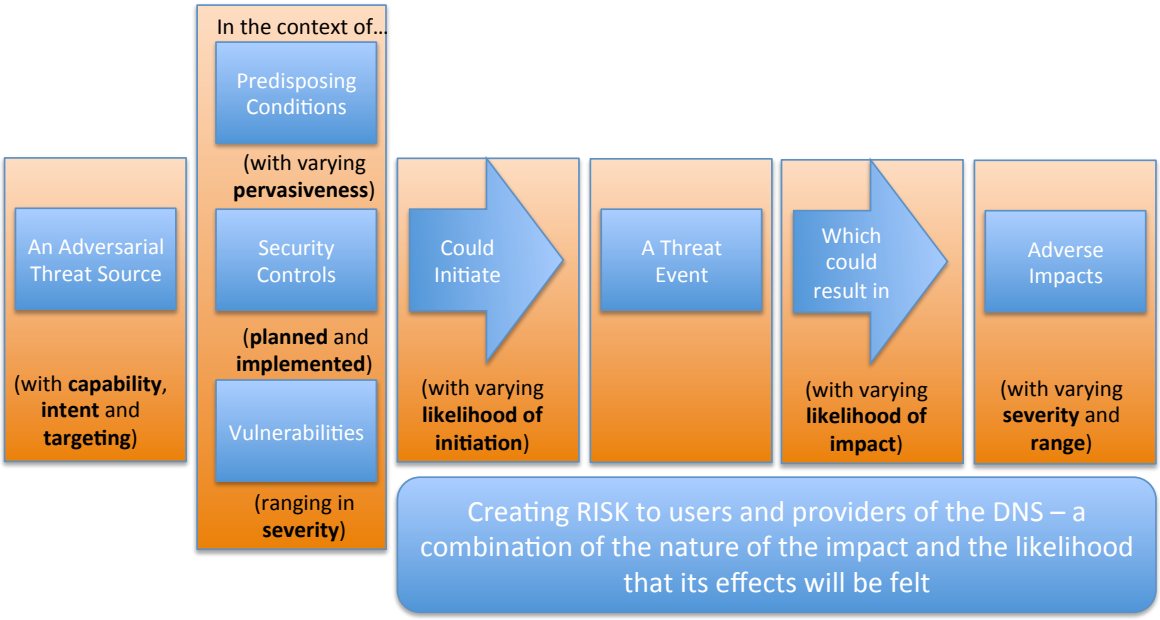
The DSSA developed its risk scenarios by composing "compound sentences" based on a tailored version of the NIST 800-30 risk framework. This section describes the three broad "adversarial" scenarios; the following section describes two more "non-adversarial" scenarios.

The difference between adversarial and non-adversarial risk scenarios is in the treatment of "threat-sources."

Adversarial threat-sources are analyzed along three scales – their capability, their intent and how narrowly they are targeting the DNS. Examples of adversarial threat-sources include nation-states, rogue elements, organized crime and so on.

Examples of non-adversarial threat sources include a range of sources that is broader than adversarial threat-sources, but they are only evaluated with a "range of effect" scale since their actions are not intentional.

Reading the words in the following diagram from left to right results in the compound sentence that was used to formulate adversarial risk scenarios.



This framework has also been published as an Excel worksheet and is available to the community on the DSSA wiki. Here is a link to the page where all of the risk scenario worksheets (templates and completed worksheets) are archived.

https://community.icann.org/display/AW/Risk+Scenario+worksheets

We strongly encourage members of the community to explore the (very rich) details of the risk-management framework by downloading this worksheet. A more traditional narrative version of the framework is published in Appendix [___] but most readers have found the worksheet to be much easier to understand and use.

These scenarios will be used as the starting point for the detailed analysis that the DSSA will do in the next phase of its work. These are not an answer to the charter question about actual threats to the DNS – they are the starting point from which those answers will come.

