DNS

安全性、稳定性和灵活性审核小组最终报告

呈报互联网名称与数字地址分配机构 (ICANN)

--最终报告--

2112 年 6 月 20 日

目录

1 摘要

本报告陈述了 DNS 安全性、稳定性和灵活性审核小组（下文简称“SSR 审核小组”）的工作和结果。根据 ICANN 和美国商务部之间签订的《义务确认书》，本次审核分析了 ICANN 对下述承诺的履行程度，即“提高域名系统（“DNS”）运作的稳定性、可靠性、灵活性、安全性和全球互操作性”。

本次审核涵盖了 ICANN 现有的 SSR 计划，此计划必须定期更新以反映 DNS 面临的新风险。根据《义务确认书》的指示，要尤其注意：

> “(a) 与安全稳定地协调互联网 DNS 相关的实体和网络安全性、稳定性和灵活性事务；
>
> (b) 确保制定适当的应急计划；以及
>
> (c) 维持清晰的流程。”

《义务确认书》进一步指出，SSR 审核将评估 ICANN 成功实施安全计划的程度、该计划应对实际与潜在挑战和威胁的有效性，以及安全计划是否足够稳健从而可应对互联网 DNS 未来在安全性、稳定性和灵活性方面的挑战和威胁，并审核是否符合 ICANN 的有限技术使命。

SSR 审核小组是在各利益主体组织代表参与的情况下由 ICANN 总裁兼首席执行官和 GAC 主席共同成立。它通过实际会议、电话会议、电子邮件和其他沟通方式运作。SSR 审核小组会对来自各种渠道的材料进行分析，包括文档、访谈以及会议。部分关键性文档可应请求由 ICANN 工作人员提供。

本次审核重点关注 ICANN 对其 SSR 相关职能的管理。它既非技术运营层级的正式安全性审核，也非对 ICANN 与其他实体（如政府和政府间组织）之间关系的大规模管理的审核。本报告中，DNS 是指在全球互联网范围内将域名映射到 IP 地址的协议、服务器、网络、组织和公司的系统。在使用不同含义（例如单指 DNS 协议）时，报告会给予明确说明以避免歧义。

SSR 审核小组会确定 ICANN 在哪些领域表现出色，在哪里领域有待改进，以及在其他哪些领域应该确定和实施 SSR 的关键要素。

我们发现 ICANN 在以下诸多领域都表现出色：对不同控制和影响层级内的运营方式进行了解和沟通；遵守其 SSR 职权范围和有限技术使命；改进 SSR 框架的构成；参与良好的 SSR 相关运营实践；以及在 DNSSEC 方面进行思维领导。

本报告指出了许多待改进的领域：ICANN 对 SSR 职权范围的描述应该更清晰；更明确定义与支持组织和咨询委员会的 SSR 相关关系；结构更清晰和优先级更高的 SSR 框架；更具体的举措和计划来执行 SSR 架构；具有可衡量的目标；更详细描述用以支持 SSR 职能所分配的预算；更密切定义支持组织和咨询委员会执行的 SSR 相关任务。

SSR 审核小组还应敦促 ICANN 迅速完成工作，以创建和发布一个正式而全面的 DNS 风险管理框架。另外，ICANN 还应该继续进行明确而有针对性的外展工作，以积极影响 ICANN 直接职责范围外的更大互联网生态系统。还应支持发展 SSR 相关的最佳实践以及公布关于 DNS 威胁和减轻威胁策略的信息的工作。

提交以征求公众意见的最终草案版本提出：

“SSR 审核小组会在公众意见征询期内和最终报告发布前对更多的意见反馈展开进一步的研究。这些意见反馈包括：最近特许的理事会 DNS 风险管理工作组的建议或进展，以及 DNS 安全稳定分析联合工作组的建议。”

这是 SSR 审核小组的最终报告，此报告将取代已于 2012 年 3 月 15 日发布的报告草案。自该报告草案发布后，提供了 45 天的意见征询期以确保收到机构群体的反馈意见。该小组召开了两次公开网络会议，并与 GAC 召开了一次网络会议，以征求其他反馈意见。

SSR 审核小组已讨论了提交的所有反馈意见。我们已将我们的结论整合到此处呈交的最终报告中。在某些特殊情况下，我们讨论了我们执行上述任务的方式和范围，其中包括接受意见及在某些情况下完全或部分拒绝意见。其中大部分意见已纳入到报告之中，以便理事会利用它们指导 ICANN 与机构群体共同开展的行动。

SSR-RT 对机构群体中各方在此过程中付出的努力表示感谢，对为我们的工作提供宝贵支持的 ICANN 工作人员和其他各方表示感谢。我们对 Alice Jansen、Olof Nordling、Patrick Jones、Denise Michel、Jeff Moss、Steve Crocker 和 Rod Beckstrom 表示特别感谢。

以下章节罗列了审核中提出的关键建议：

1.1 建议列表

建议 1：ICANN 应该就其 SSR 职权范围和有限技术使命发布唯一、清楚且一致的声明。ICANN 应该征询并获取公众意见以达成基于共识的声明。

建议 2：ICANN 应该对其 SSR 职权范围和有限技术使命的定义和执行进行审核，以达成共识并征询机构群体的反馈意见。应该定期重复该流程，可能需要连同未来 SSR 审核的周期进行。

建议 3：在 ICANN 对其 SSR 职权范围和有限技术使命发布基于共识的声明后，ICANN 应在所有材料中一致地应用本声明中的术语和描述。

建议 4：ICANN 应该记录并明确定义其在 ICANN 机构群体内拥有的 SSR 关系的性质，以便为理解不同组织之间的相互依赖性提供单一关注点。

建议 5：ICANN 应使用其 SSR 关系的定义来保持有效的工作安排，并说明如何利用这些关系实现每个 SSR 目标。

建议 6：ICANN 应该发布一个文档，其中明确罗列 SSAC 和 RSSAC 的角色和职责，以便明确描述这两个组织的活动。ICANN 应该认识到两个组织的成立历史和情况，据此在两个组织之间寻求共识。ICANN 应该考虑根据对这两个组织提出的要求向其提供相关资源。

建议 7：ICANN 应该通过设立一系列明确目标并按这些目标确定其举措和活动的优先顺序，以扩展其目前的 SSR 框架。该流程应参考实际的成本收益和风险分析。

建议 8：ICANN 应该继续细化其战略计划目标，尤其是维持和推动 DNS 可用性的目标。战略计划和 SSR 框架应反映一致的工作重点和目标，以确保完全相符。

建议 9：ICANN 应根据普遍接受的国际标准（如 ITIL、ISO 和 SAS-70）评估其运营职责的认证选项。ICANN 应针对认证发布明确的路线图。

建议 10：ICANN 应该继续努力加强合同合规性的强制执行，并为此职能提供足够的资源。ICANN 还应该为监控合规性问题和调查工作制定并执行结构更清晰的流程。

建议 11：ICANN 应该最终落实并执行对以下方面所取得成绩的衡量，即与 SSR 相关计划目标明确关联的新 gTLD 和 IDN 快速通道，其中包括对减少域名滥用的机制的有效性衡量。

建议 12：ICANN 应与机构群体合作，共同确定 SSR 相关的最佳实践，并通过合同、协议、备忘录及其他机制为实施此类实践提供支持。

建议 13：ICANN 应该鼓励所有支持组织为其成员制定和发布与 SSR 相关的最佳实践。

建议 14：ICANN 应该确保其与 SSR 相关的外展活动不断发展，以保持相关、及时和适当。机构群体的反馈意见应该提供一种机制来审核和增强这种相关性。

建议 15：ICANN 应扮演推动者角色，负责公布和普及 DNS 安全威胁及防范技术。

建议 16：ICANN 应该继续实施其外展工作，以扩展机构群体参与到 SSR 框架制定流程中并提供意见。ICANN 还应该建立一个流程以便从其他生态系统参与者处获得更系统化的意见。

建议 17：ICANN 应该建立一个结构更清晰的内部流程，以展示活动和举措如何与 SSR 框架内的具体战略目标和工作重点相关。还应该为执行工作确立度量标准和里程碑。

建议 18：ICANN 应该为其在执行 SSR 框架中取得的进展执行年度运营审核，并将此评估作为一个要素纳入下一年的 SSR 框架中。

建议 19：ICANN 应该建立一个流程，以让机构群体跟踪 SSR 框架的执行情况。提供的信息应该足够清楚，以便机构群体可以跟踪 ICANN 对其 SSR 职责的执行情况，同时不损害 ICANN 的有效运营能力。用于跟踪 ATRT 建议执行情况的公告板流程可作为良好典范。

建议 20：ICANN 应该提高关于执行 SSR 框架和履行 SSR 相关职能的组织和预算的信息的透明度。提供的信息应该足够清楚，机构群体可以跟踪 ICANN 对其 SSR 职责的执行情况，同时不会妨碍 ICANN 的有效运营能力。

建议 21：ICANN 应该建立结构更清晰的内部流程，以展示组织和预算决策与 SSR 框架的相关性，包括基本的成本收益分析。

建议 22：ICANN 应该发布、监控和更新管理 SSR 问题并引入新 gTLD 所需的组织和预算资源的文档。

建议 23：ICANN 必须根据对 SSR 相关工作组和咨询委员会提出的要求为其提供适当资源。ICANN 还必须确保工作组和咨询委员会所做的决策是在不受外部或内部压力的情况下客观地作出的。

建议 24：ICANN 必须明确定义首席安全官小组的章程、角色和职责。

建议 25：ICANN 应该制定相关机制来确定其风险管理框架中的短期和长期风险及战略因素。该流程应该参考来自研究、企业合作伙伴、ICANN 支持组织和其他渠道的见解。ICANN 应该发布风险相关信息，认识到其中一些因素的敏感性。

建议 26：ICANN 应该优先及时完成风险管理框架。此工作应该符合高标准的参与度和透明度。

建议 27：ICANN 的风险管理框架在 SSR 职权范围和有限使命范围内应该全面周到。

建议 28：ICANN 应该继续积极开展威胁检测和降低工作，并参与宣传威胁和事故信息的工作。

2 DNS 安全性、稳定性和灵活性审核小组的背景

DNS 安全性、稳定性和灵活性审核小组（下文简称“SSR 审核小组”）根据 ICANN 和美国商务部之间签订的《义务确认书》（“AoC”）第 9.2 节成立。根据《义务确认书》的要求，SSR 审核小组由志愿者群体成员组成，包括 GAC 主席、ICANN 首席执行官、相关咨询委员会和支持组织的指定代表以及独立专家。这是第一次 SSR 审核，已于 2010 年 10 月启动，后续审核开展的频率不会低于每三年一次。

如《义务确认书》第 9.2 节所述，ICANN 已制定一份计划来增强 DNS 运营的稳定性、可靠性、灵活性、安全性和全球互操作性，ICANN 将定期更新该计划以反映 DNS 面临的新威胁。《义务确认书》指示要尤其注意：

(a) 与安全稳定地协调互联网 DNS 相关的实体和网络安全性、稳定性和灵活性事务；

(b) 确保制定适当的应急计划；以及

(c) 维持清晰的流程。

《义务确认书》还进一步指出，根据第 9.2 节开展的各项 SSR 审核将评估 ICANN 成功实施安全计划的程度、该计划应对实际和潜在挑战和威胁的有效性，以及安全计划是否足够稳健从而可应对互联网 DNS 未来的安全性、稳定性和灵活性挑战和威胁，并审核是否符合 ICANN 的有限技术使命。

SSR 审核小组成立于 2010 年 10 月，负责两次 ICANN 会议中间以及 ICANN 会议召开期间的工作事宜。该小组由其各自的支持组织和机构群体选择的申请人组成，申请人的最终人选由 GAC 主席和 ICANN 首席执行官兼总裁决定。

ICANN 网站上对小组构成进行了定义和描述[1]，但可以归纳为

支持组织/咨询委员会候选人

- Alejandro Pisanty (MX) — 工作组主席；
- Anders Rafting (SE)；
- Bill Manning (US)；
- David Cake (AU)；
- Hartmut Glaser (BR)；
- Jeff Brueggeman (US)；
- Martin Hannigan (US)；
- Ondrej Filip (CZ)；
- Rodney Joffe (US)；
- Simon McCalla (UK)；
- Atif Nazar (PK)（2011 年 6 月辞职）；
- 李晓东 (CN)（2012 年 2 月辞职，现于 ICANN 任职）。

[1] http://www.icann.org/en/about/aoc-review/ssr/composition

独立专家：

- Andrea Rigoni (IT)；
- Paul Mockapetris (US)；

指定提名人：

- Alice Munyua (KE) — GAC 主席提名人；
- Jeff Moss (ICANN) — ICANN 首席执行官提名人（2011 年 5 月辞职，现于 ICANN 任职）。

审核小组在卡塔赫纳会议上开始正式工作，并已在报告期内召开六场面对面会议，具体如下所述：

- ICANN 会议 — 哥伦比亚卡塔赫纳 — 2010 年 12 月；
- ICANN 会议 — 美国旧金山 — 2011 年 3 月；
- ICANN 会议 — 新加坡新加坡市 — 2011 年 6 月；
- SSR 起草小组会议 — 美国华盛顿特区 —2011 年 7 月；
- ICANN 会议 — 塞内加尔达喀尔 — 2011 年 10 月；
- ICANN 会议 — 哥斯达黎加圣约瑟 — 2012 年 3 月；
- SSR 起草小组会议 — 美国华盛顿特区 —2012 年 6 月。

3 审核方法

为了根据《义务确认书》履行其使命，SSR 审核小组将工作重点放在三大类问题上：

- 在其有限技术使命基础上 ICANN 的 SSR 职责范围；
- ICANN 的 SSR 计划有效性、计划的执行及其 SSR 职责；以及
- ICANN 用于评估 DNS 风险局面的流程，为应对目前和以后的挑战实施应急计划的流程，以及让其他必要方参与到执行 ICANN 的 SSR 使命的流程。

SSR 审核小组最初建立了三个子工作组来收集相关文档、对材料进行初步分析并准备第一组问题。

三个子工作组的工作方法都是分析以下 4 个关键领域的信息：

- ICANN 针对 SSR 相关文档的公共文库；
- 与 SSR 和 ICANN 的 SSR 角色相关的外部文件和报告；
- 与 ICANN 工作人员、支持组织、机构群体成员、外部专家等人员的会谈；
- 来自于组建的 SSR 审核小组内的见解和经验。

该小组负责处理涵盖逾百份单独文件和信息资源的文库，但有 5 份关键文件是审核小组工作的核心内容，并为 ICANN 的 SSR 立场奠定了基础：

- ICANN 章程（包括使命和核心价值）；
- 美国商务部/ICANN《义务确认书》；
- ICANN 2011 财年安全性、稳定性与灵活性框架的职责范围描述；
- ICANN 2012 财年安全性、稳定性与灵活性框架的职责范围描述；
- ICANN 2011-2014 年战略计划职责范围描述。

审核流程包括详细分解从文件文库获取的信息。适当情况下，可以向机构群体成员和 ICANN 工作人员征询建议和反馈意见，以便于分析关键主题和支持结论与建议。某些情况下，访谈个人或社群有助于引导小组对具体问题的研究，还可向 ICANN 工作人员索取更多尚未发布的信息或内部文件信息。

值得指出的是，在审核早期便已就以下事宜做出决定，即小组不会参与签订与 ICANN 的正式不披露协议。小组认为，如果自身是 ICANN 内部信息披露的参与方，就会导致无法在报告中公开讨论，继而难以保持透明和公正。

一旦记录在案，这三个子工作组获得的分析意见就会在审核小组内部传达和讨论。将进行多回合的讨论和深入分析以达成共识性意见，从而制定出最终建议。以下章节详细叙述了具体的分析和建议。

4 调查结论

4.1 ICANN 的 SSR 职责的范围和结构

本节分析了 ICANN 在促进 DNS 安全性、稳定性和灵活性方面的职责范围，ICANN 的这一职责范围与其有限的技术责任相一致。要了解 ICANN 的计划和行动，审核小组必须先研究 ICANN 组织其活动的方式。审核小组采用了以下结构来分析和了解 ICANN 的 SSR 活动：

