Report of Public Comments

Title:	DNS Risk Management Framework Report
Publication Date:	18 October 2013
Prepared By:	Patrick Jones, ICANN Security

Comment Period:	
Comment Open Date:	23 August 2013
Comment Close Date:	13 September 2013
Reply Close Date:	5 October 2013
Time (UTC):	23:59 UTC

Important Information Links
Announcement
Public Comment Box
View Comments Submitted
Report of Public Comments

Staff Contact:	Patrick Jones	**Email:**	patrick.jones at icann.org

Section I: General Overview and Next Steps

ICANN engaged Westlake Governance to assist in the development of a DNS Risk Management Framework, under the oversight of the Board-level DNS Risk Management Framework Working Group (http://www.icann.org/en/groups/other/dns-risk-mgmt). A draft Framework was presented at the ICANN meeting in Beijing, China and revised following the ICANN Durban meeting in July 2013. The Framework was published for public comment on 23 August 2013.

Public comments were received from four organizations and individuals (Rick Koeller, ALAC, Verisign, and Anne-Marie Eklund Löwinder). Staff has prepared the following public comment summary.

Following the conclusion of the public comment process, the final DNS Risk Management Framework is to be implemented by ICANN staff, with oversight maintained by ICANN's Board Risk Committee.

Section II: Contributors

At the time this report was prepared, a total of 5 community submissions (2 from ALAC) had been posted to the Forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials.

Organizations and Groups:

Name	Submitted by	Initials
Rick Koeller, Canadian Internet Registration Authority (CIRA)	Rick Koeller	RK
At Large Advisory Committee	ICANN At Large Staff	ALAC
Verisign	Chuck Gomes	VRSN

Individuals:

Name	Affiliation (if provided)	Initials
Anne-Marie Eklund Löwinder	.SE (The Internet Infrastructure Foundation)	AMEL

Section III: Summary of Comments

General Disclaimer: This section is intended to broadly and comprehensively summarize the comments submitted to this Forum, but not to address every specific position stated by each contributor. Staff recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

RK and AMEL recognized that the Framework document provides a mature framework for ICANN to use as an internally facing document. AMEL noted that the report lacked references to activities that had been done already to address DNS risks. She also stated that the report is not clear if it is for ICANN the organization or for DNS risk management specifically. RK noted a similar issue with the report.

RK and AMEL also stated that there is nothing in the framework clearly tailored to DNS risks, and RK and ALAC acknowledged the work of the DNS Security and Stability Analysis Working Group (DSSA) as work that did provide tools and processes tailored for DNS risks. Both RK and ALAC stated it did not appear that the report analyzed the DSSA risk management tools. VRSN noted it was their view that the report was about risks to DNS systems, and they believe the issue ICANN should be concerned about is risks resulting from the DNS, without overlooking the former.

RK noted the framework lacks integration with the management of an incident and there's no obvious linkage with existing processes such as ICANN's Coordinated Vulnerability Disclosure process.

VRSN stated that the proposed Expert Panel must be independent of ICANN in the sense of being able to operate 'without fear or favor' of management or Board reactions, especially if the Expert Panel may have identified a risk that ICANN staff or managers were unwilling to address.

"ALAC deplores that the framework that is proposed is the proprietary and business oriented Risk Management methodology ISO31000 framework whilst the [DSSA] had proposed to use the Open Standard NIST 800-30 methodology. The use of a proprietary methodology effectively locks ICANN into a methodology from a vendor requiring licensing, which is likely to preclude the use of the methodology for other purposes by the community." AMEL also commented on this, stating, "while it is preferable to use common standards…I am convinced that ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization. This approach to formalizing risk management practices will facilitate broader adoption by companies who require an enterprise risk management standard to harmonize and get the work coordinated."

ALAC recommended that ICANN staff pursue a two-pronged approach for addressing the near term urgency of completing a DNS Risk Management Framework. First, ALAC recommended that staff examine the resource implications of implementation and maintenance of this specific Framework before recommending that it be adopted by the ICANN Board. Staff should evaluate whether this proposed Framework is indeed suited to the technical and political risks to the DNS.

Secondly, ALAC recommended that ICANN select quick wins to implement part of a risk mitigation framework. "The urgency in addressing purely technical risks to its own DNS operations is possible today thanks to the resources that ICANN already has at its disposal."

Section IV: Analysis of Comments

General Disclaimer: This section is intended to provide an analysis and evaluation of the comments received along with explanations regarding the basis for any recommendations provided within the analysis.

In response to the comments raised by RK, the Final Westlake report has been modified to clarify the scope of the DNS Risk Management Framework. Specifically, RK said "There is nothing within this framework that is clearly tailored for DNS related risk, unlike the tools and processes prepared by the DSSA Working Group." This is noted and more detailed processes will be incorporated in the implementation phase. Staff intends to use the work developed by the DSSA for analyzing DNS risks.

Further, in response to the comments from ALAC (they were "disappointed that the Framework as proposed was not built in a substantial way from the work undertaken by the DSSA"), staff will incorporate work developed by the DSSA in the implementation of the DNS Risk Management Framework.

In response to RK and AMEL's comments, the Final Report and implementation work will show better integration of ICANN's enterprise management processes and incident management handling (Coordinated Vulnerability Disclosure process, as an example). The implementation phase will also provide more granularity, as sought by ALAC. The DNS RMF a high-level principles-based Framework. Development of the "more granular" processes and tools is a separate task, which forms an essential part of the implementation phase.

ALAC commented that ISO 31000 is a business-oriented framework. This point was addressed in some detail during the Board Working Group Workshop at ICANN47 in Durban. As noted there, ISO standards are intended to be widely adopted and, as specifically noted within the Standard, to be adapted to the specific context within which it is to be applied. The "proprietary" nature of an ISO Standard relates in particular to the purchase of an original copy of the Standard and we are advised that ICANN has already done this. We do not accept that ISO31000 is a "business-oriented" methodology; it has been developed to be applicable within all types of organisations. ICANN is evaluating ISO 31000 along with NIST 800-30 and other recognized methodologies for examining risks (such as COSO, from the Committee of Sponsoring Organizations of the Treadway Commission,

http://www.coso.org/). Whichever methodology is used as part of ICANN's overall enterprise risk management, it needs to be a methodology that is global in scope and used by international organizations. In addition, whether it be ISO or COSO, the framework will be incorporated into the overall Enterprise Risk Management Framework once one iteration of risk assessment is conducted on the DNS RMF.

As noted by VRSN, a DNS Risk Management Framework needs to help ICANN with risks resulting from the DNS, without overlooking risks to DNS systems. Staff confirms that as part of implementation, risks resulting from the DNS (and the overall unique identifier system) will be part of the enterprise risk management process.

The accountability and transparency of ICANN's handling of enterprise and DNS risk management is important, and has been observed by the SSR Review Team. In response to VRSN's comment, the interests of the broader Internet community are being considered in the handling of enterprise risks and this will be highlighted during the implementation phase of the Framework. As noted above, ISO will be leveraged for the DNS risk evaluation and will be integrated into the COSO model, which is being used by the ICANN Enterprise Risk Management department.