第二轮安全、稳定和弹性 (SSR2) 审核小组最终报告——执行摘要与建议

摘自 SSR2 审核小组最终报告

2021 年 1 月 25 日

目录

A. 执行摘要

根据互联网名称与数字地址分配机构 (ICANN) 章程（第 4.6 (c) 节）的规定：

“*董事会应指示就 ICANN 对以下义务的履行情况展开审核（SSR 审核）：增强内外部系统和流程的运营稳定性、可靠性、弹性、安全性和全球互用性，这些系统和流程与 ICANN 负责协调的互联网唯一标识符系统之间存在着直接的相互影响关系。*”[1]

这些 SSR 审核是完成 ICANN 组织“运作上秉承公开和透明的原则实现最大程度的可行性，并遵守那些为确保公正性而设计的程序”使命[2]的重要组成部分。这是开展的第二轮 SSR 审核，并且根据章程规定，审核报告中包含了对 ICANN 组织处理第一轮 SSR 审核建议的综述以及供 ICANN 组织审议的新建议。

SSR2 审核小组提出了 24 组建议，包括 63 项具体建议，从对 ICANN 组织针对 SSR1 建议的回复的评估开始。我们采用这种将建议进行细分的方法是为了解决 SSR1 建议中缺乏明确性的问题。然后再将这些建议分门别类，以提供对以下几方面情况的分析：ICANN 组织内部运营、ICANN 组织合作（特别是对合同和投诉的处理），以及 ICANN 组织如何采取措施来改善自身的 SSR 工作并帮助其他人了解如何改善他们的 SSR 工作。整个文档中的各项建议往往会相互影响，并且各项建议之间存在相互依赖关系。ICANN 组织和董事会在制定实施规划时应考虑到这一点。每项建议都获得了审核小组全体成员的一致同意。

为支持未来 SSR 审核小组提高评估效率，SSR2 审核小组努力制定符合 SMART 标准（*具体*、*可衡量*、*可分配*、*相关且可跟踪*）的建议。在许多情况下，使每项建议都完全符合 SMART 标准所需的详细信息，包括指定适当的时间表，都离不开实施团队的审慎思考和行动，因此应纳入最终实施计划中。审核小组还就如何处理未来审核轮次提出了几项建议供审议，同时认识到这些建议所涉及的问题不属于 SSR 审查本身的直接使命范围。“附录 C：流程和方法”中提供了关于 SSR2 审核小组在履行自己的使命时所遵循的流程和采用的方法的更多信息。

1. 背景

如 A.2 部分“SSR 审核目标”中所述，《ICANN 章程》要求定期评估域名系统 (DNS) 的安全、稳定与弹性。2012 年 9 月 13 日，ICANN 董事会正式收到第一轮 SSR 审核报告。五年后，于 2017 年 3 月 2 日举行的 SSR2 审核小组启动会议开始了第二轮审核工作。然而，SSR2 审核小组自成立以来遇到了一些挑战，致使审核持续时间远远超出了所有人的预期。SSR2 审核小组定期举行会议，直到 2017 年 10 月 ICANN 董事会暂停了该审核小组的活动。[3] 2018 年 6 月 19 日，小组成员重组后再次召开会议。[4]

[1] ICANN，“互联网名称与数字地址分配机构章程：第 4.6 (c) 节：特定审核：安全、稳定与弹性审核”，2019 年 11 月 28 日修订，https://www . ICANN . org/resources/pages/governance/negotiation-en/# article 4。
[2]《ICANN 章程》，第 3.1 节：https://www.icann.org/resources/pages/governance/bylaws-en/。
[3] ICANN 董事会主席史蒂夫 • 克罗克 (Stephen D. Crocker) 博士致 SSR2 审核小组的信函，2017 年 10 月 28 日，https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf。
[4] ICANN 博客“第二轮 DNS 安全、稳定和弹性审核 (SSR2) 重新启动”，2018 年 6 月 7 日，https://www.icann.org/news/announcement-2-2018-06-07-en。

在审核流程延长期间，全球唯一标识符生态系统的格局继续不断变化。新型冠状病毒肺炎 (COVID-19) 疫情导致国际商务和差旅中断，给 SSR2 审核流程带来了更多延误，尽管如此，SSR2 审核小组仍然完成了这一轮审核。在审核流程的最后一年，审核小组选择不重新开始评估其最初的建议，而是保留以前的基本建议。审核小组认为，这些建议在很大程度上仍然与 ICANN 组织息息相关，并可为全球 DNS 的安全、稳定与弹性提供有力支持。

2. SSR 审核目标

《ICANN 章程》第 4.6 (c) 节规定："*董事会应指示就 ICANN 对以下义务的履行情况展开审核（SSR 审核）：增强内外部系统和流程的运营稳定性、可靠性、弹性、安全性和全球互用性，这些系统和流程与 ICANN 负责协调的互联网唯一标识符系统之间存在着直接的相互影响关系。*"[5]

具体而言，它规定了：

"ii. 负责 SSR 审核的审核小组（即"SSR 审核小组"）可能评估的议题包括以下内容：

1. *与协调互联网唯一标识符系统有关的物理和网络方面的安全、运营稳定性和弹性事项；*
2. *是否符合互联网唯一标识符系统的适当安全应急规划框架；*
3. *对于 ICANN 协调的互联网唯一标识符系统的相应部分，是否维护了明确且全球互用的安全流程。*

iii. 此外，SSR 审核小组还将遵循 ICANN 的使命，评估 ICANN 组织成功实施其安全工作的程度，安全工作在处理 DNS 安全与稳定性的实际与潜在挑战及威胁方面的效果，以及安全工作在多大程度上足以充分而有效地应对 DNS 安全、稳定与弹性在未来所面临的挑战和威胁。

iv. SSR 审核小组也将评估此前 SSR 审核建议的实施程度，以及这些建议在实施后达到预期效果的程度。

v. 自上一轮 SSR 审核小组召开会议之日算起，执行 SSR 审核的频率不得低于每五年一次。"

3. 其他审核小组和咨询委员会的影响

根据《ICANN 章程》的规定，ICANN 组织必须与多个审核小组和咨询委员会 (AC) 合作。虽然这些小组和委员会都有各自具体的职责，但他们提出的建议可能而且确实与其他审核小组和委员会的工作领域重叠。SSR2 审核小组评估了其他审核小组和 AC 的建议，以确定他们发布的建议会对 ICANN 组织以及全球 DNS 的安全、稳定与弹性 (SSR) 造成怎样的影响。在某些情况下，SSR2 审核小组发现有必要纳入并借鉴这些建议，为 ICANN 组织制定与 SSR 相关的必要指南（详情请参阅第 E.1 节：未实现的新通用顶级域项目保护措施，以及第 E.3 节：PDP 替代方案）。SSR2 审核小组认为，建议中的这些重叠之处是对相应问题重要性的默示确证，并且还认为，在 SSR2 审核小组的建议与其他团体的建议之间达成共识，是对提出这些建议的必要性的实证支持。SSR2 建议旨在对其他审核小组的建议进行补充。

[5] 《ICANN 章程》第 4.6 (c) 节，https://www.icann.org/resources/pages/governance/bylaws-en。

B. SSR2 建议

每项建议都获得了 SSR2 审核小组全体成员的一致同意。

1. 汇总表

序号	建议	所有者	优先级
SSR2 建议 1：进一步审核 SSR1 建议			
1.1	ICANN 董事会和 ICANN 组织应进一步全面审核 SSR1 建议，并执行一项新计划来完成 SSR1 建议的实施（请参阅附录 D：与 SSR1 建议相关的审核结果）。	ICANN 董事会和 ICANN 组织	低
SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理			
2.1	ICANN 组织应在组织内部的高级管理层设立一个首席安全官 (CSO) 或首席信息安全官 (CISO) 职位，同时聘请适当的合格人员担任此职务并分配足够的具体预算助其履行自身职责。	ICANN 组织	中 - 高
2.2	ICANN 组织应在这个职位的职责说明中指出，此职务负责管理 ICANN 组织的安全职能，并监督所有可能会影响安全性的相关领域的员工互动。这一职务应负责定期向 ICANN 董事会和社群提供关于 ICANN 组织内所有 SSR 相关活动的报告。现有的安全职能部门应进行重组并调整组织架构，均向此新职务负责人汇报。	ICANN 组织	中 - 高
2.3	ICANN 组织应在这个职位的职责说明中指出，此职位负责制定安全战略和战术以及风险管理。这些职责领域包括：领导并战略性地协调组织内部安全领域的集中风险评估、业务连续性 (BC) 和灾难恢复 (DR) 计划（另请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序），包括 ICANN 管理的根服务器（IMRS，也称为 L 根），并与外部全球标识符系统所涉及的其他利益相关方协调，以及发布风险评估方法。	ICANN 组织	中 - 高
2.4	ICANN 组织应在这个职位的职责说明中指出，此职务将负责所有与安全相关的预算项目，参与 ICANN 组织进行的所有与安全相关的合同谈判（例如，注册管理机构和注册服务机构协议、硬件和软件供应链，以及相关的服务水平协议），并代表 ICANN 组织签署所有与安全相关的合同条款。	ICANN 组织	中 - 高

SSR2 建议 3：提高 SSR 相关预算的透明度			
3.1	首席安全官（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）应代表 ICANN 组织每年两次向社群简要介绍 ICANN 组织的 SSR 战略、项目和预算，同时更新并发布年度预算概述。	ICANN 组织	高
3.2	ICANN 董事会和 ICANN 组织应确保，与 ICANN 组织履行 SSR 相关职能有关的特定预算项目符合特定的 ICANN 战略规划目标和宗旨。ICANN 组织应通过连贯一致的详细年度预算和报告流程来实施这些机制。	ICANN 董事会和 ICANN 组织	高
3.3	在战略规划周期内，ICANN 董事会和 ICANN 组织应创建、发布，并征询公众对有关成本以及 SSR 相关预算的详细报告的意见和建议。	ICANN 董事会和 ICANN 组织	高
SSR2 建议 4：改进风险管理流程和程序			
4.1	ICANN 组织应继续集中统一风险管理，明确阐述其安全风险管理框架，并确保该框架在战略上符合 ICANN 组织的要求和目标。ICANN 组织应明确相关的成功衡量标准以及评估方法。	ICANN 组织	高
4.2	ICANN 组织应采用并实施 ISO 31000“风险管理”标准，并通过适当的独立审计来验证实施情况。ICANN 组织应向社群提供审计报告，可以是修订后的版本。风险管理工作应纳入 BC 和 DR 计划和程序（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）。	ICANN 组织	高
4.3	ICANN 组织应指定或任命一名专门负责安全风险管理的人员，该人员将向高级管理层安全负责人报告工作（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）。该人员应定期更新、报告安全风险记录，并指导 ICANN 组织的活动。发现的问题应纳入 BC 和 DR 计划和程序（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）以及信息安全管理系统 (ISMS)（请参阅 SSR2 建议 6：遵守适当的信息安全管理系统和安全认证规定）。	ICANN 组织	高
SSR2 建议 5：遵守适当的信息安全管理系统和安全认证规定			
5.1	ICANN 组织应实施 ISMS，并由第三方按照行业安全标准（例如 ITIL、ISO 27000 系列标准、SSAE 18）对其运营责任进行审计和认证。计划应包括获得认证的路线图和里程碑日期，并注明未来有待持续改进的目标领域。	ICANN 组织	高

5.2	在 ISMS 的基础上，ICANN 组织应根据组织内各个职位的认证和培训需求拟定计划，跟踪计划中各项认证和培训活动的完成率，阐明选择每项活动的理由，并记录各项认证如何纳入 ICANN 组织的安全与风险管理战略。	ICANN 组织	高
5.3	ICANN 组织应要求向 ICANN 组织提供服务的外部相关方遵守相关安全标准，并妥善记录对供应商和服务提供商展开的尽职调查。	ICANN 组织	高
5.4	ICANN 组织应与社群和更广泛的人群进行交流，通过清晰的报告展示 ICANN 组织在安全领域所做的工作和已取得的成就。如果这些报告能够提供信息，介绍 ICANN 组织是如何遵循最佳做法，并不断完善和持续优化用于管理风险、安全和漏洞的流程的，那么这些报告将非常有用。	ICANN 组织	高
SSR2 建议 6：SSR 漏洞披露和透明度			
6.1	ICANN 组织应积极推动签约方自愿采用 SSR 最佳做法和漏洞披露目标。如果自愿措施被证明不足以推动采用此类最佳做法和漏洞披露目标，那么 ICANN 组织应在合同、协议和谅解备忘录中列明实施最佳做法和漏洞披露目标的要求。	ICANN 组织	高
6.2	ICANN 组织应实施协调性弱点披露报告流程。关于 SSR 相关问题的披露和信息，例如任何签约方的数据外泄以及发现并向 ICANN 组织报告的关键漏洞，均应及时通知值得信赖的相关方（例如，受影响的或需要解决特定问题的相关方）。ICANN 组织应定期报告漏洞（至少每年一次），包括匿名的衡量标准并使用负责任的披露机制。	ICANN 组织	高
SSR2 建议 7：改进业务连续性和灾难恢复流程和程序			
7.1	ICANN 组织应根据 ISO 22301“业务连续性管理”制定适用于其自有或管辖的所有系统的业务连续性计划，并在计划中确定可接受的 BC 和 DR 时间表。	ICANN 组织	中 - 高
7.2	ICANN 组织应确保适用于公共技术标识符 (PTI) 运营（即，IANA 职能）的 DR 计划涵盖了可促进 DNS 安全与稳定的所有相关系统以及根区管理，且符合 ISO 27031 相关标准。ICANN 组织应与根服务器系统咨询委员会 (RSSAC) 和根服务器运营商 (RSO) 密切合作，共同制定此计划。	ICANN 组织	中 - 高
7.3	同样，ICANN 组织也应根据 ISO 27031 相关标准制定适用于其自有或管辖的所有系统的 DR 计划。	ICANN 组织	中 - 高

7.4	ICANN 组织应为 ICANN 组织自有或管辖的所有系统建立一个新的灾难恢复站点，用于替代洛杉矶或库尔佩珀站点或增加一个永久性的第三站点。ICANN 组织应将这个新站点设在北美地区和美国领土之外的其他地方。如果 ICANN 组织选择替换其中一个现有站点，无论替换哪一个，ICANN 组织都应先确认新站点可以完全运行并且能够为 ICANN 组织处理这些系统的灾难恢复，然后再关闭要被替换的现有站点。	ICANN 组织	中 - 高
7.5	ICANN 组织应发布一份总体 BC 和 DR 计划和程序的摘要。这样做可以提高透明度和可信度，而不仅仅只是解决符合 ICANN 组织的战略目标和宗旨的问题。ICANN 组织应聘请外部审计人员来验证这些 BC 和 DR 计划是否合规。	ICANN 组织	中 - 高
SSR2 建议 8：在与签约方的谈判中维护并展现公共利益			
8.1	ICANN 组织应委托一个谈判小组（由不附属于签约方或不是由签约方聘请的滥用和安全领域专家组成）来代表非签约实体的利益，并与 ICANN 组织合作，双方本着诚信、公开透明的原则重新谈判签约方合同，主要目标是提高 DNS 的安全、稳定与弹性 (SSR) 以维护最终用户、企业和政府的利益。	ICANN 组织	中
SSR2 建议 9：监督并强制实施合规			
9.1	ICANN 董事会应指示合规团队监督并严格要求签约方遵守合同、基本协议、临时规范以及社群政策中关于现有和未来 SSR 以及滥用相关的义务。	ICANN 董事会	高
9.2	ICANN 组织应主动监督并强制要求注册管理机构和注册服务机构履行合同义务，以提高注册数据的准确性。这种监督和强制实施应包括验证地址字段，以及定期审核注册数据的准确性。ICANN 组织的强制合规工作应重点关注那些因提供不准确数据而每年受到向 ICANN 组织投诉或报告超过 50 起的注册服务机构和注册管理机构。	ICANN 组织	高
9.3	ICANN 组织应至少每年请外部人员对合规活动进行审计，并公布审计报告和 ICANN 组织对审计建议的回复，包括实施规划。	ICANN 组织	高
9.4	ICANN 组织应责成合规职能部门发布定期报告，列举他们缺少的工具，他们需要这些工具来支持 ICANN 组织作为一个整体，有效地利用合同杠杆来应对 DNS 中的安全威胁，包括需要更改合同条款的措施。	ICANN 组织	高

SSR2 建议 10：明确滥用相关术语的定义			
10.1	ICANN 组织应发布一个网页，明确 DNS 滥用的有效定义，即，适用的项目、文档和合同。定义应明确指出 ICANN 组织目前认为在其职权范围内通过合同和合规机制可以解决的安全威胁类型，以及 ICANN 组织认为属于其职权范围之外的安全威胁类型。如果 ICANN 组织使用其他类似术语（例如，安全威胁、恶意行为），那么 ICANN 组织应同时指明这些术语的有效定义，以及 ICANN 组织如何将这些术语与 DNS 滥用区分开。本页面应包含具体链接，指向与签约方签订的合同中各项与滥用相关的现有义务的摘要，包括应对滥用的相关程序和协议。ICANN 组织应每年更新此页面，注明最新版本的日期，并链接到具有相关发布日期的旧版本。	ICANN 组织	高
10.2	组建一个由员工提供支持的跨社群工作组 (CCWG)，负责确立一个流程来不断完善阻止 DNS 滥用的定义，至少每两年一次按照可预测的时间表（例如，隔年的一月份）更新一次 DNS 滥用的定义，在 30 个工作日内完成此流程。跨社群工作组应包括来自消费者保护、运营网络安全、学术界或独立网络安全研究机构、执法机构，以及电子商务领域的利益相关方。	ICANN 组织	高
10.3	ICANN 董事会和 ICANN 组织应在公共文档、合同、审核小组实施规划以及其他活动中一致地使用共识定义，并在出现此类使用情况时参考本网页。	ICANN 组织	高
SSR2 建议 11：解决 CZDS 数据访问问题			
11.1	ICANN 社群和 ICANN 组织应采取措施，以确保请求人员能够及时访问集中化域资料服务 (CZDS) 数据，不会遭受不必要的障碍，例如没有自动续订访问凭证。	ICANN 社群和 ICANN 组织	中
SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核			
12.1	ICANN 组织应创建一个由独立专家（即，没有财务利益冲突的专家）组成的 DNS 滥用分析咨询小组，对 DNS 滥用报告活动提出全面改进建议，将可操作的数据、验证、透明度和独立的可重复性分析作为最高优先级事项。	ICANN 组织	中
12.2	ICANN 组织应与数据提供商达成协议，允许进一步共享非商业用途的数据，特别是用于验证或需要进行同行评审的科学研究。这种特殊的免费非商业数据使用许可，可能会存在时间上的滞后，以免影响数据提供商的商业收入机会。ICANN 组织应在 ICANN 网站上发布所有数	ICANN 组织	中

	据共享合同条款。ICANN 组织应终止任何不允许对拦截清单背后的方法进行独立验证的合同。		
12.3	ICANN 组织应发布报告，揭示其域名最易造成滥用的注册管理机构和注册服务机构。ICANN 组织发布的报告不仅应包含当前报告中的图形数据，还应包含机读格式的数据。	ICANN 组织	中
12.4	ICANN 组织应整理并发布注册管理机构和注册服务机构采取的措施报告，包括自愿行动和履行法律义务的做法，以便根据与使用 DNS 相关的适用法律对非法和/或恶意行为的投诉做出回应。	ICANN 组织	中
SSR2 建议 13：提高滥用投诉报告的透明度和问责制			
13.1	ICANN 组织应构建并维护用于集中管理 DNS 滥用投诉的门户，该门户可将每份滥用报告自动分发给相关方。它将纯粹作为一个信息流入系统，ICANN 组织只收集和处理摘要和元数据，包括时间戳和投诉类型（分类）。所有通用顶级域 (gTLD) 都必须使用该系统；每个国家和地区顶级域 (ccTLD) 自愿参与。此外，ICANN 组织还应与所有 ccTLD 共享滥用报告（例如，通过电子邮件）。	ICANN 组织	高
13.2	ICANN 组织应以允许独立第三方分析关于 DNS 投诉类型的形式发布其收到的投诉数量。	ICANN 组织	高
SSR2 建议 14：制定临时规范，提高基于证据的安全性			
14.1	ICANN 组织应制定临时规范，要求所有签约方将已修订的 DNS 滥用报告中确定为滥用的域名所占百分比保持在合理范围和已发布的阈值之下（请参阅 SSR2 建议 13.1）。	ICANN 组织	高
14.2	为促进反滥用行动，ICANN 组织应根据关于独立审核域名数据和拦截清单方法的 SSR2 建议 12.2，向签约方提供其域名组合中被认定为滥用的域名列表。	ICANN 组织	高
14.3	如果与滥用活动相关的域名数量达到 SSR2 建议 14.1 中所述的已发布阈值，ICANN 组织应展开调查以确认数据和分析的准确性，然后向相关方发出通知。	ICANN 组织	高
14.4	ICANN 组织应给签约方 30 天时间，供对方将滥用域名的比例降低到阈值以下或证明 ICANN 组织的结论或数据存在问题。如果签约方在 60 天内未能纠正错误，ICANN 合同合规部应开始取消认证流程。	ICANN 组织	高

14.5	ICANN 组织应考虑提供财务激励措施：域名组合中滥用域名比例低于特定百分比的签约方，将有机会获得适当程度减免应付交易费用的奖励。	ICANN 组织	高
SSR2 建议 15：启动 EPDP 以提高基于证据的安全性			
15.1	制定临时规范后（请参阅 SSR2 建议 14：制定临时规范，提高基于证据的安全性），ICANN 组织应建立由员工提供支持的快速政策制定流程 (EPDP) 以制定反滥用政策。EPDP 志愿者应代表 ICANN 社群，使用 gTLD 注册数据临时规范 EPDP 团队章程中的号码和分配作为模板。	ICANN 组织	高
15.2	EPDP 应参考 SSR2 建议 10.2 中拟议的 CCWG 基本定义。该政策框架应明确定义针对不同类型的滥用行为的适当对策和补救措施，签约方采取措施的时间框架（例如滥用报告/响应报告时间表），以及在出现违反政策的情况下，ICANN 合同合规部可采取的强制措施。如果任何签约方有包庇滥用行为的方式和做法，ICANN 组织应坚持要求终止合同。结果应包括建立一个机制，每两年对滥用相关的基准和合同义务更新一次，通过一个不超过 45 个工作日的流程来完成这项工作。	ICANN 组织	高
SSR2 建议 16：隐私要求和 RDS			
16.1	ICANN 组织应在其网站上提供一致的交叉引用，以提供关于隐私和数据管理主题的所有举措（过去、现在和计划中）的一致且易于查找的信息，特别是注册目录服务 (RDS) 相关信息。	ICANN 组织	中
16.2	ICANN 组织应在合同合规职能部门内建立专门小组，负责深入了解隐私要求和原则（例如，收集限制、数据资格、目的规范以及数据披露的安全保护措施），并在 RDS 框架下促进执法需求，因为社群已修订和批准了该框架（另请参阅 SSR2 建议 11：解决 CZDS 数据访问问题）。	ICANN 组织	中
16.3	ICANN 组织应定期审计注册服务机构隐私政策履行情况，确保注册服务机构制定了用于处理侵犯隐私行为的流程。	ICANN 组织	中
SSR2 建议 17：衡量域名冲突			
17.1	ICANN 组织应制定框架，总结各类域名冲突的性质和发生频率以及所产生的问题。该框架应包括具体衡量标准和若干机制，用于衡量控制性中断在多大程度上可成功识别并消除域名冲突。可通过启用受保护的域名冲突披露实例这一机制来提供支持。此框架应允许适当处理敏感数据和安全威胁。	ICANN 组织	中