- ICANN 的运营职责；
- ICANN 作为协调者、合作者和推动者的影响领域；以及
- ICANN 与全球互联网生态系统中其他相关方的互动。

本报告的以下章节将参照上述 3 个“影响范围”。

4.1.1 ICANN 的 SSR 职权范围和有限的技术使命

根据 ICANN 章程[2]，其使命如下：

> “互联网名称与数字地址分配机构（The Internet Corporation for Assigned Names and Numbers，简称 ICANN）的使命是对全球互联网的唯一标识符系统进行总体协调，特别是确保互联网唯一标识符系统稳定安全地运作。具体来说，ICANN 的使命包括：
>
> 1. 协调互联网的三套唯一标识符的分配和指定。这三套唯一标识符是：
>
> a. 域名（组成被称为“DNS”的系统）；
>
> b. 互联网协议（“IP”）地址和自治系统（“AS”）号；以及
>
> c. 协议端口和参数号。
>
> 2. 协调 DNS 根名称服务器系统的运行和发展。
>
> 3. 合理适当地协调与这些技术工作有关的政策制订。”

在 ICANN 核心价值观声明中，其不仅承担协调资源分配和 DNS 运营的责任，而且还承担“保持并提高互联网的稳定性、可靠性、安全性和全球互操作性”的责任。ICANN 还声明，在可行和适当的范围内，将协调职责委托给代表相关方利益的其他责任机构，或者对这些机构的政策参与角色予以认可。这些可能存在相互竞争的责任和价值体现在 AoC 中，AoC 引述了 ICANN 的有限技术使命和维护 DNS 安全性、稳定性和灵活性的责任。

如果要通过分析相关的 ICANN 文件来获得 ICANN SSR 职权范围的简洁、明了的定义，将是很困难的。要了解该职权范围，读者必须将多个文件的信息汇集在一起。有时，由于语言和术语的细微调整，可能会

[2] *ICANN 章程是指*http://www.icann.org/en/about/governance/bylaws

导致任务和职权的解释不是很明晰。2012 财年 SSR 计划工作[3]的基础章节更为清楚地说明了此方面，这也算是在此方面的一个进步。审核小组对这一积极措施表示欢迎。

这将有助于 ICANN 拟定一个单一且明晰的 SSR 职责声明（也许仅使用一页的篇幅），所有其他举措可通过此声明相互挂钩。在 2012 财年 SSR 计划中列入基础章节，意味着朝正确方向迈出的一步；但是，还需要使此声明更加明晰，并给予它更多关注。

同样地，ICANN 在其诸多关键文件中以多种方式定义了其技术使命。ICANN 坦率地论述其所要面临的挑战：承担直接的运营或合约责任，以及在更为广泛和重要的背景下不得不同时充当协调者和参与者角色。ICANN 承认在其未直接控制的领域定义宏大的目标是很困难的。通览整篇文档，按照如下方式定义 ICANN 的有限技术使命将是适当的：

- 协调互联网唯一标识符系统的分配；
- 维护和加强这些系统的安全性、稳定性和灵活性；
- 作为机构群体的管理人维护和运营诸如 L 根名称服务器；
- 管理 ICANN 自己的内部系统，提供一个公众可访问的门户以供传播和分享信息。

显然，这将有助于 ICANN 明确说明其有限的技术使命，并在其他文件中提及这一使命时使用一致的语言。重要的是 ICANN 应考虑因用语不一致或混淆而造成的影响。

我们必须承认，ICANN 的 SSR 所发挥的作用还包括在协调政策制定方面的重大举措，这些举措对 SSR 使命的技术协调有着直接影响。虽然在本文中未明确讨论这一功能，但是审核小组承认这一功能的重要性。

为了解机构群体对 ICANN 的 SSR 职权范围和有限技术使命的看法和立场，审核小组审查了三份关键文件的公众意见，这三份文件已征询反馈意见，它们包括：

- SSR/创建 DNS-CERT 的战略举措[4]；
- ICANN 2011 财年 SSR 计划[5]；
- ICANN 2012 财年 SSR 计划[6]。

征询意见（通过 ICANN 的备案反馈流程）的文档包括 30 多个公开文档，诸如注册管理机构、注册服务商、各国政府和大型企业在内的广泛利益主体提供了反馈意见。

[3] *2012 财年 SSR 计划*，2011 年 5 月 2 日。请参阅：http://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[4] *提高 DNS 安全性、稳定性和灵活性的举措提案* http://www.icann.org/en/about/staff/security/ssr/strategic-ssr-initiatives-09feb10-en.pdf

[5] *加强安全性、稳定性和灵活性（2011 财年计划）* http://www.icann.org/en/about/staff/security/ssr/ssr-draft-plan-fy11-13sep10-en.pdf

[6] *2012 财年 ICANN 安全性、稳定性和灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

这些反馈中所提出的主题显示出惊人的一致性。机构群体显然认为，其通常通过参考 AoC 的措辞，可完全理解 ICANN 的有限技术职权范围，并希望确保 ICANN 不会偏离到“运营”角色。一些机构群体要求对特定的 SSR 问题予以澄清和关注，一些机构群体要求给出明确的目标和措施以确保成功。另一项常见的主题是缺乏合同合规性方面的专门资源，许多人认为这可能会导致命名空间的安全性、稳定性和灵活性降低。

要引起重视的一点是列表中每个文件的反馈数量减少了。到目前为止，“战略举措”文档是获得反馈意见（主要是因为 DNS-CERT 讨论）最多的。2012 财年计划是三个文件中获得反馈最少的，或许是由于没有任何重大的、有争议的话题。令人失望的是最新的 SSR 计划的参与度比较低，ICANN 应认真考虑如何提高参与度并在这样的关键领域获得更多反馈。

显然，ICANN 需认真考虑如何确保获得广泛的机构群体的意见并让他们关注 SSR 的工作。建立一套更有效的反馈机制将会有所帮助。

重要的是，ICANN 要定期审查其现有的 SSR 职权范围以及其就此所执行的举措。若更清楚地了解项目和运营，则此任务应会变得更简单，并允许有更大的透明度。但是，建议对自我审计/自我审查给予特别关注，然后从机构群体征求反馈意见。

SSR 审核小组也承认，AoC 审核、特别是这一角色以及随后的为 ICANN 的 SSR 绩效提供外部意见的 SSR 审核小组的重要性。

建议 1：ICANN 应该就其 SSR 职权范围和有限技术使命发布唯一、清楚且一致的声明。ICANN 应该征询并获取公众意见以达成基于共识的声明。

建议 2：ICANN 应该对其 SSR 职权范围和有限技术使命的定义和执行进行审核，以达成共识并征询机构群体的反馈意见。应该定期重复该流程，可能需要连同未来 SSR 审核的周期进行。

建议 3：在 ICANN 对其 SSR 职权范围和有限技术使命发布基于共识的声明后，ICANN 应在所有材料中一致地应用本声明中的术语和描述。

4.1.2 ICANN 的 SSR 相关角色和职责

2012 财年 SSR 计划分为两部分（A 部分和 B 部分），并尝试直接将该框架与“战略计划”挂钩。在此方面，这是一项积极可喜的进步，并且显然 ICANN 工作人员在过去 12 个月期间倾听了 SSR 审核小组的顾虑，并采取了行动来解决其中一些问题。

在 2012 财年 SSR 计划 A 部分中，ICANN 很好地汇集了使命陈述、核心价值和《义务确认书》的 SSR 部分，以尝试总结其 SSR 职责。这是对该计划的一项有益补充，并有助于将很多支持文档捆绑在一起。在审查 2011 财年计划时，这项工作花费了审核小组的大量时间，因此，作为一项非常受欢迎的补充，它应可以在为 ICANN 的 SSR 计划的新读者提供帮助。

ICANN 在 A 部分将其 SSR 的角色总结为包含三个类别的职责：

- ICANN 的内部运营（包括 L 根、DNS 运营等）；
- ICANN 作为机构群体内的协调者、合作者和推动者的角色（政策协调，技术推进者等）；
- ICANN 作为全球互联网生态系统中其他群体活动的观察员的角色；

欣喜的是，ICANN 还澄清了一些被认为是其没有责任的领域：

- ICANN 的身份不是网络警察，也不会在运营中直接与犯罪行为作斗争；
- ICANN 不会参与有关利用互联网从事网络间谍和网络战争的对话或活动；
- ICANN 不担当界定互联网违法行为的角色。

虽然 ICANN 声明它不能单方面暂停或终止域名，但它也承认，它可以强制执行与注册管理机构和注册服务商的合同。显然，这仅适用于与 ICANN 签订合同的机构（例如，非国家代码的注册管理机构）。

SSR 框架 A 部分的新内容“基础章节”广受欢迎，但是该章节似乎只是组合了有用的资料，而不是对 ICANN 的 SSR 角色的总结。如前所述，若明确说明与 ICANN 实际技术使命相关的 SSR 职权范围，将是非常有用的。在阅读该计划和框架的 B 部分时，这将会有显著帮助。

SSR 审核小组同意 ICANN 根据影响范围界定其职责，但是我们建议细化以下影响领域：

- ICANN 的运营职责；
- ICANN 作为协调者、合作者和推动者的影响领域；以及
- ICANN 与全球互联网生态系统中其他相关方的**互动**。

审核小组认为，这种语言上的变化将会对在更广泛的互联网生态系统中建立 ICANN 的角色非常有用 — 从被动的角色到参与更多并重点关注外展的角色。

在探讨上述各领域时，我们必须了解，围绕通过 SSR 活动取得成功的规则会有所改变，具体取决于 ICANN 对每个领域的接近度和控制度。如前所述，ICANN 在以下方面正变得越来越清晰：区分其所能控制并能负责的任务，区分其必须予以合作或协调以实现成功的任务。

4.1.2.1 ICANN 的运营职责

ICANN 自己的 SSR 运营要么在内部决定，要么通过由机构群体制定并被理事会采纳的政策建立。这些对组织的功能和其管理安全规定的方式有着直接的影响。上述 SSR 运营会考量 ICANN 组织自身的内部安全以及其管理 IANA 职能的方式。正是在此领域内 ICANN 拥有最高控制权和问责权。

鉴于 ICANN 在此领域拥有最高控制权，人们可以预期 ICANN 将拥有明晰和一致的运营计划以及这些职能的（适用任何组织）的可衡量的目标。预计 ICANN 还将作为思维领导者和关键影响者发挥重要作用，尤其是此领域的带头作用。

4.1.2.2 ICANN 作为协调者、合作者和推动者的影响领域

在 ICANN 网站的“About”（关于）一节，ICANN 在题为“What does ICANN do?”（ICANN 的职责是什么）的简短摘要中描述了其目的：[7]

> “要与其他互联网用户联系，您必须在自己的计算机中输入地址 — 一个名称或数字。这个地址必须是唯一的，这样各计算机之间才可以相互识别。ICANN 负责在全球范围内协调这些唯一标识符。没有这项协调工作，我们就不会有一个全球性的互联网。”

从更广泛的技术角度来看，ICANN 负责协调域名系统 (DNS)、互联网协议 (IP) 地址空间分配、协议标识符指定、通用 (gTLD) 和国家/地区代码 (ccTLD) 顶级域名系统管理以及根服务器系统管理职能。

ICANN 支持和促进各类组织的参与，例如营利性公司私营部门、民间社会组织、个人、政府、学术和技术组织（如科研院所、高等院校和实验室）；以及 ICANN 支持和促进直接通过 ICANN 多利益主体模式内的官方支持组织和咨询委员会参与。它们包括 RIR、ccTLD、（尤其是）gTLD，以及签约的注册管理机构。在此情况下，IETF、IAB 和 ISOC 发挥着具体、突出的作用，正如美国政府通过其商务部 的 NTIA 所做的一样。

这些相关方的关系在很大程度上具有两面性，对此，ICANN 不得不在讨论和政策制定方面同时扮演接受者和贡献者。同样清楚的是，与较 ICANN 成立更早的一些实体的关系会随着时间的推移而演变。在某些情况下，这些关系已通过合同条款确立，对于其他群体，则通过双边协定或谅解备忘录 (MoU) 确立。

4.1.2.2.1 ICANN 与 SSR 相关支持组织的关系

ICANN 组织结构图[8]显示 ICANN 理事会和领导层倚赖于多个支持组织和咨询委员会的意见，以便为 SSR 活动提供建议和贡献。在利益主体模式中，有四个与支持 SSR/技术问题相关的官方关键组织：

- SSAC（安全与稳定咨询委员会）；
- TLG（技术联络组）；
- RSSAC（根服务器咨询委员会）；
- IETF（互联网工程任务组）。

[7] 参阅 http://www.icann.org/en/about/welcome
[8] 参阅 http://www.icann.org/en/groups/chart

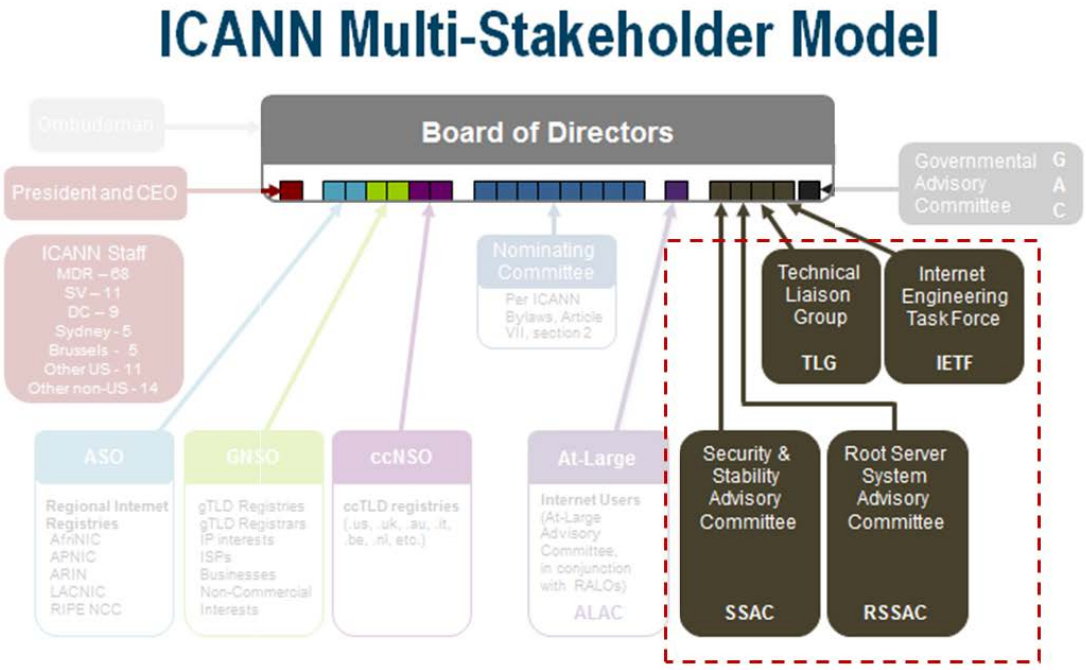

图 1 ICANN 组织结构图

上述四个团队通过不同的流程和政策成立，以便为 ICANN 理事会提供广泛的技术建议。

- SSAC — ICANN 授权的利益主体团队，直接为理事会提供安全性和稳定性建议，该团队与其他团体（如 IETF 和 TLG）合作以提供协调性意见；
- TLG — ITU、ETSI 和 W3C 等组织的联络组；
- RSSAC — ICANN 授权的利益主体团队，它将根服务器运营商聚集在一起，以向理事会提供与根区域运营相关的建议；
- IETF — ISOC 授权的组织，专门开发互联网技术和协议。

这些组织自身与 ICANN 理事会有着不同的关系，并且相互之间有时会存在着重叠或可能冲突的责任。IETF 和根服务器运营商在 ICANN 成立之前就已经存在了很长时间。

作为审查工作的一部分，如果对支持组织、咨询委员会及其之间的关系进行分析，可很快发现它们之间存在着相互交错的倚赖关系。这些方面的分析工作往往很复杂，有时对每项协议或关系的确切性质也是非常难以理解。一些协议通常跨越了很多年，并在多个文件中且以多个协议版本进行了备案。

若要向更广泛的机构群体澄清 ICANN 与其他方之间的关系，将所有相关协议汇集在一起，不论是正式签署的或议定的谅解协议，都将会对 ICANN 有帮助。这将便于理解整体 SSR 使命的有效性和每种关系对整体 SSR 使命的适用性，并可允许更深入的考查这种有效性和适用性。据审核小组了解，其中的很多关系盘根错节，如果将其中的一些关系正式化，可能会带来政治风险。提出以下建议的唯一目的是提高 SSR 安排的透明度。

该报告草案的一些意见反馈者提出质疑，认为现有的建议 4 过于宽泛，并且“更广泛的互动”一词的意义并不明确。为此，我们对该建议进行了完善，阐明 ICANN 应专注于保持高效的工作安排，同时认识到这些任务的多样性。很明显，在处理相关方的广度问题时，并不适合采取“通用”做法。

