ICANN DNS Risk Management Framework

DRAFT for Working Group comment

24 June 2013

Submitted by Westlake Governance

Westlake Governance
1st Floor | 114 The Terrace | Wellington 6011
P O Box 8052 | The Terrace | Wellington 6143 | New Zealand

t +64 4 472 2007 | m +64 21 443 137 | im (skype) westlakenz1
e richard@westlakegovernance.com | w www.westlakegovernance.com | b www.boardsrus.net

Table of Contents

Context – ICANN and the DNS

Our Terms of Reference require the development of a DNS Risk Management Framework for ICANN, covering risks that are within ICANN's sphere of concern but not necessarily under its control.

ICANN's mission is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In addition, the first of ICANN's Core Values set out in Article II is:

> *Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet.*

This mission and value empower ICANN to take an overall view of the DNS as it has been doing for many years, for example through its Security and Stability Advisory Committee (SSAC).

At ICANN 46 in Beijing, in April 2013, we presented the principles on which we had based our work. These were as follows:

- *ICANN is a unique identity, embedded in a community of interest*

  ICANN is not a regular commercial company: it has a limited technical mandate, but within this it must consider the full breadth of risks to the security, stability and resilience of the DNS. ICANN's policy development is a collaborative bottom-up stakeholder-driven process, rather than the prescriptive, top-down, board-directed process more commonly evidenced in commercial entities, and in many governmental and not-for-profit organisations.

- *The DNS is a technically unique and important system, comprising:*

  1. The files of information mapping labels to IP addresses (zone files)

2. The hardware and software required to interrogate the zone files (name servers)
3. The technical standards that set out how name resolution works and how name servers interoperate

The DNS is distributed in that parts of it are run in different locations under the control of various organisations. There is no one body responsible for the operations of the entire DNS, nor is there a central repository of DNS contents.

- *Provide a means of fostering an enduring risk culture within ICANN*

  This risk culture should pervade the whole of ICANN, led from the most senior levels, and must not be confined to one particular division.

- *Avoid a monoculture*

  It is important to find multiple approaches to identifying and addressing risk, to reduce the potential for groupthink, or for risk management to become a compliance function rather than a strategic tool for protecting the DNS.

- *Adapt not reinvent*

  In order to deliver a robust and relevant Risk Management Framework, we have built on currently accepted authoritative frameworks and on work already done, notably by the DNS Security and Stability Analysis (DSSA) Working Group.

- *Process is not a substitute for thought*

  The DNS is evolving rapidly, and so is the threat environment in which it operates. While a coherent set of risk management processes is

essential, those involved in protecting the DNS must not follow process blindly: they and the framework for managing risk must be able to sense and respond to changes in the external and internal context and the understanding of threats.

We aimed to adapt an existing RMF, rather than inventing a new process …

Internationally, organisations have a range of choices regarding standardised risk management approaches, including, among the best known:

- The Committee of Sponsoring Organizations of the Treadwell Commission (COSO) "Enterprise Risk Management-Integrated Framework," published in 1994 and revised in 2004.
- The United States National Institute of Standards and Technology (NIST) 800 Series of Risk Management Standards for Computer Security, and in particular Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems."
- The International Organization for Standardization (ISO) Risk Management Standard ISO: 31000-2009 (ISO 31000), developed from the Australian/New Zealand Standard 4360, published in 2004.

Because of the uniqueness of ICANN and the DNS, we concluded that any existing framework would require modification. We eliminated the COSO Framework, largely because of its complexity, which we consider is more suited to very large and complex corporations and government entities.

We also looked in some detail at the significant work already undertaken by the DSSA Working Group regarding standardised risk assessment approaches. We understand that the DSSA selected and tailored a risk-assessment methodology based on the NIST 800 series of risk management standards. The DSSA modified the NIST assessment approach (while remaining true to the essence of the methodology)

by developing a framework for assessing and treating an identified "Adversarial" or "Non-Adversarial Threat Source."

However, in developing a comprehensive Risk Management Framework, we consider it important to address the broader context, as well as the process for assessing and treating DNS risks, and for consulting, communicating, monitoring and reviewing, in order for the Framework to become an embedded and enduring part of 'how ICANN does things,' and with potential for wider adoption across ICANN.

We concluded for several reasons that the most suitable 'platform' from which to develop a DNS Risk Management Framework for ICANN was ISO 31000:

- It is widely accepted as the global Standard for risk management
- It is suited to organisations in all sectors, of all types and sizes
- It is reflects current best practice risk management, having been published in 2009
- It specifically notes that "one size does not fit all" and implementation of the Standard requires adaptation to meet the needs of each organisation.

In practice, the choice of framework as the platform from which to build is less important than the logic applied in adapting and implementing it to the specific context of ICANN and the DNS (refer Principle: Process is not a substitute for thought). Most of the published frameworks discuss some variant on the four main steps: understanding the context, assessing the risks (identification, analysis, evaluation), treating the risks, and monitoring. In the specific context of the DNS, its operations involve a wide range of organisations and people, including, among others:

- IANA (a service operated by ICANN)
- NTIA (part of the US Department of Commerce)

- Root server operators (including ICANN)
- TLD registries
- Name server operators
- Internet Service Providers

Other bodies, although not DNS operators, have an involvement in DNS security including CERTs, ISOC, IETF and DNS OARC.

ICANN itself has several roles in the DNS, but it does not exclusively operate any part of the DNS except IANA. (ICANN operates L root, but it is one of several root operators.) ICANN's policy role also is one of coordination – it provides a forum and structures for the development of policy.

We built on the platform that we selected …

Several commentators (most recently Mikes and Kaplan, Harvard Business Review June 2012) suggest that standardised rules-based approaches to managing risk often do not deliver what is expected of them and propose that risks in different categories need to be managed in different ways, again reinforcing that one size does not fit all.

Analysis of the interviews we have conducted with ICANN stakeholders (internal and external), and our further research and testing, led us to the view that a combination of improved risk categorisation and a standardised approach to management would provide the best possible outcome for the successful implementation of a framework that ICANN will use to manage DNS risks, within the technical mission specified in its by-laws.

Protecting the DNS involves preserving its important features in the face of various threats. This leads to the question - what are the DNS's important features? Various

answers have been proposed, but we conclude that these all fall under one the following:

- ***Availability*** – meaning that a properly configured resolver that is connected to the Internet can resolve a name within a reasonable response time.
- ***Consistency*** – a request to resolve a name on the Internet should return the same result wherever it is asked and whenever it is asked (subject to the DNS records not being changed in the meantime).
- ***Integrity*** – DNS lookups will be an accurate reflection of the records in the zone files.

DNS risk management requires that threats to one or more of these key features of the DNS should be identified and made the subject of a formal management regime. Put another way, an event that does not affect the Availability, Consistency or Integrity of the DNS is outside the scope of the risk management framework.

The analysis into Availability, Consistency and Integrity (ACI) above is consistent with ICANN's traditional focus on the DNS's Stability, Security and Reliability (SSR). Our objective in developing the Risk Management Framework is to provide ICANN and its community with a tool to meet its security, stability and resiliency obligations.

SSR represents an internal view of the DNS, from the perspective of people who understand its workings and many of the threats it faces. ACI is an external view that does not require understanding of the complexity of the technology or the threats it faces, emphasising what the DNS delivers rather than the prerequisites for its successful operation.

Our initial steps in adapting the basic platform were to recognise the differing sources of risk, as identified by Mikes and Kaplan:

- Risks described as 'controllable' – most usually of an operational or internal nature. These are risks that provide the organisation no strategic benefit, so

the organisation's response is to reduce, eliminate, avoid or transfer such risks to the extent that the benefits (financial or non-financial) outweigh the cost. The organisation treats such risks by reducing the probability of the risk event occurring, and/or the severity of the impact if it does occur. For such risks, a traditional rules-based approach is often the most appropriate.