17.2	ICANN 社群应制定一项明确的政策，用于避免和处理与新 gTLD 相关的域名冲突，并在下一轮 gTLD 相关工作启动之前实施该政策。ICANN 组织应确保由与 gTLD 扩展没有财务利益关系的相关方来评估该政策。	ICANN 社群和 ICANN 组织	中
SSR2 建议 18：为政策辩论提供信息			
18.1	ICANN 组织应跟踪同行评审研究社群中的进展，主要应当关注网络和安全研究会议，其中至少包括 ACM CCS、ACM Internet Measurement Conference（ACM 互联网衡量标准会议）、Usenix Security（Usenix 安全）、CCR、SIGCOMM、IEEE 安全与隐私讨论会、运营安全会议，以及事故响应和安全团队论坛 (FIRST)，并发布一份概述报告以总结与 ICANN 组织或签约方行为有关的出版物的结论，供 ICANN 社群参阅。	ICANN 组织	低
18.2	ICANN 组织应确保此类报告中包含可能与可行措施建议相关的观察结果（包括针对与注册管理机构和注册服务机构签署的合同进行的更改），这些措施应有助于缓解、预防或纠正同行评审文献中指出的消费者和基础架构所遭受的 SSR 损害。	ICANN 组织	低
18.3	ICANN 组织应确保这些报告中还包含开展其他研究的建议，以确认经过同行评审的研究结果，其中应介绍社群需要哪些数据才能开展其他研究，以及 ICANN 组织如何为代理提供协助以通过 CZDS 来访问此类数据。	ICANN 组织	低
SSR2 建议 19：完成 DNS 回归测试套件的开发工作			
19.1	ICANN 组织应完成 DNS 解析程序行为测试套件的开发工作。	ICANN 组织	低
19.2	ICANN 组织应确保实施并维护这项继续针对不同配置和软件版本进行功能测试的性能。	ICANN 组织	低
SSR2 建议 20：用于指导密钥轮转的正式程序			
20.1	ICANN 组织应通过正式流程建模工具和建模语言的支持，制定所需的正式流程，以详细说明后续密钥轮转的细节，包括决策点、例外路径、完整的控制流等等。对密钥轮转流程进行验证时，应发布编程过程（例如程序、有限状态机 (FSM)）以征询公众意见，并且 ICANN 组织应收集社群反馈意见。该流程的每个阶段都应具有凭借经验可验证的验收标准，只有达到这些标准，流程才能正常运行。该流程应接受反复评估，评估频率通常不应低于轮转本身的频率（即，相同的频率），以便	ICANN 组织	中

	ICANN 组织能够及时运用已吸取的经验教训对流程进行调整。		
20.2	ICANN 组织应组建一个由来自 ICANN 组织或社群的相关人员构成的利益相关方小组，该小组定期依照根区密钥签名密钥 (KSK) 轮转流程运行桌面演练。	ICANN 组织	中
SSR2 建议 21：提高与 TLD 运营商的通信安全性			
21.1	ICANN 组织和 PTI 运营部门应加快实施新的根区管理系统 (RZMS) 关于针对请求的更改进行身份认证和授权的安全措施，并为 TLD 运营商提供利用这些安全措施的机会，特别是 MFA 和加密电子邮件。	ICANN 组织和 PTI	中
SSR2 建议 22：服务衡量标准			
22.1	对于 ICANN 组织权威管辖的每项服务（包括根区服务、gTLD 相关服务以及 IANA 注册管理机构），ICANN 组织应创建一个统计信息和衡量标准列表来反映该项服务的运营状态（例如，可用性以及响应性），并在 icann.org 网站的单个页面上，例如，Open Data Platform（开放数据平台）下发布这些服务、数据集和衡量标准的目录。ICANN 组织应对这些服务中的每一项进行衡量，作为去年和纵向总结（以阐释基准行为）。	ICANN 组织	低
22.2	ICANN 组织应每年征询社群对这些衡量标准的反馈意见。在每次报告发布后，应审议并公开总结相关反馈，并纳入后续报告。用于衡量这些报告结果的数据和相关方法应妥善存档，并公开发布以促进重复利用。	ICANN 组织	低
SSR2 建议 23：算法轮转			
23.1	PTI 运营部门应更新 DNSSEC 实践声明 (DPS)，以允许从一种数字签名算法过渡到另一种数字签名算法，包括预期的从 RSA 数字签名算法过渡到其他算法或未来的后量子算法，这些算法可提供同等或更高的安全性，并且可保持或增强 DNS 的弹性。	PTI	中
23.2	鉴于根区 DNSKEY 算法轮换是一个非常复杂且敏感的流程，PTI 运营部门应与其他根区合作伙伴和全球范围内的社群合作，根据从 2018 年第一次根区 KSK 轮转汲取的经验教训，共同制定用于指导今后根区 DNSKEY 算法轮换的计划。	PTI	中

SSR2 建议 24：提高 EBERO 流程的透明度和改进端到端测试			
24.1	ICANN 组织应使用测试计划按预定时间间隔（至少每年一次）协调整个 EBERO 流程的端到端测试，测试计划包括用于测试的数据集、进展状态以及截止日期，同时应提前与 ICANN 签约方协调，以确保所有例外条款得到执行并公布测试结果。	ICANN 组织	中
24.2	ICANN 组织应在 EBERO 网站上提供链接，以便用户更容易找到《共同过渡流程手册》。	ICANN 组织	中

2. 优先顺序

SSR2 审核小组已根据《ICANN 2021-2025 财年战略规划》及其目标和宗旨调整了所有 SSR2 建议。[6]审核小组删除了本报告中与战略规划明显不一致的建议。SSR2 审核小组提出的所有建议均符合 ICANN 组织的战略规划，因此这些建议都非常重要。

SSR2 审核小组使用了一款在线调查工具（基于互联网的解决方案 Qualtrics），供所有小组成员就本报告中每组建议的优先级发表意见。[7]这项调查允许按五个等级（非常低优先级、低优先级、中等优先级、高优先级，以及非常高优先级）对每组建议的优先级进行排名。

审核小组认为，这 24 组建议中有 27 项具体建议应被视为高优先级建议，其中大部分建议涉及 ICANN 组织的内部安全管理和反滥用举措。9 项建议为中高优先级。18 项建议（主要来自全球 DNS 部门）为中等优先级，其余 8 项建议为较低优先级。

[6] 请参阅附录 G：了解 SSR2 建议与《ICANN 2021-2025 财年战略规划》和《ICANN 章程》的关系。
[7] 请参阅 https://www.qualtrics.com/。

C. SSR1 实施与预期效果

2012 年，ICANN 董事会认为*“[SSR1] 最终报告中的 28 项建议可行且可实施”*，于是一致采纳并指示员工实施所有 28 项 SSR1 建议。[8] SSR2 审核小组的其中一项任务是评估*“此前 SSR 审核建议的实施情况，以及这些建议在实施后达到了怎样的预期效果”*。

“附录 C：流程和方法”中总结了 SSR2 审核小组在评估实施情况与预期效果时所采用的流程和方法。这部分概述了评估流程、证据类型和使用的数据，以及得出建议实施情况的结论所采用的方法。“附录 D：与 SSR1 建议相关的审核结果”中介绍了 SSR2 审核小组针对每项 SSR1 建议的结论和支持理由。

每一轮审核都是一个学习机会，SSR2 审核小组在评估了 SSR1 建议后，指出了提供基于可量化绩效指标的建议的重要性和必要性，SSR1 建议中经常缺乏可量化的绩效指标。这个结论的基础是需要确保未来审核小组的各项建议能够得到有效实施和评估。

[8] ICANN，“ICANN 董事会例行会议”，上次更新日期是 2012 年 10 月 18 日，https://www.icann.org/resources/board-material/minutes-2012-10-18-en 以及“DNS 安全、稳定和弹性审核小组最终报告”，SSR 审核小组，2012 年 6 月 20 日，https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf。

摘要：SSR1 审核

SSR2 审核小组审核了所有 28 项 SSR1 建议，认为截至本报告发布之日，这 28 项建议仍然十分重要（请参阅表 2）。[9] 审核小组认为，各项建议均未充分实施，具体原因请参阅附录 D：与 SSR1 建议相关的审核结果。

表 2：SSR1 建议概述

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
相关性	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
已实施	P	P	P	P	P	N	P	P	-	P	P	P	N	N	P	P	-	N	-	P	P	P	P	P	P	P	P	P
有效性	N	N	N	Y	-	N	N	N	-	N	-	N	N	N	-	N	-	-	N	N	N	N	-	N	N	-	N	N

含义： Y = 是　　N = 否　　P = 部分　　- = 无法确定

SSR2 审核小组指出了以下再次出现的问题：

1. SSR1 建议中通常缺乏指标、衡量结果和目标点，还缺少可让社群和 ICANN 组织跟踪并了解安全领域以及他们自己的活动的相关实施计划。

2. 缺少公开可用的证据、定义和程序，阻碍了对 SSR 活动的独立观察。缺少相关信息导致无法清晰了解 ICANN 组织是否实施了 SSR1 建议，也无法了解 ICANN 组织实施 SSR1 建议的方式。

3. 缺少针对各种实施规划的社群审核和问责制，导致 ICANN 社群没有机会提供关于 SSR 问题的意见和建议。

4. ICANN 组织目前没有一个总体战略、可确定的目标或明确而全面的 SSR 政策。缺乏有效运行的 SSR 战略和综合性安全与风险管理机制（例如，政策、程序、标准、基准和指南），造成无法分配、衡量和跟踪 SSR 相关责任，进而导致 ICANN 组织的 SSR 相关责任缺乏透明度、问责制并且差距明显。

[9] ICANN，SSR 审核实施报告，2015 年 6 月，https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf。

SSR2 审核小组认识到，SSR1 审核小组提供的原始指南并不是在所有情况下都可以充分衡量；另一方面，尽管 ICANN 组织指出他们认为所有建议都已得到实施，但是这些建议的实施计划通常不清不楚且无法充分衡量。因此，SSR2 审核小组无法认为 SSR1 建议已完成实施。考虑到 SSR2 审核小组提供的审核结果，ICANN 组织应进一步全面审核 SSR1 建议的实施情况。

此外，这份报告还提供了超出 SSR2 直接审核范围的推荐（请参阅附录 A - 更多推荐），以便未来审核小组避免 SSR2 审核小组遇到的一些挑战。

SSR2 建议 1：进一步审核 SSR1 建议

1.1. ICANN 董事会和 ICANN 组织应进一步全面审核 SSR1 建议，并执行一项新计划来完成 SSR1 建议的实施（请参阅附录 D：与 SSR1 建议相关的审核结果）。

D. ICANN 内部的重要稳定性问题

这部分重点关注与《ICANN 章程》第 4.6(c) (ii) A 节、第 4.6(c) (ii) B 节和第 4.6(c) (iii) 节相关的领域。[10]这些领域包括：与互联网唯一标识符系统的协调有关的物理和网络运营的安全、稳定和弹性问题；互联网唯一标识符系统的安全应急规划框架；以及 ICANN 组织的内部安全流程和 ICANN 安全框架的完整性与有效性。

导致提出这部分建议的根本问题是，SSR2 审核小组没有找到证据能够证明 ICANN 组织拥有一份高效、全面且透明的 SSR 计划。小组在审核 ICANN 组织的内部安全性期间，很明显地发现 ICANN 组织执行了各种与安全性相关的计划和措施。但是，审核小组没有发现充足的全面证据，无法证明 ICANN 组织适当管理且妥善记录了信息管理和安全计划（请参阅第 B.3 部分，风险与安全管理），无法证明 ICANN 组织制定了业务连续性计划和灾难恢复流程（请参阅第 D.4 部分，业务连续性管理），也无法证明 ICANN 组织拥有一个适宜的基本独立的安全架构，可为互联网运行至关重要的系统提供支持（请参阅第 D.1 部分，优化组织结构）。

根据《ICANN 章程》的规定，ICANN 组织必须“*运作上秉承公开和透明的原则实现最大程度的可行性，并遵守那些为确保公正性而设计的程序*”。[11]提供这部分建议是为了帮助 ICANN 组织在考虑到安全目标的情况下，最大程度地改善组织各个方面的 SSR 问题披露并提高透明度。通过实施这些建议，ICANN 组织将能够有效地解决信息透明度，以及缺乏清晰明确的安全领导层和组织的基本问题。

[10]请参阅本报告中与 SSR2 建议最相关的“附录 H - 章程与战略规划”部分，了解与 SSR 最相关的《ICANN 章程》和《2021-2025 财年战略规划》部分内容。

[11] 《ICANN 章程》第 3.1 节，https://www.icann.org/resources/pages/governance/bylaws-en/#article3

1. 优化组织结构 - 安全性高级管理层职位

目前，ICANN 组织将 SSR 相关活动划分到整个组织。SSR2 审核小组认识到，首席技术官办公室 (OCTO) 的职责包括但不仅限于：

研究与互联网唯一标识符系统有关的问题（域名、IP 地址/AS 编号、协议参数等）

为提升这些标识符的安全、稳定与弹性提供支持。[12]

首席信息官通常负责*“监控并维护 ICANN 系统和技术运营、企业安全和信息技术，ICANN DNS 工程团队 (http://www.dns.icann.org/) 负责管理 L 根和 ICANN 的 DNS 网络服务”*[13]，还负责保护、监控和管理数据资产，包括签约方的私有数据。

ICANN 组织应设立一个高级管理层职位，全面负责所有安全相关事宜，包括制定战略目标、管理监管合规和预算，以及保护组织的资产安全。[14]

此职位负责管理《ICANN 章程》中的一些规定，以及《2021-2025 财年战略规划》中的承诺。此外，SSR1 建议 24 也呼吁组建一个首席安全办公室团队。[15]当前的组织结构将这些职责分配给了 ICANN 组织中的两个独立部门。集中管理通过将工作整合由一个职位统一领导并提供适当的预算，可以更有效地推动所有相关活动的战略调整。[16]这将为社群和未来审核小组制定连贯一致的文档提供有力支持。

SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理

SSR2 审核小组认为，ICANN 组织有必要设立一个高级管理层职位，负责协调并战略性地管理 ICANN 组织的安全和安全风险活动，同时负责履行 ICANN 组织的使命并实现战略安全目标。[17]

[12] ICANN 首席技术官办公室 (OCTO)，访问时间 2019 年 12 月 27 日，https://www.icann.org/octo。
[13] ICANN “信息系统与创新”，访问时间 2020 年 1 月 21 日，https://www.icann.org/resources/pages/technical-functions-cio。
[14] 教育科学研究所 (IES)：国家教育统计中心，“第 3 章 - 安全政策：制定与实施”，访问时间 2020 年 12 月 9 日，https://nces.ed.gov/pubs98/safetech/chapter3.asp。
[15] 请参阅附录 D：与 SSR1 建议相关的审核结果。
[16] 请参阅国际标准化组织中第 5.1 条的标准，以及 ISO 27001、ISO/IEC 27001:2013 系列标准中的“信息技术 - 安全技术 - 信息安全管理系统 - 要求”，这与 SSAE18 2017 信托服务标准 CC1.3/COSO 原则 3 的要求也是一致的，https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/othermapping/trust-services-map-to-iso-27001.xlsx。
[17] ICANN 董事会可以参考各种资源，例如，《网络安全风险手册：全国公司董事协会》，“关于网络风险监督的 NACD 董事手册”，2017 年，http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html。

2.1. ICANN 组织应在组织内部的高级管理层设立一个首席安全官 (CSO) 或首席信息安全官 (CISO) 职位，同时聘请适当的合格人员担任此职务并分配足够的具体预算助其履行自身职责。

2.2. ICANN 组织应在这个职位的职责说明中指出，此职务负责管理 ICANN 组织的安全职能，并监督所有可能会影响安全性的相关领域的员工互动。这一职务应负责定期向 ICANN 董事会和社群提供关于 ICANN 组织内所有 SSR 相关活动的报告。现有的安全职能部门应进行重组并调整组织架构，均向此新职务负责人汇报。

2.3. ICANN 组织应在这个职位的职责说明中指出，此职位负责制定安全战略和战术以及风险管理。这些职责领域包括：领导并战略性地协调组织内部安全领域的集中风险评估、业务连续性 (BC) 和灾难恢复 (DR) 计划（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序），包括 ICANN 管理的根服务器（IMRS，也称为 L 根），并与外部全球标识符系统所涉及的其他利益相关方协调，以及发布风险评估方法。

2.4. ICANN 组织应在这个职位的职责说明中指出，此职务将负责所有与安全相关的预算项目，参与 ICANN 组织进行的所有与安全相关的合同谈判（例如，注册管理机构和注册服务机构协议、硬件和软件供应链，以及相关的服务水平协议），并代表 ICANN 组织签署所有与安全相关的合同条款。

当 ICANN 组织按照这些建议所述，设立首席安全官职位且聘请适当的合格人员担任此职务来履行相应的职责时，可以认为已实施这项建议。

当 ICANN 组织集中安全责任使 ICANN 组织可以明确地协调 SSR 活动和预算，且能够在适当的管理层讨论安全问题时，可以认为这项建议有效。

2. SSR 相关预算和报告

尽管 ICANN 组织可能在其年度预算内完成各个项目下的 SSR 相关活动，但目前尚不清楚 ICANN 组织如何将资金分配给 SSR 相关的特定职能部门。这部分 SSR2 报告审核了与 SSR 预算和报告相关的 SSR1 建议的目的和可发现且可量化的结果。

SSR1 建议 20、21 和 22 都提到了 SSR 相关预算项目需要更细化和更透明的预算和报告流程。例如，SSR1 建议 20 提出需要提高对 SSR 相关预算项目的审核和公共评议的精细化程度，并开展定期审核。[18] [19] SSR1 建议 21 指出，ICANN 组织应制定更有条理的内部流程，以展现组织和预算决策如何与 IS-SSR 框架（包括基础的成本效益分析在内）息息相关。SSR1 建议 22 则提议，随着新通用顶级域 (NgTLD) 的引入，ICANN 组织应发布、监管并更新关于管理 SSR 问题所需组织资源和预算资源的文档。

SSR2 审核小组仔细查看公开发布的文档、ICANN 组织向审核小组提供的文档和 SSR1 实施报告，以及收到的关于发送给 ICANN 组织工作人员的许多问题的答案，评估了 ICANN 组织实施这些建议的情况。[20] 除了员工提供的与 SSR1 相关的详细信息（导致制定了 SSR1 建议 20、21 和 22 这些初步建议）之外，ICANN 组织没有向 SSR2 审核小组提供任何其他信息。审核小组发现，尽管通过 IS-SSR 框架文件和年度报告确实提供了 SSR 相关活动的年度报告，但与 SSR 预算事项有关的大多数信息级别过高，与 SSR1 审核小组提出的建议不符。ICANN 组织的年度预算没有提供关于 SSR 相关活动的详细信息，也不再制定 IS-SSR 框架文件。[21]

专门查看了 ICANN 组织的新通用顶级域项目，新项目的结构和预算反映了与新通用顶级域项目相关的高层次 SSR 问题（例如，域名系统 (DNS) 稳定性专家组和域名注册管理后端应急运行机构 (EBERO)）。[22] 但是，ICANN 组织未能实现预期结果，例如，未提供更详细的数据，未提高关于实施 IS-SSR 框架和履行与新通用顶级域项目相关 SSR 职能的组织和预算信息的清晰度。值得注意的是，ICANN 标识符系统安全、稳定和弹性 (IS-SSR) 文档存档中没有任何特定于新通用顶级域项目的文档。[23] 在仔细查看 2016 年 IS-SSR 框架文档和年度报告后，发现两次提到了 gTLD，一次是在模块 A 中提到 gTLD 是互联网生态系统的趋势，另一次是在模块 B 中提到 gTLD 是 ICANN 总体战略规划的一部分。[24] 在 2013 年 3 月发布的一份以前的框架文档中，ICANN 组织提出新通用顶级域项目是一种“趋势”，是推动通用名称支持组织 (GNSO) 制定政策的驱动因素。[25] 其他唯一提到新通用顶级域项目的情况是在关于 SSR1 建议实施情况的报告章节中。尽管 ICANN 组织发布了一份年度报告，其中包含共享资源的直接成本和分配给负责处理

[18] 请参阅附录 D - SSR1 建议 20 和 SSR1 建议 22，详细了解 SSR2 审核小组针对这些建议的审核结果和结论。
[19] ICANN，“2015 - 2016 财年标识符系统安全、稳定与弹性框架”，2016 年 9 月 15 日，https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf。
[20] ICANN SSR2 审核小组维基页面，背景资料，访问时间 2020 年 12 月 10 日，https://community.icann.org/display/SSR/Background+Materials。
[21] ICANN“ICANN 最新财务信息（2020 - 2021 财年）”，未注明发布日期，https://www.icann.org/resources/pages/governance/current-en，以及 ICANN“IS-SSR 文档存档”，未注明发布日期，https://www.icann.org/ssr-document-archive。注：ICANN 预算没有报告任何与 SSR 相关的特定支出。“IS-SSR 文档存档”没有显示任何 2015 - 2016 财年之后的 IS-SSR 框架文档。
[22] ICANN“已批准的互联网名称与数字地址分配机构 (ICANN) 2021 财年预算”，2020 年 5 月 7 日，第 26-28 页，https://www.icann.org/en/system/files/files/adopted-budget-fy21-07may20-en.pdf。
[23] IS-SSR 文档存档，https://www.icann.org/ssr-document-archive
[24] ICANN 2015 - 2016 财年 IS-SSR 框架，https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf。
[25] ICANN 安全、稳定和弹性框架，2013 年 3 月，第 8 页，https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf。