建议 4：ICANN 应该记录并明确定义其在 ICANN 机构群体内拥有的 SSR 关系的性质，以便为理解不同组织之间的相互依赖性提供单一关注点。

建议 5：ICANN 应使用其 SSR 关系的定义来保持有效的工作安排，并说明如何利用这些关系实现每个 SSR 目标。

4.1.2.2.2 SSAC 和 RSSAC 的具体 SSR 角色

SSAC 和 RSSAC 在某些领域的责任是接近或甚至是重叠的，这些责任很大程度上源自相同的组织和机构群体；并在理事会和其他机构群体中设有具有同等代表权的联络人作为代表。他们担任不同的角色并且相互之间设有一道“防火墙”，但是他们有时还需要密切合作。

鉴于 SSAC 是由与 ICANN 使命相关的 ICANN 机构群体内挑选的个人组成，RSSAC 是由性质迥异的企业实体组成。所以，SSAC 通常从事由 ICANN 负责或与机构群体进行紧密合作通过各种渠道确定的任务，尽管 RSSAC 的基本任务是以最佳的方式、就运行根服务器系统的运作事项、向 ICANN 理事会提供建议，但是对于运营商和包括作为企业实体的 ICANN 在内的其他实体，RSSAC 拥有最大程度上的独立性。

因此，ICANN 理事会和工作人员会发现自己在以不同的方式与每个群体合作。通过 SSAC，理事会可要求 SSAC 根据其章程和对 ICANN 的承诺开展工作。ICANN 必须通过 RSSAC 开展工作，或通过每个根区域运营商独立工作。像 SSAC 一样，RSSAC 成员可选择是否留意请求。

SSAC 和 RSSAC 之间角色差异的典型示例之一就是根区域升级研究。一般的回忆和记录流程都显示，很难确定 SSAC 或 RSSAC 是否会承担研究责任，或他们是否能相互合作。一般预期是指这项研究将由 RSSAC 进行并由 SSAC 收尾。虽然表达对此项任务的偏爱不在审核小组的使命（特别是该使命已结束的情况下）范围内，但是审核小组指出未明确 SSAC 和 RSSAC 之间的职责会对 DNS 的 SSR 带来风险。如要进行改进，则需要更好的沟通和协调。在实践中，结果是通过 ICANN 资助 SSAC 活动而非 RSSAC 活动的情况来预测的。

建议 6：ICANN 应该发布一个文档，其中明确罗列 SSAC 和 RSSAC 的角色和职责，以便明确描述这两个组织的活动。ICANN 应该认识到两个组织的成立历史和情况，据此在两个组织之间寻求共识。ICANN 应该考虑根据对这两个组织提出的要求向其提供相关资源。

4.1.2.3 ICANN 在全球互联网生态系统中与其他群体的合作

技术性 DNS（和其他协议层）运营商的群体很大，他们构成了 DNS 基础设施的重要组成部分，而 ICANN 对此的影响力甚微。数以万计的全球性企业运营着 DNS 服务器和基础架构，但未以任何方式参与到 ICANN 机构群体或政策决策过程中。就 ICANN 对这些机构群体的 SSR 外展而言，通过直接的方法大幅推动 SSR 的进步面临着巨大挑战，特别是考虑到 ICANN 企业实体的规模及其有限的预算。但是，对 DNS 运营商和互联网用户有更直接影响的其他组织，应可以增加对它们的外展。

迄今为止，最为庞大的互联网参与者群体还没有直接参与 ICANN。他们绝大多数是普通互联网用户，无论是个人或组织，对于他们而言，ICANN 及其机构群体的行动可能会对他们的互联网体验产生影响。这个群体往往不了解 ICANN，甚至不知道有这个组织存在，更不用说 ICANN 政策和程序了，虽然结果可能对他们使用互联网有直接的影响。新 gTLD 流程就是一个典型的例子，其中围绕该计划的讨论和争辩已成为国际新闻。

4.1.3 ICANN 偏离了经其同意的 SSR 职权范围吗？

ICANN 已特别谨慎确保其涉及了所承担的全部 SSR 任务的各类活动。2011 财年和 2012 财年 SSR 计划表明，ICANN 正在对该计划的各个领域采取经考虑的具体做法。ICANN 在处理其拥有直接控制权的领域和在更广泛的生态系统中必须将自身视为合作伙伴的领域时，这一点特别重要。

在过去 18 个月期间有过一些时刻 ICANN 似乎是超出了其当前限定的技术使命。针对运营 DNS-CERT 的提案的讨论和公告，曾在广泛的机构群体中引起了混淆和恐慌。然而，ICANN 针对机构群体的严重不安已作出适当的响应，并且现已撤销了这一提案。

2011 财年和 2012 财年计划都显示，ICANN 将遵循其有限的技术使命，并建立一个涵盖绝大部分 SSR 基层的活动计划。但是审查这些计划内的不同层次的细节还存在着挑战：一些任务是具体和可衡量的，而一些任务的概念是含糊不清的，没有明确的定义。DNS 运营商之间关于“应急计划演练”的讨论就是一个很好的例子。

ICANN 还将“DNS 安全性和稳定性”确定为其战略计划 (2011-2014) 中的四个“战略重点领域”之一。在这一计划中，它提到了四项战略目标：

- 保持并延长全球 DNS 正常运行时间；
- 提高整个唯一标识符系统的安全性；
- 增强唯一标识符安全性活动的国际参与性；
- 协调全球 DNS 风险管理。

这些主题已被引入 2012 财年 SSR 计划。这是相较于 2011 财年文件的一个可喜变化，否则将很难将两个文件联系在一起。

AOC 和 ICANN 章程均显示，这些 SSR 战略目标是与章程声明“确保互联网唯一标识符系统能够稳定而安全地运行”和“协调 DNS 根名称服务器系统的运行和发展”保持紧密一致的。其中，留有讨论余地的是在为“根”名称服务器系统和为“全球”DNS 系统（根据第四个战略目标）执行此事项之间的差别。正如本文后面所讨论的，如果处理不当，微小的区别可能会对范围和职权产生重大分歧。

4.2 SSR 框架的有效性和实施

SSR 审核小组分析了 ICANN 现有 SSR 框架建立有效战略以提高 DNS 安全性、稳定性和灵活性的程度。它还分析了 ICANN 实施该框架的进度及其在预算、组织、战略计划和政策制定过程中解决 SSR 问题的流程。除了审查 SSR 框架结构外，我们还评估了 ICANN 在三类 SSR 相关责任的各类责任中所确定的实质性项目。此外，我们还考量了 ICANN 在定义、更新和实施其 SSR 框架中是否有“明确的进展”的跨领域问题。

4.2.1 ICANN 的 SSR 框架和战略计划

AoC 承认，ICANN 已制定了一项旨在提高 DNS 运营稳定性、可靠性、灵活性，安全性，和全球互操作性的计划，该计划将由 ICANN 定期更新，以反映 DNS 面临的新威胁。SSR 审核小组的分析涵盖 SSR 框架的形式、SSR 框架中所包含的优先度和举措内容、SSR 框架的长期演变和连续性。我们还审查了 ICANN 的战略计划，其中包含有关 ICANN 战略和运营重点、ICANN 组织结构及其 SSR 相关预算的重要细节。

4.2.1.1 SSR 框架

ICANN 现在依据其 SSR 框架第三次重述进行运营。在审查中，我们仔细分析了在 2010 年 11 月定稿的 2011 财年 SSR 框架，以及在 2011 年 5 月定稿并由 ICANN 理事会于 2011 年 7 月 28 日决议认可的 2012 财年 SSR 框架。正如理事会所指出的，2012 财年 SSR 框架提前发布，以便配合 SSR 框架和 ICANN 2012 财年运营计划和预算周期的发布。[9] ICANN 已启动了 2013 财年 SSR 框架的制定工作，该框架预计将于 2012 年 6 月 ICANN 会议前定稿。

如前所述，SSR 框架结构和 ICANN 正在采取的举措似乎是与其 SSR 职权范围和职责范围是一致的。重点关注 2012 财年活动模块的 2012 财年 SSR 框架 B 部分，包含了作为 SSR 框架基础章节的 B 部分中所确定的三个责任领域。[10] 这些类别通常被纳入到用于组织具体计划和举措的“关切领域”。[11] 列入这些关切领域有助于在外部澄清 ICANN 的角色，并在内部维护其活动记录。

一个积极的发展是 ICANN 已在 2012 财年 SSR 框架中添加了一些 AoC 承诺的内容。[12] 这是一个有益的改进，ICANN 跟踪在执行 AoC 审核小组结果方面的进展时，这些改进在未来甚至会更有帮助。在 2012 财年 SSR 框架所确定的具体重点领域是连续性的和应急性的工作、以及维护清晰的流程并关注新出现的威胁和风险。[13] 在我们报告的第 3 节将进一步分析和讨论这些问题。

---

[9] 第 2011.07.28.05 号理事会决议，*2012 财年 SSR 框架*，2011 年 7 月 28 日通过。请参阅 http://www.icann.org/en/minutes/resolutions-28jul11-en.htm

[10] **幻灯片 4**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[11] **幻灯片 5-8**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[12] **幻灯片 17-23**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[13] **幻灯片 17**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

然而，2012 财年 SSR 框架始终没有确定 ICANN 三个责任领域中任一责任领域内的具体项目和举措。例如，ICANN 确定机构群体工作、安全小组核心领域和 2012 财年 SSR 活动的单独列表。[14] 该框架的每个章节都包含了一系列不同的活动，但它们不是按照 ICANN 的角色或责任区来组织的。而且，2012 财年 SSR 活动的冗长清单还包括全球安全性外展类别、协作、机构安全性计划和跨组织活动，但是不包括其他 ICANN 关切领域。[15] 这种结构将会使评估具体项目和举措与 ICANN 的一般责任领域相关联的方式、变得更加困难。

ICANN 做了描述属于 2012 财年 SSR 框架中的责任区的活动之类型的彻底工作，[16]但是个别项目仅在高层级的列表项中描述，并且几乎无背景内容或详细描述。ICANN 还没有明确地排列其 SSR 活动的优先次序。对比而言，2011 财年 SSR 框架通常提供了更多有关 ICANN 的优先事项和正在开展项目的特性的信息。SSR 审核小组发现形式上有了很多变化，这是一个积极的进步，特别是在帮助澄清该计划方面。同时，它也将有助于构建 SSR 的框架，以便更好地传达 ICANN 的工作重点和具体目标，这是衡量 ICANN 在履行 SSR 责任时是否有进展和是否成功的重要组成部分。

2012 财年 SSR 框架的组织结构是对 2011 财年 SSR 框架的一个相当不错的实质性新改进，后者不包括基础性的 A 部分，而是按照一系列计划和责任来组织的。例如，在 2011 财年 SSR 框架第 5 节中，ICANN 确定了一些正在开展的项目，这些项目按照小节分组，譬如 SSR 核心职责、TLD 注册管理机构和注册服务商 SSR 问题，以及 ICANN 支持组织和咨询委员会的活动。第 6 节确定了一些新的项目，并按照相同的一般类别对它们进行了组织。使用这种一致的组织结构有助于转达不同类型的 ICANN 活动和小组相关的项目。

另外一个发现是，年复一年更改 SSR 框架形式，使得 ICANN 更难以监督在计划实施方面的进展，更难以确定发生了什么变化。ICANN 应设法保持一致的 SSR 框架结构，以增强对 ICANN 项目和活动与其整体 SSR 职权和责任关联方式的关注。

今后，ICANN 应考虑如何提供一个明确、一致的 SSR 框架组织结构。具体来说，ICANN 应在整个框架的三个责任范围内组织所有项目。ICANN 应划分举措的优先顺序，并像在 2011 财年 SSR 框架中所做的一样考虑小节内容，这样有助于根据活动类型将项目分组到更分散的类别中。

ICANN 应对其所有 SSR 活动进行实际的成本收益分析，同时确保完全涵盖发展中地区的活动，并且不会基于成本或风险取消这些活动。ICANN 可以与更广泛的机构群体合作，力求确定具有稀缺资源的各方能够做出的技术贡献，并帮助推动这些贡献。

建议 7：ICANN 应该通过设立一系列明确目标并按这些目标确定其举措和活动的优先顺序，以扩展其目前的 SSR 框架。该流程应参考实际的成本收益和风险分析。

[14] **幻灯片 -10**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[15] **幻灯片 12-15**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[16] **幻灯片 -8,5**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

4.2.1.2 战略计划

除了 SSR 框架本身外，ICANN 连续三年一直在制定战略计划。该“战略计划”涉及到在 SSR 框架中所确定的一些计划，并提供了与 ICANN 的 SSR 职权范围有关的 ICANN 活动的更多相关详细信息。与 SSR 框架一样，该战略计划区分了在 ICANN 控制范围内的活动与 ICANN 能实施一些影响的领域。[17] SSR 审核小组已分析了 2011-14 年战略计划和 2012-15 年战略计划，后者已在我们审查过程中发布。我们对具体的实质性问题和目标的分析已包含在本报告的相关章节中。

2012 财年 SSR 框架引用了 2011-14 年战略计划的四个主要目标，所以这两个文件之间有着明确的联系。[18] ICANN 随后将最终确定 2012-15 战略计划，该计划实质上是与 SSR 框架相一致的。2012-15 年战略计划确定了与 ICANN 的 SSR 责任相关的五个战略目标：(1) 维护并推动 DNS 可用性；(2) 加强 DNS、IP 地址和参数的风险管理和灵活性；(3) 推动 DNSSEC 的普及；(4) 加强国际 DNS 合作；以及 (5) 提高对 DNS 事件的响应能力。此外，战略计划提供了一些 SSR 相关工作重点的其他细节，特别是 DNS 稳定性和安全性的重点领域，以及包括 IANA 在内的核心业务。[19] 它还制定了衡量 ICANN 绩效和进展的战略标准，而 SSR 框架自身没有包含这些内容。因此，该战略计划添加了额外细节和指标的重要组成部分，它们为 SSR 框架中规定的高层次计划和目标提供了补充。

总之，对于提供有关单个 SSR 相关目标和活动的详细信息的流程而言，ICANN 应保持它的一致性，包括所要达到目标的说明和项目所包含的工作。这一详细的文件并不一定要在 SSR 框架中有所反应，但是它应可在 SSR 框架中交叉引用，并在战略计划或其他可随时提供给 ICANN 机构群体的公开文件中有所反映。

如果 ICANN 要建立更细致的联系，以展示 SSR 框架是如何通过战略计划中的工作重点和项目、ICANN 预算和工作人员的决定来实施的，那么这也将是有帮助的。SSR 审核小组发现 SSR 框架和战略计划之间一致性的程度已很高。

通过加强 SSR 框架和战略计划中的项目之间的联系，并采用一致的组织结构和计划说明，ICANN 将确保能一致地关注优先项目，提高实现运营目标方面的进展情况的透明度。它也将使 ICANN 机构群体更容易确定 ICANN 的工作重点，并跟踪其在实现战略和运营目标方面的进展情况。最终的结果应是有一个计划，它说明了 ICANN 履行其职责的方式，并且它将项目和活动整合到一个全面的战略和运营计划中。

建议 8：ICANN 应该继续细化其战略计划目标，尤其是维持和推动 DNS 可用性的目标。战略计划和 SSR 框架应反映一致的工作重点和目标，以确保完全相符。

[17] 第 6 页，*ICANN 战略计划：2012 年 10 月至 2015 年 6 月*，2011 年 10 月 3 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[18] 幻灯片 9，B 部分，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[19] 第 1 页，*ICANN 战略计划：2012 年 10 月至 2015 年 6 月*，2011 年 10 月 3 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

4.2.2 ICANN 运营职责

SSR 审核小组同意 ICANN 在 2012 财年 SSR 框架中对其运营职责的描述。ICANN 的 DNS 运营职责覆盖 IANA 职能、L 根的管理和 DNSSEC。它具有内部机构安全职责，包括 IT 和网络安全，并对新 gTLD 计划、合同合规性和 IDN 快速通道管理负有行政管理责任。SSR 审核小组认为风险管理和业务连续性计划是 ICANN 运营职责的重要组成部分，因而在本报告的第 4.3 节阐述了这些议题。我们没有对超出 AoC 审核流程范围的 ICANN 会议或人员安全方面进行分析。

4.2.2.1 DNS 运营

在 2012 财年 SSR 框架中，ICANN 强调 IANA 职能、L 根的 DNS 运营以及 DNSSEC 是其运营职责范围内的计划和举措。[20] ICANN 的机构安全性计划清单包括从 L 根应急演练着手实施改进和 L 根单节点。[21]