- External events – over whose probability of occurrence the organisation has no control. For these, the only practicable option is to anticipate and where appropriate mitigate their impact. These risks typically divide into three further categories:
    - Short-term (sometimes immediate): for example natural disasters – floods, hurricanes, landslides and earthquakes.
    - Medium-term: for example economic or political change – the economic growth environment, currency or interest rate movements, or changes in government policy.
    - Longer-term: for example social or demographic changes – movements in the global strategic balance, the 'grey tsunami' in the population of many developed nations, demographic changes resulting in new channels for accessing the Internet or evolving norms for privacy of information.
- Strategic risks – those risks that the organization chooses to incur in order to generate a strategic benefit: for example organizational, financial or reputational stress incurred as a result of a major strategic initiative. Once identified, the benefit/cost ratio of mitigating such risks is considered as a part of the overall strategic decision.

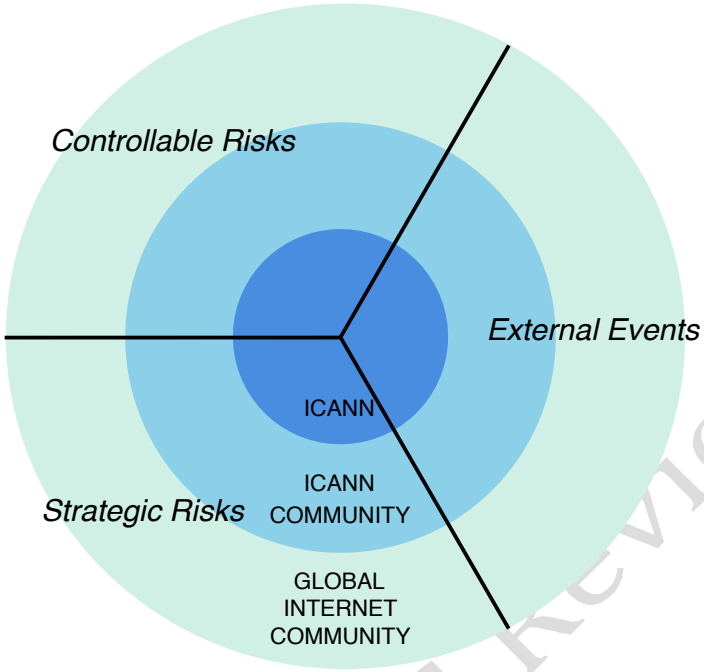
This categorization provides a useful foundation for ensuring that the organization does not approach, identify or treat all types of risk similarly.

The unique nature of ICANN provides a further dimension, because its 'community of interest' is far broader than its span of control, or even in many cases of its ability to influence significantly or manage its risks directly.

These considerations led to our developing a conceptual taxonomy for the Risk Management Framework, as in the diagram shown on the following page.

- The *three sectors* relate to the three categories of risk, while
- The *increasing radius from the centre* of the circle represents, in diminishing order, the ability of ICANN to apply risk mitigations or controls (as illustrated in the ICANN presentation "ICANN Security Ecosystem Map – Security Overview" – See Appendix 2):

    1. The *central* circle represents ICANN itself, within which the ICANN board has direct influence and control.
    2. The *second* ring represents the ICANN community, of which ICANN is a part and within which consensus for action is sought and built.
    3. The *outer* ring represents the global Internet community, which may be the subject of outreach from the ICANN community when changes affecting the DNS are being considered.



Some institutional risks are inherent to all organisations …

ISO 31000 defines risk as 'the effect of uncertainty on objectives.' As commentators including Kaplan and Mikes have noted, risk management is not a natural process: it runs directly counter to the positive, 'can do' culture of achievement and success that many organisations foster. The essence of risk management by contrast is about identifying and assessing what could go wrong, or could deflect an organization from achieving its goals. As a result, an organisation's culture, resulting from the structures, processes, accepted behaviours and incentives that evolve over many years may actively discourage or hinder (whether consciously or subconsciously) implementation of effective risk management.

In its 2012 report, "Roads to Ruin", the British Association for Risk and Insurance Management Professionals (Airmic) has analysed the origins and impact of many corporate crises over the last decade. The report identifies seven key risk areas that

are potentially inherent in all organisations and that can pose a major threat to any firm that fails to identify and manage them:

- Limitations on board skills and the ability of non-executive board members effectively to monitor and control the executives.
- The failure of boards to understand and engage with important risks, to the same degree that they focus on opportunity and reward.
- Poor leadership of an organisation's ethics or culture.
- Risks arising from the defective internal flow of information, including to senior management and board (where, for example, a risk may be identified at an operational level but not adequately communicated to more senior levels, where the strategic importance of the risk might be appreciated and acted upon).
- Risks arising from excessive complexity, such as the development of complex products or services which generate risks that are not fully appreciated, or a strategy of driving multiple strategic change projects simultaneously without analyzing or testing the cumulative or consequential impacts.
- Risks arising from inappropriate incentives, where success and growth typically generate higher rewards than effective risk management.
- Risk 'glass ceilings' arising from the inability of risk managers, or those who have identified significant risks, to report such risks at a more senior level, whether because of unwillingness at senior levels to hear bad news, which may be seen as a challenge to existing strategies, or an organisational culture of "shoot the messenger".

We consider that an external perspective may mitigate these threats …

It is immensely difficult for people inside an organisation to remain completely objective about its culture. Therefore, we recommend that one means of providing greater assurance against such threats is to appoint a qualified and experienced group to help with identifying, classifying and understanding the relevant risks, and for ensuring that they are treated appropriately, including, if necessary, through escalation to higher – or the highest – decision-making levels in the organization.

We have therefore recommended that ICANN should create a "DNS Risk Advisory Group" (Advisory Group) to help ensure the continued effectiveness of the DNS Risk Management Framework when it has been implemented.

The members of the Advisory Group would be drawn from highly capable people likely to have significant experience in technical aspects of the DNS. Its members may come from, for example, the Root Server System Advisory Committee (RSSAC) or the Security and Stability Advisory Committee (SSAC), or they may be employees of organisations with extensive DNS-related operations. Advisory Group membership should be balanced so that all the important areas of DNS operation are represented.

To be effective, the Advisory Group must be independent of ICANN in the sense of being able to operate 'without fear or favour' of management or board reactions, especially if the Advisory Group may have identified a risk that ICANN staff or managers were unwilling to address. Such unwillingness may, for example, arise because mitigation strategies could threaten achievement of managers' targets (see above – inappropriate incentives), so ICANN employees or voting board members would not be members of the Advisory Group, although members of staff would need to participate in its activities and provide it with administrative support. This group will in effect act as ICANN's 'guardians of the risk culture' in relation to the DNS.

We have considered the skills that ICANN staff need in order to implement the DNS Risk Management Framework …

To implement the Framework effectively, risk management skills will be needed at several levels in the organisation.

1. Effective risk management must operate and report independently of line management engaged in the organisation's core activities. The role of risk managers is to analyse and question, and it is important that they are not subjected to conflicting incentives.

2. Effective risk management must operate at all levels in the organization. To this end we note ICANN's intention (announced at ICANN 46) to appoint a Chief Risk Officer who will operate as a member of the Chief Executive's leadership team. We also note that the new Chief Operating Officer is described as having significant senior risk management experience and expertise. Both of these are positive steps in ensuring a full awareness and more effective risk management.

3. It would appear that the capacity of existing staff to assume additional risk management responsibilities or tasks is limited. Any significant new or expanded function is likely to require a new staff position.

4. Under its current and proposed structures, ICANN

    a. Has a Board Risk Committee whose activity is likely to increase with implementation of the DNS Risk Management Framework. This committee will have the tasks of regularly reviewing the Risk Management Framework, holding risk managers accountable and making risk-related recommendations to the board. This provides the high level oversight to ICANN's DNS risk management activities.

b. Will have an independent and highly qualified DNS Risk Advisory Group whose main job will be to assess and manage highly technical risks, escalating these to appropriate levels of management where necessary, that may be beyond the direct expertise of the Board Risk Committee or other risk managers.

c. To provide support to these two groups, and the employees currently charged with managing various risk aspects in ICANN, we consider that ICANN will need to engage one or more risk management support staff. They will be responsible for day-to-day management of the Risk Management Framework and will work closely with the current staff. They will have more generic administrative and risk management experience and skill, and potentially less detailed technical understanding, than members of the Advisory Group, since their role is largely to support the substantive operation of the Framework.

d. We recommend that a capability assessment be undertaken to determine the appropriate number of risk management staff. Because the nature of threats and the environment in which the DNS operates change constantly, the skills and attributes required to manage risk effectively will also change. Accordingly is important that regular review of these is an integral part of the overall process of continuous improvement when the DNS Risk Management Framework has been established.