SSR 问题的支持职能部门的成本，但该报告没有提供关于新通用顶级域项目的资金、资源或其他活动的明细。[26]

概括来说，审核小组在这方面的关切就是，尽管 ICANN 组织可能在其年度预算内的各个项目下涵盖了 SSR 相关活动，但是目前尚不清楚 ICANN 组织如何将资金分配给 SSR 相关的特定职能部门。审核小组无法找到任何证据证明 ICANN 组织提供了任何关于 SSR 事件的预算和相关资源影响的报告；如果存在这些材料，目前尚未提供。

SSR2 建议 3：提高 SSR 相关预算的透明度

3.1. 首席安全官（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）应代表 ICANN 组织每年两次向社群简要介绍 ICANN 组织的 SSR 战略、项目和预算，同时更新并发布年度预算概述。

3.2. ICANN 董事会和 ICANN 组织应确保，与 ICANN 组织履行 SSR 相关职能有关的特定预算项目符合特定的 ICANN 战略规划目标和宗旨。ICANN 组织应通过连贯一致的详细年度预算和报告流程来实施这些机制。

3.3. 在战略规划周期内，ICANN 董事会和 ICANN 组织应创建、发布，并征询公众对有关成本以及 SSR 相关预算的详细报告的意见和建议。

当 ICANN 组织将所有相关职能和预算项目划归到新设立的高级管理层职位负责范围内时，可以认为已实施这项建议。

当 ICANN 社群能够清晰明确地了解 SSR 相关预算时，可以认为这项建议有效。

3. 风险和安全管理

安全风险管理是一个持续过程，让组织能够识别安全风险并实施缓解风险的相关安全战略。审核小组发现，尽管 ICANN 组织在安全风险管理领域启动了全面且适当的活动，促成 DNS 风险管理框架工作组编写了相关报告和 2015 - 2016 财年 IS-SSR 框架文档，但是这些活动的成果没有持续更新。[27] 缺乏行动使得安全风险管理工作的成熟程度，尤其是流程的可重复性和定义很成问题。

[26] ICANN 2018 财年 SSR 相关活动运营规划，未注明发布日期，https://community.icann.org/x/DqNYAw。
[27] ICANN“DNS 风险管理框架报告”，DNS 风险管理框架工作组，上次修订时间是 2013 年 10 月 4 日，https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en 以及 ICANN 2015 - 2016 财年 IS-SSR 框架文档。

由于缺乏最新的文档，审核小组无法找到证据来证明 ICANN 组织遵守行业标准和最佳做法。[28]缺乏的文档中包括一份关键的第三方针对 ICANN 组织的方法和实施情况的审核文档。相比之下，审核小组注意到，各签约方和 ccTLD 均遵守相关安全和行业标准，表明这些标准适用于 DNS 领域的问题。[29] 最终，审核小组无法确定 ICANN 组织在安全风险管理方面所做的工作是否充分。

由于缺乏最新的公开发布的可用信息，社群成员和其他相关方（例如，政府和注册人）也无法评估 ICANN 组织的工作。信息缺乏导致透明度不足，进而会影响 ICANN 组织的核心价值，以及全球社群对 ICANN 组织和 DNS 生态系统的信任。适当的风险和安全管理离不开清晰的流程，这些流程应遵循国际标准和最佳做法指南，同时也离不开清晰且公众可访问的岗位职责和组织架构。如果根据大众认可的标准执行第三方审核，并发布公众可访问的审核报告，那么将会提供一种不同的视角，确认相关措施是适当的，且会增进社群与 ICANN 组织之间的信任。设立并维护安全管理架构和程序，将有助于 ICANN 组织更全面地维持其安全立场，不受单独的员工和成员的影响。

SSR2 审核小组敏锐地意识到，过度共享某些运营信息可能会带来问题，尤其是安全方面的问题。但是，ICANN 组织管理着具有全球影响力的关键系统，应向社群提供安全相关信息及相关数据。高级管理层职位应负责监管披露流程（风险、安全与漏洞），包括确定暂时停止时间和公开披露（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）。

SSR2 建议 4：改进风险管理流程和程序

4.1. ICANN 组织应继续集中统一风险管理，明确阐述其安全风险管理框架，并确保该框架在战略上符合 ICANN 组织的要求和目标。ICANN 组织应明确相关的成功衡量标准以及评估方法。

4.2. ICANN 组织应采用并实施 ISO 31000“风险管理”标准，并通过适当的独立审计来验证实施情况。[30]ICANN 组织应向社群提供审计报告，可以是修订后的版本。风险管理工作应纳入 BC 和 DR 计划和程序（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）。

[28] 请参阅 SSR2 建议 5：遵守适当的信息安全管理系统和安全认证规定，SSR2 建议 6：SSR 漏洞披露和透明度，以及 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序。
[29] 根据 ISO/IEC 27001:2013 和/或 ISO 22301:2012 通过认证的各种 ccTLD 示例：DENIC https://www.denic.de/en/content-pool/information-security-master/、IIS https://internetstiftelsen.se/docs/27001-eng-Certificate.pdf、nic.at https://www.nic.at/en/the-company/certificates-and-awards 和 Nominet https://www.nominet.uk/security-at-nominet/。
[30] 国际标准化组织，*ISO 31000 风险管理*，https://www.iso.org/iso-31000-risk-management.html。

4.3. ICANN 组织应指定或任命一名专门负责安全风险管理的人员，该人员将向高级管理层安全负责人报告工作（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）。该人员应定期更新、报告安全风险记录，并指导 ICANN 组织的活动。发现的问题应纳入 BC 和 DR 计划和程序（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）以及信息安全管理系统 (ISMS)（请参阅 SSR2 建议 5：遵守适当的信息安全管理系统和安全认证规定）。

当 ICANN 组织按照国际标准（例如，ISO 31000）充分记录了风险管理流程，并且 ICANN 组织为这个计划制定了一个定期审核周期（包括发布审核摘要报告）时，可以认为已实施这项建议。

当 ICANN 组织制定了清晰记录的强大风险管理计划时，可以认为这项建议有效。

SSR2 建议 5：遵守适当的信息安全管理系统和安全认证规定

5.1. ICANN 组织应实施 ISMS，并由第三方按照行业安全标准（例如 ITIL、ISO 27000 系列标准、SSAE 18）对其运营责任进行审计和认证。计划应包括获得认证的路线图和里程碑日期，并注明未来有待持续改进的目标领域。

5.2. 在 ISMS 的基础上，ICANN 组织应根据组织内各个职位的认证和培训需求拟定计划，跟踪计划中各项认证和培训活动的完成率，阐明选择每项活动的理由，并记录各项认证如何纳入 ICANN 组织的安全与风险管理战略。

5.3. ICANN 组织应要求向 ICANN 组织提供服务的外部相关方遵守相关安全标准，并妥善记录对供应商和服务提供商展开的尽职调查。

5.4. ICANN 组织应与社群和更广泛的人群进行交流，通过清晰的报告展示 ICANN 组织在安全领域所做的工作和已取得的成就。如果这些报告能够提供信息，介绍 ICANN 组织是如何遵循最佳做法，并不断完善和持续优化用于管理风险、安全和漏洞的流程的，那么这些报告将非常有用。

当 ICANN 组织拥有以公认的标准（例如 ITIL、ISO 27000 系列标准、SSAE-18）为导向的 ISMS，并且通过定期审核验证相应的安全管理和管理程序时，可以认为已实施这项建议。

当 ICANN 组织拥有信息安全管理系统，同时此系统可详实记录和充分解决当前安全威胁并提供应对未来潜在安全威胁的规划时，可以认为这项建议有效。

SSR2 建议 6：SSR 漏洞披露和透明度

SSR2 审核小组建议 ICANN 组织优化其内部流程，通过以下措施为管理和报告 SSR 相关漏洞提供支持：

> 6.1. ICANN 组织应积极推动签约方自愿采用 SSR 最佳做法和漏洞披露目标。如果自愿措施被证明不足以推动采用此类最佳做法和漏洞披露目标，那么 ICANN 组织应在合同、协议和谅解备忘录中列明实施最佳做法和漏洞披露目标的要求。
>
> 6.2. ICANN 组织应实施协调性弱点披露报告流程。关于 SSR 相关问题的披露和信息，例如任何签约方的数据外泄以及发现并向 ICANN 组织报告的关键漏洞，均应及时通知值得信赖的相关方（例如，受影响的或需要解决特定问题的相关方）。ICANN 组织应定期报告漏洞（至少每年一次），包括匿名的衡量标准并使用负责任的披露机制。

当 ICANN 组织促进签约方自愿采用 SSR 最佳做法来披露漏洞并执行相关的漏洞披露报告时，可以认为已实施这项建议。

当 ICANN 组织和签约方针对漏洞披露采用了 SSR 最佳做法和目标时，可以认为这项建议有效。

3. 业务连续性管理和灾难恢复计划

鉴于 ICANN 组织正常运营在从 DNS 到 IANA 注册管理机构（包括对根区、IP 地址和 AS 编号，以及协议注册管理机构之类的重要注册管理机构的管理与维护）方面所发挥的重要职能作用，ICANN 组织需要精心规划、谨慎执行并妥善记录业务连续性 (BC) 管理和灾难恢复 (DR) 计划。基于这项关键职能，SSR2 审核小组认为 ICANN 组织应制定更稳健且条理更清晰的 BC 和 DR 计划。ICANN 将从遵循行业最佳做法中获益，特别是实施和记录符合适用的国际标准（例如，ISO/IEC 27001、NIST 800-53）的活动。独立审核应按照这些最佳做法来确认程序的适当性。

小组审核了关于 BC 和 DR 的可用文档。最新的文档是 2017 年编写的。[31] 根据 ISO 22301 和 22730 的规定，最佳做法要求对这些政策和流程进行年度审核。必须进行独立审核，以确保 BC 和 DR 计划最新并且符合维护 DNS 重要性的最佳做法。总体而言，SSR2 审核小组和 ICANN 组织员工无法找到和提供足够详细的文档，无法对 ICANN 组织的 BC 和 DR 计划的实施情况进行适当的评估。对于其提供的基本功能，ICANN 组织在处理 BC 和 DR 的方式上还有很大的改进空间。[32]

对于运行互联网关键基础设施的任何组织来说，由外部第三方审核确认其遵循公认的国际标准至关重要，即使法律没有要求合规也是如此。外部专家将通过针对审计师的公开招标，以及随后发布的最终审计报告（如果需要为修订版报告），为 ICANN 组织的 BC 和 DR 计划以及程序的透明度和合法性提出意见和建议。尤其是，ISO 31000“风险管理”、ISO/IEC 27000 系列标准“信息安全管理系统”，以及 ISO 22301“业务连续性管理”都是有用的指导方针，更重要的是，它们是第三方独立审核的目标标准。[33]尽管 ICANN 组织的组织架构和使命是独一无二的，但是 ISO 标准比较灵活且适用于 ICANN 组织，特别是在 ICANN 组织和 IANA 职能方面。审核小组还认为，只要 ICANN 组织详实记录流程并接受由公认的第三方进行独立审核，所使用的就应该是适用的 NIST 标准。[34]

如上文 B.3 部分“风险和安全管理”中所述，评估适当的 BC 和 DR 流程和程序的工作建立在更常规的风险评估活动基础之上。由于 ICANN 要为对互联网运行具有重要作用的系统提供支持，因此比常规的 BC 和 DR 具有更高的要求。疑似与密钥签名密钥 (KSK) 相关的程序遭到破坏，特别是在危机期间，可能会造成相当重大的问题，因此必须避免。2020 年是全球时局较为动荡的一年，从 COVID-19 疫情到重大社会骚乱，证明了在同一国家/地区（在这里指美国）部署两个站点有何不足之处，并且给 ICANN 组织内的 BC 和 DR 计划带来了意想不到的高风险。旅行限制同样也影响了美国境内的不同站点，与此同时，美国大多数主要城市还发生了暴力事件。此外，尽管这种情况极不可能发生，但两个站点都有可能受到其他不利事件的影响，例如地震、火灾或其他自然灾害。可能影响 ICANN 组织运营的风险类型将会不断演变，ICANN 组织必须通过定期对 BC 和 DR 计划进行评估且妥善记录来做出相应的回应，包括及时制定适当的计划并执行必要的更改。

---

[31] SSR2 维基页面，审核小组文档与草案，“SSR2 问题和答案”，未注明发布日期，2，https://community.icann.org/pages/viewpage.action?pageId=64076120。注：根据对 ICANN 工作人员的采访，“这些文件是机密文件，出于安全考虑没有公开发布。 目前已经制定了系统的灾难恢复计划，IANA 职能的连续性计划，并且正在为广大 ICANN 组织制定范围更广泛的连续性计划，这项计划将于 2019 年发布。”

[32] 审核小组意识到，ISMS、BC、DR 以及 ISO 合规风险管理相互影响且相互依存。尽管如此，审核小组认为应该提供关于已确定的需求、实施和必要步骤的详细信息。

[33] 国际标准化组织标准和系列标准 *ISO 31000*，*ISO/IEC 27000:2018 信息技术 - 安全技术 - 信息安全管理系统 - 概述与词汇*，以及 *ISO 22301:2019 安全和弹性 - 业务连续性管理系统 - 要求*。

[34] 美国商务部国家标准与技术研究院，*NIST 特别出版物 (SP) 800-30 修订版 1，风险评估指南*，马里兰州盖瑟斯堡：美国商务部，2012 年，https://doi.org/10.6028/NIST.SP.800-30r1 以及美国商务部国家标准与技术研究院计算机安全资源中心，*SP 800-53 修订版 5，信息系统和组织的安全与隐私控制*，马里兰州盖瑟斯堡：美国商务部，2020 年，https://doi.org/10.6028/NIST.SP.800-53r5。

SSR2 建议 7：改进业务连续性和灾难恢复流程和程序

7.1. ICANN 组织应根据 ISO 22301“业务连续性管理”制定适用于其自有或管辖的所有系统的业务连续性计划，并在计划中确定可接受的 BC 和 DR 时间表。[35]

7.2. ICANN 组织应确保适用于公共技术标识符 (PTI) 运营（即，IANA 职能）的 DR 计划涵盖了可促进 DNS 安全与稳定的所有相关系统以及根区管理，且符合 ISO 27031 相关标准。[36] ICANN 组织应与根服务器系统咨询委员会 (RSSAC) 和根服务器运营商 (RSO) 密切合作，共同制定此计划。

7.3. 同样，ICANN 组织也应根据 ISO 27031 相关标准制定适用于其自有或管辖的所有系统的 DR 计划。

7.4. ICANN 组织应为 ICANN 组织自有或管辖的所有系统建立一个新的灾难恢复站点，用于替代洛杉矶或库尔佩珀站点或增加一个永久性的第三站点。ICANN 组织应将这个新站点设在北美地区和美国领土之外的其他地方。如果 ICANN 组织选择替换其中一个现有站点，无论替换哪一个，ICANN 组织都应先确认新站点可以完全运行并且能够为 ICANN 组织处理这些系统的灾难恢复，然后再关闭要被替换的现有站点。

7.5. ICANN 组织应发布一份总体 BC 和 DR 计划和程序的摘要。这样做可以提高透明度和可信度，而不仅仅只是解决符合 ICANN 组织的战略目标和宗旨的问题。ICANN 组织应聘请外部审计人员来验证这些 BC 和 DR 计划是否合规。

当 ICANN 组织根据公认的行业标准详实记录 BC 和 DR 计划及流程，包括这些流程之后的定期审核，并且当一个非美国、非北美站点完全投入运营时，可以认为已实施这项建议。

当 ICANN 组织能够展示他们如何处理影响全美或北美地区的事件时，可以认为这项建议有效。

[35] ISO 22301:2019

[36] 国际标准化组织标准和系列标准 *ISO 27031，ISO/IEC 27031:2011 信息技术 - 安全技术 - 用于促进业务持续性的信息和通信技术配备指南。*

E. 关于 DNS 滥用的合同、合规和透明度

ICANN 自成立以来，使命就包括“*通过自上而下、基于共识的多利益相关方流程来协调政策的制定与实施，这些政策旨在确保互联网唯一域名系统稳定和安全运行*”。[37] SSR2 审核小组的结论是，尽管做出了上述承诺，但是当前 ICANN 协调的系统不足以应对 DNS 滥用及其相关危害。ICANN 社群内部和外部的团体多年来都注意到了这一差距。[38] 有关此主题的一些观点最明确的通信来自世界各国政府的政府咨询委员会 (GAC) 代表，这些代表指出，十多年来他们一直认为 ICANN 流程和程序不足以解决危害公共安全利益的问题。[39]

在 ICANN 组织成立之前，出于欺诈或犯罪目的而滥用 DNS 的问题已经存在。[40] 过去以垃圾邮件、网络钓鱼和欺诈为主的威胁态势，已扩展到包含各种更复杂的攻击，例如，恶意软件、勒索软件和商业电子邮件诈骗 (BEC)，它们以企业、政府和物联网 (IoT) 为攻击目标。[41] 现在，恶意不法分子包括受国家资助的商业不法分子，他们会开发行业平台为滥用活动提供支持。COVID-19 疫情及相关的隔离措施为伺机而动的犯罪分子提供了更大的攻击面。[42]

如下 C.1. 部分“未实现的新通用顶级域项目保护措施”中所述，DNS 滥用是当时所有利益相关方关注的重点，ICANN 组织有很多机会来制定政策，确保互联网唯一域名系统在全球域名空间扩展期间稳定和安全运行。如 C.2. 部分“挑战：定义与数据”中所述，ICANN 组织还有机会作为领导者，指导整个 DNS 和安全社群建立一套通用的术语、定义和数据，以促进通信和协作。

ICANN 组织仍然还有这些机会。这部分建议为 ICANN 组织提供了具体推荐内容，指明在哪些方面以及如何改进其履行自身使命，并成为 DNS 和安全社群中更强大的领导者。

[37] 《ICANN 章程》第 1.1(a) 节，https://www.icann.org/resources/pages/governance/bylaws-en/#article1。
[38] 例如：“注册管理机构利益相关方团体致 ICANN 社群的公开信”，2020 年 8 月 19 日，https://docs.wixstatic.com/ugd/ec8e4c_00d2dbac27b24330b8342686e9c2e53a.pdf，以及“ICANN 企业选区致 ICANN 董事会、ICANN 总裁兼首席执行官马跃然 (Göran Marby)、GNSO 理事会主席基思 • 德拉泽克 (Keith Drazek) 以及 ICANN 社群的信函”，2019 年 10 月 28 日，https://www.bizconst.org/assets/docs/positions-statements/2019/2019_10October_28%20BC%20Statement%20on%20DNS%20Abuse.pdf。
[39] ICANN 政府咨询委员会“关于 DNS 滥用的 GAC 声明”，2019 年 9 月 18 日，https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf。
[40] 请参阅“附录 E：关于 DNS 滥用趋势报告的研究数据”，了解有关 DNS 滥用历史趋势的更多信息。
[41] ICANN 安全与稳定咨询委员会，“SAC105：域名系统 (DNS) 和物联网：机遇、风险和挑战”，2019 年 5 月 28 日，https://www.icann.org/en/system/files/files/sac-105-en.pdf。
[42] 国际刑警组织，“关于 COVID-19 网络威胁的全球态势”，2020 年 4 月，https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf。

1. 未实现的新通用顶级域项目保护措施

2010 年启动新通用顶级域项目时，DNS 滥用是各方关注的重点。执法机构、政府、安全社群以及商业和用户利益团体一致认为，应在《新 gTLD 注册管理机构基本协议》和 2013 年《注册服务机构认证协议》(RAA) 中规定合同方负有缓解 DNS 滥用问题的义务。在这些审议过程中，ICANN 社群在 2009 年编写了一份备忘录，其中提出了针对新通用顶级域项目中恶意行为的缓解措施建议。[43] 备忘录中的建议包括审核注册管理运行机构，定义注册管理机构级别的滥用问题联系人和程序，以及集中访问域文件。遗憾的是，这份备忘录中所述的缓解措施与 ICANN 组织和注册管理机构双方闭门谈判得出的结论之间存在差距。后来曾尝试通过合同修订来改善安全做法，但却因缺乏透明度且社群没有参与这一流程而遭到批评。[44]

2013 年，ICANN 竞争、消费者信任和消费者选择 (CCT) 审核小组审核了这些明确旨在缓解新通用顶级域项目中的滥用率、恶意行为和犯罪活动的保护措施的有效性。CCT 审核小组委托独立研究机构使用公开数据源开展了一项研究（以下简称 SADAG 报告），研究显示新通用顶级域项目中的滥用率高于传统 TLD 中的滥用率，这说明保护措施无效。[45] CCT 最终报告的结论是：

“尽管滥用情况并非普遍持续存在于所有 NgTLD 中，但在很多 NgTLD 中屡见不鲜。更令人堪忧的是，社群目前几乎没有办法遏制存在严重滥用问题的 NgTLD 注册管理机构和注册服务机构。上述问题促使网络运营商单方面阻止来自特定 TLD 或注册服务机构的所有流量，而这又与社群希望实现的 NgTLD 普遍适用性目标背道而驰。

社群先前已经发现针对 NgTLD 的某些滥用活动，但未能阻止这类活动的进一步扩散，这一点值得引起重视。CCT 审核小组发现，域名是滥用活动的温床，这些滥用活动会影响 DNS 的安全、稳定和弹性，破坏消费者信任，最终影响全球最终用户。因此，在进一步扩展 DNS 之前必须妥善解决这个迫切问题，审核小组为此提出了几点建议，以期弥补当前的不足，提高 DNS 的安全性。”[46]

[43] ICANN“缓解恶意行为”，新通用顶级域解释性备忘录，2009 年 10 月 3 日，https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf。

[44] ICANN GNSO 企业选区，“关于《新 gTLD 注册管理机构基本协议》拟议修订的意见”，企业选区提交，版本 3，2016 年 7 月 20 日，https://www.bizconst.org/assets/docs/positions-statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf。