ICANN 在 2012 财年 SSR 框架中纳入的运营活动建立在 2011 财年 SSR 框架的基础之上，其中包括：在所有根服务器上推广 DNSSEC；透过根区域请求的自动化和认证来改进根区域的管理；以及业务连续性演练活动。在 ICANN 的运营职责方面采取的具体举措包括：将根区域签名作为实施 DNSSEC 的组成部分、L 根区域升级研究，以及在捷克共和国、土耳其和拉丁美洲增加额外的 L 根服务器。

ICANN 2012-15 年战略计划中所包含的四个重点战略领域之一是“核心运营，包括 IANA”。根据 SSR 框架，ICANN 将 IANA 无错运营和 L 根灵活运营作为关键战略目标纳入到这一重点领域中。[22] 这些目标随即在以下具体战略标准中体现：(i) 达到或超过 IANA 合同服务等级协议规定的绩效；(ii) 通过欧洲质量管理基金会（“EFQM”）模型来证明流程的日益改善；(iii) 计划有效期内的 RPKI 部署；以及 (iv) 100% L 根正常运行时间。[23]

ICANN 组建了一个 IANA 运营小组，并已确立 SSR 相关问题的管理流程。SSR 小组与 ICANN 工作人员进行了面谈，并获取了 ICANN 程序的相关信息。我们得知，ICANN 使用了诸如 ISO 等正式标准为指导，但尚未寻求获得相关标准认证。ICANN 拥有若干 L 根管理运营程序，包括部分人员可靠性标准和一个变更管理流程，即一个模拟 ITIL 变更控制方法的变更和批准流程。IANA 也拥有一个信息安全计划，为发起、实施、维护和改进信息安全活动提供指导。我们注意到，RZ KSK 流程已获得 SysTrust 认证。

一直以来，ICANN 的一项主要运营举措就是实现根区域的自动化。2011 年，ICANN 实现了一个重要的里程碑。在并行人工和自动流程六个多月后，2011 年 7 月 21 日，ICANN 开始接受来自自动化系统的根区域变更为主要流程。自动化系统将向最终用户生成流程通知，提供确认请求、技术详情和状态更新。为确保平稳过渡，在流程内部建立了若干安全保护机制。

---

[20] **幻灯片 5，B 部分**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[21] **幻灯片 13**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[22] **第 11-12 页** *ICANN 战略计划：2012-2015 年*，2010 年 10 月 31 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[23] **第 12-13 页** *ICANN 战略计划：2012-2015 年*，2010 年 10 月 31 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

在与 ICANN 工作人员的探讨中，我们了解到作为 L 根变更流程的一部分，文件记录被保留下来，用于辅助进行运营事件的事后剖析，目的是改进基础架构和相关流程，避免相同的错误反复发生。变更流程旨在提供运营小组成员间的同行审核，确保变更不会显得突兀。同时，数据自动从特定的基础架构要素（例如使用变更控制软件维持的服务器、路由器/交换机要素）上收集，从而能够发现在变更控制流程之外所做的任何变更。这在一定程度上在运营小组内部提供了一个专门的审计职能，但对这一流程的正式审计既没有 ICANN 也没有任何第三方来执行。

ICANN 的运营职责包括其作为 DNSSEC 根区域密钥签名密钥 (RZ KSK) 管理者的重要角色。2010 年，ICANN 获得 SysTrust 认证，其中包括一项审计，确保 ICANN 在关于 RZ KSK 系统管理的可用性、流程完整性和安全性目标方面，已经有相应的控制措施。最近的认证更新已于 2012 年 1 月 23 日发布。

ICANN 已适当地确定了数个与其核心运营职责相关的战略目标，并且在制定用于衡量达到这些目标的战略标准方面取得了进展。它在阐明和提炼运营目标（除在早期版本的战略计划中使用的“100% DNS 正常运行时间”以外）上取得了进展，使之成为基本在其控制范围内的目标。SSR 审核小组认同 ICANN 应继续关注 IANA 合同履行、流程改进的实施及 DNSSEC 和 RPKI 部署。

我们有一个发现，即 ICANN 应用 ISO 和 ITIL 安全标准作为指导，但基本上没有获得这些标准下的认证，也没有进行过此类认证所要求的特定类型的正式审计。如前所述，变更控制流程的 SysTrust 认证和审计流程除外。我们注意到，安全认证流程的广泛应用可能没有很好地配合 ICANN 的运营和发展，还可能将工作人员的注意力从规定的任务上分散。然而，鉴于 ICANN 依赖已有的安全标准，其应该公布这些标准以及所进行的任何审计的结果。当然，任何公开报告都应以不损害 ICANN 的 SSR 立场的方式进行。

如该报告草案的意见反馈者所强调的，ICANN 的一些 SSR 活动是唯一的，为它们创建认证流程将是一种浪费。另一方面，软件开发、技术运营、外包和 IT 安全已经享受到标准化带来的好处。虽然这样做并不会干扰 ICANN 的运营、分散其重心或以其他方式降低优良的计划和运营绩效，但仍应取得那些适当的认证并将作为标准使用。

建议 9：ICANN 应根据普遍接受的国际标准（如 ITIL、ISO 和 SAS-70）评估其运营职责的认证选项。ICANN 应针对认证发布明确的路线图。

4.2.2.2 内部机构安全

在 2012 财年 SSR 框架中，ICANN 确定了一系列与其内部机构安全工作相关的项目。这包括从漏洞评估和测试着手实施流程改进、培训 IT 和安全工作人员，以及保留一名全职员工为业务连续性计划和应急措施演练提供支持。[24]

虽然 ICANN 没有将任何机构安全措施纳入 2012-15 年战略计划当中，但它致力于持续改进运营绩效这一战略目标，包括提升开展运营工作的能力和运营工作的可度量性。[25]

[24] **幻灯片 13-14**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

ICANN 的 IT 和安全工作人员执行了许多程序来保护其内部机构安全。工作人员为 SSR 审核小组提供了各种安全程序的相关信息。其中包括一个多层次的信息安全计划，覆盖 ICANN 用于实现服务的计算和通信系统。这一计划以 ISO 17799/27002 中阐明的安全控制框架为指导，每年审核一次，并根据 ICANN 信息安全风险评估中的变化进行必要的修改。

此外，ICANN 还制定了覆盖一系列其他安全议题的程序和指导原则。这包括一个信息资源备份政策、一个用户帐户管理政策、一个信息资源的变更管理政策和一个跟踪和管理技术问题的问题管理计划。此外还有针对员工和会议安全的程序，SSR 审核小组没有审核这些程序，因为这些议题不属于本报告的范围。

SSR 审核小组对 ICANN 将改进流程和开展工作人员培训作为履行 SSR 职责的一部分而付出的努力表示认同。对于 ICANN 而言，纳入关于这些活动的更多细节和 ICANN 力求实现的目标将有所帮助。这些具体信息不一定要体现在 SSR 框架中，但是可以纳入战略计划或关于 ICANN 管理活动的公开报告当中，这些报告可以在 SSR 框架中交叉引用。另外需要指出的是，我们提出的 ICANN 应公布其用作指导的任何安全标准、并考虑制定一个路线图以争取让其 SSR 相关流程获得更正式认证的建议也适用于 ICANN 的内部安全。

4.2.2.3 管理

作为 SSR 的相关举措，ICANN 将合同合规性、IDN 快速通道管理和新 gTLD 的实施纳入到其行政管理职责当中[26]。然而，在 2012 财年 SSR 框架中，这些方面的具体项目被认定为跨组织活动。[27] 这引发了对 ICANN 工作人员所承担的责任范围的疑问。同时，ICANN 确定了由自己负责实施的具体活动，例如新 gTLD 的漏洞测试、增加工作人员并改进注册管理机构和注册服务商的合同合规性、以及支持 IDN 计划的字符串评估小组和 DNS 稳定性小组。[28]

在 2012-15 年战略计划中，ICANN 陈述，随着新 gTLD 市场渐趋成熟，DNS 安全性、完善的合规性机制和消费者信任度成为越来越重要的问题。[29] ICANN 将消费者信任度概括为唯一标识符始终有效并在使用时交付一致结果的概念。[30] SSR 审核小组认同 ICANN 对消费者信任度的重视，及其对消费者信任度定义的概括。

[25] **第 12 页** *ICANN 战略计划：2012 年 10 月至 2015 年 9 月*，2011 年 10 月 3 日。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[26] **幻灯片 5，B 部分**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[27] **幻灯片 14-15**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[28] **幻灯片 14-15**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[29] **第 8 页** *ICANN 战略计划：2012 年 7 月至 2015 年 6 月*，2011 年 10 月 3 日。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[30] **第 8 页** *ICANN 战略计划：2012 年 10 月至 2015 年*，2011 年 10 月 3 日。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

ICANN 也适当地承认了它在 SSR 问题方面面临着严峻的考验。它指出，网络安全攻击在规模和复杂程度上继续增长，且执法机构所涉及的方面继续增加。[31] 除此之外，ICANN 指出新 gTLD 的迅速扩张带来了 SSR 方面的挑战，并且 IDN 及其变体还可以通过增加网络钓鱼来增加漏洞，从而导致各种稳定性问题。[32]

因此，作为战略目标的一部分，ICANN 承诺在竞争、消费者选择、恶意行为、权利保护和其他问题上衡量新 gTLD 的效应。[33] ICANN 确定的目标是通过支持可能对互联网参与者的行为产生影响的项目，减少注册滥用和恶意行为的发生及影响。[34] 有关项目旨在通过鼓励制定注册管理机构和注册服务商最佳规程用于处理域名注册滥用问题，并纳入《注册服务商委任协议》修订，进而完善 gTLD 注册管理机构和注册服务商的合同合规制度，确保可预测的用户环境安全。

相关的战略性度量标准包括：(i) 为新 gTLD 和 IDN 快速通道实施符合 ICANN 核心价值和计划目标的成功测量标准；(ii) 衡量新 gTLD 计划中权利保护机制的有效性；(iii) 制定、公布并执行用于处理新扩展的 TLD 空间的合同合规性制度；以及 (iv) 处理不符合 IDNA2008 协议的域名。[35]

ICANN 对新 gTLD 计划、合同合规性和 IDN 计划管理的行政管理是与 SSR 相关的重大问题，应当在 SSR 框架中重点考虑，并借助一套更具体的活动和目标来实施。对于这些行政管理问题，ICANN 应继续发展并实施有效性衡量标准、寻求机构群体的意见，如 2012-15 年战略计划中所述。它还应将更多有关这些重要活动的实质性信息纳入 SSR 框架本身。ICANN 应在其新 gTLD 计划管理中增加 SSR 框架（不断发展）、度量标准、目标和影响评估。

SSR 审核小组还分析了 ICANN 在其组织和预算流程中对合同合规性和新 gTLD 计划的处理方式。我们注意到，ICANN 已发起多项计划，并分配了专门的工作人员来管理合同合规性和新 gTLD 计划。不过，SSR 审核小组认为，针对合同合规性和其他行政管理职责制定和实施更加具体的度量标准，将有助于增强 ICANN 对这些问题的专注和效力，并使机构群体利益主体能够更好地衡量 ICANN 所取得的进展。我们与 ICANN 预算流程有关的分析和建议、以及与新 gTLD 计划启动有关的与日俱增的资源需求评估将在本报告后文中阐述。

建议 10：ICANN 应该继续努力加强合同合规性的强制执行，并为此职能提供足够的资源。ICANN 还应该为监控合规性问题和调查工作制定并执行结构更清晰的流程。

[31] 第 5 页，ICANN 战略计划：2012 年 10 月 3 日至 2015 年 6 月（草案）。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[32] 第 5 页，ICANN 战略计划：2012 年 10 月 3 日至 2015 年 6 月（草案）。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[33] 第 9 页，ICANN 战略计划：2012 年 10 月 3 日至 2015 年 6 月（草案）。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[34] 第 9 页，ICANN 战略计划：2012 年 10 月 3 日至 2015 年 6 月（草案）。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[35] 第 9 和 10 页，ICANN 战略计划：2012 年 10 月 3 日至 2015 年 6 月（草案）。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

建议 11：ICANN 应该最终落实并执行对以下方面所取得成绩的衡量，即与 SSR 相关计划目标明确关联的新 gTLD 和 IDN 快速通道，其中包括对减少域名滥用的机制的有效性衡量。

4.2.3 ICANN 作为协调者、合作者和推动者的影响领域

ICANN 具有广泛的协调、合作和推动责任。通过这些活动，ICANN 能通过自身的影响力（虽然不是命令或控制）带来诸多进展。在这一影响范围内，ICANN 与美国商务部、RIR、根服务器运行机构、ccTLD 运营商及其他 DNS 基础架构运营商进行协调。ICANN 还在政策制定上与许多社群组织互动并为其提供支持，包括：私营部门，营利性公司；民间团体组织；用户和个人；GAC；学术及科技组织，如研究所、高等院校和实验室；以及与 ICANN 签订了合同的注册管理机构和注册服务商。

ICANN 的协调、合作和推动责任包含各种各样的活动。在这一方面，ICANN 维系了一系列双边关系，在这些关系中能够通过 ICANN 工作人员的支持和积极健康的关系，促成理性的决策并同时把握形势分析和民情民意。鉴于这一复杂性，SSR 框架中有相当一部分是 ICANN 没有直接控制权但却能施加一定影响的计划和举措，这一点不足为奇。与 ICANN 影响领域有关的目标和活动在战略计划中也有陈述。

4.2.3.1 技术和运营问题

在 2012 财年 SSR 框架中，ICANN 就 DNS 技术和运营问题确定了一系列机构群体工作项目，它们是：DNSSEC 的采用；WHOIS 国际化注册数据；DNS 安全解决方案；IPv6 推出和 IPv4 耗尽风险管理；与 RIR 合作部署 RPKI；以及 IDN 变体案例研究。[36]

ICANN 将通过一系列运营相关项目来实施这些总体优先事项，这些项目包含在 2012 财年 SSR 框架的“合作”章节。这些合作项目包括：支持 DNS 度量与衡量工具，与 NTIA 和 VeriSign 共同实现根区域自动系统；与 RIR 共同发展资源公共密钥基础架构 (RPKI) 的资源认证；以及完成系统信任审核和 DNSSEC 密钥滚动的 KSK 仪式。[37]

SSR 审核小组认同 ICANN 在 2012 财年 SSR 框架中确定的总体计划。我们还承认 ICANN 在管理和履行其 SSR 相关运营职责的过程中与其他方面合作的重要性。但 SSR 框架应明确指出 ICANN 将展开的具体活动以及它希望达到的更加具体的目标。在某些情况下，ICANN 可能需要与其他方面合作，共同确定这些具体的活动和目标。

此外，2012-15 年度战略计划包括一系列 SSR 相关技术和运营问题，这些问题受 ICANN 影响，但不受其控制。在 DNS 稳定性和安全性章节，ICANN 致力于维护并推动 DNS 可用性，不仅是通过执行对 L 根运营的控制，还通过充分利用与 TLD 及注册服务商的合同及其他关系。[38] 战略项目包括促进 IPv6 的采用以及充

[36] **幻灯片 10**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[37] **幻灯片 12-13**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[38] **第 5 页** *ICANN 战略计划：2012 年—2015 年 2010 年 3 月 3 日 草案* http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

分利用与 TLD 及注册服务商的合同及其他关系，以支持 DNS 正常运行时间，包括注册管理机构和注册服务商的业务连续性计划。[39]

与此同时，ICANN 将继续推动 DNSSEC 的广泛采用作为其战略目标之一。[40] 为达到这一目标，ICANN 将与机构群体合作，监督并提高 DNS 的灵活性，并协调互联网资源认证的发展。[41] ICANN 计划继续与互联网群体和执法机构合作，共同制止恶意行为，并推动机构群体中的工作，开发业务连续性计划和测试以应对风险和威胁。[42]

ICANN 已确立一系列度量标准，用于衡量其在实现这些战略目标的过程中取得的进展。它将发动机构群体确定关键绩效指标，用于测量 100% DNS 正常运行时间，并监督 TLD 正常运行时间服务等级协议的合同执行情况。[43] 它将衡量全球业务连续性标准认证的进展。[44] 计划期间它还将跟踪 DNSSEC TLD 签名的数量和提升 IPv6 认知的活动。[45] ICANN 还将启动互联网号码资源认证安全工作，并与机构群体就计划有效期内的实施工作展开合作。[46]

在“核心运营，包括 IANA”章节中，ICANN 指出它负责协调 IP 地址空间及官方 DNS 根服务器系统的运营；以及协调三套唯一标识符（DNS、IP 及端口和参数）的分配。[47]

SSR 审核小组支持 ICANN 与 TLD 运营商及其他方面合作与协调，共同加强 DNS 安全性、稳定性和灵活性的计划和目标。我们认同 100% DNS 可用性的总体目标应当通过更具体的度量标准来细化和实施。此外，通过与注册管理机构和注册服务商合作，ICANN 能够在推动 SSR 相关最佳实践的开发和实施上发挥重要作用。这些努力还可供其他 DNS 运营商借鉴。