The DNS Risk Management Framework

Purpose of the DNS Risk Management Framework

The DNS Risk Management Framework (DNS RMF) defines risk as 'the effect of uncertainty on the DNS achieving Availability, Consistency and Integrity (ACI)'. While this uncertainty may be either negative or positive, the principal focus of the risk management framework is on negative uncertainty, i.e. downside risk.

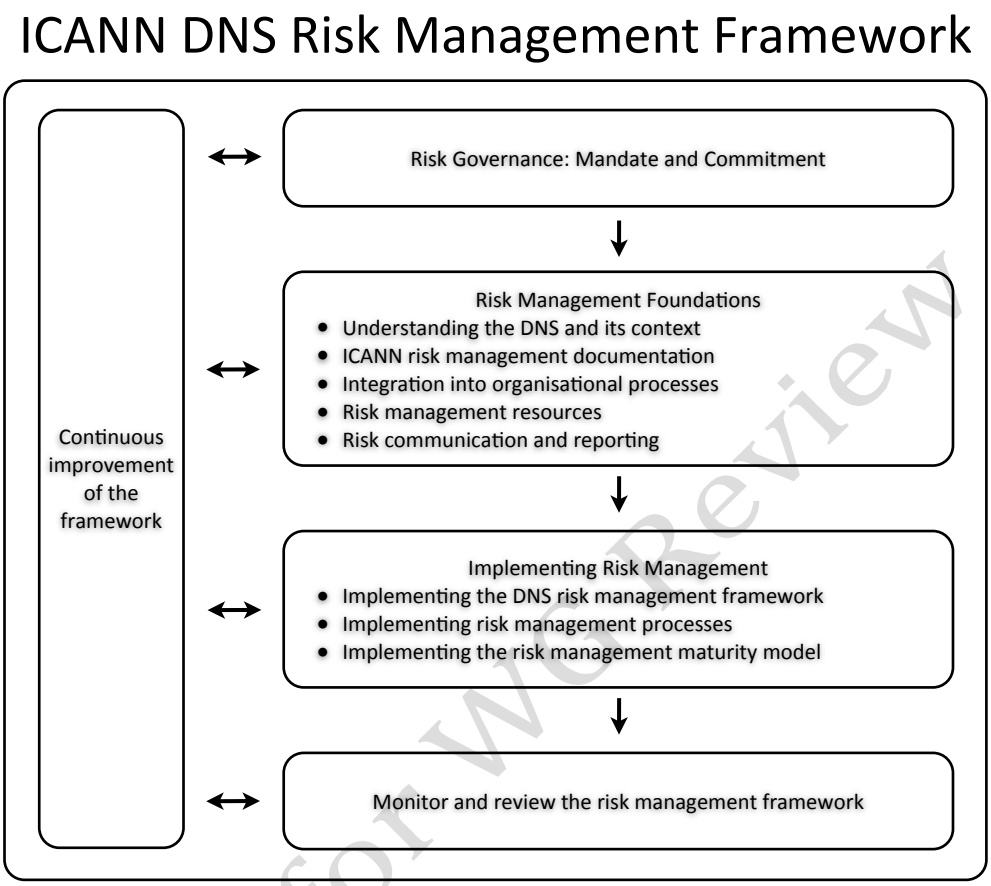
The DNS RMF sets out ICANN's arrangements for ensuring that robust, reliable risk management occurs throughout the organisation and community, and assists the Board to meet its risk management governance obligations.

The purpose of the DNS risk management framework is to:

- Describe the components of the DNS risk management system
- Assure the Board that ICANN has the necessary arrangements in place to ensure that effective risk management is implemented appropriately given ICANN's mandate in relation to the DNS
- Inform ICANN staff and the community of ICANN's arrangements and expectations in regard to DNS risk management

The DNS RMF is aligned with ISO 31000 and represents current best practice. The framework specifically addresses risks arising from three different risk categories (controllable risks, external events and strategic risks). The framework also reflects the unique and distributed nature of the DNS and the broad range of community members potentially involved in identifying, analyzing and mitigating risks.

The DNS Risk Management Framework Diagram



Risk governance - mandate and commitment

The mandate for DNS risk management comes from the ICANN Board and Board Risk Committee (BRC). The continuous engagement and support of these governance bodies is critically important – without it, risk management will fail. Members of ICANN's governing bodies must understand this and be committed to ensuring sustainable and effective risk management in the DNS.

The ICANN Board and BRC lead this commitment by:

- Endorsing and implementing the DNS RMF and overseeing work to ensure that it remains relevant
- Understanding the value added by risk management and communicating this to the community and staff
- Aligning risk management activities with the achievement of organisational objectives
- Ensuring legislative and regulatory compliance
- Assigning accountabilities and responsibilities for risk management to appropriate staff
- Ensuring that risks can be raised to the highest level without fear of punitive outcomes
- Allocating the necessary resources to risk management, for example: expert advice, education, facilitation, coordination
- Challenging executive and management decisions and proposals
- Encouraging transparent identification and open discussion of risks
- Monitoring the effectiveness of DNS risk management and ensuring its continual improvement.

Risk management foundations

Five foundations must be in place for the successful implementation of DNS risk management. These foundations are:

1) Understanding ICANN and the DNS

2) ICANN DNS risk management documents as set out in the table below.

3) Integration of risk management into organisational processes

4) Risk management resources

5) Risk communication and reporting mechanisms

1. Understanding the DNS and ICANN

The risk management framework has been designed to be effective given the unique nature of both ICANN and the DNS.

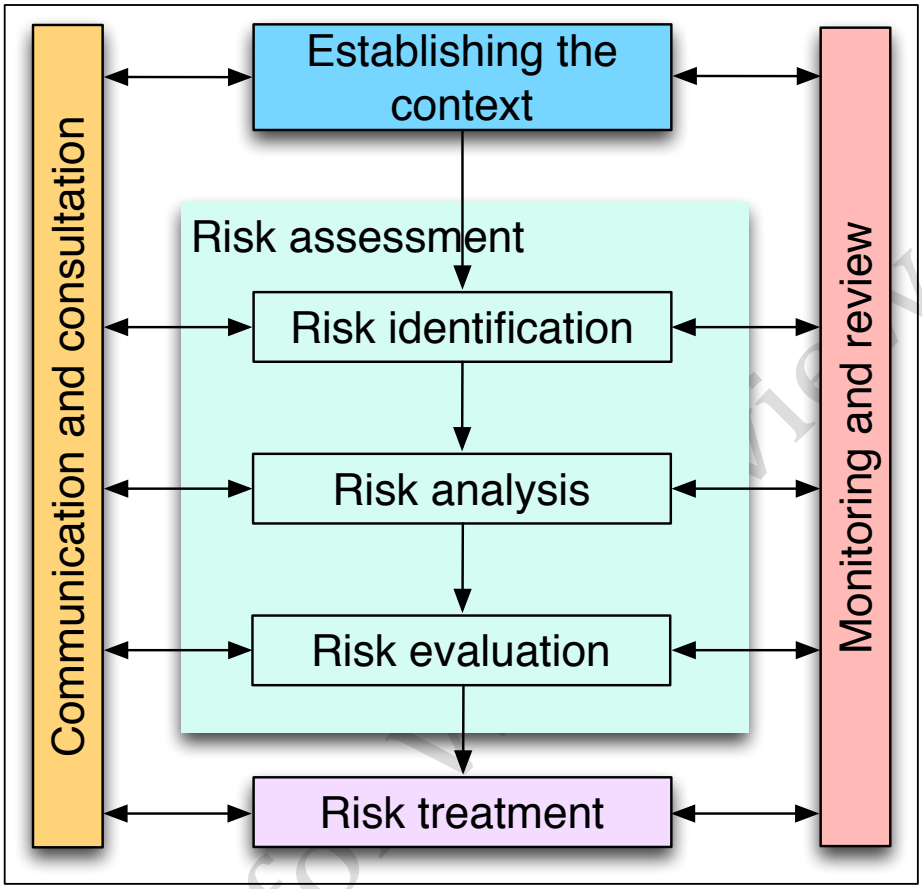
The context within which ICANN and the DNS operate has been described in the earlier section, Context – ICANN and the DNS.