[45] 克钦斯基 (Korczyński)、马切伊 (Maciej)、马腾 • 吴林克 (Maarten Wullink)、莎曼内 • 塔嘉利扎德胡 (Samaneh Tajalizadehkhoob)、基奥云尼 • C.M. • 莫拉 (Giovane C.M. Moura) 和克里斯蒂安 • 海瑟曼 (Cristian Hesselman)，“关于 gTLD 中 DNS 滥用的统计分析最终报告”，SIDN 实验室和代尔夫特理工大学，访问时间 2018 年 8 月 3 日，https://www.icann.org/public-comments/sadag-final-2017-08-09-en。

[46] 竞争、消费者信任和消费者选择审核小组，“竞争、消费者信任和消费者选择：最终报告”，ICANN，2018 年 9 月 8 日，https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf，以及皮卡特洛 (Piscatello) 和戴维 (Dave)，“武器化域名：批量注册如何助推全球垃圾邮件活动”，Spamhaus，2020 年 3 月 21 日，https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns。

CCT 审核和相关的 SADAG 报告，以及其他第三方报告还发现，在启动新通用顶级域项目后，某些注册管理机构和注册服务机构立即制定做法来快速大幅增加域名注册，例如，批量注册，其中很多注册的域名用于滥用和犯罪活动。[47] Spamhaus（及其他机构）还发布了他们预计滥用最严重的 TLD 和注册服务机构，某些实体每年都出现在这些列表中。[48] SADAG 报告着重指出，Alpnames 是涉嫌 DNS 滥用问题最严重的注册服务机构之一，它提供廉价的批量注册服务，并且*“是被 Spamhaus 列入黑名单的新通用顶级域中 53.97%（59,044 个）的域名的责任注册服务机构”*。[49] 即使许多组织一再呼吁重视这个问题，但 ICANN 合同合规部仍然没有充分解决这个持续存在的系统性滥用问题。[50] ICANN 合同合规部直到得知 Alpnames 停止运营后才取消 Alpnames 的认证资质。[51] 我们希望 ICANN 组织和 DNS 业界能够展示在 DNS 滥用预防和缓解方面的可量化进展。否则，各国政府可能会认为 ICANN 的行业自治模型已不再适合其发展目标。

如 WHOIS2/RDS 审核报告中所述，ICANN 合同合规部有机会积极解决*“疑似系统性问题、报告的不准确性投诉，RDS 准确性研究或审核或 DAAR 报告，以研究、分析并强制纠正注册数据中的错误”*。[52]

[47] 同上，戴夫 • 匹斯特洛 (Dave Piscitello)，“武器化域名：批量注册如何助推全球垃圾邮件活动”，Spamhaus，2020 年 3 月 21 日，https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns。

[48] Spamhaus，“全球滥用最严重的 TLD”，访问时间 2020 年 12 月 5 日，https://www.spamhaus.org/statistics/tlds/，以及 Spamhaus，“全球滥用最严重的域名注册服务机构”，访问时间 2020 年 12 月 5 日，https://www.spamhaus.org/statistics/registrars/。注：Spamhaus 页面上的支持资料提供了关于他们如何确定“不法”域名和注册服务机构的分析。

[49] SADAG 报告，第 19 页，https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf。

[50] Adobe Systems、DomainTools、eBay、Facebook、Microsoft 和 Time Warner（也称为“独立合规工作组”）致 ICANN 合同合规部高级副总裁兼消费者权益保护主管杰米 • 赫德伦 (Jamie Hedlund) 的一封信，华盛顿办公室，2018 年 2 月 27 日，https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf。

[51] ICANN 合同合规部高级副总裁兼消费者权益保护主管杰米 • 赫德伦致 Alpnames Limited 伊恩 • 罗奇 (Iain Roache) 的一封信，华盛顿办公室，“回复：注册服务机构认证协议终止通知”，2019 年 3 月 15 日，https://www.icann.org/uploads/compliance_notice/attachment/1113/hedlund-to-roache-15mar19.pdf。

[52] RDS-WHOIS2 审核小组“注册目录服务 (RDS)-WHOIS2 审核最终报告”，2019 年 9 月 3 日，https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf，第 46 页。注：请参阅建议 4.1：*“ICANN 董事会应采取行动，确保 ICANN 合同合规部按照指示主动监控并强制执行注册服务机构关于 RDS (WHOIS) 数据准确性的义务，使用收到的不准确性投诉中的数据和 RDS 准确性研究或审核结果来查找并解决系统性问题。应采用基于风险的方法来评估和了解数据不准确性问题，然后采取适当的措施缓解问题。”*

SSR2 建议 8：在与签约方的谈判中维护并展现公共利益

8.1. ICANN 组织应委托一个谈判小组（由不附属于签约方或不是由签约方聘请的滥用和安全领域专家组成）来代表非签约实体的利益，并与 ICANN 组织合作，双方本着诚信、公开透明的原则重新谈判签约方合同，主要目标是提高域名系统的安全、稳定与弹性 (SSR) 以维护最终用户、企业和政府的利益。

当 ICANN 组织聘请 DNS 滥用和安全专家参与这些谈判，且域名系统的管理符合公共安全和消费者利益，而不仅只是符合域名行业的利益时，可以认为已实施这项建议。

当范围更广范且代表性更均衡的利益相关方能够直接就与签约方的合同谈判发表意见时，可以认为这项建议有效。

SSR2 建议 9：监督并强制实施合规

9.1. ICANN 董事会应指示合规团队监督并严格要求签约方遵守合同、基本协议、临时规范以及社群政策中关于现有和未来 SSR 以及滥用相关的义务。

9.2. ICANN 组织应主动监督并强制要求注册管理机构和注册服务机构履行合同义务，以提高注册数据的准确性。这种监督和强制实施应包括验证地址字段，以及定期审核注册数据的准确性。ICANN 组织的强制合规工作应重点关注那些因提供不准确数据而每年受到向 ICANN 组织投诉或报告超过 50 起的注册服务机构和注册管理机构。

9.3. ICANN 组织应至少每年请外部人员对合规活动进行审计，并公布审计报告和 ICANN 组织对审计建议的回复，包括实施规划。

9.4. ICANN 组织应责成合同合规职能部门发布定期报告，列举他们缺少的工具，他们需要这些工具来支持 ICANN 组织作为一个整体，有效地利用合同杠杆来应对 DNS 中的安全威胁，包括需要更改合同条款的措施。

当定期开展审核并发布摘要报告时，可以认为已实施这项建议。

当 ICANN 组织成功完成审核并向社群报告审核结果时，可以认为这项建议有效。

这项建议要求 ICANN 董事会和 ICANN 组织采取措施。在完成反滥用快速政策制定流程 (EPDP) 后，董事会可能必须更新其立场和指示（请参阅 SSR2 建议 15：启动 EPDP 以提高基于证据的安全性）。

2. 挑战：定义与数据访问

SSR2 审核小组发现了两类阻碍继续推进工作的持续挑战：一是关于 ICANN 合同合规部可以管理的滥用的定义和范围，二是关于对数据的访问，这些数据可为检测、缓解、防范和响应滥用提供相关信息。SSR2 建议 11 至 14 主要是关于提高这两方面工作的透明度和问责制。

A. 滥用的定义

在 2018 年 4 月与 SSR2 审核小组的对话中，ICANN 合同合规部指出，与注册管理机构和注册服务机构签订的现有合同未授权 ICANN 组织要求注册管理机构暂停或删除存在滥用风险的域名，导致他们无法有效地参与应对系统性 DNS 滥用问题的工作。[53] ICANN 合同合规部在致独立合规工作组的信函中也公开提出了这个问题。[54]

一年后，2019 年 4 月，ICANN 合同合规部在给 SSR2 审核小组的报告中表示，合同中缺乏对“系统性 DNS 滥用”的禁止规定，导致 ICANN 合同合规部无法有效解决这个问题，除非有一项社群共识性政策明确定义 DNS 滥用并阻止这个问题。[55] 此外，ICANN 董事会近期还宣布将推迟处理 CCT 审核建议 14 和 15，这两项建议提议修订现有协议以协助阻止 DNS 滥用。董事会强调这次推迟是因为“*社群仍在持续讨论，以期能够达成对 DNS 滥用及相关术语的共识*”。[56] SSR2 审核小组指出，这些既无组织又未明确界定范围的讨论使寻找解决方案变得复杂，从而使 ICANN 组织和签约方有理由无限期推迟解决这个问题。我们建议采取三管齐下的方式来解决这个问题，包括短期内制定一个临时规范，中期组建一个有时限的 CCWG，以及制定一个长期的结构化 EPDP。

[53] 简报材料：与 ICANN 合同合规部的讨论 - 完成时间 2019 年 5 月 14 日，ICANN 合同合规部对 SSR2 问题的回复（截至 2019 年 4 月 26 日），https://community.icann.org/display/SSR/Briefing+Materials。
[54] ICANN 合同合规部高级副总裁兼消费者权益保护主管杰米 • 赫德伦致独立合规工作组的信函，华盛顿办公室，“回复：独立合规工作组 2018 年 2 月 27 日信函”，2018 年 4 月 4 日，https://www.icann.org/en/system/files/correspondence/hedlund-to-vayra-04apr18-en.pdf。另请参阅脚注 44 “回复：独立合规工作组 2018 年 2 月 27 日信函”。
[55] 简报材料，https://community.icann.org/display/SSR/Briefing+Materials，4。注：请参阅问题 6 的回复。
[56] ICANN 董事会，“通过的决议 | ICANN 董事会例行会议”，主要议程，竞争、消费者信任和消费者选择审核小组 (CCT-RT) 未决建议，2020 年 10 月 22 日，https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a。

十多年来，ICANN 组织已将“DNS 滥用”及其相关术语的描述和有效定义与其活动相结合，包括但不仅限于 2009 至 2017 年 ICANN 组织的安全、稳定与弹性框架，[57] ICANN 社群在新通用顶级域项目中的共识性发现以及随后关于保护措施的共识，[58] 2013 年规范 11b 合同义务中列举的滥用活动，[59] 以及 ICANN 自己的 DNS 滥用活动报告 (DAAR) 项目。[60]

GNSO 理事会还要求注册滥用政策工作组 (RAPWG) 检查有关非法使用域名的问题。最终报告指出：

“RAPWG 确认，电子犯罪是 ICANN 社群的重要问题。互联网群体经常向 ICANN 表示其对恶意行为，特别是犯罪分子充分利用域名注册和域名解析服务犯罪的担心。各相关方 - 包括企业、消费者、政府和执法机构在内 - 都要求 ICANN 及其签约方监视恶意行为，适当时还应采取合理措施检测、拦截和缓解此类恶意行为。” [61]

RAPWG 曾建议建立一个由 ICANN 资源提供支持的社群流程，制定不具约束力的最佳做法，帮助注册服务机构和注册管理机构解决域名非法使用问题。十年后，ICANN 组织在这些问题上仍未取得实质性进展。[62]（另请参阅 SSR2 建议 9：监督并强制实施合规。）

[57] IS-SSR 文档存档，https://www.icann.org/ssr-document-archive。

[58] ICANN GNSO 注册滥用政策工作组，“注册滥用政策工作组最终报告”，2010 年 5 月 29 日，https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf，第 3 页。注：在这份报告中，将滥用定义为“*一种具有以下性质的行为：a) 导致实际和实质损害的行为，或可引发损害的实质行为；以及 b) 非法或不正当行为，或者以其他形式违背所规定合法目的的意图和企图（若此类目的已公开）的行为。*”另请参阅，ICANN 运营和政策研究，“新通用顶级域项目针对 DNS 滥用的保护措施”，2016 年 7 月，https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf，第 3 页。注：这份报告还使用了 RAPWG 对*注册*与*滥用*的区别，指出注册滥用在 ICANN 和 GNSO 政策制定中定义的范围更加明确。他们确定了注册滥用的示例，包括：域名抢注、抢先交易、牢骚网站、欺骗性和/或诋毁性域名、虚假续约通知、域名排列注册、每点击支付额、流量转移、虚假附属、跨 TLD 注册骗局、域名重复注册/体验。此外，RAPWG 还确定了滥用形式：网络钓鱼、垃圾邮件、恶意软件/僵尸网络命令与控制、分布式拒绝服务 (DDoS) 以及快速通量。

[59] ICANN“《注册管理机构基本协议》- 更新时间 2017 年 7 月 31 日”，规范 11 (3)(a) 和规范 11 (3) (b)，https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf 以及 ICANN“公告：《新 gTLD 注册管理机构协议》规范 11(3)(b)”，2017 年 6 月 8 日，https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en。

[60] 请参阅问题“DAAR 观察到哪些类型的安全威胁？”ICANN 组织 DAAR 常见问题解答，https://www.icann.org/octo-ssr/daar-faqs/#security-threats。具体而言：网络钓鱼、恶意软件、僵尸网络命令与控制，以及垃圾邮件。

[61] RAPWG 最终报告，第 6 页，https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf。

[62] ICANN 企业选区主席克劳迪娅 • 谢利 (Claudia Selli) 致互联网名称与数字地址分配机构 (ICANN) 董事会主席马腾 • 波特曼 (Maarten Botterman) 的信函，2019 年 12 月 9 日，第 1 页和第 3 页，https://www.icann.org/en/system/files/correspondence/selli-to-botterman-09dec19-en.pdf。

B. 数据访问

第二个主要挑战是对域名数据的访问，这些数据可为安全运营和研究提供信息。最受关注的四类数据分别是：注册数据，有助于跟踪相关域名的所有者和运营商的滥用行为；TLD 域文件数据（通过集中化域资料服务 (CZDS)），为安全研究提供支持；报告的滥用数据，用于为 ICANN 分析 DNS 滥用问题提供信息；以及合规数据，为趋势分析和运营方法评估提供支持，以缓解滥用。

i. 注册数据

至少从 2003 年开始，ICANN 组织就已经意识到需要在域名注册元数据（也就是，域名所有者的联系信息）的透明度和问责制，以及全球范围内的一些法律要求（某些情况下，禁止或复杂化此类信息的共享）这两方面之间实现平衡。[63]RAPWG 发现，注册目录服务（RDS，正式名称为 WHOIS）的基本可访问性与域名注册流程的滥用之间存在必然的联系，并且前者是域名恶意使用的关键问题。[64] 他们还发现，对 RDS 数据的访问有时并没有保障或不具有法律效力，注册服务机构没有以可靠、统一或具有前瞻性的方式提供此类 RDS 数据，用户在不同地方或通过不同方式查找 RDS 数据时会得到不同的结果。有鉴于此，RAPWG 提出了两项建议：

“GNSO 应要求 ICANN 合规部至少每年发布一次关于 WHOIS 可访问性的详细数据。这些数据应包括 a) 显示存在不合理限制访问端口 43 的 WHOIS 服务器情况的注册服务机构的数量，以及 b) 每年合同规定的所有 WHOIS 访问义务的合规审计结果。”

以及

“GNSO 应确定要确保 WHOIS 数据通过适当可靠、统一且具有法律效力的方式访问可能需要增加哪些研究和程序。” [65]

2018 年 6 月，为应对因新的 GDPR 生效导致难以访问注册数据这种情况，ICANN 安全与稳定咨询委员会 (SSAC) 紧急建议 ICANN 董事会修改合同，以解决持续存在的数据访问问题。这些建议均未实施。[66] 根据 ICANN 组织向 SSR2 审核小组提交的状态报告（2020 年 7 月 2 日），ICANN 组织将这些 SSAC101 建议授权给了 GNSO，用于制定关于访问注册数据的 EPDP 第二阶段工作

[63] ICANN“用于处理 WHOIS 与隐私法冲突问题的修订版 ICANN 程序”，2017 年 4 月 18 日，https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law。
[64] RAPWG 最终报告，第 71-80 页，https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf。
[65] 同上，第 79-80 页。
[66] ICANN 安全与稳定咨询委员会，“SAC101：关于访问域名注册数据的 SSAC 公告”，咨询委员会，2018 年 6 月 14 日，https://www.icann.org/en/system/files/files/sac-101-en.pdf。注：SSAC 发布了该文档的“第 2 版”，其中显著削弱了第 1 版中的以下建议：ICANN 董事会修改合同，以解决持续存在的数据访问问题。https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf。请参阅第 4-5 页，了解 SSAC101 第 2 版建议的完整文字内容。

计划。[67] EPDP 第 2 阶段工作计划中从未包含这些建议，EPDP 中也没有讨论过相关主题，GNSO 也从未开展任何相关工作。SSAC 还进行了其他尝试，但没有产生任何显著的影响。[68] 有些安全研究人员指出，现在的《gTLD 注册数据临时规范》允许 gTLD 域名注册服务机构修订 RDS 中发布的所有域名联系人数据，即使这些数据记录不在 GDPR 之类的隐私法规定范围之内。[69]

这个最新的 EPDP 是关于访问注册数据的辩论的最新且最详细版本。[70] 少数派声明持续指出，报告中的建议没有适当地权衡向注册管理机构和注册服务机构提供数据的注册人权益与公共利益，以防范利用 DNS 的恶意活动造成的相关损害。[71] 针对最终报告的诸多异议表明，这个流程未能使社群就关于数据访问的政策达成共识。注意到“*现有的分散式披露系统*”以及相对不确定的法律框架这些问题，ICANN 首席执行官最近要求欧盟委员会在法律层面明确阐述 GDPR 控制权条款。[72]

2013 年 RAA 中包含关于域名注册地址数据的字段交叉验证要求。[73] 字段交叉验证是一项常见的自动化有效性检查（例如，城市和省/自治区/直辖市街道中是否存在住址编号，以及邮政编码是否正确）。截至本报告发布之日，ICANN 组织尚未执行这项验证要求。关于隐私和代理注册，ICANN 组织的 GNSO 理事会一致支持一项针对隐私/代理服务提供商的认证政策，其中可能包括

[67] 珍妮弗 • 布莱斯 (Jennifer Bryce) 发送至 SSR2 审核小组电子邮件清单的邮件，2020 年 7 月 2 日，主题：SAC097 和 SAC102 第 2 版状态，https://mm.icann.org/pipermail/ssr2-review/2020-July/002280.html。请参阅邮件附件第 2 页。

[68] ICANN 安全与稳定咨询委员会致注册管理机构服务和合作主管鲁斯 • 维恩斯坦 (Russ Weinstein) 以及 ICANN 合同合规部高级副总裁兼消费者保护经理杰米 • 赫德伦的信函，“主题：SSAC2019-02：注册数据服务查询报告”，2019 年 5 月 3 日，https://www.icann.org/en/system/files/files/ssac2019-02-03may19-en.pdf。注：SSAC 发布了 SSAC 2019-2 报告，建议 ICANN 组织向所有注册管理运行机构发布指南，阐明报告端口 43 查询和 RDAP 查询的目标、期望及合同义务。但是，没有证据表明这些建议被采纳并执行。

[69] 格雷格 • 亚伦 (Greg Aaron)、莱曼 • 查宾 (Lyman Chapin)、戴夫 • 匹斯特洛 (David Piscitello) 以及科林 • 斯特乌特 (Colin Strutt) 博士，“2020 年网络钓鱼态势：网络钓鱼范围和分布情况研究”，Interisle Consulting Group, LLC，2020 年 10 月 3 日，http://www.interisle.net/PhishingLandscape2020.pdf。

[70] ICANN 通用名称支持组织，“gTLD 注册数据临时规范快速政策制定流程第 2 工作阶段最终报告”，2020 年 7 月 31 日，https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf。

[71] 同上，附录 F - 少数派声明，第 151-154 页。包含以下各方的少数派声明：一般会员咨询委员会 (ALAC)、企业选区 (BC)/知识产权选区 (IPC)、政府咨询委员会 (GAC)、非商业利益相关方团体 (NCSG)、注册服务机构利益相关方团体 (RrSG)、注册管理机构利益相关方团体 (RySG)，以及安全与稳定咨询委员会 (SSAC)。

[72] ICANN 总裁兼首席执行官马跃然致欧盟委员会通信网络、内容和技术总司总干事罗伯托 • 维奥拉 (Roberto Viola) 先生、欧盟委员会移民与内政总司总干事莫妮卡 • 帕里亚 (Monique Pariat) 女士，以及欧盟委员会司法与消费者总司代理总干事萨拉 • 萨斯塔莫宁 (Salla Saastamoinen) 女士的信函，2020 年 10 月 2 日，https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf。

[73] ICANN，《2013 版注册服务机构认证协议》，访问时间 2020 年 12 月 8 日，https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en。注：请参阅“WHOIS 准确度项目规范”第 1(e) 节，https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy。

加强涉及对执法机构和知识产权持有人的回应的运营做法。[74] ICANN 董事会于 2016 年 8 月批准了该政策。[75] 截至 2020 年 10 月，ICANN 尚未实施这些要求，并且自 2018 年 3 月以来，此工作项目的专用网站一直没有更新。[76]

ii. 集中化域资料服务

域文件访问始终是与安全相关的运营和研究的重要方面。作为新通用顶级域项目的组成部分，社群同意新 gTLD 注册管理机构接受合同义务，以便“*在完成新通用顶级域的技术授权后，向获得批准的请求者（例如，执法机构代理人、IP 律师、研究人员）提供域资料。*”[77] 然而，关于对此类数据的全面访问以及数据的可用性方面一直存在各种问题，例如，请求访问和续订访问，以及获取实际文件。[78] 目前，注册管理机构不仅未按预期授予数据访问权限，而且由于漫长的续订流程还在不断削弱访问权限。[79] 这些数据通常用于 DNS 滥用情况研究。[80] 三年多以前，SSAC 在 2017 年 6 月撰写了一份关于这个主题的公告 (SAC097)。[81] 尽管 ICANN 董事会接受了相关建议，但一直没有执行。[82] SSR2 审核小组认识到，出于品牌保护或安全方面的考虑，可能需要为通过 CZDS 访问某些 TLD（例如，品牌 TLD）数据提供便利；但总体而言，通过 CZDS 访问此类关键数据仍然存在诸多问题。[83]

---

[74] ICANN，“隐私和代理服务”，访问时间 2020 年 12 月 8 日，https://whois.icann.org/en/privacy-and-proxy-services。注：请参阅第 2 部分“采纳政策建议的流程”。

[75] 同上。

[76] 注册服务机构 WHOIS 验证工作组，“文档”，上次更新时间：2018 年 3 月 21 日，https://community.icann.org/display/AFAV/Documents。

[77] ICANN，“集中化域资料服务 (CZDS)”，访问时间 2020 年 12 月 7 日，https://czds.icann.org/home。

[78] 戴夫 • 匹斯特洛，“不具体的 CZDS 合同措辞使域资料访问批准变得不确定”，博客文章，“安全怀疑论者”，2019 年 8 月 13 日，https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html。