但是，机构群体对 ICANN 在 SSR 问题上承担运营角色表示担忧，并且 SSR 审核小组认为 ICANN 不应越权成立应急响应小组 (DNS CERT)，这超出了 ICANN 自身的运营责任范围。[48]

---

[39] 第 5 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[40] 第 5-6 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[41] 第 6 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[42] 第 6 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[43] 第 6 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf.
[44] 第 6 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[45] 第 7 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[46] 第 7 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[47] 第 11 页，ICANN 战略计划：2011 年 10 月至 2015 年 7 月（草案）
请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

4.2.3.2 组织支持

2012 财年 SSR 框架确定了以下涉及 ICANN 自身内部合作的机构群体工作项目：GNSO 与《注册服务商委任协议》相关的活动；SSAC 和 RSSAC 活动；共同应对唯一标识符系统的恶意滥用（如 Conficker 工作组）；以及政策制定，包括滥用注册政策工作组和国际化 WHOIS。[49]

在某些情况下，ICANN 工作人员依靠其他方面来领导具体的 SSR 相关活动。例如，2012 财年 SSR 框架在 DNS 安全性解决方案方面提到了 DSSA 工作组，并指出此工作组将在 WHOIS 的技术发展上支持其他方面的工作。[50] 该框架还在滥用注册和《注册服务商委任协议》(RAA) 方面引出了 GNSO 和 ccNSO 的政策制定活动。[51]

同样地，ICANN 在 2012-15 年战略计划中引用了一系列机构群体支持工作。ICANN 表示它将在机构群体工作组的引领下探索寻求解决方案的途径，例如协调一支应急响应小组或其他解决方案来解决互联网安全问题。[52] ICANN 还将与机构群体共同探寻低成本高效益的途径，以此制定 SSR 解决方案。[53]

长期以来一直存在一个问题，即在标准政策流程的范围内，部分为解决滥用注册和其他 SSR 相关问题的机构群体工作进展缓慢。例如，政府和执法机构代表就应当纳入 RAA 的条款确定了一系列建议。迫于不断增加的压力，ICANN 继续推进与委任注册服务商的积极谈判，纳入一系列将影响执法机构的 RAA 修订，包括与 WHOIS 验证相关的条款，要求注册服务商维护报告滥用的联系点、分销商义务、隐私/代理服务方面的更高义务，以及增加的合规机制，等等。

ICANN 承认了实施有效的机制以防止、发现和响应唯一标识符系统被恶意滥用的重要性。它也发起了许多活动来解决这些问题。但是，SSR 审核小组担心 SSR 相关问题并非始终得到及时地解决。在可能对合同签约方造成成本和运营负担的做法上，可能也很难达成一致。因此，我们建议 ICANN 在最近的活动和优先事项的基础上，开发和实施一套与 SSR 相关的最佳实践，这些做法可以纳入 RAA 以及与合同签约方签署的其他协议当中。[54]

建议 12：ICANN 应与机构群体合作，共同确定 SSR 相关的最佳实践，并通过合同、协议、备忘录及其他机制为实施此类实践提供支持。

[48] **第 6 □***ICANN* *战略计划* *年 10 月 23 年日 □修正 2015 年*
http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[49] **幻灯片 16，B 部分**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：
https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[50] **幻灯片 10 和 13**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[51] **幻灯片 13**，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[52] **第 6 □***ICANN* *战略计划* *年 10 月 23 年日 □修正 2015 年*
http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[53] **第 6 □***ICANN* *战略计划* *年 10 月 23 年日 □修正 2015 年*
http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[54] ICANN 的合同执行框架对 ICANN 合

建议 13：ICANN 应该鼓励所有支持组织为其成员制定和发布与 SSR 相关的最佳实践。

已收到的针对建议 13 的报告草案意见建议评估实施最佳实践对组织产生的影响：使其更加合理，提高其质量、效率并降低成本。很明显，最佳实践必须可行并与每个相关组织有关，同时还可能需要为不同的支持组织和机构群体量身定制。

4.2.4 ICANN 与全球互联网生态系统中其他相关方的互动

除 ICANN 可以施加影响的领域外，ICANN 还关系到全球互联网生态系统中的其他各方。这包括政府、执法机构、政府间组织和更广泛的互联网用户群体。ICANN 可协助支持互联网的安全性、稳定性和灵活性，方式为从事外展和教育活动，而这些活动常涉及与其他组织的合作。SSR 审核小组认识到，更广阔的“世界其他地方”正是某些最重大的 DNS 安全性、稳定性和灵活性风险的发源地。除从事教育和外展活动以外，这些更广泛的风险还是 ICANN 风险管理和业务连续性计划工作的重要组成部分，相关内容在下文第 4.3 节中讨论。

ICANN 确定了一系列涉及更广泛互联网利益主体的参与以及 SSR 相关问题能力培养的项目。例如，ICANN 在其工作重点计划中列出了推动 SSR 问题全球研讨会[55]、ccNSO 会议和技术日等活动的开展。它还列出了与区域 TLD 组织、ISOC 以及机构群体中的其他团体合作，共同开展 DNS 能力培养工作。[56]

在 2012 财年的具体活动列表中，ICANN 纳入了与更广泛群体的全球安全外展和参与活动，包括商业界、学术界、科技界和执法机构。[57] ICANN 还确定了就政府要求会对唯一标识符产生的技术影响开展教育活动，以及支持合作伙伴与利益主体。[58] 此外，ICANN 为其 DNS 能力培养计划确定了多项活动，包括与网络启动资源中心合作开展培训、在非洲、拉丁美洲和亚洲地区轮流开展各种培训活动。[59]

在 2012-15 年战略计划中，ICANN 指出工作人员和机构群体的工作重点将是全球安全外展和与 RIR 运营商合作，共同加强总体安全并支持区域和地方组织。[60] ICANN 还寻求继续与互联网群体和执法机构合作，共同制止恶意行为，并以合作的方式，在发展中国家建立 SSR 的机制。[61] 随着 IDN 和新 gTLD 计划在各区

---

[55] 幻灯片 12，B 部分，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[56] 幻灯片 6，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[57] 幻灯片 12，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[58] 幻灯片 15，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[59] 幻灯片 19，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[60] 第 6 页，*ICANN 战略计划：2012 年 7 月至 2015 年 6 月*，2010 年 10 月 3 日。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[61] 第 6 页，*ICANN 战略计划：2012 年 7 月至 2015 年 6 月*，2010 年 10 月 3 日。请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

域催生更多注册管理机构和注册服务商，ICANN 将与 ISOC、本地 TLD 运营商以及本地互联网群体合作执行教育和培训计划。[62]

在具体目标方面，ICANN 承诺说明地区培训计划的工作重点并报告进展情况，并在 2012 年将 IDN 指南成文并公布。[63] SSR 审核小组认同 ICANN 着重于更广泛的参与和能力的培养，我们也支持确定工作重点和编写进度报告。正如 ICANN 所指出的，随着 IDN 和新 gTLD 的扩展，这些工作将变得更加重要。

SSR 审核小组认识到，对于更广泛的全球互联网群体，ICANN 没有任何直接的权力，甚至没有直接的沟通方式。鉴于大量私营 DNS 运营商可能与 ICANN 的互动有限或没有互动，ICANN 应该将扩大工作范围，以便与这些运营商在关键的 SSR 问题（例如 DNSSEC 部署）上进行技术协调作为工作重点之一。很多 DNS 运营商将是专业团体、同类组织或行业论坛的成员，并且他们的技术工作人员很可能订阅了相关的行业和技术期刊及文献。对于 ICANN 而言，一个有利的做法是考虑自己如何才能利用其他类似渠道来讨论重大的 SSR 问题（例如 DNSSEC），在这些讨论中，有针对性的沟通方式可能会激起各方的强烈兴趣，否则将无法使其参与进来。尽管由于采用了一致和固定的方式，ICANN 机构群体内部的许多外展活动办得非常成功（例如注册管理机构运营商对 DNSSEC 的关注度），但 DNS 价值链中的其他相关方（例如 ISP）对相同的 SSR/DNSSEC 问题关注度一直非常低。

在分析 ISOC 在其全球 IPv6 知晓度宣传中所执行活动的过程中，可能会发现已采用自身方法进行外展的组织的卓越范例。在这方面，很明显 ISOC 已选择将影响范围扩大到其普通受众以外，直接与大小企业合作，以积聚外展日背后的动力[64]。

建议 14：ICANN 应该确保其与 SSR 相关的外展活动不断发展，以保持相关、及时和适当。机构群体的反馈意见应该提供一种机制来审核和增强这种相关性。

此外，ICANN 应继续为本机构及其群体成员探索积极影响环境，使环境有利于 SSR 的方法。在这一方面，ICANN 能够作为一个发现问题并连结机构群体成员的论坛，发挥有益的召集作用。我们建议 ICANN 的安全工作人员继续将工作重心放在加强关键 SSR 问题（例如 DNSSEC 部署）的技术协调，以及支持 ICANN 内部为 SSR 相关问题所做的工作上。

除继续开展各种参与和外展活动以外，ICANN 应继续深入，公布有关 DNS 威胁和风险降低策略的信息，包括发布业务连续性计划指南，为政府、执法机构以及更广泛的互联网群体中的其他各方提供指导。这可能包括想办法面向更大范围发布由 SSAC、DSSA WG、新成立的理事会 DNS 安全框架工作组和 ICANN 机构群体内部的其他团体编写的材料。最近建议的针对根服务器和其他 DNS 基础架构的攻击是可能已实现这一目标的一个良好示例。对 ICANN 安全小组而言，这将是其发挥主导作用的最佳机会，以确保机构群体为应对此类攻击（如果发生）做好准备。

[62] 第 9 □ICANN 战略计划 年 10 2012 3 日至 2015 请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[63] 第 10 □ICANN 战略计划 年 10 2012 3 日至 2015 请参阅 http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[64] http://www.worldipv6launch.org/

互联网的多利益主体环境 — ICANN 是开创者 — 常常遭到质疑，无论是直接的质疑，还是因其他行动而遭受的质疑。目前，针对即将召开的 ITU WCIT 和 WTSA 大会，有国家提议对 ITR 进行变更，这些变更可能会挑战多利益主体模式，从而妨碍该模式的发展。ICANN 必须与那些支持多利益主体、自下而上的决策模式发展的其他各方通力合作，提供信息并积极开展外展活动，以开放的姿态进行关于这些问题的对话，同时立场坚定地反对对 DNS SSR 的粗暴破坏。

建议 15：ICANN 应扮演推动者角色，负责公布和普及 DNS 安全威胁及防范技术。

4.2.5 拥有针对 SSR 问题的清晰流程

AoC 指示 SSR 审核小组特别注意 ICANN 是否拥有针对 SSR 问题的清晰流程。SSR 审核小组分析了 ICANN 制定 SSR 框架并获取机构群体意见的流程。我们还审查了 ICANN 跟踪 SSR 框架的实施并不断完善其计划的流程。

4.2.5.1 机构群体意见

ICANN 拥有一个向机构群体宣传 SSR 框架并在框架草案完成之前获取公众意见的既定流程。2010 年 9 月 13 日发布了 2011 财年 SSR 计划草案，并在 2010 年 11 月 3 日之前开放了一个公众意见论坛。根据 ICANN 的公众意见摘要，只有七方就 2011 财年 SSR 框架提交了书面意见。在 ICANN 工作人员进行的六个机构群体简报活动期间收到了其他意见。2011 财年 SSR 框架的终稿纳入了公众意见论坛期间收到的意见，于 2010 年 11 月 23 日发布。其修改囊括了对 ICANN 持续进行的 SSR 活动、及其与互联网群体在合同合规性方面关系的描述的多处更新和修订。

2011 年 5 月 2 日，ICANN 发布了 2012 财年 SSR 框架草案，并启动了一个公众意见论坛。与之前 SSR 计划所用的报告格式不同，该计划以新的演示文稿格式发布。应 ccNSO 的要求，2012 财年 SSR 框架草案的公众意见征询期延长到 2011 年 6 月 7 日。O 在意见征询期间，只有五方就 2012 财年 SSR 框架草案提交了书面意见，并且注册管理机构利益主体组织还向 ICANN 工作人员提交了问题。此外，在意见征询期之前及期间（日期如下），ICANN 工作人员还就 SSR 框架和 ICANN 在 SSR 方面的活动做了简报，包括：

- SSR 框架 SSAC 预审（2011 年 4 月 7 日）；
- ALAC 公开电话预审（2011 年 4 月 26 日）；
- ccNSO 工作小组电话简报（2011 年 5 月 9 日）；
- 在华盛顿特区召开的 IT 部门协调委员会国际委员会会议（2011 年 5 月 10 日）；
- 在宾夕法尼亚州匹兹堡召开的美国国家网络刑事鉴定及培训联盟 (National Cyber-Forensics and Training Alliance) SpyEye/Zeus 会议（2011 年 5 月 19 日）。

2011 年 6 月，ICANN 开始制定 2012-2015 年战略计划。10 月 3 日，ICANN 发布了战略计划草案，其中反映了来自 GNSO、ALAC、ccNSO 和 ICANN 工作人员重点关注领域工作会议的意见，以及战略性度量标准的更新。公众意见征询期截止于 2011 年 11 月 17 日。

有五个团体提交了对 2012-15 年战略计划的意见，分别是 IPC、BC、ccNSO、AFNIC 和 ALAC。这些意见提出 ICANN 应改进计划，明确其要达到的目标，同时继续将影响与控制区别开来。此外，还有建议要求减少战

略目标的数量并完善用于衡量进展的度量标准。还有意见表示支持为打造一个健康的互联网生态系统而开展的外展和能力培养活动。为纳入公众意见和提交的其他意见，对 2012-15 年战略计划做了若干修改。

ICANN 有一个既定的有效流程，旨在提供一个透明的决策流程并征求建议和公众意见。SSR 框架和战略计划的草稿、红线更新和公众意见摘要的发布，有助于建立一个透明的流程。此外，为 2012 财年 SSR 计划和相关解释所用的新框架有助于评论者更好地理解计划草案。这反过来有助于打造一个清晰的流程 — 本次审核的对象之一。ICANN 在内部与有直接双方合作关系的各方提高了 SSR 方面流程的清晰度，也提高了其他方面流程的清晰度。

除针对 SSR 框架的 ICANN 公众意见和外展流程之外，ICANN 还从事了许多外展和参与活动，这些活动有助于为 SSR 框架提供信息并形成该框架。ICANN 与 SO 和 AC 的互动使其有更多机会争取意见，并将它们纳入到 SSR 框架的开发和发展过程之中。

ICANN 应想方设法提高认知并增加公众对 SSR 计划草案的意见量。鉴于评论者对 ICANN 的适当角色和职责问题的关注，SSR 审核小组特别建议 ICANN 执行一个程序，结合 ICANN 有限的技术使命，直接关注它在确保 DNS 安全性、稳定性和灵活性中的角色问题。SSR 审核小组还相信 DSSA WG 可以提供一个良好的平台，扩大机构群体对 SSR 问题的参与和意见范围，包括但不限于 SSR 框架本身。

建议 16：ICANN 应该继续实施其外展工作，以扩展机构群体参与到 SSR 框架制定流程中并提供意见。ICANN 还应该建立一个流程以便从其他生态系统参与者处获得更系统化的意见。

正如此报告草案的意见反馈者所建议的，参与 SSR 相关问题的 IETF 讨论是有必要的。虽然已经在参与此类讨论，并且 ICANN 提供了许多关于 IETF 和 IAB 的正式和非正式链接，但仍应注意所强调的建议。

4.2.5.2 实施情况跟踪

ICANN 没有一个正式的流程来公开跟踪 SSR 框架的实施情况，或在财年结束之时审核 SSR 框架的状态。就 ICANN 跟踪 SSR 框架实施情况并评估实施进展，为 SSR 框架的持续制定和发展提供信息的流程，SSR 审核小组与 ICANN 工作人员进行了面谈。ICANN 保留了与各 SSR 相关活动情况有关的内部信息，并使用这一信息来制定战略计划和预算，但是没有一个综合的流程来跟踪 SSR 框架的实施情况。

ICANN 应当拥有一个跟踪和评估 SSR 框架实施情况、并随时间做出任何必要调整的一致内部流程。在与 SSR 审核小组的讨论中，ICANN 工作人员认同了我们的建议，即在明年 SSR 框架的制定流程中，对实施情况进展进行一个年度运营评估将有所帮助。