The DSSA has identified three broad adversarial risk-scenarios that it will analyze in the next phase of its work:

- Gaps in Policy, Management and Leadership Lead to Splitting the Root
- "Reductive" Forces (Security, Risk-mitigation, Control through rules, etc.) Lead to Splitting the Root
- Attacks Exploiting Technical Vulnerabilities of the DNS Bring Down the Root

Substantial analysis of these scenarios has already been completed by the DSSA and is contained in [Appendix ___]

6.2.2. Adversarial Risk Scenario – Gaps in Policy, Management and Leadership Lead to Splitting the Root

6.2.2.1. Examples

6.2.2.1.1. Nation-state blocking policy and configuration error.

In order to fulfill an IP infringement resolution, one nation-state requires all providers under its sovereignty to block access to a certain domain name and also all related resolved IP addresses. It happens that the country also hosts some authoritative servers. Unfortunately due to the wording in the resolution the authoritative-DNS hosting provider makes an error while changing configuration files on the authoritative server while fulfilling its obligations under the resolution. This change also causes problems in the resolution of the address for users from other countries

6.2.2.1.2. Nation-state alternate root, cyber terrorism and DNS hacking.

A country or a certain number of countries develop their own internal domain system and isolates itself from the rest of the Internet. The same actors are behind a well known cyber terroristic group. Due to the fact that they do no belong to the root servers system anymore, the need of an operable Internet is not required for them anymore. The geopolitical group acquires a 0day regarding an undisclosed vulnerability of the DNS on the black market (the same scenario can be applied also to DNSSEC) and deploys it in retaliation after an international security organization resolution. The vulnerability has a domino effect: affecting not only the authoritative but also the recursive servers and disrupting the resolution all around the world. Since there is no central incident response coordination and due to the fact the malfunctions propagates with different timings the problem has major impacts to the Internet at a worldwide level.

6.2.2.1.3. US National Information Protection Plan (NIPP) -- "Policy, Governance, and Knowledge Failures" alternate-root scenario

The Internet is an open and global system, providing individuals and organizations a variety of opportunities for attacking the DNS infrastructure. Actors attack the infrastructure for various motivations and objectives. An incident that originates from a nation-state may be motivated by a desire for political influence or to achieve military objectives. In contrast, an incident from an individual or a small group may only be a manifestation of their desire to exercise control over a key part of the Internet infrastructure or to demonstrate their technical prowess. Policy, governance, and knowledge failures could cause significant economic and national security impacts to the DNS critical function, and they could result in political and diplomatic tensions between nation-state threat actors. An attacker could try to establish an alternate Internet root, to which DNS inquiries could be diverted, instead of being directed to the “real” DNS root. The establishment of regional or alternative Internets could decrease interoperability and cause technical confusion. Such a situation could cause strategic consequences across multiple sectors. Internet market influences may not be strong enough to avoid the emergence of an alternate, authoritative root, if

the political and strategic environment provides an opportunity to establish and manage an alternative root system.

6.2.2.2. Risk Factors to Analyze

6.2.2.2.1. Threat Sources

- Nation states
- Geo-political groups

6.2.2.2.2. Vulnerabilities

External relationships/dependencies

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

6.2.2.2.3. Predisposing Conditions that Reduce Risk

Contractual relationships between entities

- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches
- Diverse, distributed system architecture and deployment
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities

6.2.2.2.4. Predisposing Conditions that Increase Risk

- Definitions of responsibility, accountability, authority between DNS providers
- Diverse operational environments and approaches

- Legal standing (and relative youth) of ICANN

6.2.2.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- Incident Response
- Planning
- Program Management
- Risk Assessment

6.2.2.2.6. Threat Events

- Zone does not resolve or is not available
- Zone is incorrect or does not have integrity

6.2.2.2.7. 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.

6.2.3. Adversarial Risk Scenario – "Reductive" Forces (Security, Risk-mitigation, Control through rules, etc.) Lead to Splitting the Root

6.2.3.1. Examples

6.2.3.1.1. ISOC "Moats and Drawbridges" scenario.

Suggests the world of the Internet would be heavily centralized, dominated by a few big players with their own rules in "big-boys' clubs." Conflicts would be resolved through negotiation, not competition. Connections between networks would be the result of extensive negotiation and deal making. There would likely be strong regulation as governments seek to impose some public interest obligations and perhaps even controls on the equipment users can connect to the network. Much content would be proprietary and protected by strong intellectual property rights. Governments would control the behavior of networks and network users through legal mechanisms and sanctions. Barriers to entry would be high, with little incentive to expand networks beyond the largest and richest customers or regions. Innovation would be slow, only occurring when it would benefit the network owners. All players would have close political links to their mutual benefit.

6.2.3.1.2. ISOC "Boutique Networks" scenario.

Envisions a future in which political, regional and large enterprise interests fail to maximize the social and economic potential of a shared, global set of richly connected networks (the Internet). It carries the weight of self-interest brought by factions seeking to optimize control in small sectors (political and otherwise). It also suggests these fractionalized networks will continue to leverage the benefits of existing Internet standards and technology. Each proprietary provider draws as much as possible from the common pool while giving little back.