[79] 戴夫 • 匹斯特洛，“不具体的 CZDS 合同措辞使域资料访问批准变得不确定”，博客文章，“安全怀疑论者”，2019 年 8 月 14 日，https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html，以及 ICANN SSAC，“SAC 096：关于集中化域资料服务 (CZDS) 和注册管理运行机构月度活动报告的 SSAC 公告”，2017 年 6 月 16 日，https://www.icann.org/resources/files/1207653-2017-06-16-en。

[80] KC • 克拉菲 (KC Claffy) 和戴维 • 克拉克 (David Clark)，“互联网经济学工作坊 (WIE 2019) 报告”，2020 年 4 月，https://ccronline.sigcomm.org/2020/ccr-april-2020/workshop-on-internet-economics-wie-2019-report%EF%BB%BF/。

[81] ICANN 安全与稳定咨询委员会，“SAC097： 关于集中化域资料服务 (CZDS) 和注册管理运行机构月度活动报告的 SSAC 公告”，2017 年 6 月 12 日，https://www.icann.org/en/system/files/files/sac-097-en.pdf。

[82] ICANN 安全与稳定咨询委员会，“安全与稳定咨询委员会 (SSAC) 建议状态”，上次更新时间：2020 年 10 月 30 日，https://features.icann.org/board-advice/ssac。请参阅“SAC097：关于集中化域资料服务 (CZDS) 和注册管理运行机构月度活动报告的 SSAC 公告，版本 1（2017 年 6 月 12 日）。”

[83] 马克 • VB • 帕特里奇 (Mark VB Partridge) 和乔丹 • A. • 阿诺特 (Jordan A. Arnot)。“域名系统的扩展：优势、异议和争论。”DePaul J. Art Tech.& Intell.Prop.L 22 (2011)：317（请参阅文章第 5 页），以及“CZDS-API-试验床 - 用于注册并参与 API 讨论主题的 CZDS API 用户的电子邮件清单”，https://mm.icann.org/mailman/listinfo/czds-api-testbed。请参阅存档中的投诉线索（请注意，只有用户才能访问，但订阅是开放的。）

2018 年 6 月董事会决议之后，域文件访问投诉数量有所增加，并且仍然高于 2018 年年中的数量。现在，这类投诉占据对注册管理运行机构投诉的最大比例。[84] 有时候，在提交 ZFA 投诉后，ICANN 合同合规部几个月都不处理。[85] 2018 年，ICANN 组织要求新通用顶级域后续流程工作组（通常称为 SubPro WG）解决这个问题。[86] 但是，SubPro WG 在其近期发布的一份长达 363 页的报告草案中完全没有提及这个问题。[87] 没有任何证据表明 ICANN 组织、ICANN 董事会或注册管理机构社群采取了充分的措施来解决 CZDS 数据访问问题。“SSR2 建议 11 - 解决 CZDS 数据访问问题”正是专门针对这个问题提出的。

iii. DNS 滥用活动报告

ICANN DNS 滥用活动报告 (DAAR) 计划是一个“*用于研究顶级域 (TLD) 注册管理机构和注册服务机构内的域名注册和安全威胁（域名滥用）行为的平台*”，总体目标是“*向 ICANN 社群报告安全威胁活动，社群可以利用这些数据做出明智的决策。*”[88] ICANN 组织于 2017 年启动了 DAAR 计划。ICANN 组织称，DAAR 旨在为社群提供一种用于报告 DNS 滥用情况的透明且可复制的科学方法。[89] 自 2018 年 1 月以来，ICANN 首席技术官办公室 (OCTO) 根据对 DAAR 数据的分析持续发布简要月度报告，但报告的详细程度无法得出关于哪些注册服务机构/注册管理机构存在严重滥用行为的结论。ICANN 组织也没有与帮助改进方法或确认审核结果的研究人员共享完整的（原始）数据。OCTO 员工告知 SSR2 审核小组，这些目标（可行的数据、验证）不是 DAAR 计划的初衷。[90] SSR2 审核小组认为 ICANN 组织与数据提供商达成协议的方式显然成为了实现这些目标的重大阻碍，同时提议全面改革 DNS 滥用分析计划，以透明度、可重复性和可行的数据产品为主要目标。

识别滥用情况比例不甚合理的注册管理机构和注册服务机构，将有助于制定明智的政策，并提高至今尚不存在的域名注册系统的透明度和问责制。实际上，如果数据和分析既不可行又无法满足可重复性和验证要求，审核小组也不确定 ICANN 在这方面的投资有什么作用。SSR2 审核小组认为，如果社群和 ICANN 组织无法全面改进 DAAR 以实现这些目标，则应中止 DAAR 计划。SSR2 建议 12：针对这个问题，全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核。

---

[84] ICANN，“合同合规情况评估”，访问时间 2020 年 12 月 7 日，https://features.icann.org/compliance/dashboard/report-list。请注意，截至 2020 年 3 月，域文件访问投诉占总投诉量的 85.5%，而 2018 年 3 月时，此类投诉数量占 31.9%。

[85] “CZDS-API-试验床 - 用于注册并参与 API 讨论主题的 CZDS API 用户的电子邮件清单”，https://mm.icann.org/mailman/listinfo/czds-api-testbedS。请参阅存档中的投诉线索（请注意，只有用户才能访问，但订阅是开放的。）

[86] ICANN，“新通用顶级域后续流程工作组章程”，2016 年 1 月 21 日，https://gnso.icann.org/sites/default/files/filefield_48475/subsequent-procedures-charter-21jan16-en.pdf。

[87] ICANN 新 gTLD 后续流程工作组，“GNSO 新 gTLD 后续流程最终报告草案”，访问时间 2020 年 12 月 7 日，https://www.icann.org/public-comments/gnso-new-gtld-subsequent-draft-final-report-2020-08-20-en。

[88] DAAR 常见问题解答，https://www.icann.org/octo-ssr/daar-faqs/#security-threats。

[89] 戴夫 • 匹斯特洛，“域名滥用活动报告 (DAAR) 系统”，ICANN APWG 欧盟报告，2017 年 10 月，https://www.icann.org/en/system/files/files/presentation-daar-31oct17-en.pdf。

[90] 电话会议文稿，“关于 DAAR 的 SSR2 电话会议 - 2020 年 6 月 24 日 15:00 UTC”，https://community.icann.org/x/WIJIC。

iv. 投诉

CCT 报告指出，由于 ICANN 合同合规部在投诉方面缺乏透明度，并且缺乏对合同中公共利益承诺的强制执行，因此难以评估保护措施的影响。[91]SSR2 审核小组指出，恶意域名举报人面临的一个关键问题是投诉提交流程比较复杂，这个流程对签约方的要求不同，且往往缺乏（及时的）回复或措施。SSR2 审核小组认为，开发一个用于提交滥用投诉的集中系统可能会简化投诉流程，有益于投诉提交者和签约方，并且会减少误导投诉数量。

SSR2 审核小组认为，全面改革 DNS 滥用分析计划可使 ICANN 合同合规部能够制定关于普遍存在的滥用行为的标准预期。鉴于黑名单可能不是 100% 准确且可能被操纵，ICANN 必须努力验证分析结果，同时签约方必须有机会反驳 ICANN 的通知。

SSR2 建议 10：明确滥用相关术语的定义

10.1. ICANN 组织应发布一个网页，明确 DNS 滥用的有效定义，即，适用的项目、文档和合同。定义应明确指出 ICANN 组织目前认为在其职权范围内通过合同和合规机制可以解决的安全威胁类型，以及 ICANN 组织认为属于其职权范围之外的安全威胁类型。如果 ICANN 组织使用其他类似术语（例如，安全威胁、恶意行为），那么 ICANN 组织应同时指明这些术语的有效定义，以及 ICANN 组织如何将这些术语与 DNS 滥用区分开。本页面应包含具体链接，指向与签约方签订的合同中各项与滥用相关的现有义务的摘要，包括应对滥用的相关程序和协议。ICANN 组织应每年更新此页面，注明最新版本的日期，并链接到具有相关发布日期的旧版本。

10.2. 组建一个由员工提供支持的跨社群工作组 (CCWG)，负责确立一个流程来不断完善阻止 DNS 滥用的定义，至少每两年一次按照可预测的时间表（例如，隔年的一月份）更新一次 DNS 滥用的定义，在 30 个工作日内完成此流程。跨社群工作组应包括来自消费者保护、运营网络安全、学术界或独立网络安全研究机构、执法机构，以及电子商务领域的利益相关方。

10.3. ICANN 董事会和 ICANN 组织应在公共文档、合同、审核小组实施规划以及其他活动中一致地使用共识定义，并在出现此类使用情况时参考本网页。

[91] CCT 报告，第 9-10 页，https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf。

当 ICANN 组织发布包括 CCWG 的首个输出成果在内的网页内容，且通过相应流程保持更新网页内容时，可以认为已实施这项建议。

当 ICANN 组织能够提高关于已接受和通过社群审核的描述的透明度和问责制，并且能够清晰说明社群讨论成果和对政策文件的解读，从而使其他利益相关方能够定义 DNS 滥用的行为准则时，可以认为这项建议有效。

SSR2 建议 11：解决 CZDS 数据访问问题

11.1. ICANN 社群和 ICANN 组织应采取措施，以确保请求人员能够及时访问 CZDS 数据，不会遭遇不必要的阻碍，例如没有自动续订访问凭证。

当 ICANN 组织和社群使 CZDS 数据可以及时访问，而不会给请求者带来不必要的障碍时，可以认为已实施这项建议。

当 ICANN 组织报告关于域文件访问的投诉数量减少，且研究人员提高了针对 DNS 安全运营相关的研究能力时，可以认为这项建议有效。

这项建议旨在确立对学者和安全专家所使用的与安全相关的域文件数据的适当访问权限。这项建议要求 ICANN 董事会、ICANN 组织以及 GNSO 采取相应措施。

SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核

12.1. ICANN 组织应创建一个由独立专家（即，没有财务利益冲突的专家）组成的 DNS 滥用分析咨询小组，对 DNS 滥用报告活动提出全面改进建议，将可操作的数据、验证、透明度和独立的可重复性分析作为最高优先级事项。

12.2. ICANN 组织应与数据提供商达成协议，允许进一步共享非商业用途的数据，特别是用于验证或需要进行同行评审的科学研究。这种特殊的免费非商业数据使用许可，可能会存在时间上的滞后，以免影响数据提供商的商业收入机会。ICANN 组织应在 ICANN 网站上发布所有数据共享合同条款。ICANN 组织应终止任何不允许对拦截清单背后的方法进行独立验证的合同。

12.3. ICANN 组织应发布报告，揭示其域名最易造成滥用的注册管理机构和注册服务机构。ICANN 组织发布的报告不仅应包含当前报告中的图形数据，还应包含机读格式的数据。

12.4. ICANN 组织应整理并发布注册管理机构和注册服务机构采取的措施报告，包括自愿行动和履行法律义务的做法，以便根据与使用 DNS 相关的适用法律对非法和/或恶意行为的投诉做出回应。

当 ICANN 组织的 DNS 滥用分析计划引入了衡量标准，遵守这些标准可生成可行、准确且值得信赖的数据时，可以认为已实施这项建议。

当 ICANN 组织可用的所有数据也可供社群成员和独立研究人员使用（可能会有时间上的延迟）来进行验证和提供反馈时，可以认为这项建议有效。

SSR2 建议 13：提高滥用投诉报告的透明度和问责制

13.1. ICANN 组织应构建并维护用于集中管理 DNS 滥用投诉的门户，该门户可将每份滥用报告自动分发给相关方。它将纯粹作为一个信息流入系统，ICANN 组织只收集和处理摘要和元数据，包括时间戳和投诉类型（分类）。所有通用顶级域 (gTLD) 都必须使用这个系统；每个国家和地区顶级域 (ccTLD) 可自愿选择是否使用这个系统。此外，ICANN 组织还应与所有 ccTLD 共享滥用报告（例如，通过电子邮件）。

13.2. ICANN 组织应以允许独立第三方分析关于 DNS 投诉类型的形式发布其收到的投诉数量。

当 ICANN 组织简化提交和接收滥用投诉流程，同时提供针对投诉数量的分析，并向研究人员和社群成员提供一些元数据（例如，举报的滥用类型、日期、解决时间）时，可以认为已实施这项建议。当门户网站保持运行和更新时，可以认为这项建议有效落实。

当签约方花费更少的时间处理误导投诉，研究社群和更广泛的 ICANN 社群能够查看和研究关于这些投诉的相关数据时，可以认为这项建议有效。

由于组织的复杂性，ICANN 董事会批准实施这项建议后，执行这项建议预计需要数年（至少三年）时间。

3. 政策制定流程 (PDP) 替代方案

务必要破除通过政策制定流程 (PDP) 来制定共识性政策是实施多项建议的唯一途径这一主张。ICANN 董事会可以通过多种途径来推动实施我们的建议。董事会可以选择合同谈判、向签约方发布公告，或组建有时限且由专家提供支持的跨社群工作组。[92]董事会认为 DNS 滥用是一项迫切需要重视的严重公共安全问题，因此，ICANN 组织甚至发布了一份临时规范。一个实用的案例就是：

[92] 注册服务机构公告网站 (https://whois.icann.org/en/registrar-advisories) 上提供了以前针对签约方的公告示例。

董事会近期在回复关于欧盟《通用数据保护条例》(GDPR) 与 ICANN 组织的章程不一致的问题时使用了临时规范。ICANN 社群多年来致力于制定与 GDPR 一致的注册数据访问政策，但这个问题却迟迟未解决。而在 DNS 滥用和访问注册数据以打击滥用行为方面，我们看到了类似的情况。

ICANN 组织可以并且确实进行了双边合同谈判。在没有通过 PDP 制定共识性政策的情况下，对 ICANN 组织与注册服务机构和注册管理机构的合同进行了更改。当 ICANN 组织更新 2013 年 RAA 和 2017 年《注册管理机构基本协议》时，ICANN 组织和谈判小组代表各自的行业管理这个流程，没有采用任何 PDP。社群本有机会对草案文本提供意见，但是只有谈判小组参与了讨论和决策。[93] ICANN 组织与签约方之间的闭门谈判是推动工作进展的重要工具，但当提及 DNS 滥用问题时这些谈判的作用却非常有限，因为谈判将所有其他利益相关方（包括会从减少滥用注册中受益的政府、企业和公众）排除在外。SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，实现透明度和独立审核，以填补这一差距。

尤其是在 EPDP 无法解决注册数据访问问题之后，巨大的利益冲突使 PDP 流程陷入困境且解决 DNS 反滥用问题的进展非常缓慢，审核小组认为有关 DNS 滥用的 EPDP 流程本身不会提出有效的解决方案。花费了数年时间才完成注册数据访问 EPDP，但却遭到了多数 ICANN 社群的反对，一般会员咨询委员会 (ALAC)、企业选区和知识产权选区 (BC/IPC)、非商业利益相关方团体 (NCSG)、注册服务机构利益相关方团体 (RrSG) 以及注册管理机构利益相关方团体 (RySG) 都发表了大量的少数派声明。BC/IPC 少数派报告警告指出：“*监管机构和立法机构应该注意到，ICANN 多利益相关方模型已经不能满足消费者保护、网络安全和执法的需要。*”[94] SSAC 少数派报告也警告指出，ICANN 的政策制定流程“*没有提供合理适当的安全性和稳定性结果。*”[95]

总之，由于现有术语和合同要求模糊不清，需要采取措施的相关方之间存在利益冲突，以及各国政府对通过其他法律流程解决 DNS 滥用做出了不同的承诺，缓解、防范和阻止现有的 DNS 滥用问题面临着诸多挑战。尽管某些 DNS 滥用相关政策和合同条款已经存在，但 ICANN 组织和签约方需要更加有效地予以落实和强制实施，同时社群需要制定其他政策、合同条款并开展活动来跟上 DNS 滥用的发展态势。SSR2 审核小组认为解决 DNS 滥用是一项非常重要的需求，可保障和证明 ICANN 在这方面的强大领导力。GDPR 临时规范表明，ICANN 董事会保持响应各种需求的决策权限。而且，ICANN 组织作为加利福尼亚的一家非营利性公益型组织，其任务是监督 DNS 的安全与稳定运营，且政策制定符合公共利益，为此，ICANN 董事会有诚信义务确保 ICANN 组织政策和衍生合同符合其使命和职责。也许最好的方法是制定一份新的临时规范，以及一个新的 EPDP。[96]

---

[93] 2013 年《注册服务机构认证协议》，https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en。注：根据 RAA 第 1.2 节“共识性政策和临时政策规范”的规定，ICANN 可通过共识性政策或 ICANN 组织与其他相关方之间的谈判来修订合同，https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary。

[94] GNSO EPDP 第 2 阶段报告，BC/IPC 少数派声明，第 114-121 页，https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf。

[95] 同上，第 145-162 页，SSAC 少数派声明。

[96] SSR2 审核小组认为，ICANN 组织已经收集了足够的信息，包括制定 DAAR 计划和自己撰写 DAAR 报告所需的信息来编写问题报告，因此有理由启动 EPDP 而不是 PDP。

SSR2 建议 14：制定临时规范，提高基于证据的安全性

14.1. ICANN 组织应制定临时规范，要求所有签约方将已修订的 DNS 滥用报告中确定为滥用的域名所占百分比保持在合理范围和已发布的阈值之下（请参阅 SSR2 建议 13.1）。

14.2. 为促进反滥用行动，ICANN 组织应根据关于独立审核域名数据和拦截清单方法的 SSR2 建议 12.2，向签约方提供其域名组合中被认定为滥用的域名列表。

14.3. 如果与滥用活动相关的域名数量达到 SSR2 建议 14.1 中所述的已发布阈值，ICANN 组织应展开调查以确认数据和分析的准确性，然后向相关方发出通知。

14.4. ICANN 组织应给签约方 30 天时间，供对方将滥用域名的比例降低到阈值以下或证明 ICANN 组织的结论或数据存在问题。如果签约方在 60 天内未能纠正错误，ICANN 合同合规部应开始取消认证流程。

14.5. ICANN 组织应考虑提供财务激励措施：域名组合中滥用域名比例低于特定百分比的签约方，将有机会获得适当程度减免应付交易费用的奖励。

SSR2 建议 15：启动 EPDP 以提高基于证据的安全性

15.1. 制定临时规范后（请参阅 SSR2 建议 14：制定临时规范，提高基于证据的安全性），ICANN 组织应建立由员工提供支持的 EPDP 以制定反滥用政策。EPDP 志愿者应代表 ICANN 社群，使用 gTLD 注册数据临时规范 EPDP 团队章程中的号码和分配作为模板。[97]

15.2. EPDP 应参考 SSR2 建议 10.2 中拟议的 CCWG 基本定义。该政策框架应明确定义针对不同类型的滥用行为的适当对策和补救措施，签约方采取措施的时间框架（例如滥用报告/响应报告时间表），以及在出现违反政策的情况下，ICANN 合同合规部可采取的强制措施。如果任何签约方有包庇滥用行为的方式和做法，ICANN 组织应坚持要求终止合同。结果应包括建立一个机制，每两年对滥用相关的基准和合同义务更新一次，通过一个不超过 45 个工作日的流程来完成这项工作。

[97] ICANN，“PDP 团队章程”，页面上次编辑时间：2018 年 7 月 23 日，第 12-14 页，https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter。

当 ICANN 合同合规部开发了适当的工具，用于应对签约方不响应 DNS 滥用问题的情况，具体来说就是所有相关合同和协议中都包含与反滥用相关的义务时，可以认为已实施 SSR2 建议 14 和 15。

当 ICANN 合同合规部使用这些工具来处理签约方严重违反政策的行为时，可以认为 SSR2 建议 14 和 15 有效。

SSR2 建议 14 和 15 的预期目标是赋予 ICANN 合同合规部处理最严重的 DNS 滥用问题的能力，因为 ICANN 合同合规部曾表示缺乏足够的工具来解决这个问题。

这些建议要求 ICANN 组织和 ICANN 社群采取措施，同时旨在指导政策制定。这些建议是可实现的，但 ICANN 组织只能逐步实施这些建议。

4. 隐私和数据管理

由于第三方（除了传统的政府实体之外）不断增加数据收集数量和数据分析，以及不断演变的隐私立法形势，隐私问题在持续变化。SSR2 审核小组得出的结论是，面对不断变化的形势，ICANN 组织并没有做到应有的积极主动，证据就是关于 RDS 数据的可用性存在不一致。[98]

整个 ICANN 网站上谈论注册数据隐私问题各个方面的网页数量激增，但都没有标注相关的日期。缺乏时间戳导致审核小组无法针对 ICANN 组织在这个主题上所做工作的历史展开合理的研究。[99] 此外，截至 2020 年 10 月，RDS 网站和相关文档均已过时，且不包含或未引用相关社群文档。ICANN 网站上确实有一些关于 RDS 的网页，但这些网页都不包含任何交叉引用。ICANN 当前的 RDS 网页最后一次更新是在 2017 年，因此没有参考最新的临时规范衡量标准或 EPDP 状态。[100] 审核小组认为，缺乏信息和网页内容不一致反映了 ICANN 组织在隐私问题上缺乏清晰度和一致性。

[98] 请参阅本报告中第 C.2.b.i. 部分“注册数据”以及第 C.2.b.ii. 部分“集中化域资料服务”。
[99] 示例包括：https://whois.icann.org/en/privacy-and-proxy-services、https://whois.icann.org/en/privacy、https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law 和 https://www.icann.org/rdap。注：这些页面似乎都已存在多年，其中一些页面底部还包含注释：“2018 年 5 月 17 日，ICANN 董事会采纳了《gTLD 注册数据临时规范》。本页面目前正处于审核状态，届时将会进行更新以反映这项临时规范。”
[100] ICANN，“关于 WHOIS”，上次更新时间：2017 年 7 月，https://whois.icann.org/en/about-whois。

在第 C.2.b.i.部分“注册数据”中，审核小组还指出，需要根据 GDPR 等各种隐私法规来平衡域名注册元数据的透明度和问责制。通过确保 ICANN 网站内容以及与注册管理运行机构和注册服务机构达成的共识性政策和协议的一致性，ICANN 组织将有助于确保对注册数据的收集、保留、托管、转移和显示进行安全管理和保护，注册数据包括注册人、管理联系人和技术联系人的联系信息，以及域名相关的技术信息。