既然 ICANN 有机会制定三个版本的 SSR 框架，那么，在 SSR 框架制定流程中纳入一个定期的审核和评估机制，将会提升流程的稳定性和连续性。ICANN 还开发了一个公开公告板来跟踪问责制和透明度审核小组 (ATRT) 建议的实施情况。在与 ICANN 工作人员的讨论中，他们提出 ATRT 公告板可以作为跟踪 SSR 框架和 SSR 审核小组建议实施情况的模板。为改进 ICANN 与 SSR 问题相关的清晰流程，我们赞同这一提议并已将它纳入到我们的建议中。

建议 17：ICANN 应该建立一个结构更清晰的内部流程，以展示活动和举措如何与 SSR 框架内的具体战略目标和工作重点相关。还应该为执行工作确立度量标准和里程碑。

建议 18：ICANN 应该为其在执行 SSR 框架中取得的进展执行年度运营审核，并将此评估作为一个要素纳入下一年的 SSR 框架中。

建议 19：ICANN 应该建立一个流程，以让机构群体跟踪 SSR 框架的执行情况。提供的信息应该足够清楚，以便机构群体可以跟踪 ICANN 对其 SSR 职责的执行情况，同时不损害 ICANN 的有效运营能力。用于跟踪 ATRT 建议执行情况的公告板流程可作为良好典范。

4.2.6 ICANN 的 SSR 相关预算和工作人员

在 SSR 职能方面，ICANN 有专门的预算和工作人员。在 2012 财年 SSR 框架中，ICANN 估计 SSR 举措约占 ICANN 总体运营计划和预算的 17%（约为 6980 万美元支出中的 1200 万美元）。[65] ICANN 还表示它将增加 3 名以上的合同合规性工作人员。[66] SSR 框架中没有对工作人员和预算问题做其他阐述。

在 2012-15 年战略计划中，ICANN 承诺通过定义度量标准以确保 ICANN 预算有适当百分比专门用于 DNS 稳定性、安全性和灵活性，从而改进预算流程的透明度和结构。[67] 它大致讨论了需要投入专门的资源和人员，来应对 IDN 和新 gTLD 扩张所带来的合同合规性和 SSR 挑战。[68] ICANN 还承诺实施一个新的财务体系，据称该体系将改善战略计划和运营计划之间的相互关系，并帮助确定分配到四个战略重点区域的运营预算，以及提供不同支出等级的依据。[69]

4.2.6.1 SSR

ICANN 还在其 2011 财年和 2012 财年运营计划和预算文件中重点提到了 SSR 计划，并用 SSR 事务定义了四个“战略重点领域”之一（在 DNS 稳定性和安全性的标题下）。在分析 SSR 工作的预算配置时我们看到：

- 2011 财年 — 708.7 万美元（总预算的 12% — 较 2010 财年预算增长了 23.2%）
- 2012 财年 — 783.6 万美元（总预算的 11.7% — 较 2011 财年预算增长了 10.6%）[70]

---

[65] 幻灯片 25，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[66] 幻灯片 14，*2012 财年 ICANN 安全性、稳定性与灵活性框架*，2011 年 5 月 2 日。请参阅：http://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[67] 第 7 页，*ICANN 战略计划：2012 年 7 月至 2015 年 6 月*，2011 年 10 月 3 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[68] 第 89 页，*ICANN 战略计划：2012 年 7 月至 2015 年 6 月*，2011 年 10 月 3 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[69] 第 12 页，*ICANN 战略计划：2012 年 7 月至 2015 年 6 月*，2011 年 10 月 3 日。请参阅：http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[70] 第 13 页，*2012 财政年度预算*，2012 年 6 月 30 日，2011 年 6 月 24 日通过。请参阅：http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09aug11-en.pdf

这显然是一大笔预算，表明 ICANN 有意将 SSR 作为重点战略目标之一。不过，SSR 审核小组注意到，在 2012 财年 SSR 框架中确定的 SSR 相关预算的金额（约为 1200 万美元）大大超出了在预算本身中直接分配给 SSR 相关工作的预算（即 783.6 万美元）。这一差异加大了跟踪 ICANN 在 SSR 相关活动上支出的难度。

2011 财年和 2012 财年运营计划都显示了这一预算配置将用到的一些具体方面。这些支出反映了在 SSR 框架和战略计划中确定的计划和活动。举例如下：

- 在 2013 年前进行风险评估活动；
- 通过推动 DSSA-WG 的工作来为其提供支持，以便它在 2012 年年底前提供 DNS 风险和威胁的缺口分析；
- 在 DNSSEC 上与 DNS 运营商开展合作，包括定期密钥滚动和审核；
- 从 2011 财年 L 根应急计划演练着手实施改进；
- 实现 2012 财年 SSR 框架中包含的目标；
- 制定一份长期计划并获取资源以支持在发展中国家进行的 TLD 能力培训；以及
- 消除使用 ISO 27002 标准确定的 ICANN 内部信息安全的差距，并制定全面的 BCP 计划。[71]

然而，如果我们试图跟踪这一总额在这些活动中的分配方式，只有极少的细节能够支持在计划内的进一步分析。向 ICANN 工作人员提出要求后，我们获得了进一步的预算分配方式，显示了 2012 财年在 CSO 控制下的预算为：

- 人员成本 — 120 万美元
- 管理成本 — 35,500 美元
- 差旅 — 244,325 美元
- 专业服务 — 115 万美元
- **总计：255 万美元**

在分析 ICANN 在 SSR 等举措上的支出时，我们必须考虑到配置的预算将分散到多个部门和人员当中。培训和外展活动就是一个很好的示例，这些活动可能包含安全要素，但不受安全小组的管辖。

然而，在 2012 财年划拨给 SSR 活动的 783.6 万美元中，似乎有 468.3 万美元（SSR 预算的 60%）不在 CSO 的控制或职权范围内，认识到这一点是很重要。随着我们力图了解 SSR 预算的支出方式以及获得预算的活动在何种程度上更好地完成了 ICANN 的 SSR 使命，预算信息的缺乏使得预算在具体项目和经费上的使用方式很难评估。此外，关于预算款项如何分拨给计划中所列任务的管理者（运营商和财务上），也没有清楚的说明。这又使得外界对内部花销和项目执行的效力跟踪困难重重。虽然我们认识到大部分 SSR 预算将分配至多个部门和多项举措中，但了解资金的主要“类别”将有助于了解整体预算的效力。

安全小组由七位向首席安全官 (CSO) 报告的工作人员组成。该小组负责管理 ICANN 的内部安全运营，支持 SSR 相关的政策制定并支持组织活动，包括理事会风险委员会、SSAC 和 DSSA 工作组以及新成立的理事

[71] 第 134 页 *2012 财年运营计划和预算*，2012 年 6 月 30 日，2011 年 6 月 24 日通过，请见 http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09aug11-en.pdf

会 DNS 风险工作组。此外还有一个单独的组织，其中有专门负责 IANA 职能（十位向 IANA 和技术运营副总裁 [VP] 报告的工作人员）和 DNS 运营（五位向 IANA 和技术运营 VP 报告的工作人员）的工作人员。

根据对可用预算信息的审核，SSR 审核小组得出结论：ICANN 应仔细考虑改进本机构计划和细分年度预算和工作人员要求的方式，并明确这些巨额款项如何支出和跟踪，以及组织中的哪些人员管理 SSR 计划的整体绩效。ICANN 已承诺定义度量标准以确保 ICANN 预算有适当百分比专门用于 SSR 相关问题。制定更详细的预算信息将增加预算流程的透明度，还将支持 ICANN 自身提出要实施的度量标准。

4.2.6.2 合规性

2012 财年预算为合同合规性活动分配了 425 万美元的资金，较 2010 年增长了 25%。[72] 这囊括了雇佣合规性工作人员，以及借助来自注册管理机构联络部门、注册服务商联络部门、法务部门、政策部门、安全部门和 IT 部门的支持，加大合规性工作的力度。合规性活动包括：

- 巩固主动监控和执行注册服务商和注册管理机构的合同条款所需的流程；
- 改善与机构群体的交流和向机构群体的报告；
- 强制实施与 WHOIS 有关的现有政策，其中包括改进端口 43 的监控工具和方法；
- 执行 2012 财年 WHOIS 数据提醒政策的审核并公布结果；
- 强制实施与数据托管程序有关的现有政策；
- 实施 WHOIS 数据问题报告系统的进一步改进并分析投诉数据；
- 收集合规性统计数据和资料并进行沟通；
- 实施消费者投诉受理系统 (CTicket) 的升级或更换；以及
- 2012 年 6 月 30 日前，通过专门的外展活动进一步发展同欧洲、中东、南美及亚太地区的注册管理机构和注册服务商的关系。

合规性组织目前由一名合同合规部门高级主管和十一名工作人员组成，全部向 ICANN 总顾问报告工作。2012 财年预算包括为新增三名合规性工作人员拨款。

合同合规性已经成为 ICANN、GAC、某些单独的政府以及执法机构之间关系的关键要素。执法机构对迅速、明确地确认域名注册人的要求，与部分注册管理机构和注册服务商没有能力提供可靠、更新的信息之间的矛盾在 2011 年达到了必须解决的地步。可以乐观地预测，通过领导力和人力资源来加强合规职能将有利于这一矛盾的解决。

注册管理机构和注册服务商的数据托管是合规性的一个关键方面，也是顶级域名灵活性和安全性的一个关键要素。SSR 审核小组鼓励密切监视并执行数据托管合规性的所有方面。

从 DNS SSR 的角度上说，合规性至关重要，因为更好的合同合规性有望更好地阻止域名滥用以及对 DNS 的某些攻击和滥用，并减少涉及 ICANN、注册管理机构和注册服务商、执法机构和 GAC 的争议。尽快证明合规性方面的能力与进步，将给那些担心新 gTLD 一旦建立并投入运营，ICANN 将会面临诸多挑战的各方带来一定信心。

[72] 第 14 页，2012 财政年度运营计划和预算，2011 年 6 月 30 日，2011 年 6 月 2
http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09aug11-en.pdf

4.2.6.3 新 gTLD 计划

正如 ICANN 在 2012 财年战略计划中所指出的，新 gTLD 计划将带来 SSR 方面的挑战，并且 IDN 及其变体还可以通过增加网络钓鱼来增加漏洞，从而导致各种稳定性问题。[73] 因此，随着新 gTLD 计划的实施，ICANN 必须准备好分配合理数量的人员及其他资源来维护 DNS 的安全性、稳定性和灵活性，这一点将非常重要。

SSR 审核小组已就新 gTLD 计划的预算和人员配置计划流程与 ICANN 工作人员进行了面谈。这一分析涵盖 ICANN 在处理申请和授权批准字符串方面的准备程度，也提供了对 ICANN 内部授权后运营准备的高度概括。ICANN 的计划工作在假设未来有 500 个新授权的 gTLD、以及可能出现数量极少（如 100 个新 gTLD）和数量极多（如 1000 个新 gTLD 的总量）的情况的基础上，考虑了一系列人员配置需求。

根据 ICANN 工作人员提供的信息，SSR 审核小组进行了对可能会受到新 gTLD 计划影响的关键 SSR 相关职能的分析。

gTLD 计划办公室 (GPO)。GPO 是全面负责 gTLD 申请处理的新部门。这包括为一系列新 gTLD 流程选择、签约和“吸收”第三方，例如统一快速暂停 (URS) 和商标信息交换机构流程。GPO 评估了与申请处理计划有关的启动前风险和运营风险。其中一个重点领域是数据安全性，ICANN 已与第三方独立安全顾问签订了合同，审核并测试申请流程的安全性。

法律。ICANN 的总顾问办公室将为新 gTLD 计划提供法律支持和建议，包括申请审核和处理，以及异议和争用解决流程的处理。它还将在注册管理机构与成功的新 gTLD 申请人之间所达成协议的执行中发挥核心作用。标准注册管理机构协议的制定有望使这些协议的审核与执行更加高效。

财务。ICANN 的财务部门将支持新 gTLD 计划的所有申请定金和费用交易。这将涵盖初步建立流程和付款的持续处理。除这些申请处理活动外，预期会有大量的新注册管理机构和注册服务商的计费和收费工作。2011 年秋天实施了一个旨在适应新环境的新财务系统。

IANA。IANA 部门负责新 gTLD 带来的升级问题。对于 331 个现有 TLD，根区域管理职能包括初步授权、TLD 迁移和现有 TLD 的日常维护。某些步骤需要与 NTIA 和 VeriSign 互动。在为新 gTLD 计划准备的过程中，IANA 进行了一项卓越经营审核，目的是分析现有的流程并确认风险、差距和要改进的方面。职能分析指出，IANA 流程的某些要素已精简和自动化，但人工审核步骤依然必要，以确保根区域变更得到适当授权，且对安全性和稳定性没有任何负面影响。

注册管理机构联络部门。注册管理机构联络部门的职能包括负责管理注册管理机构协议合同、处理新注册管理机构服务请求、解释和实施政策以及推动社群支持。目前正在努力将现有流程标准化并进行记录，以减轻人员配置和吸收工作的压力。ICANN 确认了一系列重大风险，包括资源和人员配置、新注册管理机构经验不足的可能、以及注册管理机构出现问题的潜在可能。除了标准化工作以外，ICANN 还计划实施客户关系管理 (CRM) 系统，旨在为注册管理机构提供自助服务流程。

[73] **第 5 口** *ICANN* *战略计划* *年 10 月 23 年 口 修正 2015 年*
http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

注册服务商联络部门。注册服务商联络部门目前正与大约 970 个 ICANN 委任的、根据《注册服务商委任协议》(RAA) 运营的注册服务商合作。这一职能包括审核注册服务商委任申请、解释并实施政策和 RAA 条款、确保域名的顺利迁移以及与其他小组协调，共同促进注册服务商的合规性。正在考虑的重大风险包括人员配置和资源要满足更庞大的注册服务商群体的需要，这一群体更加缺乏经验；还包括需要与合同合规部门协调。尽管某些任务不能自动化，ICANN 仍计划加强部分流程的自动化，以便降低风险并提高注册服务商支持流程的效率。

合同合规性。正如前面所讨论过的，合同合规部门的工作重心是 18 个 gTLD 注册管理机构和约 970 个注册服务商的合同执行和监督活动。正在考虑的重大风险包括合同合规要求预期会增加，以及注册服务商市场的地理扩张。合同合规部门将与注册管理机构联络部门合作，共同开发有效的吸收流程，该流程有望从标准化的合同中受益。ICANN 的长期计划是重点进行主要任务的进一步正规化和自动化，并建立一个专门的支持机构和一个升级的、集中的客户投诉记录系统。

根据我们对 ICANN 工作人员所提供信息的分析，ICANN 似乎已经在与 SSR 问题直接相关的一系列职能上确认了关键问题和风险。它还启动了结合更多的资源和精简的流程来管理这些风险的计划流程。下一步，ICANN 应发展公众评估，该评估要记录 ICANN 的计划工作，并让机构群体审核与新 gTLD 计划有关的未来预算和人员配置及资源要求。

发布报告草案之后，ICANN 启动了新 gTLD 计划的申请流程，并收到约 2000 份申请。最近围绕申请流程稳定性的活动（发布报告草案之后）强调了 ICANN 有效管理新 gTLD 计划的重要性，特别是其在此次 DNS 扩展过程中的 SSR 责任的重要性。

建议 20：ICANN 应该提高关于执行 SSR 框架和履行 SSR 相关职能的组织和预算的信息的透明度。提供的信息应该足够清楚，机构群体可以跟踪 ICANN 对其 SSR 职责的执行情况，同时不会妨碍 ICANN 的有效运营能力。

建议 21：ICANN 应该建立结构更清晰的内部流程，以展示组织和预算决策与 SSR 框架的相关性，包括基本的成本收益分析。

建议 22：ICANN 应该发布、监控和更新管理 SSR 问题并引入新 gTLD 所需的组织和预算资源的文档。

4.3 了解风险情况和应急计划

4.3.1 当前和未来短期内的风险

目前，安全与稳定咨询委员会（“SSAC”）的成立是为了就那些对 DNS 的稳定运营有着即时或短期影响的风险相关事务，向理事会提供建议。SSAC 与 ICANN CSO 小组合作，提供对安全威胁和风险的迅速响应。SSAC 已为 ICANN、IANA 和机构群体提供了宝贵的建议。多年来，它共编写 53 份报告和咨询意见（截止到撰写本报告时），涵盖许多种问题。[74]

SSAC 就诸如运营事务（如根名称系统的正确可靠运行）、行政管理事务和注册事务（注册管理机构和注册服务商服务，如 WHOIS）等问题提供了建议。SSAC 一直从事互联网名称和地址分配服务的威胁评估和风险分析工作，评估哪里存在严重的稳定性和安全性威胁。SSAC 对 DNS 问题的关注超过互联网号码分配和地址问题。