2. ICANN DNS risk management documents

A suite of four documents will be developed to describe ICANN's DNS risk management system and processes. These are the foundation documents for risk management of the DNS within ICANN.

As discussed in the Context Section of this report, ISO 31000 was chosen as a 'platform' to build the DNS RMF. The risk management processes within the Standard (summarised below) form part of the foundation for the framework.

ISO 31000 Risk management process
(Refer Appendix 1 for a detailed explanation of each step)



The table below describes the purpose of each of the documents and who is responsible for endorsing them.

Document	Purpose	Endorsed by
DNS Risk Management Framework	**Why and how ICANN ensures effective risk management of the DNS.** • To describe the rationale for risk management and ICANN's foundations and arrangements for ensuring that effective risk management is implemented.	ICANN community and Board
DNS Risk Management Strategy	**What risk management strategies ICANN will implement.** • To define ICANN's vision for risk management. • To specify ICANN's commitment to providing an organisational environment that supports effective risk management. • To specify ICANN's risk appetite.	ICANN Board/BRC
DNS Risk Management Policy	**How the RMF and strategy will be implemented and who is responsible for various aspects of implementation.** • To specify: o the responsibilities and accountabilities of staff for implementing risk management within their area of control o the linkages between and within business processes to ensure that risk management is fully integrated into all organization activities, while avoiding duplication and gaps o how risk management performance will be measured and reported o communication mechanisms for: community members, confidential risks and escalating risks.	ICANN BRC and staff
DNS Risk Management Manual	**How to manage risk.** • To provide detailed guidance, tools and templates to ICANN staff and the community to assist them consistently implement effective and efficient risk management.	ICANN Staff and DNS Risk Advisory Group

3. Integration into organisational processes

Effective risk management must be embedded in ICANN's systems and processes to ensure that they are part of 'the way we work'.

In particular where planning processes introduce potential new risks to the DNS, these must be addressed using the management processes outlined in the risk management processes outlined in the section, The DNS Risk Management Process.

Risk management responsibilities should be included in:

- Position descriptions
- New staff induction
- Education and training programmes and
- Staff performance reviews

All Board papers that propose action relevant to the DNS should contain a section about DNS Risk Management.

4. Risk management resources

The ICANN Board allocates the resources necessary to ensure organisational risk management capability.

- *Personnel with relevant knowledge, skills and experience*
    - Chief of Assurance and Risk
    - Assurance and Risk: Risk Management Specialist
    - Internal audit

- DNS Risk Advisory Group (refer Appendix for Terms of Reference)

- *Specialised risk control functions within ICANN's management systems including:*
  - Internal audit
  - Business continuity/emergency response planning
  - Security systems
  - Contracting
- *Risk management system support including:*
  - Risk management documents
  - ICANN DNS risk register

5. Risk communication and reporting mechanisms

Robust risk communication and reporting mechanisms encourage and support accountability and ownership of risks, as well as building community confidence in ICANN's capacity for identifying and addressing DNS risks.

- *Internal communication and reporting*
  - Clear responsibilities and accountabilities for risk management are stated in position descriptions, policy documents, delegations of authority and performance review documents
  - Quarterly risk reports are provided to the Senior Leadership Team and the Board Risk Committee

- Advisory Group conducts quarterly (or as required) reviews to identify emerging and decreasing risks
- Risk management staff inform the Board Risk Committee of any new or emerging risks that may impact DNS ACI
- ICANN is committed to an environment where risks are openly discussed, and escalated as required

- *External communication and reporting*
  - ICANN will develop and implement a policy, that specifies what risk management information from the risk register will be made available to the community

Implementing DNS Risk Management

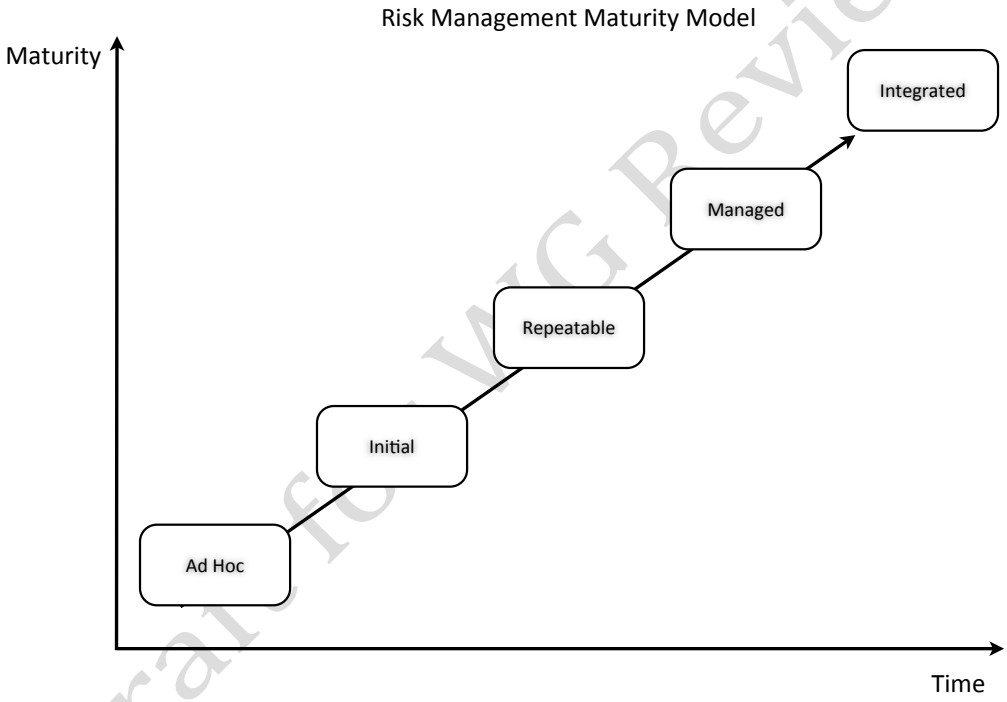
To successfully implement the DNS RMF, ICANN will need to:

- Assess current capabilities and resources, compared to requirements
- Define and agree the appropriate timing for implementation
- Develop and integrate the risk management policies and processes into current organizational processes
- Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes
- Hold information and training sessions, and
- Communicate and consult with community members

Risk Management Maturity Model

- The risk management maturity model (see below) illustrates the different stages of maturity of risk management.

- At any point in time, different parts of ICANN may be at different levels of maturity.
- ICANN should assess its current level of risk management maturity and then develop a plan to improve maturity, since, as described in the matrix on the next two pages, the greatest benefits of risk management are gained at the integrated level.