6.2.3.2. Risk Factors to Analyze

6.2.3.2.1. Threat Sources

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

6.2.3.2.2. Vulnerabilities

- External relationships/dependencies
- Inconsistent or incorrect decisions about relative priorities of core missions and business functions

- Interventions from outside the process
- Lack of effective risk-management activities
- Poor inter-organizational communications

6.2.3.2.3. Predisposing Conditions that Reduce Risk

- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches
- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Multi-stakeholder, consensus-based decision-making model

6.2.3.2.4. Predisposing Conditions that Increase Risk

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

6.2.3.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- Planning
- Program Management
- Risk Assessment

6.2.3.2.6. Threat Events

- Zone is incorrect or does not have integrity

6.2.3.2.7. 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.

6.2.4. Adversarial Risk Scenario – Attacks Exploiting Technical Vulnerabilities of the DNS

6.2.4.1. Examples

6.2.4.1.1. Global, massive attack against a day zero vulnerability in DNS software, sustained until remediation is implemented.

6.2.4.1.2. DDOS attack on root server(s) or .com

6.2.4.1.3. Disgruntled employee.

An employee has just been fired due to HR cut from a company that operates several critical DNS services. The employee was in charge of these critical services and his credentials haven't been revoked immediately. The employee was normally dealing with issues due to the replication of the zone file and decides to implement a change and let it propagate. Due to the company resizing and lack of backup knowledge, an immediate response to customers complains is not provided and a major top-level domain experiences several hours of outages.

6.2.4.2. Risk Factors to Analyze

6.2.4.2.1. Threat Sources

- Rogue elements
- Insiders

6.2.4.2.2. Vulnerabilities

Inadequate incident-response

- Inadequate training/awareness
- Infrastructure vulnerabilities
- Operational vulnerabilities
- Security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems)
- Technical vulnerabilities

6.2.4.2.3. Predisposing Conditions that Reduce Risk

- Contractual relationships between entities

- Diverse, distributed system architecture and deployment
- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Managerial vs operational vs technical security skills/focus/resources

6.2.4.2.4. Predisposing Conditions that Increase Risk

- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities

6.2.4.2.5. Missing or Insufficient Security Controls

- Configuration Management
- Identification and Authentication
- Incident Response
- Operational Controls
- Security Assessment and Authorization
- System and Communications Protection

6.2.4.2.6. Threat Events

- Zone is incorrect or does not have integrity
- Zone does not resolve or is not available