SSR2 建议 16：隐私要求和 RDS

16.1. ICANN 组织应在其网站上提供一致的交叉引用，以提供关于隐私和数据管理主题的所有举措（过去、现在和计划中）的一致且易于查找的信息，特别是注册目录服务 (RDS) 相关信息。

16.2. ICANN 组织应在合同合规职能部门内建立专门小组，负责深入了解隐私要求和原则（例如，收集限制、数据资格、目的规范以及数据披露的安全保护措施），并在 RDS 框架下促进执法需求，因为社群已修订和批准了该框架（另请参阅 SSR2 建议 11：解决 CZDS 数据访问问题）。

16.3. ICANN 组织应定期审计注册服务机构隐私政策履行情况，确保注册服务机构制定了用于处理侵犯隐私行为的流程。

当 ICANN 组织妥善记录了关于隐私及其 RDS 管理的措施，且特别分配了 ICANN 组织内的资源来确保 ICANN 遵守这方面的现有最佳做法和法律要求时，可以认为已实施这项建议。

当 ICANN 组织能够证明其在数据处理和隐私方面持续遵守最佳做法和法律要求时，可以认为这项建议有效。

F. 关于全球 DNS 的其他 SSR 相关问题

SSR2 审核小组认识到，ICANN 组织只是 DNS 生态系统诸多实体的其中之一。尽管如此，ICANN 组织仍处于独特地位，可影响和引导整个 DNS 生态系统的 SSR 相关措施。这部分提供了具体建议，供 ICANN 组织为自身以及整个全球 DNS 改进政策和做法。 通过对 IMRS 管理的最佳做法进行建模，共享研究人员的综合意见，提供用于测试和分析的工具，以及本部分中讨论的其他可能的措施，ICANN 组织可以采取措施来改善自身的 SSR 工作并帮助其他机构了解如何改善他们的 SSR 工作。

1. 域名冲突

尽管 ICANN 组织提供了关于域名冲突的详细资料和培训，但没有限制注册人利用与公域存在冲突的私域的唯一标识符。SSR2 审核小组认为，最近完成并发布的研究报告（下文简称 2019 NCAP 研究）是朝着处理不必要的域名冲突的正确方向迈出的一步。[101]然而，这项研究没有解决对于未报告（恶意和偶然）域名冲突的发现机制的持续需求。这项研究还得出结论，自 2017 年以来没有关于域名冲突的最新研究，同时将报告的域名冲突数量减少视为当前机制正在起作用的指标。[102]

另一方面，2016 年经同行评审后的一项研究发现，上一轮次 gTLD 显著加剧了域名冲突问题。[103]传统报告机制表明报告的域名冲突数量减少，可能并不意味着不存在域名冲突。相反，域名冲突的本质可能以规避那些传统机制的方式发生了变化。此外，近年来新通用顶级域名授权数量也有所减少，这可能进一步影响了报告的域名冲突的绝对数量。[104]

尽管 2014 年 ICANN 委托编写的一份报告（下文简称“第一阶段报告”）中拟议制定一个控制性中断框架来避免潜在的域名冲突，但这个控制性中断框架从未针对不断演变的域名冲突攻击情景进行测试。[105] 例如，SSAC 曾建议“*ICANN 应引入滚动中断周期（而不是一个单一的控制性中断周期），并按正常运行周期划分，以便受影响的最终用户系统在 120 天的测试周期内能够持续运行，降低对业务造成灾难性影响的风险。*”[106] 在第一阶段报告中，作者以缺乏二级域名注册人的电子邮件和电话为基础得出了他们的某些推断，这不足以反应域名冲突问题的复杂性。[107] 此外，第一阶段报告还讨论了一些控制性中断框架的替代方案，包括使用蜜罐、DNAME 以及字符串到字符串方法，但从未考虑过实施这些方法。[108] 与第一阶段报告相反，SSR2 审核小组得出的结论是，域名冲突仍是一项重大挑战，需要进一步研究和缓解。

---

[101] 卡伦 • 斯卡尔福内 (Karen Scarfone)，“管理顶级域名冲突的风险：域名冲突分析项目 (NCAP) 研究成果”，ICANN OCTO，2020 年 5 月 27 日，https://www.icann.org/en/system/files/files/managing-risks-tld-2-name-collision-07may20-en.pdf。

[102] 同上，第 43 页。

[103] 奇-阿尔弗雷德-陈 (Qi Alfred Chen)、埃里克 • 奥斯特维尔 (Eric Osterweil)、马修 • 托马斯 (Matthew Thomas) 和 Z-莫尔里-毛 (Z. Morley Mao)“借用域名冲突发起的 MitM 攻击：新通用顶级域时代的原因分析和漏洞评估。”2016 年 IEEE 安全与隐私 (SP) 讨论会（2016 年 5 月），第 675-690 页，doi:10.1109/sp.2016.46。

[104] ICANN，新通用顶级域网站，https://newgtlds.icann.org/en/program-status/statistics。注：截至 2020 年 12 月 12 日，在最初 1930 个可用的 gTLD 中，只有 9 个仍在处理中。

[105] ICANN“缓解 DNS 命名空间冲突风险第一阶段报告”，2014 年 7 月 6 日，第 6 页，https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf，以及 ICANN“域名冲突事件管理框架”，2014 年 7 月 30 日，第 2-3 页，https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf。

[106] ICANN SSAC，“SAC066：SSAC 针对有关缓解 DNS 命名空间冲突风险的 JAS 第一阶段报告的意见”，2014 年 6 月 6 日，第 4 页，https://www.icann.org/en/system/files/files/sac-066-en.pdf。

[107] 缓解 DNS 命名空间冲突风险第一阶段报告，第 22 页，https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf。

[108] 同上。

SSR2 建议 17：衡量域名冲突

17.1. ICANN 组织应制定框架，总结各类域名冲突的性质和发生频率以及所产生的问题。该框架应包括具体衡量标准和若干机制，用于衡量控制性中断在多大程度上可成功识别并消除域名冲突。可通过启用受保护的域名冲突披露实例这一机制来提供支持。此框架应允许适当处理敏感数据和安全威胁。

17.2. ICANN 社群应制定一项明确的政策，用于避免和处理与新 gTLD 相关的域名冲突，并在下一轮 gTLD 相关工作启动之前实施该政策。ICANN 组织应确保由与 gTLD 扩展没有财务利益关系的相关方来评估该政策。

当 ICANN 组织通过确定衡量标准和设计机制制定一个框架，用于撰写域名冲突性质和频率以及由此引发的担忧的研究结果，从而衡量控制性中断机制的成效时，可以认为已实施这项建议。

当 ICANN 组织和社群能够检测、应对，并最终尽可能减少域名冲突的存在，同时针对不断演变的域名冲突情况做出适当的响应时，可以认为这项建议有效。

这项建议必须在启动下一轮次 gTLD 之前完成。

2. 研究和简报

目前，学术研究社群正在大量开展与命名、路由和寻址层中的 SSR 问题相关的研究活动。ICANN 社群有机会利用此类研究活动和专业知识为政策制定和技术开发提供信息，这将显著减少 DNS 生态系统中与 SSR 相关的危害。但是，现在没有一个职能部门可确保 ICANN 组织本身及其服务的社群能够及时了解这些研究的最新进展情况。

SSR2 建议 18：为政策辩论提供信息

18.1. ICANN 组织应跟踪同行评审研究社群中的进展，主要应当关注网络和安全研究会议，其中至少包括 ACM CCS、ACM Internet Measurement Conference（ACM 互联网衡量标准会议）、Usenix Security（Usenix 安全）、CCR、SIGCOMM、IEEE 安全与隐私讨论会、运营安全会议，以及事故响应和安全团队论坛 (FIRST)，并发布一份概述报告以总结与 ICANN 组织或签约方行为有关的出版物的结论，供 ICANN 社群参阅。[109]

[109] 会议链接：ACM CCS <https://dl.acm.org/conference/ccs>，ACM 互联网衡量标准会议 <https://www.sigcomm.org/events/imc-conference>，Usenix 安全 <https://www.usenix.org/conferences>，CCR <https://www.ccrsummit.com/>，SIGCOMM <https://www.sigcomm.org/>，IEEE 安全与隐私讨论会 <https://www.ieee-security.org/index.html>，事故响应和安全团队论坛 (FIRST) <https://www.first.org/>。注：建议的实施方式是与组织方（技术项目委员会主席、指导小组组织方等）联系，在某个 ICANN 社群活

18.2. ICANN 组织应确保此类报告中包含可能与可行措施建议相关的观察结果（包括针对与注册管理机构和注册服务机构签署的合同进行的更改），这些措施应有助于缓解、预防或纠正同行评审文献中指出的消费者和基础架构所遭受的 SSR 损害。

18.3. ICANN 组织应确保这些报告中还包含开展其他研究的建议，以确认经过同行评审的研究结果，其中应介绍社群需要哪些数据才能开展其他研究，以及 ICANN 组织如何为代理提供协助以通过 CZDS 来访问此类数据。

当 ICANN 组织编写并维护来自各种网络和安全研究会议的摘要或回顾会议的公共存档时，可以认为已实施这项建议。

当政策制定者可以更容易地获取研究社群关于 SSR 相关问题的研究成果的信息时，可以认为这项建议有效。

3. DNS 试验床

由于 DNS 生态系统已经非常庞大且仍在不断扩大，维护并监控用于分析 DNS 行为和交互的回归测试套件和试验床至关重要。SSR2 审核小组得出的结论是，OCTO 持续开展的 DNS 试验床一旦完成，将足以解决这方面的关切。[110]审核小组进一步指出，应要求 ICANN 组织为此试验床提供支持和维护（并提供测试结果和研究发现的摘要）。

及时完成并维护这个试验床，让 ICANN 社群能够测试和研究解析器行为，这是确保 DNS 的完整性和全球可用性至关重要的一个环节。

SSR2 建议 19：完成 DNS 回归测试套件的开发工作

19.1. ICANN 组织应完成 DNS 解析器行为测试套件的开发工作。

19.2. ICANN 组织应确保实施并维护这项继续针对不同配置和软件版本进行功能测试的性能。

当 ICANN 组织完成开发用于社群测试和针对解析器行为研究的公众可访问的测试套件时，可以认为已实施这项建议。

当开发了一个年度更新的测试套件，可协助确保 DNS 的完整性和全球可用性时，可以认为这项建议有效。

动中，要求提供会议记录摘要和/或邀请与会的委员会成员每年介绍其参加的会议摘要。在实施这项建议时，ICANN 组织应将回顾会议内容保留在存档报告中。

[110] “解析器试验床”，ICANN GitHub 库，https://github.com/icann/resolver-testbed。

4. 根区和注册管理机构问题

A. 密钥滚动更新

自确立特定畸形根区域 (DURZ) 密钥以来，根区 DNSSEC 密钥签名密钥 (KSK) 于 2018 年 10 月 11 日首次轮转。[111] 在轮转过程中，开展了大量辩论并召开电话会议来分析轮转细节。[112] SSR2 审核小组的一个分析结果是，他们了解到，要安全且成功地进行密钥轮转，需要在程序中正常运行例外路径。[113] 尽管 ICANN 组织采用衡量标准来缓解担忧，但 ICANN 组织仍将轮转推迟了一年。ICANN 社群内已经开始讨论关于未来轮转的时间和程序，包括对潜在的新算法轮转的复杂性的考量。[114] ICANN 组织随后又举行公开电话会议，征询关于计划的下一轮次 KSK 轮转流程的意见。[115]

由于现在（以及未来）源自 DNSSEC 签名的根区的安全保护非常重要，因此务必实施正式的可验证流程来开展分析，以确保在根区 KSK 密钥轮转过程中用于维护 DNSSEC 保护的流程的安全、稳定与弹性。[116] 正式流程建模采用方法和/或编程环境来指定流程中的每项任务，评估任务执行情况（成功、失败、其他等），以及指定不同结果下的后续操作。像这样的流程规范已显示出它在复杂的人际交互过程（包括选举安全、医疗流程安全等）中的效用。[117] 在这些情况下，人员任务（人工操作方面）比较复杂，采用了正式的流程规范语言建模，同时对关键（性命攸关）的选择和后果进行了象征性地建模和正式跟踪。这种建模方式允许对应该做什么，以及选择的预期后

[111] ICANN“首轮根区密钥签名密钥 (KSK) 轮转圆满结束”，2018 年 10 月 15 日，https://www.icann.org/news/announcement-2018-10-15-en。

[112] ICANN“最近实行的 KSK 轮转：摘要和后续步骤”，ICANN 博客，2018 年 1 月 30 日，https://www.icann.org/news/blog/the-recent-ksk-rollover-summary-and-next-steps，以及莫瑞兹 • 穆勒 (Moritz Müller)、马修 • 托马斯、杜亚尼 • 韦瑟尔 (Duane Wessels)、维斯 • 哈达克 (Wes Hardaker)、钟大江 (Taejoong Chung)、威勒姆 • 图洛普 (Willem Toorop)、罗兰 • 维 • 斯维克-德吉 (Roland van Rijswijk-Deij)，“轮转根区：对首次 DNSSEC 根 KSK 轮转的全面分析”，2019 年 10 月，https://dl.acm.org/doi/10.1145/3355369.3355570。

[113] SSR2 第 97 次全体会议文稿 - AM 会议，2020 年 1 月 17 日，第 35 页，https://community.icann.org/x/HJkzBw。

[114] 公众意见员工报告程序：针对今后根区密钥签名密钥 (KSK) 轮转的提案，2020 年 8 月 7 日，https://www.icann.org/en/system/files/files/report-comments-proposal-future-rz-ksk-rollovers-07aug20-en.pdf。注：日本注册管理机构服务、ICANN 企业选区、ICANN 非商业利益相关方团体、ICANN 根服务器系统咨询委员会、ICANN 安全与稳定咨询委员会，以及若干个人都提出了意见。

[115] “针对今后根区密钥签名密钥 (KSK) 轮转的提案”，2019 年 11 月 1 日， https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en。

[116] 埃里克 • 奥斯特维尔“网络安全行将终结：在失去它之前充分利用。”*IEEE 安全和隐私部*，卷 18，第 4 辑（2020 年）：第 67-70 页。

[117] 里昂 • J. • 奥斯特威尔 (Leon J.Osterweil)、马特 • 比什 (Matt Bishop)、海瑟 • 康博伊 (Heather Conboy)、洪潘 (Huong Phan)、鲍里斯拉瓦 • I. • 西米奇耶娃 (Borislava I. Simidchieva)、乔治 • 阿夫鲁宁 (George Avrunin)、罗瑞 • A. • 克拉克 (Lori A. Clarke) 和肖恩 • 佩塞特 (Sean Peisert)，“旨在改进关键的人员密集型流程之重要属性的迭代分析：选举安全示例”，ACM 隐私及安全性事务 (TOPS)，卷 20，第 2 辑，2017 年 5 月，第 5 张幻灯片：1-31，(UM-CS-2016-012)，以及罗瑞 • A. • 克拉克、姚辰 (Yao Chen)、乔治 • S. • 阿夫鲁宁、陈斌 (Bin Chen)、雷切尔 • 科布雷 (Rachel Cobleigh)、吉姆 • 雷德里克 (Kim Frederick)、伊丽莎白 • A. • 亨尼曼 (Elizabeth A. Henneman) 以及里昂 • J. • 奥斯特威尔，“对流程进行编程为医疗安全提供支持：关于输血的案例研究。”软件流程研讨会，第 347-359 页。施普林格柏林海德堡出版社，2005 年。

果、期望和成功执行结果进行定量描述和定性规定。[118] 与选举和医疗流程相比，DNS 根区 KSK 轮转本身是一个相对容易管理的流程，这个流程的安全性和正确性对全球 DNS 至关重要。

SSR2 建议 20：用于指导密钥轮转的正式程序

20.1. ICANN 组织应通过正式流程建模工具和建模语言的支持，制定所需的正式流程，以详细说明后续密钥轮转的细节，包括决策点、例外路径、完整的控制流等等。对密钥轮转流程进行验证时，应发布编程过程（例如程序、有限状态机 (FSM)）以征询公众意见，并且 ICANN 组织应收集社群反馈意见。该流程的每个阶段都应具有凭借经验可验证的验收标准，只有达到这些标准，流程才能正常运行。该流程应接受反复评估，评估频率通常不应低于轮转本身的频率（即，相同的频率），以便 ICANN 组织能够及时运用已吸取的经验教训对流程进行调整。

20.2. ICANN 组织应组建一个由来自 ICANN 组织或社群的相关人员构成的利益相关方小组，该小组定期依照根区密钥签名密钥 (KSK) 轮转流程运行桌面演练。

当 ICANN 组织制定正式的流程和验证机制，在每次密钥轮转后提供对密钥轮转流程的验证，且当 ICANN 组织开始定期开展桌面演习来测试密钥轮转流程并使参与者熟悉这个流程时，可以认为已实施这项建议。

当可以正式验证根区 KSK 密钥轮转期间用于维护 DNSSEC 保护的流程的安全、稳定与弹性 (SSR) 时，可以认为这项建议有效。

完成每次密钥轮转都必须参考这项建议。

B. 根区变更管理

SSR2 审核小组指出，PTI 在实施机制以降低操纵 TLD 数据和根区的可能性方面做得很好。[119] 根区管理按照一套工作流程系统来管理根区的 TLD 标签，该系统称为根区管理系统 (RZMS)。这个工作流程采用保守的方法来管理变更，因为每项变更都需要多个相关方进行审核。[120]

[118] 旨在改进关键的人员密集型流程之重要属性的迭代分析：选举安全示例，Leon J.Osterweil、Matt Bishop、Heather Conboy、Huong Phan、Borislava I.Simidchieva、George Avrunin、Lori A.Clarke、Sean Peisert，《ACM Transactions on Privacy and Security》(ACM 隐私及安全性事务，TOPS），卷 20，第 2 辑，2017 年 5 月，第 5 张幻灯片：1-31。(UM-CS-2016-012)。

[119] 珍妮弗 • 布莱斯发送至 SSR2 审核小组电子邮件清单的邮件，2019 年 3 月 27 日，主题：DNS SSR 答复，https://mm.icann.org/pipermail/ssr2-review/2019-March/001569.html。

[120] 互联网号码分配机构 (IANA)，“根区变更请求流程”，访问时间 2020 年 12 月 8 日，https://www.iana.org/help/root-zone-process。

即使目前没有任何已知的 RZMS 滥用方面的安全性和稳定性问题，但对于 RZMS 工作流程中涉及的所有各方，在身份验证过程中仍可能会发生小规模网络攻击。现在，通过发送明文电子邮件并使用简单的用户名/密码组合访问系统即可完成与 TLD 运营商之间的通信。使用电子邮件时，应实施更严格的变更请求身份验证，并包含多重要素验证 (MFA) 和安全通信（例如，加密）。

IANA 职能部门目前正在构建下一代 RZMS，其中包括对身份验证模型的大量重写。[121] 下一代 RZMS 应包含用于提交和批准请求以及其他功能的强大且安全的身份验证和授权模型，以增强全球 DNS 系统的安全性和稳定性，包括：

- 确保 TLD 数据变更请求的完整性和真实性。
- 在涉及请求管理的所有级别上强制实施安全通信。
- 保持弹性以应对涉及根和 TLD 区域的权威 DNS 服务器的潜在欺骗活动。
- 能够快速响应删除请求（移除 NS 记录或 DS 记录）。
- 考虑（涉及 SSAC 和 RSSAC 评估以及公众批准流程）其他自动化技术检查和程序，以快速修复可能影响 TLD DNS 流畅运营的问题。
- SSAC 和 RSSAC 考虑实施 RFC 8078 以及关于自动化 DNSSEC 授权信任维护 (CDS/CDNSKEY) 的相关更新。[122]

尽管 ICANN 组织之前已宣布开发和实施包含更严格的通信安全要求的新 RZMS 系统，但是 SSR2 审核小组没有发现有关 ICANN 组织计划何时将新系统投入使用的迹象。

SSR2 建议 21：提高与 TLD 运营商的通信安全性

> 21.1. ICANN 组织和 PTI 运营部门应加快实施新的根区管理系统 (RZMS) 关于针对请求的更改进行身份认证和授权的安全措施，并为 TLD 运营商提供利用这些安全措施的机会，特别是 MFA 和加密电子邮件。

当 ICANN 组织和 PTI 拥有包含用于提交和批准请求的健全且安全的认证和授权模型，以及可增强全球 DNS 系统安全性和稳定性的其他功能的新一代 RZMS 时，可以认为已实施这项建议。

当 ICANN 组织通过改进的身份管理程序减少了与滥用 RZMS 有关的潜在安全性和稳定性问题时，可以认为此建议有效。

[121] PTI“ccNSO 成员会议 - IANA 域名职能更新”，ICANN 第 60 届会议，2017 年 10 月 31 日，幻灯片 11-14，https://ccnso.icann.org/sites/default/files/field-attached/presentation-pti-members-31oct17-en.pdf。
[122] 古德蒙德森 • O (Gudmundsson O) 和 P.•胡特斯 (P. Wouters)，“通过 CDS/CDNSKEY 管理源自父系统的 DS 记录”，RFC 8078，DOI 10.17487/RFC8078，2017 年 3 月，<https://www.rfc-editor.org/info/rfc8078>。

C. 根区数据和 IANA 注册管理机构

IANA 注册管理机构包括由互联网工程任务组 (IETF)、互联网研究任务组 (IRTF) 和独立提交流程中的 RFC 指定的关键参数。[123] 这些参数注册管理机构的可用性和正直诚信至关重要，需要通过正式的关键绩效指标 (KPI) 向社群明确说明。当前，社群无法获取 ICANN 组织提供的有关服务可用性的衡量标准。而利益相关方需要使用该信息来评估在一段时间内这些服务的 SSR 方面的情况。

ICANN 组织还发现，为 DNS 根区创建 KPI（包括 DNSSEC、可用性、完整性、滥用等）是衡量、跟踪以及向社群传达与根区相关的数据趋势的最有效方法。

有用的 KPI 包括但不仅限于：

- 根区的传播延迟更改为实例。
- DNS 根区（包括 DNSSEC、可用性、完整性等），以便第三方可以跟踪 SSR 方面的情况。
- 展示 IANA 注册管理机构的规模、发展和构成以及这些注册管理机构的全球网络可用性的措施。

SSR2 建议 22：服务衡量标准

> 22.1. 对于 ICANN 组织权威管辖的每项服务（包括根区服务、gTLD 相关服务以及 IANA 注册管理机构），ICANN 组织应创建一个统计信息和衡量标准列表来反映该项服务的运营状态（例如，可用性以及响应性），并在 icann.org 网站的单个页面上，例如，Open Data Platform（开放数据平台）下发布这些服务、数据集和衡量标准的目录。ICANN 组织应对这些服务中的每一项进行衡量，作为去年和纵向总结（以阐释基准行为）。
>
> 22.2. ICANN 组织应每年征询社群对这些衡量标准的反馈意见。在每次报告发布后，应审议并公开总结相关反馈，并纳入后续报告。用于衡量这些报告结果的数据和相关方法应妥善存档，并公开发布以促进重复利用。

