EN

AL-ALAC-ST-0913-05-00-EN
ORIGINAL: English
DATE: 27 September 2013
STATUS: Final

AT-LARGE ADVISORY COMMITTEE

ALAC Statement on the DNS Risk Management Framework Report

Introduction

The following individuals composed an initial draft of this Statement after discussion of the topic within At-Large and on the Mailing Lists:

- Julie Hammer, ALAC Liaison to the SSAC and At-Large member from the Asian, Australasian and Pacific Islands Regional At-Large Organization (APRALO);
- Olivier Crépin-Leblond, Chair of the ALAC; and
- Alejandro Pisanty, At-Large member from the Latin American and Caribbean Islands Regional At-Large Organization (LACRALO).

On 4 September 2013, this Statement was posted on the At-Large DNS Risk Management Framework Report Workspace.

On that same day, Olivier Crépin-Leblond, Chair of the ALAC, requested ICANN Policy Staff in support of ALAC to send a Call for Comments on the draft Statement to all At-Large members via the ALAC Announce Mailing List.

On 19 September 2013, a version incorporating the comments received was posted on the aforementioned workspace. The Chair requested that Staff open a five day ALAC ratification vote on the Statement.

On 27 September 2013, Staff confirmed that the online vote resulted in the ALAC endorsing the Statement with 12 votes in favor, 1 vote against, and 0 abstentions. You may review the result independently under: http://www.bigpulse.com/pollresults?code=3430Htzv9HByhFUcWnLs2De7.

Summary

1. The fact that a risk management framework exists and is utilized to force rigor into the consideration of risk would be an important outcome
2. However, the ALAC deplores that the framework that is proposed is the proprietary and business-oriented Risk Management methodology ISO31000 framework whilst the DNS Security and Stability Analysis (DSSA) Working Group had proposed the use of the Open Standard NIST 800-30 methodology.
3. The ALAC also questions the use of a business methodology applied to the DNS.
4. The ALAC deplores that at this point in time, the proposed Framework is far from being detailed at a more granular level
5. The ALAC is disappointed that the Framework as proposed in the Final Report has not built in any substantial way on the work undertaken by the DSSA Working Group apart from mentioning its work.

ALAC Statement on the DNS Risk Management Framework Report

The ALAC has considered the Final Report submitted by Westlake Governance on an ICANN DNS Risk Management Framework and offers the following comments. The report provides a framework at a relatively high level, that draws on and combines several other frameworks (Mikes and Kaplan, Capability Maturity Model, ISO31000) and tailors them to some degree to the ICANN context of DNS risk. While it may be highly open to debate whether the proposed framework is optimal for ICANN, and individuals will have very different views based on their own experience of risk management and their place within the ICANN Community, to some extent the fact that a risk management framework exists and is utilized to force rigor into the consideration of risk would be an important outcome.

However, the ALAC deplores that the framework that is proposed is the proprietary and business-oriented Risk Management methodology ISO31000 framework whilst the DNS Security and Stability Analysis (DSSA) Working Group had proposed the use of 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. The DSSA had specifically chosen the NIST 800-30 methodology to allow the freedom of use associated with an Open methodology.

The ALAC also questions the use of a business methodology applied to the DNS. The Westlake Report appears to mix the Risk Framework for ICANN (the organization) with the Risk Framework for the DNS which is not a single organization, entails a wide variety of actors, both controllable and uncontrollable, and is therefore a much more complex ecosystem than a typical top-down corporate environment. In fact, the Framework appears to be for the most an inward-looking Enterprise Risk Framework for ICANN. It is unknown whether the ISO31000 methodology has ever been successfully applied to an outward facing technical risk management function.

The notion of external risk associated with unknown unknowns is minimized to reflect technical risks only. In fact, the proposed DNS Expert Panel appears to be focused almost entirely on technical risks thus lacking a component of political risk such as that caused by action in Internet Governance. Whilst technical threats to the DNS cannot be understated, recent examples of unilateral actions by Nation States has shown that political threats are to be equally taken into account, yet the use of a classical business-oriented Risk Management framework does not appear to give the ability to take those into account. The report definitely falls short of fully identifying all threats to the DNS.

In fact, the Westlake report is high level. The ALAC deplores that at this point in time, the proposed Framework is far from being detailed at a more granular level. It appears that the detail of the proposed Framework contained within the report would need to be further developed by ICANN Staff, with some input from the ICANN Community, before implementation would be feasible. In particular, the establishment of the proposed Expert Panel (previously called the Risk Advisory Group in the 24 June 13 draft), as detailed in the Appendix 4 Terms of Reference, constitutes a significant new permanent volunteer resource within ICANN. The Risk Register Template (Appendix 6) and Risk Mitigation Schedule (Appendix 7) are highly simplistic, without any metrics, and require a great deal of expansion and adaptation for the assessment and mitigation of DNS risk. It is unknown whether “treatment” and “monitoring” could all be done in-house or would need external resources or collaboration. Furthermore, the estimation of resourcing required (i.e. the information on the 'what, who and when' part of the process) seems to be pitched at what is required for the maintenance of an ongoing Risk Management system, but the ALAC considers that the initial implementation would need a much more concerted effort with considerable resourcing, both staff (ICANN the Organisation), volunteer (ICANN the Community) and outward facing (the wider Internet community).

Is this recommendation feasible, bearing in mind this Risk Management Framework is long overdue?

Indeed, the ALAC is concerned that it has been over a year since the publication of the Security, Stability & Resiliency of the DNS Review Team SSR-RT's Final Report, yet many of its recommendations are still far from being implemented. The ALAC therefore recommends that in the face of urgency, a two-pronged approach should be followed:

- ICANN Staff should examine in greater detail the resource implications of initial implementation and ongoing maintenance of this specific Risk Management Framework before recommending to the ICANN Board whether it, or some variation of it, should be adopted. It should evaluate whether this proposed Framework is indeed suited to the technical and political risks to the DNS.
- ICANN should select quick wins to implement part of a risk mitigation framework, drawing on already available resources such as SSAC, RSSAC, the DNS Community and the wider ICANN community. 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.

Those two parallel processes should be started while closely adhering to the recommendations of the SSR-RT.

On a more general note, the ALAC is disappointed that the Framework as proposed in the Final Report has not built in any substantial way on the work undertaken by the DSSA Working Group apart from mentioning its work. Most disturbingly, the instigation of this study led to a suspension of the important work of the DSSA, and effectively caused that bottom-up cross-community working group to lose all momentum for the continuation of the security risk assessment tasks which it had been chartered to undertake by ICANN’s SOs and ACs.