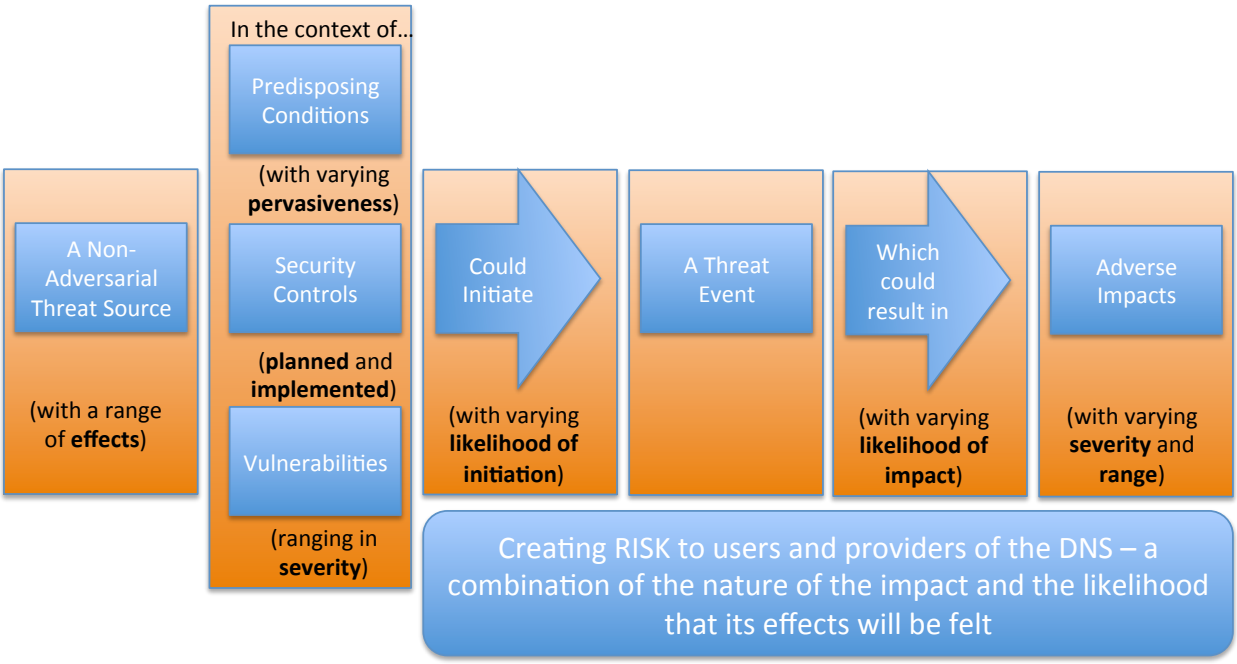
6.2.4.2.7. Adverse Impacts

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.

6.2.5. Non-adversarial risk scenarios

This section describes two broad "non-adversarial" risk-scenarios to be analyzed. As with the adversarial risk scenarios, these were developed using a tailored "compound sentence" approach based on a tailored version of the risk framework described in NIST 800-30.

The only difference between this model and the adversarial model in the preceding section is the structure and analysis of non-adversarial threat-sources. In this model, non-adversarial threat sources are only evaluated on the range of the effect of the error or accident. Unlike adversarial threats, these threats are presumed to be unintentional.



As with the previous section, these broad scenarios will be used as the starting point for the detailed analysis that the DSSA will do in the next phase of its work. These are <u>not</u> an answer to the charter question about actual threats to the DNS – they are the starting point from which those answers will come.

6.2.6. Non-Adversarial Risk Scenario – Impacts of Natural Disasters

6.2.6.1. Examples

Note: in this phase, both of the example risk-scenarios focused on power-outages when thinking about natural disasters. The DSSA may rework this a bit as it proceeds into the next phase of its work.

6.2.6.1.1. Wide-ranging power outage

Someone forgot to remove a grounding strap from a major transmission line before re-energizing it. The rest of the grid tries to compensate, leading to a long lasting, cascading failure of the entire North American power grid. Due to the caching and redundant nature of the DNS, and the fact that many operators have generators, nothing bad happens... initially. As sites run out of fuel, more and more major authoritative providers go dark. The DNS serving side is well replicated, but the provisioning side is not. Zone files begin to expire, many of these could be saved (by promoting backups to masters / bumping the serial numbers, etc.) but, while there is a good culture of collaboration between many members of the community, much of the communication / recovery work is hampered by employees not having access to their work machines, to their address books and not having power at home.

6.2.6.1.2. Power outage

Due to a major blackout in a really populated area that also hosts several global and local instances of the root servers, the domain name resolution fails. Due to the Time to Live expiration and the duration of the black out the other instances around the world are overwhelmed by the requests as they were under a non-adversarial DDOS attack.

6.2.6.2. Risk Factors to Analyze

6.2.6.2.1. Threat Sources

- Blackout/Energy Failure

6.2.6.2.2. Vulnerabilities

- Business continuity vulnerabilities
- Infrastructure vulnerabilities
- Lack of effective risk-management activities
- Poor inter-organizational communications

6.2.6.2.3. Predisposing Conditions that Reduce Risk

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

6.2.6.2.4. Predisposing Conditions that Increase Risk

Contractual relationships between entities

- Diverse operational environments and approaches

6.2.6.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- Configuration Management
- Contingency Planning
- Contingency Planning

Physical and Environmental Protection

- Risk Assessment

6.2.6.2.6. Threat Events

- Zone does not resolve or is not available

6.2.6.2.7. 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.

6.2.7. Non-Adversarial Risk Scenario – Inadvertent Technical Mishaps

6.2.7.1. Examples

6.2.7.1.1. Invalid Signature Files

An invalid signature on a zone file is created – due to a combination of DNSSEC production errors, hardware or software failures or administrative process failures. Either the root or a TLD publishes an unvalidatable zone file.