当 ICANN 组织将 ICANN 组织所支持服务的运营状态衡量标准提供给社群时，可以认为已实施这项建议。

当社群看到 ICANN 组织与 SSR 相关的运营的透明度提高时，可以认为此建议有效。

D. DNS 加密

SSR2 审核小组研究了 DNS 加密领域的两个主题。首先，该小组研究了 DNSSEC 签名从 RSA 算法到椭圆曲线算法的过渡。其次，该小组研究了过渡到后量子数字签名算法的必要性。[124] 为了跟上传统计算技术的最新发展，RSA 密钥的大小需要随着时间的推移而有所增加。或者，DNSSEC 可以从 RSA 转换到椭圆曲线加密 (ECC)，后者使用较小的公钥和签名即可提供相同的安全性。此

[123] IANA，“协议注册程序”，2020 年 1 月 3 日，https://www.iana.org/help/protocol-registration。
[124] 有关该工作组所做研究的详细信息，请参阅“附录 G：加密”。

外，有人担心大规模量子计算机的发明可能会破坏 RSA 和 ECC。在大规模量子计算机实现之前，DNSSEC 需要转换为一种量子安全算法。ICANN 组织和 PTI 在 DPS 中没有允许这种转换的规定。

ICANN 组织并非需要考量加密技术预期进展的唯一组织。行业标准组织也在为未来的后量子算法做准备。最有名的活动是 NIST 后量子加密项目，世界各地的研究人员均参与到此项目中，以开发不容易受到量子计算机攻击的新加密原语。[125] 可以预料，该项目还需要数年的时间才能将生成的算法进行标准化，但是该项目肯定正在顺利进行。

与此同时，研究人员一致认为基于哈希的签名具有后量子安全性。互联网研究任务组 (IRTF) 已在其加密技术论坛研究小组 (CFRG) 中指定了这些签名算法，这些算法使用较小的私钥和公钥，且计算成本较低。[126] 然而，由于签名的数量非常大，而私钥只能产生有限数量的签名，这两种特性使得基于哈希的签名在 DNSSEC 环境中不受欢迎。

ICANN 组织的文档并未考虑从当前算法过渡到另一种算法的必要性。这让 ICANN 组织对加密密钥签名算法的预期进展毫无准备。

SSR2 建议 23：算法轮转

> 23.1. PTI 运营部门应更新 DNSSEC 实践声明 (DPS)，以允许从一种数字签名算法过渡到另一种数字签名算法，包括预期的从 RSA 数字签名算法过渡到其他算法或未来的后量子算法，这些算法可提供同等或更高的安全性，并且可保持或增强 DNS 的弹性。
>
> 23.2. 鉴于根区 DNSKEY 算法轮换是一个非常复杂且敏感的流程，PTI 运营部门应与其他根区合作伙伴和全球范围内的社群合作，根据从 2018 年第一次根区 KSK 轮转汲取的经验教训，共同制定用于指导今后根区 DNSKEY 算法轮换的计划。

当 PTI 更新 DPS 以允许从一种数字签名算法过渡到另一种数字签名算法，并制定用于指导今后根区 DNSKEY 算法轮换的计划时，可以认为已实施这项建议。

当 ICANN 组织准备好用于密钥签名的更高级算法（包括增加密钥长度和改变密钥轮转时间）时，可以认为此建议有效。

[125] 国家标准与技术研究院 (NIST) 信息技术实验室计算机安全资源中心，“后量子加密技术”，创建日期 2017 年 1 月 3 日，更新日期 2020 年 11 月 23 日，https://csrc.nist.gov/projects/post-quantum-cryptography。
[126] IRTF，加密技术论坛研究小组，https://irtf.org/cfrg。

5. 紧急后端注册管理运行机构 (EBERO)

EBERO 提供商充当特定灾难恢复基础设施组件，并在提供必要的系统和运营能力以接管无法履行职能的 gTLD 注册管理机构的所有关键职能方面扮演重要角色。

当一个 gTLD 运营商面临无法履行关键注册管理机构职能时，会临时激活一家 EBERO 提供商。[127] 此流程可确保 gTLD 运营商职能的可用性，保护注册人，并为 DNS 提供额外的保护。正如人们所熟知的各种标准（例如 ISO 22301）所指明的那样，最佳实践指南要求定期对灾难恢复流程进行测试（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）。

SSR2 审核小组无法验证 ICANN 组织是否按照“共同过渡流程手册 - 第 3 版”中所述协调了整个 EBERO 流程的必要端到端测试。[128] ICANN 组织和 EBERO 提供商测试了流程的各个部分（一个测试使用 .doosan 进行，另一个测试使用 .mtpc 进行），最近一次测试于 2017 年进行。[129] SSR2 审核小组在会议记录中，而不是在任何专门的 ICANN 网页上找到了这些结果。[130] 审核小组认识到，SSR 审核小组没有权限查看端到端 EBERO 流程测试方法的详细信息；但是，能够验证是否已进行测试并查看这些测试的结果对于提高社群透明度至关重要。

还要值得注意的是，尽管《共同过渡流程手册》中记录了 EBERO 流程，但是由于该文档包含在 EBERO 协议中，因此很难找到。

SSR2 建议 24：提高 EBERO 流程的透明度和改进端到端测试

24.1. ICANN 组织应使用测试计划按预定时间间隔（至少每年一次）协调整个 EBERO 流程的端到端测试，测试计划包括用于测试的数据集、进展状态以及截止日期，同时应提前与 ICANN 签约方协调，以确保所有例外条款得到执行并公布测试结果。

[127] ICANN，“紧急后端注册管理运行机构”，未注明发布日期，https://www.icann.org/resources/pages/ebero-2013-04-02-en。
[128] ICANN，“紧急后端注册管理运行机构协议”，2019 年 8 月，https://www.icann.org/en/system/files/files/cira-ebero-15aug19-en.pdf。注：请参阅附录 B - 共同过渡流程。
[129] ICANN，EBERO 演习报告，ICANN 第 55 届技术日上的演讲，2016 年 3 月 7 日，https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ebero-07mar16-en.pdf，以及凯文 • 墨菲 (Kevin Murphy)“紧急注册管理机构第二次测试已停用的 .brand”，Domain Incite，2017 年 4 月 27 日，http://domainincite.com/21724-second-emergency-registry-tested-with-dead-dot-brand。
[130] 弗朗西斯科 • 阿瑞亚斯 (Francisco Arias)，“EBERO 演习”，在 ICANN 第 60 届技术日上的演讲，2017 年 10 月 30 日，https://ccnso.icann.org/sites/default/files/field-attached/presentation-ebero-exercises-30oct17-en.pdf。

24.2. ICANN 组织应在 EBERO 网站上提供链接，以便用户更容易找到《共同过渡流程手册》。

当 ICANN 组织协调了整个 EBERO 流程的年度端到端测试以及结果的公共文档时，可以认为已实施这项建议。

当 ICANN 组织能够验证 EBERO 流程是否按预期运行，保护注册人并为 DNS 提供额外的保护时，可以认为此建议有效。

附录 A：进一步推荐

在整个审核过程中，SSR2 审核小组注意到，一些领域中的变更将能够提高未来审核小组的工作效率和能力。尽管这些项目不在审核小组的职责范围内，但我们希望 ICANN 组织可以将以下推荐项作为意见和建议纳入到未来的审核工作中。这些推荐项按优先级顺序列出。

推荐 1

ICANN 组织应针对每个审核小组提出的建议实施在线进度跟踪职能。通过在整个实施过程中提供在线进度可视性，整个社群可以观察实施详细信息，并就任何不足之处提供反馈意见。要实现所需的透明度和可视化，需要提供比当前在 CCT 实施网页上显示的更详细的实施规划和进展情况。[131] SSR2 审核小组认为，如果已针对 SSR1 审核小组建议的实施履行了这项职能，建议 1 就没有必要了。此外，基于 CCT 实施管理人的概念，ICANN 组织应向提出建议的审核小组成员提供季度报告，让审核小组成员自己就实施是否产生预期效果定期提供反馈意见，并避免下一代审核小组在评估实施时遇到问题。SSR2 审核小组认为，如果在成立 SSR2 审核小组之前就有此类职能，那么 SSR1 审核小组建议的评估就会很简单直观。

推荐 2

为避免造成误解和期望破灭，ICANN 组织应制定清晰的书面流程，为审核小组获取合同资源，包括里程碑和要点，以供审核小组批准。每个审核小组都需要一名技术撰稿人，因此 ICANN 组织应从审核小组的第一次会议开始，就向该审核小组提供一名技术撰稿人。

推荐 3

为便于在公共评议期结束后不久进行调查，以及“*满足日益增长的包容性、问责制和透明度需求*”（如战略目标 2.1 中所述），SSR2 审核小组推荐 ICANN 组织创建一个电子邮件清单，以发布有关公共评议期的公告。目前，查找有关公众意见的信息可能非常具有挑战性。实施此推荐项将有助于提高公共评议期的电子邮件清单订阅者的意识，而无需开展其他工作。这些邮件的存在可让未来审核小组的成员以及其他相关方通过易用的邮件存档搜索工具，轻松查找相关信息。

[131] ICANN，“竞争、消费者信任和消费者选择审核小组 (CCT-RT) 获批建议 - 实施计划和后续工作现已出炉”，访问时间 2020 年 12 月 19 日，https://www.icann.org/public-comments/cct-rt-implementation-plan-2019-09-11-en。

SSR2 审核小组推荐，ICANN 组织应该在每个公共评议期至少向此电子邮件清单发送三封邮件。第一封邮件应在公共评议期开始时发送，其中应包含指向相关草案文档的稳定 URL。第二封邮件应在公共评议期结束时发送，其中应包含指向已提交意见集合的稳定 URL。第三封邮件应指明是否达成共识，如果达成共识，则还应包含指向最终文档的稳定 URL。其他邮件也可能有用，例如关于公共评议期延期的邮件。此外，SSR2 审核小组还推荐 ICANN 组织创建一个专用于列出所有公开征求意见的网页，然后将其链接到相关文档的页面。

推荐 4

为了使安全性相关的讨论透明化，ICANN 组织应考虑建立一个开放的信息保证平台，以共享安全性和滥用信息，进而更流畅、更快速地披露信息。

附录 B：定义和缩略语

定义

这类评估需要对审核相关的关键术语有共同的理解。最初，SSR2 审核小组遵循以下定义运营：[132]

- 滥用：请参阅下面的“DNS 滥用”
- 商业电子邮件诈骗 (BEC)：一种针对公司的诈骗，犯罪分子伪造或骗取员工的电子邮件帐户以进行欺诈性电汇行为。
- 僵尸网络：感染了恶意软件并在计算机所有者不知情的情况下被整体控制的计算机网络。
- 数字证书欺诈：攻击者违反证书颁发机构 (CA) 规定生成并获取欺诈性证书来发起进一步攻击；攻击者还可以使用欺诈性证书以另一个人或系统的身份进行身份验证，或伪造数字签名。
- 分布式拒绝服务 (DDoS) 攻击：一种恶意攻击，企图通过来自多个（分布式）源的大量互联网流量淹没目标或其周围基础设施，以此来破坏目标服务器、服务或网络。
- DNS 滥用：将 DNS 提供的通用标识符恶意滥用于网络犯罪基础设施，并将用户引至可能存在其他形式犯罪的网站，如儿童剥削、知识产权侵权和欺诈。
- 域名系统 (DNS)：DNS 是一种分布式在线数据库服务，可将易于记忆的域名转译为数字互联网协议 (IP) 地址；例如，DNS 会将 www.icann.org 转译为 192.0.34.65（如 RFC 1034 和 1035 中所述）。
- 标识符系统安全、稳定与弹性 (IS-SSR) 框架：定期更新的文档，“描述了 ICANN 在支持统一的全球互用性互联网方面的职责和职能界限，以及互联网的唯一标识符系统所面临的挑战。”
- 恶意软件：专为破坏、损坏或未经授权访问计算机系统而设计的软件。
- 网络钓鱼：通过在电子通信中伪装成可信赖的实体来获取敏感信息的欺诈性行为。
- 勒索软件：除非支付一定金额，否则就会阻止访问计算机系统的恶意软件。
- 弹性：标识符系统在不中断或停止服务的情况下，有效抵御、经受恶意攻击及其他干扰事件并在此之后继续正常运行的能力。
- 诈骗：伪装成旨在赚钱的真实商业活动或投资机会的欺诈性的骗局。
- 安全性：保护互联网唯一标识符以防止其被滥用的能力。
- 安全威胁：网络钓鱼、诈骗、恶意软件、勒索软件、垃圾邮件、DDoS 攻击、数字证书欺诈以及僵尸网络是最主要的安全威胁。
- 垃圾邮件：未经允许的批量发送的电子邮件。
- 稳定性：确保标识符系统能正常运行且唯一标识符的用户相信系统能够正常运行的能力。
- 唯一标识符：ICANN 的技术使命包括从总体上帮助协调互联网唯一标识符系统的分配：具体来说就是顶级域名、分配给地区互联网注册管理机构的互联网协议 (IP) 地址段和自治系统 (AS) 号码，以及 IETF 指示的协议参数。

[132] ICANN，“SSR 职责和职权范围”，访问时间 2019 年 12 月 27 日，https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en。

缩略语

- AS：自治系统
- BC：业务连续性
- CISO：首席信息安全官
- CSO：首席安全官
- CZDS：集中化域资料服务
- DAAR：域名滥用活动报告
- DNS：域名系统
- DNSSEC：DNS 安全扩展（如 RFC 4033、4034 和 RFC 4035 中所述）
- DoH：基于 HTTPS 的 DNS
- DoT：基于 TLS 的 DNS
- DPS：DNSSEC 实践声明
- DR：灾难恢复
- DURZ：特定畸形根区域
- EBERO：域名注册管理后端应急运行机构
- EPDP：快速政策制定流程
- FSM：有限状态机
- gTLD：通用顶级域
- GNSO：通用名称支持组织
- HTTP：超文本传输协议
- HTTPS：安全超文本传输协议
- IANA：互联网号码分配机构
- IETF：互联网工程任务组
- IMRS：ICANN 管理的根服务器
- IP：互联网协议
- IRTF：互联网研究任务组
- IS-SSR 框架：互联网标识符系统安全、稳定和弹性 (IS-SSR) 框架
- ISMS：信息安全管理系统
- ISO：国际标准化组织
- ITIL：IT 基础设施库
- KSK：密钥签名密钥
- NCAP：域名冲突分析项目
- NIST：国家标准与技术研究院
- OCTO：首席技术官办公室
- PII：个人验证信息
- PTI：公共技术标识符
- RDS：注册目录服务
- RAA：注册服务机构认证协议
- RAPWG：注册滥用政策工作组
- RDAP：注册数据访问协议

- RSSAC：根服务器系统咨询委员会
- SADAG：通用顶级域 (gTLD) 中域名系统 (DNS) 滥用的统计数据分析
- SMART：具体、可衡量、可分配、相关且可跟踪
- SOP：战略和运营规划
- SSAC：安全与稳定咨询委员会
- SSAE：关于鉴证约定标准的声明
- SSR：安全、稳定与弹性
- SSR1：第一轮 SSR 审核流程
- SSR2：第二轮 SSR 审核流程
- TLS：安全传输层协议

附录 C：流程和方法

审核 SSR1 建议的流程和方法

下面概述的 SSR2 审核小组的评估流程是基于以下内容编写而成的：负责实施的 ICANN 组织员工提供的简报以及同他们的讨论；对 ICANN 组织创建的大量相关 ICANN 文件和实施报告的系统审核；以及其他研究和访谈。[133]该小组还利用在巴塞罗那和神户举行的 ICANN 公共会议期间的外展会议来与相关社群利益相关方进行联络。评估根据具体建议尽可能定量和定性。

很多 SSR1 建议都是高度概括，缺乏明确性。SSR2 审核小组无权访问和分析 ICANN 的内部工作，因此该工作组要求 ICANN 组织向 SSR2 审核小组成员提供其实施规划以及有关成功实施的证据。这些建议本身以及 ICANN 组织提供的文档缺乏明确的 KPI 和目标、可衡量目标以及实施规划。这导致衡量或跟踪实施具有挑战性。此外，一些建议的措辞还有解释的余地。这有时候会导致 SSR2 小组对建议的理解与 ICANN 组织员工不一致。

在 2017 年，ICANN 组织员工就针对每项建议向审核小组提供了有关实施的初始答复，并报告了他们实施 SSR1 建议的方式。ICANN 的工作人员引用了网页或文件，整理了 ICANN 组织内不同部门的演示文稿，并在 9 个月的时间里向审核小组提供了有关建议的简报。审核小组还审核了与此次审核相关的大量背景文档。审核小组与 ICANN 组织员工进行了访谈，要求提供更多信息，并利用利益相关方的意见以及自己的研究成果，在适当的情况下进行了进一步研究。

收到 ICANN 组织对所提交问题的答复，并尽其所能完成其研究和尽职调查后，该审核小组在 2018 年下半年针对每项建议起草了评估草案，并在线上会议、小组每周的电话会议以及面对面会议上就评估草案进行了讨论。该小组根据需要对文本进行了编辑，并批准了每项 SSR1 建议的结论和调查结果，意在将其纳入 SSR2 工作组报告草案，附上工作组批准的协商一致协议，并在适用的情况下指出少数群体的反对意见。

在线上会议和电话会议上讨论并多次修改评估草案后，工作组决定按照以下方法来整理评估草案，这种方法重点关注任务完成情况、相关性以及所需的进一步工作这几个方面：

1. 为实施建议开展了哪些工作？
2. 建议是否已得到完全实施？
3. 实施是否达到了预期的效果？
4. 评估是如何进行的？
5. 该建议目前是否仍然有意义？
6. 如果是，还需要开展哪些进一步的工作？如果不是，理由是什么？

[133] ICANN SSR2 审核小组维基页面，https://community.icann.org/display/SSR/SSR2+Review。请特别参阅背景资料和简报材料。

第一个问题涉及到 ICANN 组织为实施建议所开展的工作。第二个问题是工作组在“充分实施日期”之前对员工提供的实施级别进行评估。工作组遇到过很多似乎只得到部分实施或缺少实施规划的建议。在这些情况下，工作组确定了需要改进的具体方面。在某些情况下，由于缺少实施规划、文档和绩效指标，因而难以建立成功实施所需的明确先决条件和目标。第三个问题涉及到实施是否达到预期效果，以及达到预期效果的程度。第四个问题涉及到 SSR2 工作组如何进行评估。读者可以在每项建议的基础上跟踪工作组所使用的文档和其他证据。根据问题五，工作组还评估了每项建议在 2018 年是否仍然有意义。最后，工作组根据当前情况决定是否需要开展额外的工作来实施这种形式的建议，然后将自己的建议告知 SSR2 工作组。

ICANN SSR、DNS SSR 的流程和方法以及未来面临的挑战

SSR2 审核小组与 ICANN 组织员工进行了一系列访谈。[134] 问题集中在 ICANN 组织安全流程的完整性和有效性，以及 ICANN 组织安全框架的有效性方面。

SSR2 审核小组围绕一个特定流程进行了组织，以确认调查结果并制定建议以供 ICANN 审议，其中包括：

- 审核、分析和总结相关文档。
- 在已确定的问题领域进行调查。
- 视情况进行相关访谈。
- 起草依据、调查结果和建议的摘要。

第 2 工作阶段侧重于 ICANN 组织内部的 SSR 问题，而第 3 工作阶段则侧重于全球标识符系统的 SSR：全球 DNS、IANA 编号数据库（IP 分配和 ASN）以及 IANA 协议注册管理机构。审核小组专门审议了有关 DNS 风险、威胁和滥用的报告和其他意见，然后将结果数据提供给相关的 ICANN 组织、流程和政策机构。

在有关 SSR 未来面临的挑战的第 4 工作阶段中，SSR2 审核小组审议了关于 DNS 滥用的当前研究、DNS 中设备类型和数量持续增长的影响、新兴技术、在其他工作阶段中确定的可能对未来产生影响的问题领域，以及 ICANN 用于分析和减少威胁的制度化方法。

SSR2 审核小组认识到，此工作流程依赖于其他相关领域中新出现的主题。更具体地说，除了共同确定的挑战之外，DNS 的稳定性和弹性还会遇到工作阶段中与 ICANN SSR 和 DNS SSR 相关的其他特定挑战。

[134] ICANN SSR2 审核小组维基页面，https://community.icann.org/display/SSR/SSR2+Review。请特别参阅简报材料。

附录 D：与 SSR1 建议相关的审核结果

这部分包括对每项 SSR1 建议的详细评估。这里的审核结果讨论了具体实施、问题以及工作组对开展进一步工作的想法。SSR2 审核小组指出了以下重复出现的问题：

1. 目前还缺乏能够让社群和 ICANN 组织跟踪和了解安全领域和自身活动的指标、衡量标准和目标点。

2. 缺乏公开可用的证据、定义和流程，这妨碍了对 SSR 活动的观察，进而导致大家对正在开展的工作，开展工作的时间、对象和方式都没有明确的认知。

3. 缺乏社群审核和问责制，剥夺了 ICANN 社群就 SSR 问题提供意见的机会。

4. ICANN 组织目前没有一个总体战略、可确定的目标或明确而全面的 SSR 政策。如果没有有效的 SSR 战略和集成的安全与风险管理（例如政策、程序、标准、基准、准则），就无法分配、衡量和跟进 SSR 相关的职责，从而导致缺乏透明度和问责制。

SSR1 建议 1

“ICANN 应就其 SSR 职权范围和有限的技术使命发布一个明确且一致的声明。ICANN 应征求并获取公众反馈意见，以发布基于共识的声明。”

SSR2 结论：此建议仍然有意义，因为该建议已得到部分实施但并未达到预期效果，也就是尚未发布一份描述 ICANN 组织的 SSR 职权范围和技术使命的基于共识的明确且一致的声明。

依据：

- 工作组发现存在声明，并且 ICANN 组织在社群进行审核之后更新了该声明（但不再维护）。[135] 尽管存在此声明以及其对“安全、稳定与弹性”的明确定义，但这些定义的使用仍存在不一致。与有权查看 ICANN 组织与各个签约方签署的合同文本的工作组成员开展的单方会谈已指明，ICANN 组织的协议中所使用的“安全”和“稳定”的定义与签约方所使用的定义不同。[136]