Maturity Level	Ad Hoc	Initial	Repeatable	Managed	Integrated
Leadership	Senior leaders address high-level risks as they arise. Short-term RM focus. Reactive RM.	Board mandate for risk management. One senior leader has responsibility for RM. Specific risks discussed at senior leadership meetings.	Senior leaders regularly review risk reports. Strong focus on compliance risks. Medium-term RM focus.	Organisational risks are identified and a plan is developed to address these. Each senior leader actively promotes risk management within their areas as a means to achieve business goals and to add value.	Board and senior leaders model best practice RM. RM is not a separate agenda item but incorporated into 'the way we work'. Customer and supplier input sought. Proactive approach.
Culture	Perception that notifying a risk is a sign of failure. RM seen as a cost, not a benefit.	Recognition that some risks exist and need to be addressed. Risks are discussed informally and escalated as deemed appropriate by the individual.	Growing awareness of risk. Increasing willingness to use formal channels to notify and escalate risks. Low morale of risk champions	Risks are regularly identified by staff and managers and escalated as required. There are no surprises. RM still seen as an add-on to business as usual. Longer-term RM focus implemented.	RM is central to business as usual. All decision-making involves explicit consideration of risks. Increasing focus on opportunities, process improvement, innovation and adaptability.
RM Procedures	No standardised RM procedures. Ad hoc approaches applied on a case-by-case basis.	RM procedures are beginning to be identified and are communicated verbally. High reliance on the knowledge of individuals.	RM policy and procedures documented but only partial/ inconsistent implementation. Some RM tools and templates developed.	RM policy and procedures are regularly reviewed to incorporate best practice RM. Appropriate RM tools and templates are available to staff. RM implementation plan exists. All key risks recorded in one repository.	RM framework and strategy documented and known to staff. RM procedures are continuously improved based on benchmarking/learning from other organisations.

Maturity Level	Ad Hoc	Initial	Repeatable	Managed	Integrated
Capability	No understanding or experience of risk management and its link to the achievement of business objectives.	External expert RM advice obtained. Some RM education may be provided to senior leaders. Heavy reliance on historical practice.	One or more in-house RM experts appointed. RM education sessions provided to some staff and managers. RM expertise limited to a few.	Adequate in-house RM support appointed. RM responsibilities are documented in all position descriptions. All new staff receive key RM information. RM education sessions regularly available.	Most staff and managers are competent in RM. External advisors may be used under the initiative of in-house personnel. RM success is celebrated.
Integration	RM is seen as an 'extra' which must be done in response to a crisis situation.	RM is seen as an additional requirement to business as usual	RM is applied primarily to projects.	RM is applied vertically through the line management structure. Silo thinking results in duplication of effort to address the same risk separately in different areas. Silo responses to risks may negatively impact on other services.	RM occurs across hierarchies and organisation boundaries. RM is applied to key business processes operating across the organisation.
Monitoring	No monitoring or reporting of risks.	RM reports provided to Board annually or six-monthly. These are narrative and based on the knowledge of key individuals.	Compliance with RM policy is variable across the organisation. Risk reporting remains largely qualitative.	Compliance with RM procedures is monitored and actions taken to address non-compliance. Achievement of risk plans is reported at least quarterly. Some quantitative RM analysis occurs.	Full qualitative and quantitative RM trend analysis occurs. Effectiveness of RM is monitored and informs future RM. RM failures reviewed to identify learnings.

Monitoring and review of the risk management framework

The DNS risk management framework has been developed at a point in time. As the DNS, ICANN and community objectives change, it is important that the framework evolves to remain both relevant and effective.

The framework should be monitored and reviewed annually, with any gaps or duplication of activity documented and remediated.

Table of proposed monitoring/review actions:

Action	Responsibility	Timeframe
Report on the following indicators: • % required risk treatment plans (as specified in the DNS Risk management policy) documented and held on central record (target = 100%). • % ICANN managers who have attended/completed risk management education sessions (target = 100% within two years).		Quarterly
Provide evidence that risk treatments are successful in reducing / managing DNS risk levels, and that emerging risks are identified as soon as possible		Quarterly
Audit compliance with the risk management policy so that any changes needed can be made as part of the policy review process.		Annually
Review the effectiveness of the ICANN DNS risk management framework.		Annually
Present an annual report on ICANN's DNS risk management performance and effectiveness to the BRC and Board (include: learning from experience; emergency and continuity preparedness; compliance and changes to context)		Annually
Evaluate ICANN's culture of risk awareness.		Every 3 years

Continual improvement of the DNS risk management framework

The DNS risk management framework should be reviewed annually to identify whether changes are required to make it more effective in achieving increasing maturity of risk management in the organisation. These changes are made as needed.

The DNS Risk Management Process

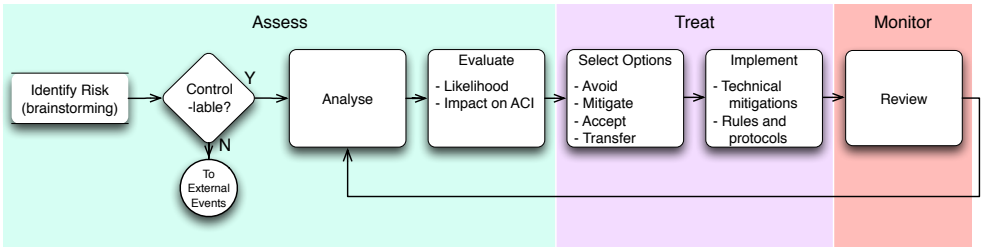
This section sets out the processes for ICANN's DNS risk management. They are divided into processes for controllable risks, external events and strategic risks, in terms of the definitions discussed above.

Each process is set out as a flowchart, and every step is described below (under colour-coded headings for easy reference to the relevant step in the flowchart), along with the identity of its participants, its outputs, and its frequency.

1. Process for Controllable Risks

Controllable risks are those whose likelihood can be managed.

Controllable Risks



ICANN board	O	O	O	O	O	As required	O
ICANN staff	L	I	L	L	L		I
DNS RAG	P		P	P	P		P
SSAC / RSSAC	C		C	C	C		
ICANN Community	C		C	C	C		
DNS Community	C			C	C		

Legend: Oversee Lead Participate Consult Implement

Activity:	**Identify Risks**	*Risk Type:*	**Controllable**

Detail: Controllable risks are those whose likelihood can be managed as well as their impact. These risks can and should be identified by two means:

1) Brainstorming sessions of the Advisory Group led by ICANN staff
2) Soliciting input from SSAC / RSSAC, the ICANN community and wider DNS community through a dedicated email box. This should be sanity checked by ICANN staff and provided to the Advisory Group inter-sessionally if found to be urgent.

It is possible that risks identified may be confidential. Advisory Group and ICANN staff will need to be able to manage risks whose existence is confidential, and to deliberate in private where necessary.

Who does it: Advisory Group led by staff with input from SSAC / RSSAC, ICANN community and wider DNS community as those parties see fit.

When it is done: On a quarterly basis, or at least 3 times annually in line with ICANN meetings.

Inter-sessional work as necessary to deal with urgent risks as they are discovered.

Output: List of risks in the risk register.

Activity:	**Classify Risks**	*Risk Type:*	**Controllable**

Detail: Determine whether risk identified is external or controllable.

Who does it: ICANN staff.

When it is done: As risks are identified by the Advisory Group or others.

Output: Appropriate classification in the risk register.

Activity:	**Analyse Risks**	*Risk Type:*	**Controllable**

Detail: In depth analysis of risk. Likely to involve a desk exercise and possibly experimentation.

Who does it: The Advisory Group supported and led by ICANN staff. Input will be sought from SSAC / RSSAC and from the ICANN community if necessary.

When it is done: As part of regular Advisory Group session, or inter-sessionally if urgent.

Output: A detailed description of the risk in the risk register.

Activity:	**Options**	*Risk Type:*	**Controllable**

Detail: For each controllable risk, consider options to:

- Avoid the risk
- Mitigate the impact of the risk
- Accept the risk
- Transfer the risk to others

Any decision to accept or transfer a risk (assessed as being above an agreed threshold of materiality) would need to be made by the Board.

Who does it: Advisory Group supported and led by ICANN staff, with input from the SSAC / RSSAC, ICANN Community and wider DNS community as appropriate.

When it is done: As part of regular Advisory Group session, or inter-sessionally if urgent.

Output: Noted in risk register. A Board minute if necessary.

Activity:	**Evaluate Risks**	*Risk Type:*	**Controllable**
Detail:	For each controllable, evaluate: • Its likelihood • Its impact on availability, consistency and integrity		
Who does it:	The Advisory Group supported and led by ICANN staff. Depending on the potential impact and scope of any potential mitigation, input will be sought from SSAC / RSSAC, the ICANN community and possibly the wider DNS community.		
When it is done:	As part of regular Advisory Group session, or inter-sessionally if urgent.		
Output:	An evaluation of the likelihood and impact of the risk to be recorded in the risk register.		