6.2.7.2. Risk Factors to Analyze

6.2.7.2.1. Threat Sources

- Key hardware, software, process failure

6.2.7.2.2. Vulnerabilities

- Malicious or unintentional (erroneous) alteration of root or TLD DNS configuration information
- Vulnerabilities arising from missing or ineffective security controls

6.2.7.2.3. Predisposing Conditions that Reduce Risk

- Emphasis on resiliency and redundancy
- Security project and program management skills/capacity
- Managerial vs operational vs technical security skills/focus/resources
- Diverse operational environments and approaches

6.2.7.2.4. Predisposing Conditions that Increase Risk

- Reliance on immature or custom built DNSSEC technologies
- Chain of trust single point of failure

6.2.7.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- System and Information Integrity
- Incident Response

6.2.7.2.6. Threat Events

- Zone does not resolve or is not available

6.2.7.2.7. 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.

6.3. Background materials and bibliography

[Action: clean up the mind-map and insert useful bits]

6.4. Tables?

6.5. Methods – Rationale, selection, details

6.5.1. Rationale

Using a predefined methodology will save time and improve our work product

Consistent terminology
Shared model
Structured work
Sample deliverables

Reviewed several dozen alternatives -- We selected this one because it's:

Available at no cost
Actively supported and maintained
Widely known and endorsed in the community
Reusable elsewhere in ICANN

6.5.2. Selection

Methods evaluated

- A&K Analysis - ISO 17799

Austrian IT Security Handbook

- BSI - IT-Grundschutz

EBIOS - ISO 17799

- Hazard Analysis -- Critical Control Point (HACCP)

HITRUST Common Security Framework

- ISAMM
- ISO/IEC 13335-2 (27005)

ISO/IEC 17799

- ISO 27000 series
- ISO 31000 series
- Marion

NIST 800-30

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

6.5.3. Source documents

[cut/paste introduction and overview diagram from methods]

Link to source documents -- http://csrc.nist.gov/publications/PubsSPs.html

6.5.3.1. NIST 800-30 DRAFT Guide for Conducting Risk Assessments

6.5.3.2. NIST 800-53 Rev. 4 – DRAFT Security and Privacy Controls

6.5.3.3. NIST 800-53A – Guide for Assessing Security Controls

6.5.4. DSSA-tailored framework

6.5.4.1. Risk-assessment worksheet

6.5.4.2. Components and scales

Table D7 -- Adversarial Threat Sources

Threat Source

~~ International governance/regulatory bodies

~~ Nation states

~~ Rogue elements

~~ Geo-political groups

~~ External parties and contractors

~~ Insiders

~~ Organized crime

Table D-3 -- Adversary capability

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 -- 5 -- 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.

Table D-4 -- Adversary intent

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.

Table D-5 -- Adversary targeting

10 -- Very High -- The adversary analyzes information obtained via reconnaissance and attacks to persistantly 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 persistantly 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.

Table D8 -- Non-Adversarial Threat Sources

Threat Source

INDIVIDUAL AND ORGANIZATIONAL SOURCES

~~ International governance/regulatory bodies

~~ Nation states

~~ Privalaged 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

Table D-6 -- range of effect (to DNS providers)

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

Table E5 - Threat Events

Threat Event

~~ Zone does not resolve or is not available

~~ Zone is incorrect or does not have integrity

+ - Security is compromised

Define list – Definie secutiy

NOTE: The third leg of the traditional "availability, integrity, CONFIDENTIALITY" triad may drop out, as the DNS does not contain confidential information??

Table G2 -- 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 -- 0 -- Adversary is highly unlikely to initiate the threat event

Table G3 -- 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.

Table F3 - Vulnerabilities

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

** UNDER DISCUSSION

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

** SYSTEM AND NETWORK

~~ Recursive vs authoritative nameserver attacks

~~ DDOS

~~ Email/spam

** 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

TABLE F-2: ASSESSMENT SCALE - 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.

Table F6 - Predisposing Conditions

Predisposing Condition

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, accountibility, 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

Scales (enhanced by DSSA) to address whether the condition helps or hurts in the scenario

TABLE F-5a: ASSESSMENT SCALE - 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

TABLE F-5b: ASSESSMENT SCALE - 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

Table F9 - Controls

Control

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

Scale

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

Table H3 -- Amount of impact

Impact

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.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same in different contexts/circumstances, the "high water" concept is used to determine the impact level. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high- impact system is an information system in which at least one security objective is high. It is our conclusion that the DNS is a high-impact system because the goals for integrity and availability are high.

Table H5 -- 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 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.

~~ Harm to other organizations

~~ 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.

~~ Relational harms.

~~~~ Damage to trust relationships.

~~~~ Damage to reputation (and hence future or potential trust relationships).

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.