ICANN CSO 小组负责收集和实施 SSAC 的回复意见（除该小组自身自发进行的风险评估工作外）。这可能采取 ICANN 有完全控制权的内部运营形式，或者可能需要与机构群体合作以便将建议付诸实施。可直接实施行动的一个范例是根据 SSAC 和 RSSAC 对根区域升级的建议，在根区域内分阶段实施新 gTLD。与机构群体合作实施行动的一个范例是 DNSSEC 的分阶段部署，这一部署涉及众多团体和一个复杂的时间表和实施计划。对于这两种情况，ICANN CSO 小组基本上一直都能有效地实施行动。

在与 SSAC 的讨论中了解到，显然他们有时对于在一段非常有限的时间内就具体问题给出答复感到很有压力。这最终导致了评估问题的时间缩短和建议更有目的性。显然，未来在分析即时风险时，有时仍需要对研究工作施加时间限制。这是不可避免的。然而，更谨慎的做法是，确保进行合理地计划，给予 SSAC 和 RSSAC 尽可能多的时间来完成高质量的研究工作和研究结果。

更概括地说，SSR 审核小组的结论是，应当给工作组（例如理事会 DNS 风险管理工作组和 DSSA-WG）和咨询委员会（例如 SSAC 和 RSSAC）充分的工作条件，使他们能够做出好的决定。虽然 SSR 审核小组重点关注与 SSR 相关的工作组和咨询委员会，但是在属于此类别的活动中没有清楚的界线。得出高质量结果的一个前提是人员配置和其他资源与对工作组和咨询委员会的要求相符。让工作组和咨询委员会在一个能够让他们做出客观决定，不受内外部压力影响的环境下运作，这也很重要。

建议 23：ICANN 必须根据对 SSR 相关工作组和咨询委员会提出的要求为其提供适当资源。ICANN 还必须确保工作组和咨询委员会所做的决策是在不受外部或内部压力的情况下客观地作出的。

4.3.2 未来长期的风险

ICANN 的 SSR 活动不是孤立进行的。而且，DNS 不是静态的，ICANN 的 SSR 流程已经发展并且还会继续发展。在某些方面，SSR 框架的年度更新就是公布 ICANN CSO 小组的策略性活动。本节将分析 DNS 生态系统以及 ICANN 发现长期风险和做出战略性预测的能力。

[74] http://www.icann.org/en/groups/ssac/documents-by-category

正如本报告其他部分所述，SSR 审核小组不会分析 ICANN 内部组织结构的细节。我们只简单地说明，在机构群体内获得较高尊重的成熟的、可持续的总部机构对于 CSO 小组及其计划执行的成功至关重要。

ICANN 拥有许多收集长期风险相关信息的渠道，例如 SSAC、RSSAC、DSSA 工作组、理事会风险委员会和新成立的理事会 DNS 风险管理工作组。然而，在这一影响层面上，ICANN 主要是通过与 DSSA WG 和 RSSAC 的合作来发现长期风险。放眼未来，这些机制或改进后的机制必须纳入长期和系统风险，并与其他机构群体方面协调，特别是与 SSAC 和理事会 DNS 风险管理工作组。

排除“未来最难以预料”这一陈词滥调，对 DNS 的良好风险管理必须着眼于未来和全局，使利益主体能够对潜在的长期威胁有所准备。对于 SSAC、理事会风险委员会和 ICANN 利益主体，包括根服务器运营商、TLD 注册管理机构和注册服务商，预测风险的能力与其利益直接相关，它们已据此采取行动，尽管协调较差或没有协调。

ICANN 自成立以来一直在使用未来风险情况管理的其他信息来源。例如，有利于发现长期系统风险的做法如下：与 IETF/IAB 密切联系，包括通过理事会联络人；SSAC、RSSAC 及 DSSA WG 的成员工作所在的组织是在风险管理中纳入了 DNS 风险的组织；参加研讨会及其他国际会议；与研发组织互动；以及由有资质的 ICANN 工作人员执行的标准信息安全实践。

长期风险的来源多种多样，例如 DNS 性质的根本性改变、DNS 软件的新应用；以及法律和法规变化。它们还可能来源于 ICANN 运营所处环境内的重大、战略或政治因素。在这一层面，实体与个人在 ICANN 对大事无法掌控的情况下运营，情况更加复杂，而且某些长期风险出现的方式尤其难预测。

历史上，DNS 的根本性改变用了一段时间才逐步形成并被接受。然而，这些变化正在加速。在这方面值得一提的是 IPv6 的采用和推出以及在 DNS 中对 IPv6 编码的能力、IDN 编码的使用和采纳，以及 DNSSEC。这些都是 ICANN 对某些类型的长期风险进行成功计划的范例。

其他的、更难计划的战略风险可能具有可能性低、变化快和故障成本高的特点。这类战略风险在现有的 SSR 计划框架内很难解决。还有一些无法预料但影响极大的风险。例如，在 DNS 上发现 Kaminsky 漏洞就属于这类风险。这是一个具有重大影响的意外事件，需要立即采取行动以保护 DNS。

建议或尝试脱离多利益主体模式来改变互联网管理的发展给 DNS 带来了特殊的威胁。法律和法规框架的根本变化可能会影响 ICANN 的许多活动，但不一定属于现有 SSR 框架计划流程的范围。

ICANN 对这类系统风险的预防策略包括了一个多年的参与承诺，方式有工作人员的参与、与其他组织合作以及为某些活动提供资金，例如互联网管理论坛。其效果很难衡量，当组织在多个层次上对事件的发展有发言权并能将负责人纳入其人脉网，即取得了最好的效果。在这些情况下，防范措施、谈判和 ICANN 言语的微调都最终降低了风险并很好地处理了问题。

其他存在风险、变化快和故障成本高的方面是 DNS 协议及其运营特征的根本性改变。

SSR 审核小组建议 ICANN 全面分析其必须应对的风险局面所带来的挑战，在此基础上仔细考虑 CSO 小组的资源计划和结构。定义 CSO 小组与 ICANN 及其支持组织（如 SSAC 和理事会风险委员会）中的其他安全相关职能有关的角色也会有所帮助。

咨询委员会和工作组为 CSO 小组提供高质量、及时信息的能力取决于对这些活动的适当支持。

在发掘风险战略意义的过程中，必须警惕破坏性事件发生的可能性，即使它们发生的几率很低。

建议 24：ICANN 必须明确定义首席安全官小组的章程、角色和职责。

建议 25：ICANN 应该制定相关机制来确定其风险管理框架中的短期和长期风险及战略因素。该流程应该参考来自研究、企业合作伙伴、ICANN 支持组织和其他渠道的见解。ICANN 应该发布风险相关信息，认识到其中一些因素的敏感性。

4.3.3 ICANN 的风险管理流程

ICANN 已反复指出建立风险管理框架的重要性。其发展简史如下：

- 2001 年 11 月 — ICANN 成立了总裁的安全与稳定常务委员会。[75] 委员会章程于 2002 年 3 月通过，其中阐述了委员会的宗旨之一：

  > “为互联网命名和地址分配服务建立一个安全框架，界定重点关注领域并找出每个领域的责任所在。委员会将重点关注关键命名基础架构的运营事宜。”[76]

- 2002 年 5 月 — 常务委员会变更为咨询委员会 (SSAC)，但保留委员会章程。[77]

- 2009 年 5 月 — 对风险管理框架的需要在 SSAC 独立审核中得到重申，包含在以下建议中：

  > “SSAC 与 ICANN 工作人员回顾第一项任务，以作为 SSAC 首个年度计划的一项工作。第一项任务如下：‘为互联网命名和地址分配服务建立一个安全框架，界定重点关注领域并找出每个领域的责任所在。’”[78]

[75] 安全稳定常委会 *ICANN 理事会临时会议记录* http://www.icann.org/en/minutes/prelim-report-15nov01.htm#StandingCommitteeonSecurityandStability

[76] *安全委员会章程* 2012 年 3 月 14 日 http://www.icann.org/en/committees/security/charter-14mar02.htm

[77] 安全委员会 *理事会临时会议记录* http://www.icann.org/en/minutes/prelim-report-13may02.htm#SecurityCommittee

[78] 最终报告 *安全稳定咨询委员会审核* — 2009 年 5 月 14 日 JAS Communications LLC http://www.icann.org/en/reviews/ssac/ssac-review-final-15may09.pdf

- 2009 年 10 月 — 作为对独立审核的回应，SSAC 指出它不适合执行这一任务：

  > “[SSAC] 章程中的第一项‘为互联网命名和地址分配服务建立一个安全框架…’更适合于研发，而不是一个由志愿者组成的咨询委员会… 应将其删除。”[79]

- 2010 年 3 月 — 一个负责实行独立 SSAC 审核的理事会工作组提议将安全框架责任从 SSAC 章程中删除。

- 2011 年 3 月 — ICANN 理事会批准了理事会工作组提出的章程变更，并指示理事会管理委员会成立一个工作组来解决这一问题。[80]

最终，经过 SSAC 审核，理事会决定解除 SSAC 为 DNS 制定一个全面风险管理框架的责任，并开始设立一系列新的组织结构，主要体现为理事会工作组。[81] 在我们审核的过程中，理事会 DNS 风险管理工作组成立并招募了成员。其章程已公布且通过理事会批准。理事会 DNS 风险管理框架工作组的宗旨是为一个针对互联网命名和地址分配服务的 DNS 安全风险管理框架的实施制定目标和里程碑，并确定相关的时间表和预算。此外，工作组还将监督一个作为任务基线的初步评估的建立。

[79] *ICANN 安全与稳定咨询委员会 2009 年 10 月 15 日 http://www.icann.org/en/committees/security/sac039.pdf*

[80] *批准修订章程 实施 SSAC 审查工作组报告 一份以前批准的理事会决议 http://www.icann.org/en/minutes/resolutions-18mar11-en.htm#1.4*

[81] **最终报告**，*安全与稳定咨询委员会审核* — 2010 年 1 月 29 日 — **SSAC 审查工作组** *http://www.icann.org/en/reviews/ssac/ssac-review-wg-final-report-29jan10-en.pdf <http://www.icann.org/en/general/bylaws.htm* 注：审核建议应当取消此任务，因为它不在 SSAC 的活动范围内。

鉴于理事会于 2011 年 3 月 18 日批准了章程修正案，这反映了删除 SSAC 章程第一项任务的情况，其内容为”为互联网命名和地址分配服务制定安全性框架，界定重点关注的领域并确定每个领域承担的责任。委员会应重点关注关键命名基础架构的运营注意事项。”

鉴于 ICANN 理事会希望由 ICANN 执行该项任务中预期的工作。

兹此发布第 2011.03.18.07 号决议：理事会指示理事会管理委员会向理事会推荐一个工作组来监督 DNS 风险管理框架和系统的开发，因为它与 ICANN 章程中定义的 ICANN 职责有关。理事会建议 BGC 在其建议中考虑纳入来自 SSAC 的一名工作组成员。理事会要求 BGC 在 2011 年 6 月于新加坡召开的理事会会议上提交对建议的考虑内容。” http://www.icann.org/en/minutes/resolutions-28oct11-en.htm#1.8

理事会 DNS 风险管理框架工作组的工作范围限于为新创建的 DNS 安全框架的目标、里程碑和报告的确定过程提供监督。此外，工作组还将监督基线评估的建立，以及这一职能与 ICANN 工作人员日常活动的整合。考虑工作组任务时，指示工作组考查：(i) 维护 DNS 安全性和稳定性的总体要求；(ii) ICANN 在安全性和稳定性方面的有限作用；(iii) 技术群体关于框架实施的意见和建议；以及 (iv) SSAC 编写的相关文件。

赋予 DNS 风险框架工作组的权限为监督性质，也就是说，工作组要注意框架实际是由其他方创建，而不是通过自身、独立的工作来创建框架。我们强烈建议随着授权的完成和工作的启动，工作组采取必要的措施将按时完成风险管理框架的制定放到优先位置。该小组应明确责任和义务，以确保对 ICANN 的 SSR 活动产生显著的积极影响，这一点很重要。

在进行这一理事会级活动的同时，开展本报告前面提到的、关于 ICANN 促成或运行 DNS-CERT 意愿的讨论之后，ALAC、ccNSO、GNSO 和 NRO 成立了 DSSA-WG，目标是更好地理解全球 DNS 的安全性和稳定性。DSSA-WG 将就以下事项向 SO 与 AC 报告：

- DNS 所受威胁的实际级别、频率和严重性；
- 当前减轻这些威胁的工作和活动；以及
- 当前对 DNS 问题的安全响应与 DSSA-WG 认为恰当可行的安全响应之间的任何差距。

可以预见，理事会机构及其他各方将吸收来自 DSSA 的结果，并将它用作对构建风险管理框架的意见之一。

建议 26：ICANN 应该优先及时完成风险管理框架。此工作应该符合高标准的参与度和透明度。

4.3.4 风险管理框架

像 ICANN 这样的机构应当具备一个发现、理解和减轻风险的正式机制。这一活动采取的形式为一个正式和固定的风险管理框架。在此框架中，诸如风险的严重性、可能性和性质等问题均包含在内。它提供了一个机制，可使组织上下以一致的方式认定风险的优先级别。正式风险管理框架的实际益处在于，它使影响重大的风险高度透明，并将感情与政治因素剔除出风险管理。

在与 CSO 小组和支持组织的讨论中，SSR 审核小组明显认识到，由于竞争压力和有限的志愿资源，可能很难确定风险与威胁评估的优先级。在这样的情况下，一个正式的风险管理框架将有助于提供优先化的任务分配。正如前面讨论过的，到目前为止，ICANN 尚未明确指派创建和维护全面风险管理和应急计划流程的职责。这一职责最初指派给 SSAC，但现在已移交给上文提到的新理事会委员会和其他机构。

在缺少一个全面、正式的 DNS 风险管理框架的情况下，ICANN 的 CSO 小组在一个非正式的框架内运营，在此框架内可开展有组织的、成功的运营行为。不过，IANA 拥有一个正式、公开的风险管理框架，IANA 通过这一框架运营。

为 ICANN 建立的正式风险管理框架将使所有级别的风险管理具有全面性和更好的优化方案。最重要的影响将出现影响范围的中部，因为框架的建立应让各方更容易了解并接受自己的角色。它还应促进合作。

风险管理框架应具有参与性，吸收机构群体中丰富的知识，具有前瞻性、积极性、组织性，并能整合动态变化和可扩展性。

建议 27：ICANN 的风险管理框架在 SSR 职权范围和有限使命范围内应该全面周到。

4.3.5 应急响应和通知

在应急响应方面，ICANN 具有两种作用，这些作用都与本报告相关。首先，在 DNS L 根基础架构的直接运营方面，ICANN 有义务及时了解并响应公开的紧急事件。这涉及与其他 DNS 软件供应商、基础架构供应商和 DNS 运营商的合作。另一个影响的方面是 ICANN 可以作为事件报告与合作的信息交换机构。在两种情况下，ICANN 都是以被动反应的方式对现实的威胁做出响应。

SSR 审核小组注意到，作为一个组织，ICANN 已经开始采取更主动的姿态来进行威胁评估，这将给主动应急响应提供信息。现任 CSO（从事过威胁确认事务）的任用就是朝这个方向积极迈进的一步。审核小组还注意到，为确认威胁并协调应急响应，ICANN 正积极联络执法机构。

为维持一个可靠的互联网，必须确保 DNS 具有强大的应急管理、灵活性和恢复功能。在一个互连的全球环境中，一个系统的弱安全性会加大对其他系统的风险。单一实体不可能全面洞悉 DNS 及其传输网络，当事件可能威胁到所有人时，所有相关方都有义务分享关于网络的洞察并与其他方面合作。随着 ICANN 继续构建并提高自身的响应能力，它必将与其他各方（包括所有受影响的团体）合作扩展国际网络，强化全球形势认识和应急响应。

SSR 审核小组发现 ICANN 为应急响应做了长期大量的准备，并不断地提升自己的能力。CSO 小组受过相关培训并能依靠系统和支持。机构群体内部沟通良好，提升了预测和预防紧急事件并提供灵活响应的能力。但是，这一应急响应能力可能过于集中在核心团队中。组织的规模和人员更替水平要求经常进行新人员的培训和已有人员的再培训。这一结论也适用于整个 IT 系统所依赖的项目管理体系。