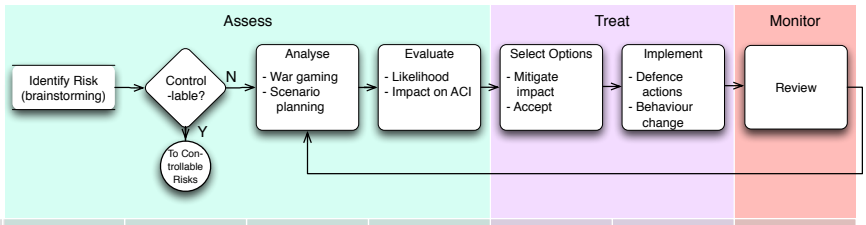
Activity:	**Treat**	*Risk Type:*	**Controllable**
Detail:	Likely to involve technical mitigations and / or behaviour changes through applying rules and protocols.		
Who does it:	Dependent on the mitigations chosen. If the mitigation involves changes in more than the span of ICANN's control, there may need to be a communications programme to influence others to change.		
When it is done:	After the decision has been made to mitigate the risk.		
Output:	Implementation.		

Activity:	**Review**	*Risk Type:*	**Controllable**
Detail:	Review the mitigations and the residual risk likelihood and impact; consider further mitigation.		
Who does it:	ICANN staff with Advisory Group participation, Board to oversee.		
When it is done:	At least annually.		
Output:	Note the review in the risk register.		

2. Process for External Events

External events are risks whose likelihood cannot be managed; all that can be done is to mitigate their impact or accept them.

External Events



ICANN board	O	O	O	O	O	As required	O
ICANN staff	L	I	L	L	L		I
DNS RAG	P		P	P	P		P
SSAC / RSSAC	C		C	C	C		
ICANN Community	C		C	C	C		
DNS Community	C			C	C		

Legend: Oversee Lead Participate Consult Implement

Activity:	**Identify Risks**	*Risk Type:*	**External**

Detail: External event risks are those for which the probability cannot easily be managed, such as natural disasters , government action or demographic shifts. They should be identified by two main routes:

1) Brainstorming sessions of the Advisory Group led by ICANN staff
2) Soliciting input from SSCA / RSSAC, the ICANN community and wider DNS community through a dedicated email box. This should be sanity checked by ICANN staff and provided to the Advisory Group inter-sessionally if found to be urgent.

It is possible that risks identified may be confidential, e.g. a zero-day exploit. Advisory Group and ICANN staff will need to be able to manage risks whose existence is confidential, and to deliberate in private where necessary.

Who does it: Advisory Group led by staff with input from SSAC / RSSAC, ICANN community and wider DNS community as those parties see fit.

When it is done: On a quarterly basis, or at least 3 times annually in line with ICANN meetings.

Inter-sessional work as necessary to deal with urgent risks as they are discovered.

Output: List of risks in the risk register.

Activity:	**Classify Risks**	*Risk Type:*	**External**

Detail: Determine whether risk identified is external or controllable.

Who does it: ICANN staff.

When it is done: As risks are identified by the Advisory Group or others.

Output: Appropriate classification in the risk register.

Activity:	**Analyse Risks**	*Risk Type:*	**External**

Detail: In depth analysis of external risk. Techniques could include war gaming and scenario planning to establish a range of possible outcomes.

Who does it: The Advisory Group supported and led by ICANN staff. Input will be sought from SSAC / RSSAC and from the ICANN community if necessary.

When it is done: As part of regular Advisory Group session, or inter-sessionally if urgent.

Output: A detailed description of the risk in the risk register.

Activity:	**Evaluate Risks**	*Risk Type:*	**External**

Detail: For each external risk, evaluate:

- Its likelihood
- Its impact on availability, consistency and integrity

Who does it: The Advisory Group supported and led by ICANN staff. Depending on the potential impact and scope of any potential mitigation, input will be sought from SSAC / RSSAC, the ICANN community and possibly the wider DNS community.

When it is done: As part of regular Advisory Group session, or inter-sessionally if urgent.

Output: An evaluation of the likelihood and impact of the risk to be recorded in the risk register.

Activity:	**Options**	*Risk Type:*	**External**

Detail: For an external risk, consider options to:

- Defend against the impact of the risk
- Accept the risk

Any decision to accept rather than defend against the risk would need to be made by the Board.

Who does it: Advisory Group supported and led by ICANN staff, with input from the SSAC / RSSAC, ICANN Community and wider DNS community as appropriate.

When it is done: As part of regular Advisory Group session, or inter-sessionally if urgent.

Output: Noted in risk register. A Board minute if necessary.

Activity:	**Treat**	*Risk Type:*	**External**

Detail: Implement defensive actions against the risk. These could be technical or involve behaviour changes.

Who does it: Depends on the mitigations chosen.

When it is done: After the decision has been made to defend against the risk.

Output: Implementation.

Activity:	**Review**	*Risk Type:*	**External**

Detail: Review the defensive actions and the risk likelihood and impact; consider further mitigation.

Who does it: ICANN staff with Advisory Group participation, Board to oversee.

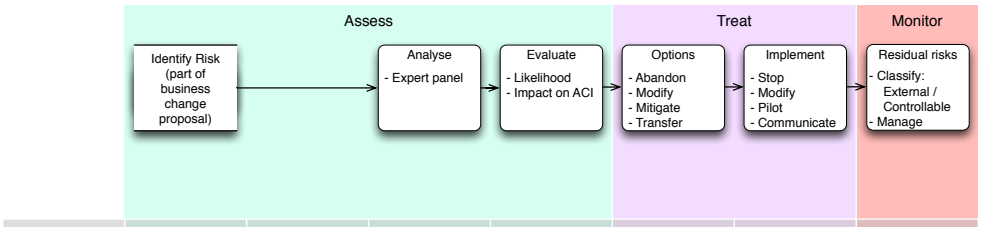
When it is done: At least annually.

Output: Note the review in the risk register.

3. Process for Strategic Risks

Strategic risks are risks that are incurred voluntarily in pursuit of some goal that assists with achieving objectives.

Strategic Risks



ICANN board	O		O	O	L		O
ICANN staff	L		L	L	P	As required	I
DNS RAG	P		P	P	P		P
SSAC / RSSAC	C		C	C	C		
ICANN Community	C		C	C	C		
DNS Community	C			C	C		

Legend: Oversee Lead Participate Consult Implement

Activity:	**Identify Risks**	*Risk Type:*	**Strategic**

Detail: All ICANN initiatives and PDPs with potential to impact the DNS should be assessed for risks to ACI. The Board should require a risk assessment to be provided as part of the papers seeking approval.

Who does it: Initiated by people promoting or sponsoring a technical or business change that potentially has impact on the DNS. It is scrutinised by the Advisory Group, led by ICANN staff support. The Board would not normally approve the initiative without evidence that this has been done.

When it is done: As part of the process of preparing any new ICANN initiative for Board approval.

Output: A list of risks that would be incurred if the proposal were implemented.

These need to be inserted into the risk register when and if the decision is made to implement the proposal.

Activity:	**Analyse Risks**	*Risk Type:*	**Strategic**

Detail: In depth analysis of the risks of proceeding with a change that might affect the DNS.

Who does it: The Advisory Group supported and led by ICANN staff. Input will be sought from SSAC / RSSAC and from the ICANN community if necessary.

When it is done: As part of the process of preparing any new ICANN initiative for Board approval.

Output: A detailed description of the risks that would be incurred if the proposal were implemented.

Activity:	**Evaluate Risks**	*Risk Type:*	**Strategic**

Detail: For each risk associated with a proposal to change, evaluate:

- Its likelihood.
- Its impact on availability, consistency and integrity.

Who does it: The Advisory Group supported and led by ICANN staff. Depending on the potential impact and scope of any potential mitigation, input will be sought from SSAC / RSSAC, the ICANN community and possibly the wider DNS community.