[stop here – breaks next section – remove b4 publication]

6.6. Guideline for handling Confidential information

6.6.1. Charter Guidelines

6.6.1.1. Principles

The DSSA-WG Charter recognizes that sub-groups may need to access sensitive or proprietary information in order for the DSSA-WG to do its work. These procedures are an exception to accountability and transparency standards. The DSSA-WG Charter does not require that members sign a formal Affirmation of Confidentiality and non-disclosure agreement (NDA) for membership in the DSSA-WG.

The primary goal of these guidelines is to make sure that the people sharing highly sensitive information with sub-groups are assured that their information will not find its way out of those sub-groups without their permission.

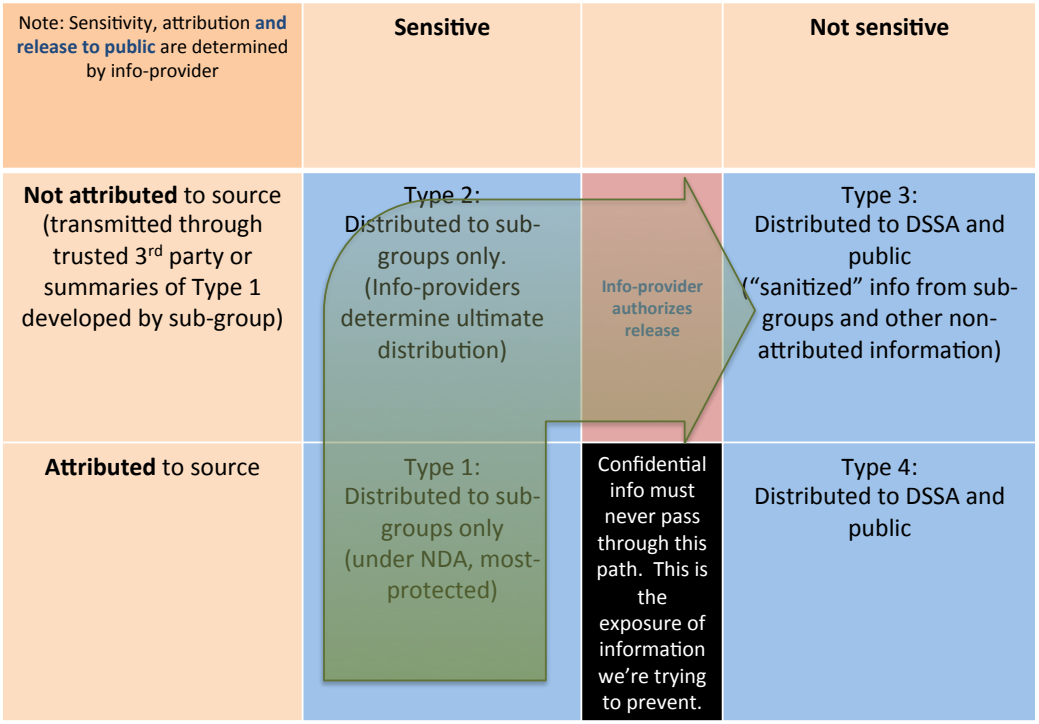
6.6.1.2. Sub-Groups

Sub-groups of the DSSA-WG may need to access sensitive or proprietary information in order for the DSSA-WG to do its work. Thus, measures may need to be established to access and protect confidential or proprietary information. The following procedures, as set forth in the DSSA-WG Charter, are an exception to the standards for transparency and accountability and only apply in cases where members of the aforementioned sub-groups of the DSSA-WG need to access and to protect confidential information:

- In certain cases under this exception, in order to ensure access to and protection of confidential or proprietary information, sub-groups' members of the DSSA-WG will be asked to sign a Formal Affirmation of Confidentiality and Non-Disclosure (See Annex B of the Charter). In addition, the sub-groups' members of the DSSA-WG may be required to sign a Non-Disclosure Agreement (NDA) for a specific project or issue.
- No formal Non-Disclosure Agreement (NDA) is required for membership in the DSSA-WG; and
- A separate email distribution list that is not publicly accessible may be established only to include the sub-groups' members who have signed a Non-Disclosure Agreement applicable to that specific project or issue.
- Information-providers may specify additional changes to these Guidelines after they've begun participating in a sub-group. The goal here is to ensure that information-providers do not find themselves trapped in an insecure situation with no mechanism to fix an unanticipated problem.