对于核心 CSO 小组以外的 ICANN 工作人员，我们找到的应急准备证据较少。事故避免预防措施已到位，但是我们没有发现后续工作或审核的证据。

在第二影响层面 ICANN 没有以相似的一致性或强度来经常分享有意的应急响应准备。支持组织和咨询委员会的响应将更为临时性，或是基于面向极少数人的既定程序，还将依赖于它们自身召集其他响应者的能力。这一点可以通过由 ICANN 领导和批准制定的最佳实践文档来改进。

对于第三层也是最外层，ICANN 的应急响应和准备策略，或者它的发展，必须为两方面：

预防：对更广泛用户和利益主体群体的外展和教育是最主要的。互联网用户和域名注册人可以充分利用教育材料。很多时候，这些材料可以当场“适时、适地、适量”提供，因而要求注册管理机构、注册服务商、ISP、OSP 以及作为用户主要联系人的其他方面提供合作。已发给注册人的 SSAC 的关于“保护域名”

的文件就是此趋势的一个例证。其他外展和教育工作必须指示注册管理机构、注册服务商、ISP、OSP 以及其他与域名注册系统关系密切的实体来完成。

应急响应和计划：如前所述，ICANN 的 SSR 权限以外的领域不在 ICANN 的管理范围内。然而更广阔的外围环境正是应急计划所针对的风险来源。黑客、事故和错误是这一广阔领域的组成部分，必须纳入 ICANN 的准备流程中。

建议 28：ICANN 应该继续积极开展威胁检测和降低工作，并参与宣传威胁和事故信息的工作。

5 术语表

A

问责制和透明度审核 (ATRT)

在 Amok 下完成的第一个审核，包含 27 条加强整个 ICANN 的活动的建议，包括理事会的管理和绩效、政府咨询委员会的作用和效力、公众意见和公共政策流程以及理事会决策的审核机制。[82]

咨询委员会

咨询委员会是一个正式的咨询机构，由来自互联网群体的代表组成，目标是就特定的问题或政策领域为 ICANN 提供建议。ICANN 章程中指定了数个咨询委员会，根据需要可能还会成立其他咨询委员会。咨询委员会没有代表 ICANN 行动的法律权限，但是能够向 ICANN 理事会报告它们的研究结果并提供建议。[83]

《义务确认书》(AoC)

2009 年 9 月 30 日由 ICANN 和美国商务部签订（确认），包含 ICANN 四个主要目标定期审核的具体条款。这些审核提供了一个评估和报告 ICANN 在实现基本组织目标方面进展的机制；这些目标是：

确保问责制、透明度和全球互联网用户的利益；

维护 DNS 的安全性、稳定性和灵活性；

促进竞争、提高消费者信任度、扩大用户选择范围；

WHOIS 政策。[84]

网络普通用户咨询委员会 (ALAC)

ICANN 的网络普通用户咨询委员会 (ALAC) 负责考虑 ICANN 的活动并提供相关建议，这些活动关系到互联网用户（“网络普通用户”群体）个人的利益。

[82] 参阅 http://www.icann.org/en/about/aoc-review
[83] 参阅 http://www.icann.org/fr/about/learning/glossary
[84] 参阅 http://www.icann.org/en/about/aoc-review

地址支持组织 (ASO)

ASO 就与互联网协议 (IP) 地址的分配与管理有关的政策问题向 ICANN 理事会提供建议。ASO 为 ICANN 理事会选拔两名理事[85]。

c

国家或地区代码域名支持组织 (ccNSO)

ccNSO 是负责制定与国家或地区代码顶级域名有关的、基于共识的全球政策，并就此向 ICANN 理事会提供建议的机构。ccNSO 的活动不仅仅是政策制定，我们还积极交流信息和国家或地区代码顶级域名 (ccTLD) 管理机构的最佳实践。[86]

国家或地区顶级域名 (ccTLD)

双字母域名，例如 .uk（英国）、.de（德国）和 .jp（日本）被称为国家或地区代码顶级域名 (ccTLD)，它们对应一个国家、地区或其他地理位置。ccTLD 域名的注册规则和政策差异巨大，ccTLD 注册管理机构仅限相应国家或地区的公民使用 ccTLD。[87]

计算机应急响应小组 (CERT)

计算机应急响应小组是一个负责处理计算机安全事件的专家小组。大多数小组在其名称后附加了缩写 CERT 或 CSIRT，后者表示计算机安全事件响应小组。对某些小组来说，CERT 指计算机应急预备小组 (Computer Emergency Readiness Team)，但该小组处理的任务与计算机应急响应小组相同。[88]

CERT 计算机网络安全工程 (CSE) 小组重点关注研究和教育，旨在帮助软件和系统的收购者、管理者、开发者和运营者在整个开发和收购生命周期 — 特别是早期阶段解决安全和生存问题。[89]

D

DNS 域名系统 (DNS)

[85] 参阅 http://www.icann.org/fr/about/learning/glossary
[86] 参阅 http://www.icann.org/fr/about/learning/glossary
[87] 参阅 http://www.icann.org/fr/about/learning/glossary
[88] 参阅 http://en.wikipedia.org/wiki/Computer_emergency_response_team
[89] 参阅 http://www.cert.org/

域名系统 (DNS) 帮助用户在互联网上识别地址。网络中的每一台计算机都有一个唯一的地址，类似于电话号码。该地址是一个相当复杂的数字串，称为“IP 地址”（IP 代表“互联网协议”）。IP 地址很难记忆。DNS 使用常见的字符串（“域名”）代替了复杂的 IP 地址，进一步简化了互联网的使用。这样您就不再需要输入 207.151.159.3，而只需输入 www.internic.net 就可以了。通过 DNS 这一“助记工具”，人们更容易记住复杂的地址。[90]

DNSSEC

DNSSEC 的工作方式是对每一个 DNS 记录进行数字签名，这样就能够发现该记录的任何篡改。数字签名和用于创建数字签名的密钥的分发与 DNS 中任何其他记录的分发相似，使得 DNSSEC 在后台能够兼容。DNS 层级结构中每一层的密钥都使用上一层的密钥签名，有效地为其提供担保，与域名的层层授权相类似。这一“信任链”用于验证伴随受 DNSSEC 保护记录的数字签名，以便发现变更。[91]

G

政府咨询委员会 (GAC)

ICANN 通过政府咨询委员会 (GAC) 接收政府的意见。GAC 的关键职能是就公共政策问题向 ICANN 提供建议，特别是当 ICANN 活动或政策可能涉及国家法律或国际协定时。GAC 通常每年召开三次会议，与 ICANN 会议联合进行，其间与 ICANN 理事会和其他 ICANN 支持组织、咨询委员会以及其他团体讨论问题。在与理事会会面期间，GAC 还可能通过面对面会议或电话会议讨论问题。GAC 主席是来自加拿大的 Heather Dryden。[92]

通用名称支持组织 (GNSO)

ICANN 的通用名称支持组织 (GNSO) 接管域名支持组织在通用顶级域名方面的职责。ICANN 章程指出 GNSO 属于三个支持组织。SO 帮助促进互联网政策的制定，并鼓励在互联网技术管理中多样化和国际化的参与。每个 SO 向 ICANN 理事会提名两名理事。[93]

通用顶级域名 (gTLD)

三个或三个以上字符的 TLD 多为“通用”TLD 或“gTLD”。它们可以再分为两类，即“行业类别”TLD (sTLD) 和“非行业类别”TLD (uTLD)。[94]

[90] 参阅 http://www.icann.org/fr/about/learning/glossary
[91] 参阅 http://www.icann.org/en/news/in-focus/dnssec
[92] 参阅 http://www.icann.org/fr/about/learning/glossary
[93] 参阅 http://www.icann.org/fr/about/learning/glossary
[94] 参阅 http://www.icann.org/fr/about/learning/glossary

I

互联网号码分配当局 (IANA)

IANA 最初是负责监督 IP 地址分配，协调互联网技术标准规定的协议参数的分配，管理 DNS，包括授权顶级域名，以及监管根名称服务器系统的管理机构。IANA 根据 ICANN 的规定，继续向区域互联网注册管理机构分配地址，与 IETF 和其他技术机构协调来分配协议参数，并监管 DNS 的运行。[95]

互联网名称与数字地址分配机构 (ICANN)

互联网名称与数字地址分配机构 (ICANN) 是一个国际化组织的非营利性机构，负责互联网协议 (IP) 地址空间分配、协议标识符指定、通用 (gTLD) 和国家/地区代码 (ccTLD) 顶级域名系统管理以及根服务器系统管理职能。最初，互联网号码分配当局 (IANA) 和其他实体在美国政府合同下执行这些服务。现在 ICANN 执行了 IANA 的职能。作为公私协作形式的组织，ICANN 致力于维护互联网的运营稳定；促进竞争；实现全球互联网群体的广泛代表性；并通过自下而上、基于共识的流程制定与其使命相应的政策。DNS 转换您所输入的相应 IP 地址中的域名，并将您连接到希望的网站。DNS 还启用电子邮件以正确运行，因此您发送的电子邮件将到达目标收件人。[96]

IDN 国际化域名

IDN 是指包含以非基本拉丁字母表 (a - z) 书写且在本地语种中使用的字符的域名。IDN 可能包含许多欧洲语言中的变音符号或非拉丁文字符号，如阿拉伯文或中文。[97]

互联网工程任务组 (IETF)

IETF 是一个由网络设计人员、运营商、供应商和研究人员组成的大型的开放性国际机构群体，关注于互联网构架的发展和互联网的顺利运行。它对任何感兴趣的个人开放。[98]

互联网协议 (IP)

IP 协议是互联网底层通信协议，它能使处于不同地点的大型计算机网络之间可以通过多种物理连接，迅速经济地相互通信。互联网协议地址是一个数字化地址，可用来识别网络中的位置。互联网中的计算机使用 IP 地址发送信息和建立相互之间的连接；而人们一般都采用通过域名系统创建的更易记忆的名称。[99]

[95] 參阅 http://www.icann.org/fr/about/learning/glossary
[96] 參阅 http://www.icann.org/fr/about/learning/glossary
[97] 參阅 http://www.icann.org/fr/about/learning/glossary
[98] 參阅 http://www.icann.org/fr/about/learning/glossary
[99] 參阅 http://www.icann.org/fr/about/learning/glossary

国际标准化组织 (ISO)

ISO（国际标准化组织）是世界上最大的国际标准制定和发布机构。[100]

互联网协会 (ISOC)

互联网协会是负责互联网及其网络技术和应用的全球合作和协调的国际组织。任何感兴趣的个人均可成为 ISOC 的成员。[101]

IPV4

IPv4 是使用最广泛的互联网协议版本。它定义 32 位格式的 IP 地址，形式如 123.123.123.123。每个三位数小节可以包括一个从 0 到 255 的数字，这就意味着可用 IPv4 地址的总数为 4,294,967,296（256 x 256 x 256 x 256 或 2^32）。[102]

IPV6

IPv6，又称 IPng（或 IP 下一代），是计划的下一版 IP 地址系统。（IPv5 是一个实验性版本，主要用于流数据。） IPv4 使用的是 32 位地址，而 IPv6 使用的是 128 位地址，使得可用地址的数量呈指数型增长。[103]

互联网服务提供商 (ISP)

ISP 是向组织和/或个人提供互联网访问权的公司。ISP 提供的访问服务包括网站托管、电子邮件、网络电话（IP 语音）以及为其他应用程序提供支持[104]。

J

DNS 安全性与稳定性分析联合工作组 (DSSA-WG)[105]

DSSA 工作组的目标是发挥参与的 SO 和 AC 的专长，征求专家的意见和建议，并就以下问题向各自的参与 SO 和 AC 报告：

DNS 所受威胁的实际级别、频率和严重性；

当前减轻这些 DNS 所受威胁的工作和活动；以及

当前 DNS 问题安全响应的差距（如有）。[106]

[100] 参阅：http://www.iso.org/iso/about.htm
[101] 参阅 http://www.icann.org/fr/about/learning/glossary
[102] 参阅http://tools.ietf.org/html/rfc791
[103] 参阅 http://tools.ietf.org/html/rfc2460
[104] 参阅 http://www.icann.org/fr/about/learning/glossary
[105] 参阅 http://ccnso.icann.org/workinggroups/dssa-wg.htm

P

网络钓鱼

网络钓鱼攻击是指利用社会工程和技术手段来窃取消费者个人身份资料和财务帐户凭证的行为。社会工程方案使用伪造电子邮件引诱消费者进入假冒网站，目的是欺骗收件人泄漏财务资料，例如信用卡卡号、帐户用户名、密码和社会保险号码等。[107]

R

注册服务商

用户可以通过许多相互竞争的不同公司（也称为“注册服务商”）来注册以 .aero、.biz、.com、.coop、.info、.museum、.name、.net、.org 和 .pro 结尾的域名。在已认证的注册服务商目录中会显示这些公司的名单。[108]

注册管理机构

“注册管理机构”是在每个顶级域名中注册的所有域名的权威性主数据库。注册管理执行机构负责维护主数据库并生成“区域文件”，从而让计算机可以与世界各地的顶级域名之间进行互联网通信。互联网用户不能直接与注册管理执行机构进行联系，但用户可以通过 ICANN 委任的注册服务商在 TLD 中注册域名，包括 .biz、.com、.info、.net、.name 和 .org 等。[109]

RIR 地区互联网注册管理机构

目前有五个 RIR：AfriNIC、APNIC、ARIN、LACNIC 和 RIPE NCC。这些非营利性组织负责在地区级向互联网服务提供商和本地注册管理机构分配 IP 地址。[110]

根服务器

根服务器包含所有 TLD 注册管理机构的 IP 地址，包括全球注册管理机构，如 .com、.org 等和 244 个特定国家/地区注册管理机构，如 .fr（法国）、.cn（中国）等。这是关键信息。如果信息不是 100% 正确或信息模糊不清，就可能无法在互联网上找到关键注册管理机构。就 DNS 而言，信息必须是唯一且真实的。[111]

资源公共密钥基础架构 (RPKI)

资源公共密钥基础架构 (RPKI) 使公共网络（如互联网）用户能够验证数据（已由数据创始者进行数据签名）的真实性。[112]

[106] 参阅 http://ccnso.icann.org/workinggroups/dssa-wg.htm
[107] 参阅 http://www.icann.org/fr/about/learning/glossary
[108] 参阅 http://www.icann.org/fr/about/learning/glossary
[109] 参阅 http://www.icann.org/fr/about/learning/glossary
[110] 参阅 http://www.icann.org/fr/about/learning/glossary
[111] 参阅 http://www.icann.org/fr/about/learning/glossary

S

安全与稳定咨询委员会 (SSAC)

安全与稳定咨询委员会的工作是就与互联网名称和地址分配系统的安全性和完整性相关的事宜向 ICANN 机构群体和理事会提供建议。这包括运作问题（例如与正确、可靠地运行根域名系统有关的问题）、管理问题（例如与地址分配和互联网号码分配有关的问题）以及注册问题（例如与注册管理机构和注册服务商提供的诸如 WHOIS 之类服务有关的问题）。SSAC 一直从事互联网名称和地址分配服务的威胁评估和风险分析工作，评估哪里存在严重的稳定性和安全性威胁，并据此向 ICANN 机构群体提供建议。[113]

SO 支持组织

SO 是三个专门的顾问团体，它们就关于域名（GNSO 和 CCNSO）和 IP 地址 (ASO) 的问题向 ICANN 理事会提供建议。[114]

T

顶级域名 (TLD)

TLD 是 DNS 命名级别中最高层次的域名。在域名中，它是最后（最右边）一个“.”后面的字母串，例如“www.example.net”中的“net”。TLD 的管理者负责控制该 TLD 下识别哪些二级域名。“根域”或“根区域”的管理者负责控制哪些 TLD 能被 DNS 识别。常用的 TLD 包括 .com、.net、.edu、.jp、.de 等。[115]

W

万维网联盟 (WW3)

W3C 是成立于 1994 年 10 月的一个国际行业联盟，工作是开发促进万维网发展并确保其互用性的常用协议。联盟提供的服务包括：面向开发者和使用者的万维网信息存储库；为体现和促进标准的参照编码实施；以及各种用于展示新技术使用的应用程序原型和示例。[116]

WHOIS

WHOIS（发音同“who is”；不是缩略词）是一个互联网协议，用于查询数据库以获取某域名（或 IP 地址）的注册信息。[117]

[112] 参阅 http://www.apnic.net/services/services-apnic-provides/resource-certification/RPKI
[113] 参阅 http://www.icann.org/fr/about/learning/glossary
[114] 参阅 http://www.icann.org/fr/about/learning/glossary
[115] 参阅 http://www.icann.org/fr/about/learning/glossary
[116] 参阅 http://www.icann.org/fr/about/learning/glossary
[117] 参阅 http://www.icann.org/fr/about/learning/glossary