When it is done: As part of the process of preparing any new ICANN initiative for Board approval.

Output: An evaluation of the risk's likelihood and impact.

Activity:	**Options**	*Risk Type:*	**Strategic**

Detail: For each risk associated with a proposal to change, consider options to:

- Abandon the proposal.
- Modify the proposal to avoid or reduce the risk.
- Mitigate the risk by technical of behavioural means.
- Transfer the risk to someone else.

Make a decision about what course will be followed in the light of the options for all risks associated with a proposal

Who does it: The decision is the ICANN Board's, where it is an ICANN proposal. The Board should be informed by work from the Advisory Group supported by ICANN staff as necessary. In most cases, it will be necessary to seek input from SSAC / RSSAC, the ICANN community and sometimes the wider DNS community – seeking this input will be managed by staff on behalf of the Advisory Group.

When it is done: As part of the process of preparing any new ICANN initiative for Board approval.

Output: An options paper with a clear recommendation for Board decision making.

Activity:	**Treat**	*Risk Type:*	**Strategic**

Detail: Implement risk treatments, could include:

- Abandoning the proposal.
- Modifying the proposal.
- Piloting the proposal, making a decision to implement fully after a review.
- Communicating with community members about a changed risk profile.
- Technical mitigations to reduce risks associated with the proposal.
- Accepting the risk as a conscious decision, if the potential impact is considered tolerable and the cost of treatment outweighs the benefit.

Who does it: Depends on the mitigations chosen.

When it is done: As part of implementing any new proposal with DNS risk implications.

Output: Implementation as discussed; also formal decisions recorded in risk register and Board minutes.

Activity:	**Review**	*Risk Type:*	**Strategic**

Detail: After proposal has become policy, the residual risks become controllable risks if their likelihood can be managed, or external events if not. This step involves

- Formally recognising the residual risks,
- Classifying them, and
- Placing them into the appropriate track for risk management by the Advisory Group and ICANN staff.

Who does it: ICANN staff; Board to oversee.

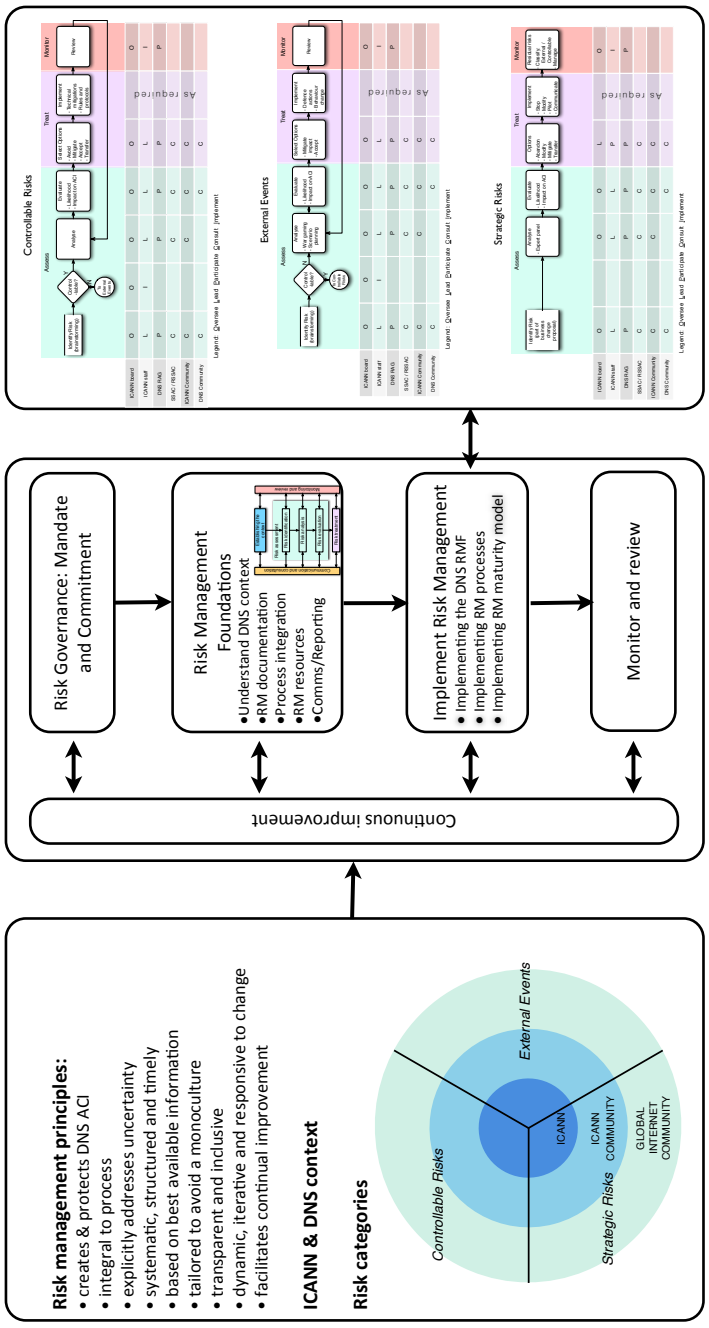
When it is done: After a proposal that has DNS risk implications becomes policy.

Output: Place these items in the risk register as new risks and bring them before the Advisory Group for decision making.

Summary – ICANN DNS Risk Management Map

The following 'ICANN DNS Risk Management Map,' summarises the three stages for developing the DNS RMF. From this it will be clear how we have followed the principles of ISO 31000, while developing the Context, Framework and Process to enable ICANN to manage DNS risks that are within its sphere of concern but not necessarily under its control.

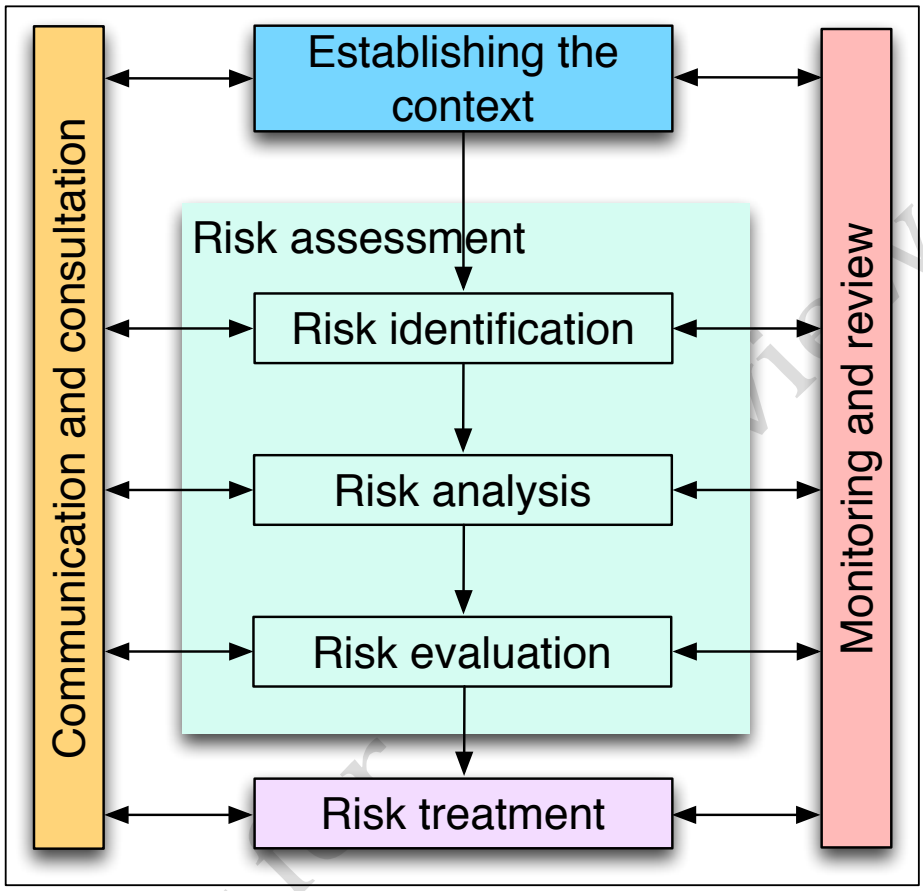
ICANN DNS Risk Management Map



Appendices

1. ISO 31000 Risk Management Process
2. ICANN Security Ecosystem Map – "Security Overview"
3. Glossary – *to be supplied*
4. DNS Risk Advisory Group terms of reference – *to be supplied*
5. Reading List – *to be supplied*
6. Risk Register Template – *to be supplied*
7. Risk Mitigation Schedule – *to be supplied*
8. DNS RMF Terms of Reference – *to be supplied*

Appendix 1: ISO 31000 Risk Management Process



Communication and Consultation

Risk management is enhanced when parties understand each other's perspectives, therefore communication and consultation with external and internal stakeholders are integral to the risk management process, and should:

- improve understanding of risks and the risk management process,
- ensure that the varied views of stakeholders are considered, and
- ensure that all participants are aware of their roles and responsibilities.