6.6.2. Dimensions of the information to be protected

This section addresses the sources and types of information that are addressed by these Guidelines.



6.6.2.1. Sensitivity

DSSA-WG members may be provided certain technical data or information that is commercially valuable and not generally known in its industry of principal use (collectively referred to as "Proprietary Information") pursuant to the DSSA-WG's performance of its tasks. As described in Annex B of the Charter, DSSA-WG members will use reasonable care to hold in confidence and not disclose any Proprietary Information disclosed to them. Written information provided to DSSA-WG members shall be considered Proprietary Information—i.e. information that is considered sensitive—if it is clearly marked with an appropriate stamp or legend as Proprietary Information. Non-written information shall be considered Proprietary Information only if the discloser of such information informs the DSSA-WG at the time of disclosure that the information being disclosed is of a proprietary nature.

DSSA-WG members have no obligation of confidentiality with respect to information disclosed to them if:

- Such information is, at the time of disclosure, in the public domain or such information thereafter becomes a part of the public domain without a breach of this Affirmation; or
- Such information is known to the DSSA-WG at the time it is disclosed; or

- Such information was independently developed by the DSSA-WG; or
- Such information is received by the DSSA-WG from a third party who had a lawful right to disclose such information to it; or
- The disclosing party provides written consent that the information is no longer confidential.

6.6.2.2. Nature

The nature of information falls into three general categories: data for analysis, information about internal processes, and information relating to trade secrets. In each case, whether this information is deemed to be Proprietary Information will be based on the decision made by the person providing the information. If the information is deemed to be Proprietary Information handling the information may require compartmentalization across sub-groups. As noted in Section 2.1 above, regardless of the nature of the information, Proprietary Information must be clearly marked with an appropriate stamp or legend as Proprietary Information. Non-written information shall be considered Proprietary Information only if the discloser of such information informs the DSSA-WG at the time of disclosure that the information being disclosed is of a proprietary nature.

6.6.2.3. Attribution

There are two options for attribution: either to attribute the information to its source or not to attribute it to its source. In each case, the provider of the information should make the decision and inform the DSSA-WG when providing the information. However, in some cases non-attributed information may be transmitted to the DSSA-WG through a trusted third party or from a sub-group to the DSSA-WG.

6.6.2.4. Distribution

There are two options for the distribution of information provided to the DSSA-WG. If the information is not proprietary, it may be distributed to the public. If the information is Proprietary Information, it may be distributed only to those DSSA-WG member and sub-group members who have signed a formal Affirmation of Confidentiality and NDA. For Proprietary Information distributed to sub-groups, the members of the sub-groups in coordination with the provider of the information shall decide whether the information may be distributed to the full DSSA-WG or elsewhere. The provider of the Proprietary Information shall make the final determination as to whom the information is distributed.

6.6.2.5. Use Cases

The following are the four types of use cases for information:

Type 1

- Sensitive, attributed

- Distribution to sub-groups only
- Governed/enforced by DSSA NDA (and project/use-specific NDAs if needed)
- Highest standard of protection

Type 2

- Sensitive, non-attributed
- Distribution to sub-groups only
- Transmitted through trusted third party or summaries of Type 1 information developed by sub-group
- Sub-group determines ultimate distribution, but the information providers have final say on "sanitized" versions of information they've submitted

Type 3

- Not sensitive, not attributed
- Distributed to the DSSA-WG and ultimately the public (via email list, wiki, report, etc.)
- "Sanitized" information developed by sub-groups
- Primarily Type 2 information that has been approved for release by the sub-group that developed it

Type 4

- Not sensitive, attributed
- Distributed to the public (via email list, wiki, report, etc.)

6.6.2.6. Data Repository

The sub-group may determine that it is useful to track the nature and status of confidential information that it receives. This is a preliminary description of what such a repository could entail. The DSSA is in continuing discussion on this item and may have additional suggestions and tools at the time that the sub-group is formed.

If the sub-group elects to establish a repository, it should be managed by a single trusted member of the sub-group.

Possible Content

- A copy of the confidential information itself (wording to be validated by the source)
- Source
- Date provided
- Mechanism by which source provided the information (e.g. email, verbally in a teleconference)
- Attribution (whether it can be attributed or not)
- Releasability (who this information can be released to)

- Distribution (who this information has been released to, when it was released, how it was released e.g. email, verbally in a teleconference, etc)
- List of any NDAs signed
- Change of status (e.g. some information may become less sensitive after a period of time, or information was withdrawn by the source)

6.6.3. Forming Sub-Groups

The following are the procedures for forming sub-groups in the DSSA-WG.[1]

The DSSA-WG may deem it suitable to ask for an existing group that is organized outside of ICANN to provide information back to the DSSA-WG. This group would be responsible for the accuracy, truthfulness, and allowable details of the threat but follow its own roles for handling of confidential information.

[1] When considering its guidelines for forming sub-groups the DSSA-WG consulted with the DNS Operations, Analysis, and Research Center (DNS-OARC) concerning its procedures. The DNS-OARC procedures follow these steps:

1. Describe/charter/document the group;
2. Documentation includes accepted rules of behavior;
3. "Seed" the group with highly-trusted core members;
4. Ask people to volunteer;
5. Publish/update the list of self-identified volunteers and request "vouches" from existing group members;
6. Group-members vouch for volunteers;
7. Admit volunteers that reach the threshold number of "vouches";
8. Monitor group membership and "vouches" to ensure that all members are above the minimum; and
9. Remove members who fall below the number-of-vouches threshold -- either because the people who vouched for them have left the group, or “vouches” are withdrawn after bad behavior.

The DSSA-WG has developed its procedures for forming sub-groups that incorporate some, but not all, of the aspects of those adopted by the DNS-OARC.

6.6.3.1. Sub-Group Charter and Membership-Selection

The Charter for each sub-group shall be the same as that of the DSSA-WG. The Sub-group members shall follow the rules of behavior set forth in the DSSA-WG Charter in addition to provisions for signing the Affirmation of Confidentiality and NDA, as applicable.

Initial sub-group members shall be selected by the Co-Chairs of the DSSA-WG in conjunction with information-providers (sometimes those discussions may be held in private) to include members solicited from the DSSA-WG, members who are acting as proxies and/or advocates for one or more information-provider, and outside experts who may have relevant information to provide relating to the issue(s) to be considered by the sub-group.

The DSSA-WG Secretariat shall publish the list of initial sub-group members. If additional sub-group members are needed beyond the initial list, new members can be proposed by any sub-group member. If further members are needed the DSSA-WG Secretariat also may send out a call for volunteers. For any additional new member to a sub-group the Secretariat shall ask the existing sub-group members to vouch for them. Volunteers will be admitted to the sub-group when two sub-group members have vouched for them and if they are acceptable to all of the information-provider members of the sub-group.

The size of the sub-group will be kept as small as possible in order to reduce the risk of information disclosure.

6.6.3.2. Sub-Group Roles

The following are the acceptable roles for the members of sub-groups:

1. Information-provider
2. Topic expert
3. Analyzer
4. Document-developer
5. Sub-group leader

6.6.3.3. Leaving the Sub-Group

Sub-group members will be removed if:

- They violate the Rules of Behavior in the Charter,
- Any information-provider sub-group member requests that they be removed from the sub-group, or

- They no longer have at least two sub-group members who have vouched for them (note: these vouching members can change, there just need to be two of them at any given time).

Any member may withdraw from a sub-group at any time. This is primarily aimed at information-providers who are no longer confident that they can participate in a way that maintains the confidentiality of their information, but applies to any member of the sub-group. Leaving the sub-group does not relieve the person of their responsibilities under any confidentiality agreements they've signed. If an information-provider leaves a sub-group, then perhaps they should specify whether the information already provided can continue to be used, or is withdrawn.

Membership in the DSSA-WG and the sub-groups will be monitored by the Secretariat.

6.7. Glossary

Adversarial threat source Individuals, groups, organizations or states that seek to exploit the DNS's dependence on cyber resources

Adverse Impact The harm to individuals and organizations that may occur as the result of a threat-event

Non-adversarial threat source Errors by individuals during the course of their everyday responsibilities, failures of equipment or software, and natural disasters and failures of critical infrastructure on which the DNS depends but which are outside the control of the providing/supporting organizations

Predisposing Conditions -- that positively or negatively impact risk A condition that exists within the DNS which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the world.

Risk -- to the DNS A measure of the extent to which the DNS is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: these risks are those risks that arise from the loss of confidentiality, integrity, or availability of the DNS and reflect the potential adverse impacts to: operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the world.

Security Controls The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Threat Event An event or situation that has the potential for causing undesirable consequences or impact.

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

6.8. Contact information

6.8.1. DSSA

6.8.2. Intermediaries for submitting information anonymously