Communication and consultation should also facilitate open, relevant, accurate and understandable

exchanges of information, while taking account of confidentiality.

Communication and consultation plans and objectives are likely to vary throughout the risk management cycle, depending on what is trying to be achieved. For example, communication or consultation could be to:

i. Learn from community members.

ii. Build awareness and understanding about a particular issue.

iii. Influence a target audience.

iv. Obtain a better understanding of the context, the risk criteria, the risk, or the effect of risk treatments.

v. Achieve an attitudinal or behavioural shift.

vi. Any combination of these.

Establishing the Context

The context, (see section, Context-ICANN and the DNS) has been defined based on ICANN's mission (as specified in its Bylaws) and the unique and distributed nature of the DNS. We have defined the following criteria as a basis for evaluation DNS of risk.

- *Availability* – meaning that a properly configured resolver that is connected to the Internet can resolve a name within a reasonable response time.
- *Consistency* – a request to resolve a name on the Internet should return the same result wherever it is asked and whenever it is asked (subject to the DNS records not being changed in the meantime).
- *Integrity* – DNS lookups will be an accurate reflection of the records in the zone files.

Risk Assessment

Risk assessment includes the process of risk identification, analysis and evaluation.

Risk identification

This process identifies the sources of risk, external events and their causes and potential consequences or impacts. The aim of this step is to generate a comprehensive list of risks. This is critical, because a risk that is not identified at this stage will not be included in further analysis. To

assist generate a comprehensive list community members with appropriate knowledge should be involved in risk identification.

Identification should include controllable risks and those that arise from external events, that is, from sources that are not under the control of the organization. Risk identification should also include an examination of potential knock-on effects of particular consequences.

Risk analysis

Risk analysis aims to establish an understanding of the level of risk and its nature. This provides an input to risk evaluation and to decisions on appropriate risk treatment actions.

Risk analysis involves consideration of the causes and sources of risk, their consequences, and the likelihood that those consequences occur. Factors that affect consequences and likelihood should also be identified.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Whatever type of analysis is used, some form of measurement of consequence and likelihood is necessary. The type of measurement used is largely dependent upon the nature and range of the consequence and the level of knowledge and variability of the likelihood.

Both qualitative and quantitative methods exist for generating information for analysis, these include:

- Qualitative, evaluation using multi-disciplinary groups; specialist and expert judgment; and structured interviews and questionnaires.
- Quantitative, consequence analysis; statistical analysis; fault tree and event tree analysis; influence diagrams; network analysis; simulation and modelling; and probability analysis.

Key questions when analysing risk include:

- What current systems may prevent, detect or lower the consequences or likelihoods of risks or external events?
- What factors might increase or decrease the likelihoods or the consequences?
- What additional factors may need to be considered and modelled?
- What are the limitations of the analysis and assumptions made?
- How confident are judgements in relation to high consequence and low likelihood risks?

Analysis documentation should include:

a) Key assumptions and limitations;

b) Sources of information;

c) Analysis method;

d) Definitions of the terms used to specify the likelihood and consequences;

e) Existing controls and their effectiveness;

f) Description and severity of consequences;

g) Likelihood of specific consequences occurring;

h) Resulting level of risk; and

i) Effect of uncertainty.

Detailed documentation is not necessary for very low risks, however a record should be kept of the rationale for initial screening of very low risks.

Risk evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for implementing treatment.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered and prioritised.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision to accept the risk. This decision will be influenced by the organization's risk attitude and the established risk criteria.

Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Implementing the treatment.

The options for treatment can include the following:

a) Avoiding the risk;

b) Accepting the risk;

c) Removing the risk source;

d) Mitigating the risk (that is reducing the likelihood and or the consequences); and

f) Transferring the risk to another party or parties

Selection of risk treatment options

Selecting the most appropriate risk treatment option involves considering the values and perceptions of stakeholders and balancing cost and implementation effort against benefits derived. Some risks, for example, high negative consequence, low likelihood risks, may warrant treatment that is not economically justifiable.

Treatment plans should clearly identify the implementation priority for individual risks.

Risk treatment can introduce further risks, including secondary risks and risks associated with the failure or ineffectiveness of treatment measures.

Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

- The reasons for selection of treatment options, including expected benefits to be gained;
- Those who are accountable for approving the plan and those responsible for implementing the plan;
- Proposed actions;

- Resource requirements including contingencies;
- Performance measures and constraints;
- Reporting and monitoring requirements; and
- Timing and schedule.

Treatment plans should be integrated with the management processes and where appropriate discussed with stakeholders.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after treatment. Residual risks should be documented, monitored, reviewed and, where appropriate, treated further.

Monitoring and Review

Monitoring and review is an essential and integral part of managing risk, and is one of the most important steps of the risk management process. It is necessary to monitor risks, the effectiveness and appropriateness of the strategies and management systems set up to implement risk treatments and the risk management plan and system as a whole.

Monitoring and review processes should be continuous and dynamic. It is not appropriate to rely only on infrequent, third party reviews or audits.

All aspects of the risk management process should be subject to ongoing monitoring and review to:

- Ensure that controls are effective and efficient in both design and operation;
- Obtain further information to improve risk assessment;
- Analyze and learn lessons from events (including near-misses), changes, trends, successes and failures;
- Detect changes in context or risks themselves; and
- Identify emerging risks.

Monitoring and review results should be recorded and reported. They should also be used as an input to the review and continuous improvement of the risk management framework.

Recording the risk management process

Documenting each step of the risk management process is important to:

a) Demonstrate to stakeholders that the process has been conducted properly;

b) Provide evidence of a systematic approach to risk identification and analysis;

c) Enable decisions or processes to be reviewed;

d) Provide a record of risks and to develop the organization's knowledge database;

e) Provide decision makers with a risk management plan for approval and subsequent implementation;

f) Provide an accountability mechanism and tool;

g) Facilitate continuing monitoring and review;

h) Provide an audit trail; and

i) Share and communicate information.

Decisions concerning the extent of documentation may involve costs and benefits and should take into account the reasons for documenting the process. Prudent practical judgment should be used to determine the level of documentation in particular circumstances.

At each stage of the process, documentation should include—

- The objectives of the stage;
- The information sources on which the outcomes were based;
- All major assumptions made in the process;
- Who was involved; and
- The decisions that were agreed.

Two particular registers should be maintained as part of the risk management process, these are the Risk register and the Risk treatment schedule.

Risk register

For each risk identified, a risk register should record:

a) A description of the risk, its classification, causes and impacts;

b) An outline of the existing controls;

c) An assessment of the consequences of the risk should it occur and the likelihood of the consequence occurring, given the controls;

d) A risk rating; and

e) An overall priority for the risk.

Refer to Risk register template in the Appendix

Risk treatment schedule

A risk treatment schedule documents the mitigating actions and controls to be implemented, and records:

a) Actions to be taken and the risks they address;

b) Who has responsibility for implementing the plan;

c) What resources are to be utilized;

d) Budget allocation;

e) Timetable for implementation; and

f) Review mechanism and frequency.

Refer to Risk treatment schedule in the Appendix

Appendix 2: ICANN Security Ecosystem Map – "Security Overview"