[135] SSR 职责和职权范围，https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en，以及“DNS 审核小组的安全、稳定与弹性 - 报告草案：公众意见报告”，上次修改时间 2012 年 5 月 18 日，http://www.icann.org/en/system/files/files/report-comments-ssr-rt-draft-report-18may12-en.pdf。

[136] 另请参阅新通用顶级域基本协议第 7.3 节 https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html 与 ICANN 组织对 S&S 的定义 https://www.icann.org/groups/ssac

- 目前并未提供任何指标来评估实施是否达到了就其 SSR 职权范围和有限的技术使命提供明确且一致信息的预期效果。鉴于术语“SSR”在整个 ICANN 中的使用方式不同，因而并未形成 SSR1 审核小组所期望的通用定义。

SSR1 建议 2

“应该审核 ICANN 对其 SSR 职权范围和有限的技术使命的定义和实施情况，以保持共识并从社群征询反馈意见。应该定期重复此流程，也许可以与未来轮次的 SSR 审核同时进行。”

SSR2 结论：此建议仍然适用，并且尚未得到充分实施。未实现对 ICANN 组织的 SSR 职权范围和相关技术使命进行定期公开审核的预期效果。

依据：

- SSR2 审核小组并没有找到证据证明已定期对 SSR 职权范围进行审核。自 2013 年以来，一直没有机会专门对职权范围和使命声明发表意见。

SSR1 建议 3

“在 ICANN 针对其 SSR 职权范围和有限的技术使命发布以共识为基础的声明后，ICANN 应该在所有材料中使用本声明中的一致术语和描述。”

SSR2 结论：此建议仍然适用，但尚未得到充分实施。未实现将一致的术语和一系列说明整合到 SSR 相关资料中的预期效果。

请参阅 SSR2 建议 13：在原有 SSR1 建议的基础上，增加 SSR2 建议的滥用投诉报告的透明度和问责制。

依据：

- 2013 年 7 月发布的博文列出了 ICANN 组织向整个社群提供的安全术语；然而，这些定义并未一致地整合到其他与 SSR 相关的文档中。[137]
- ICANN 组织关于此建议的员工报告表明，作为战略和运营规划 (SOP) 的一部分，员工会持续不断地将关键术语添加到 ICANN 组织的公共术语表中；随着 SSR 活动的进展，术语和说明将作为 SOP 的一部分进行更新。但是，自 2014 年 2 月以来，术语表（可在上述博文中找到）一直未更新。

[137] ICANN，“ICANN 的安全术语”，博文，上次修改时间 2013 年 7 月 8 日，https://www.icann.org/news/blog/icann-s-security-terminology。

SSR1 建议 4

“ICANN 应记录并明确定义其在 ICANN 社群内的 SSR 关系的性质，以便为了解组织之间的相互依赖关系提供一个关注点。”

SSR2 结论：此建议仍然适用，但尚未得到充分实施。未实现提供可描述 ICANN 组织的 SSR 关系的公开透明资源的预期效果。

请参阅 SSR2 建议 2：对于在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理。

依据：

- ICANN 组织员工为 SSR2 审核小组创建了一份文档，用于跟踪 ICANN 与 SSR 相关的职责与义务，并列出与 ICANN 组织建立了正式关系的每个组织。[138] 该文档包含对可支持每种关系的文档的特定引用，以及对该关系中 SSR 部分的说明。但是，该文档中列出的许多引用无法在网上找到。该文档通常将关系的 SSR 部分显示为“未知”。

SSR1 建议 5

“ICANN 应使用其 SSR 关系的定义来维持有效的工作安排，并展示如何利用这些关系来实现每个 SSR 目标。”

SSR2 结论：此建议仍然适用，但尚未得到充分实施。审核小组无法确定 ICANN 组织是否实现了进行有效的工作安排以支持每个 SSR 目标的预期效果。

请参阅 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

依据：

- 审核小组期望 IS-SSR 框架中包含有关如何使用 SSR1 建议 4 中要求的重要关系来实现 SSR 目标的信息；但是无法轻易获得此信息。[139]
- SSR2 工作组缺乏充足的信息来评估工作关系是否有效。

[138] “SSR 关系”，ICANN，2017 年 1 月 23 日，https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf。
[139] 同上。

SSR1 建议 6

“ICANN 应发布一份文档，明确列出 SSAC 和 RSSAC 的职责与义务，以便清楚界定这两个群体的活动。ICANN 应在这两个群体之间寻求共识，承认各自形成的历史和环境。ICANN 应该考虑为这两个群体提供适当的资源，以满足这两个群体的需求。”

SSR2 结论：此建议仍然适用，但尚未得到实施。ICANN 组织未实现向所有利益相关方明确阐明 SSAC 和 RSSAC 职责的预期效果。

依据：

- SSAC 和 RSSAC 的职责与义务已记录在文档中。[140] 但是，此公开文档仍标记为“处于审核阶段的草案”。针对这项建议的相关工作似乎已经开展，但是，该实施工作最后并没有涉及对 SSAC 和 RSSAC 的组织审核。如果已达成共识，那么 SSR2 审核小组找不到最终文档。
- 该文档是基于 IANA 管理权移交之前的《ICANN 章程》编写而成的。《章程》中描述 SSAC 和 RSSAC 的部分基本相同，但现在已经明确指出，RSSAC 负责对“董事会的信息索求或意见”进行回复。此更新并未解决《ICANN 章程》中 SSAC 和 RSSAC 之间的职责与义务重叠的潜在问题：

  > *“SSAC 负责就互联网名称和地址分配系统的安全性和完整性事宜向 ICANN 社群和董事会提供建议；*
  >
  > *RSSAC 负责就互联网根服务器系统的运营、管理、安全性和完整性事宜向 ICANN 社群和董事会提供建议。”*

SSR1 建议 7

“ICANN 应在现有 SSR 框架的基础上建立一系列明确的目标，并根据这些目标对其计划和活动进行优先级排序。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。未实现建立明确、公开审核的 SSR 目标以及开展相关的优先级排序工作的预期效果。

请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理，以及 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

[140] ICANN，“处于审核阶段的草案：ICANN 安全与稳定咨询委员会和根服务器系统咨询委员会的职责与义务”，2015 年 3 月 5 日，https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf。

依据：

- 与 SSR 相关的活动将作为战略和运营规划 (SOP) 的一部分定期进行报告，包括在 ICANN 的定期资产组合管理报告和 SSR 季度报告中。[141] SOP 参考了 IS-SSR 框架，该框架包括 SSR 优先事项、目标和活动。但是，该框架已经不再编制，这导致在 SOP 如何考虑 SSR 相关的措施方面留下了空白。自 2016 年最后一次发布 IS-SSR 框架以来，更新与 SSR 相关的文档的流程仍不明确。[142]
- IS-SSR 框架为社群提供了一个宣传 SSR 战略的机会。ICANN 组织不再编制该框架，这导致没有足够的机会来收集所有 ICANN 利益相关方团体关于 ICANN 组织如何处理 SSR 活动的社群意见。
- 安全、稳定与弹性问题的战略规划似乎以首席技术官办公室 (OCTO) 为中心，考虑到 SOP 的存在，RT 认识到 OCTO 内部存在一个围绕 SSR 活动的规划等级。但是，建议中所设想的细节和规划等级并不包括所有 ICANN 组织利益相关方之间进行的平等公开讨论。

SSR1 建议 8

“ICANN 应继续完善其战略规划目标，尤其是维护和推动 DNS 可用性的目标。明确符合框架和战略规划。”

SSR2 结论：尽管此建议目前仍然适用，并且也得到部分实施，但此建议的实施并未实现在 SSR 相关战略和运营工作之间建立更明确联系的预期效果。

请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理，以及 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

依据：

- SSR1 审核实施主页上的可用文档表明，相关报告、战略和程序中已包括并阐明 SSR 指南。[143] 但是，这些可用的报告并没有提供对 SSR 活动的充分分析，并且缺乏有关 SSR 活动的实施和执行的详细信息。
- SOP 并未指明 SOP 中哪些活动、优先级和支出与 SSR 相关。至关重要的是，SSR1 设想的机制已被其他组织和流程工具取代，这让评估和实施变得复杂。

[141] ICANN，“ICANN《2021-2025 财年战略规划》”，未注明发布日期，https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf，以及戴夫 • 匹斯特洛，“标识符系统 SSR 活动报告”，ICANN 博文，上次修改时间 2015 年 1 月 21 日，https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en。

[142] ICANN 2015 - 2016 财年 IS-SSR 框架，https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf。

[143] SSR1 审核实施主页，维基页面，上次更新时间 2017 年 8 月 22 日，https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home。

SSR1 建议 9

“ICANN 应当根据普遍接受的国际标准（如 ITIL、ISO 和 SAS-70）来评估为其各项运营职能设置的认证方案。ICANN 应发布一份明确的认证路线图。”

SSR2 结论：该建议仍然适用。SSR2 审核小组无法确定此建议是否完全实施并实现了预期效果，因为原始建议缺乏有关 ICANN 组织应根据哪个或哪些认证来进行评估，或者寻求实现何种目的的必要明确性。

请参阅 SSR2 建议 4：改进风险管理流程和程序，以及 SSR2 建议 5：对于在原始 SSR1 建议基础上扩展的 SSR2 建议，遵守适当的信息安全管理系统和安全认证规定。

依据：

- 根据与 ICANN 组织员工的访谈，ICANN 组织取得了一些针对 IANA 的认证，例如根区 KSK 系统的 SOC2/3 认证，注册分配和维护系统的 SOC2 认证，以及在根级别实施 DNSSEC 的 SysTrust 认证。[144] 在 IANA 职能之外，ICANN 组织使用 IT 和网络安全中的持续改进框架生成报告，进行年度财务审计，执行 EFQM 年度自我评估和文档审核，并获取专业建议以帮助评估绩效和推动改进。[145]
- ICANN 组织还报告，所有信息安全员工都接受过 SANS 课程的培训。[146]
- ICANN 组织报告称，内部审计的结果只会报告给 ICANN 董事会。[147]
- SSR2 审核小组无法找到任何可用作 SSR 流程认证路线图的文档，进而导致无法进行社群审核。

SSR1 建议 10

“ICANN 应继续努力加强合同合规性的强制执行，并为这一职能提供充足的资源。ICANN 还应制定和实施更加结构化的流程，以监控合规问题和调查。”

SSR2 结论：此建议仍然适用，并且尚未得到充分实施。未实现将充足的资源应用于合同合规性的强制执行，并制定一个持续的结构化流程以监控合规性的预期效果。

请参阅 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，以及 SSR2 建议 9：对于在原始 SSR1 建议基础上扩展的 SSR2 建议，监督并强制实施合规性。

[144] 请参阅工作文档，“SSR2 问题和答案”，未注明发布日期，6，https://community.icann.org/pages/viewpage.action?pageId=64076120S。
[145] 同上，24。
[146] 同上，11。
[147] 同上，6。

依据：

- 此评估基于公开可用的信息（例如合同合规报告页面），以及提供了建议实施相关证据的 ICANN 员工报告。[148] 定期公开报告合规性活动是 ICANN 组织的战略和运营规划 (SOP) 的一部分。ICANN 组织有一个专门的公共页面，用于进行合同合规性报告，其中包括月度、季度和年度数据；可查询连续 13 个月期间内的 10 种不同报告；以及不同工作组明确要求的衡量标准和数据。一些合同合规审计和外展项目现已启动。ICANN 组织在 SSR1 审核之后设立了新职位，以确保实现这一领域的目标和宗旨。
- 通过迁移到 ICANN 组织网站、自动化和启动批量投诉处理工具，更新了投诉机制。此外，ICANN 员工还表示已进行了市场倾向调查。[149] ICANN 组织启动了质量检查，以检查 RDS 数据中的不准确之处。自 2012 年 WHOIS 审核小组建议采取行动以来，RDS 准确度报告的编写工作就一直在进行。
- 尽管《新通用顶级域注册管理机构基本协议》（2017 年 7 月）包含签约方与安全性和稳定性相关的具体义务，并且可帮助进一步的实施，但 2016 年和 2017 年的合规性强制执行报告几乎没有 SSR 强制执行措施的证据。[150] SSR2 审核小组尚不清楚 ICANN 组织减少注册滥用和恶意行为的发生和影响的目标是如何通过合规行动或其他举措来实现的。SSR1 实施员工报告中的大多数问题都强调了与 WHOIS 相关的事项。此外，注册服务机构协议 (RAA 2013) 包含 ICANN 组织针对其运营危及注册服务机构和注册管理机构服务、DNS 或互联网的注册服务机构的模糊执法权。
- ICANN 组织每月发布有关其合规性执法工作的报告，但尚不清楚在合规流程中 SSR 问题得到了何种程度的处理。[151]

SSR1 建议 11

“ICANN 应最终确定并实施与其 SSR 相关计划目标明确有关的 NgTLD 和 IDN 快速通道的成功衡量标准，包括缓解域名滥用机制的有效性的衡量标准。”

SSR2 结论：此建议仍然适用，但无法衡量。尽管已采取措施减少域名滥用，但无法确定该措施是否或者在何种程度上对缓解域名滥用发挥了作用。

[148] 可在以下位置查看 SSR1 实施报告：https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2（第 28-30 页），可在以下位置查看有关此建议的 SSR2- RT 简报：https://community.icann.org/download/attachments/66085372/SSR1%20Compliance%20Briefing%20June%20201 7%20v3.pdf?version=2&modificationDate=1499814488000&api=v2。

[149] 请参阅合并后的 SSR1 实施报告中的“SSR 建议 10 实施”，https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2。

[150] ICANN，2017 年 7 月 31 日，https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf。

[151] 请参阅 ICANN 的“合同合规情况评估”报告，https://features.icann.org/compliance/dashboard/report-list。

尤其是在 NgTLD 扩展之后，自第一轮 SSR 审核小组提出建议以来，DNS 的格局已经发生了变化。然而，与 2011 年一样，将 SSR 考量因素作为管理 DNS 空间的关键成功衡量标准嵌入的建议当前仍然适用，甚至更为适用。

请参阅 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核，以及 SSR2 建议 13：对于在原有 SSR1 建议基础上扩展的 SSR2 建议，增加滥用投诉报告的透明度和问责制。

依据：

- SSR2 审核小组无法找到任何达成社群共识且描述成功衡量标准的文档，包括缓解域名滥用机制的有效性的衡量标准。最近的 CCT 报告和建议也指出缺乏可衡量的标准。[152]
- 新《注册管理机构协议》规范 11 包含注册管理机构的实质性 SSR 义务，其中包括定期进行技术分析和维护统计报告以评估 TLD 中的域是否被用于实施威胁安全的行为（例如网址嫁接、网络钓鱼、恶意软件和僵尸网络）的义务。自 2012 年开放申请以来，这些确切义务就已经成为标准《新 gTLD 注册管理机构协议》的一部分。ICANN 组织有一个合规性图表，但它衡量的是投诉数量和类别。[153] 因为其报告分布在几个页面上，所以很难跟进。

SSR1 建议 12

“ICANN 应与社群合作，确定与 SSR 相关的最佳实践，并通过合同、协议和谅解备忘录 (MOU) 以及其他机制来支持此类实践的实施。”

SSR2 结论：SSR1 建议 12 尚未得到充分实施，而且在当前仍然非常适用。未实现定义并实施与 SSR 相关的最佳实践的预期效果。

请参阅 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，以及 SSR2 建议 9：对于在原始 SSR1 建议基础上扩展的 SSR2 建议，监督并强制实施合规性。

依据：

- 《新注册管理机构协议》(RA) 规范 11 包含注册管理机构的实质性 SSR 义务。自 2012 年开放申请以来，此 RA 中的义务就已经成为了标准《新 gTLD 注册管理机构协议》的一部分。但是，ICANN 组织显然没有将这些规定用作评估其在实现 SSR1 建议 12 目标方面的有效性的基准。
- 题为“标识符系统攻击缓解方法”的报告日期为 2017 年 2 月。这份报告列出了“*在 ICANN 内部以及由整个社群的标识符系统安全专家*”提出的推荐内容。[154] 但是，尚不清楚在实现文

[152] CCT 报告，第 9 页，https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf。
[153] 请参阅 ICANN 合同合规绩效报告，https://features.icann.org/compliance 和“合同合规情况评估”报告，https://features.icann.org/compliance/dashboard/report-list。
[154] 丽莎 • 菲弗 (Lisa Phifer) 和戴夫 • 匹斯特洛，“标识符系统攻击缓解方法”，ICANN 白皮书，2017 年 2 月 13 日，https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf。

档中所列出的最佳实践时，遵循了何种流程。链接到的文件中也没有证据表明已将这些最佳实践整合到 ICANN 组织签署的协议中。报告中并未包含 2017 年之前的工作证据。

- “标识符系统攻击缓解方法”报告概述了针对标识符系统的攻击的不完整列表。尽管自 2017 年 2 月以来，已经达成了一些协议、续约、规范和 MOU，但与签约方签署的合同中并未包含这些文件中的任何内容。
- 自 2014 年以来，ICANN 安全意识资源定位符页面就一直未更新。[155]
- SSR2 审核小组并没有找到员工定期向 SO/AC 告知最佳实践或邀请他们确定其他最佳实践的证据。
- 关于此 SSR1 建议的员工报告表明，与反网络钓鱼工作组 (APWG) 互联网政策委员会合作，发布关于 Web 应用程序保护的建议并开发安全意识资源的工作已经完成。APWG 已经就“网站遭到网络钓鱼者攻击时该如何应对”提供了建议，但是在 SSR1 建议之前提出的。尽管有一份来自 2012 年在波多黎各举行的第四届全球 DNS 安全、稳定与弹性讨论会的报告，但 ICANN 网站上似乎并没有针对 Web 应用程序保护和开发安全意识资源的一系列建议。[156]

SSR1 建议 13

“ICANN 应鼓励所有支持组织为其成员制定并发布与 SSR 相关的最佳实践。”

SSR2 结论：此建议仍然适用，但尚未得到实施。未实现为支持组织 (SO) 制定常规流程，以便为其成员发布与 SSR 相关的最佳实践的预期效果。

请参阅 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，以及 SSR2 建议 9：对于在原始 SSR1 建议基础上扩展的 SSR2 建议，监督并强制实施合规性。

依据：

- ICANN 组织认为针对此项建议的工作正在进行，并作为 SOP 的一部分进行报告，ICANN 员工与所有 SO 和 AC 进行了联系，以鼓励确定并发布最佳实践存储库页面。ICANN 组织进一步表明，作为 SOP 的一部分，其员工参与了正在进行的各种活动，以鼓励在全球范围内使用 SSR 最佳实践。SSR2 审核小组无法找到 ICANN 组织已开展此外展活动的证据，也无法找到证据证明 SO 已为其成员发布了与 SSR 相关的最佳实践指南。
- ICANN 组织员工称，他们并不清楚最近采取了哪些措施来鼓励 SO 和 AC 针对与 SSR 相关的信息制定并发布最佳实践存储库，并表示“*ccTLD 网站上 2012 年的信息很可能就是支持组织发布的最新 SSR 相关信息。*”[157] 此外，ICANN 员工还表示，目前只有 ccNSO 为其成员发布了与 SSR 相关的最佳实践。

[155] ICANN 安全意识资源定位符，上次更新时间 2014 年 8 月 8 日，https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en。
[156] 第四届全球“DNS 稳定、安全与弹性”讨论会会议报告，ICANN 和 APWG，2012 年 10 月 25 日，https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf。
[157] SSR2 维基页面，审核小组，审核小组文档和草案，“SSR1 建议表格”，未注明发布日期，26，https://community.icann.org/pages/viewpage.action?pageId=64076120。

SSR1 建议 14

“ICANN 应确保其与 SSR 相关的外展活动不断发展，以保持相关性、及时性和适当性。”

SSR2 结论：此建议仍然适用，但并未得到实施，因此也没有实现改善 ICANN 与 SSR 相关的外展活动的及时性、相关性和适当性的预期效果。

请参阅 SSR2 建议 18：在原始 SSR1 建议的基础上为 SSR2 建议的政策辩论提供信息。

依据：

- 活动参与界面并没有直接阐明外展活动如何“发展”以保持相关性。[158] 相反，实施侧重于报告在任何给定时间开展的工作。因为没有将重点放在不断发展的活动上面，所以此建议并未得到实施。

SSR1 建议 15

“ICANN 应在所负责的披露和传播 DNS 安全威胁和缓解技术方面发挥促进作用。”

SSR2 结论：此建议仍然适用，并且尚未得到充分实施。尽管“理论上”存在此流程，但无法评估该流程是否实用和有效。

请参阅 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核，以及 SSR2 建议 13：对于在原有 SSR1 建议基础上扩展的 SSR2 建议，增加滥用投诉报告的透明度和问责制。

依据：

- 尽管 ICANN 组织实施了弱点披露流程，但并没有公开的统计数据或其他信息来说明调用此类流程的频率。
- ICANN 组织已针对 ICANN 面向公众的资产实施了弱点披露计划。[159] 在向 ICANN 组织报告 DNS 基础设施的弱点后，ICANN 组织（在可行时）会将信息传播给负责任的外部第三方。但是，第三方有责任修复其平台内的任何漏洞。
- 自 2013 年以来，所有 IS-SSR 报告均不包含与披露报告有关的任何统计信息或衡量标准。从已发布的材料中无法判断弱点披露报告方法是否被调用过，或者是否有效。没有 ICANN 组织作为弱点协调人的任何数据（即使是匿名的数据），也没有 ICANN 组织在紧急协调和与 SSR 相关的危机管理方面的工作数据。

[158] ICANN，活动参与界面，访问时间 2020 年 12 月 13 日，https://features.icann.org/events-near-you。
[159] ICANN，“用于报告 ICANN 组织在线服务中的弱点的流程”，访问时间 2020 年 12 月 13 日，https://www.icann.org/vulnerabilities。

SSR1 建议 16

“ICANN 应继续开展其外展工作，以扩大社群对 SSR 框架制定流程的参与和投入。ICANN 还应建立一个流程，以从其他生态系统参与者那里获取更系统的意见与建议。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。因为缺乏证据表明当前的外展活动已扩大了社群参与，所以不能认为这项建议已实现预期效果。

请参阅 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核，以及 SSR2 建议 13：提高滥用投诉报告的透明度和问责制，以及 SSR2 建议 18：对于在原始 SSR1 建议基础上扩展的 SSR2 建议，提供政策辩论信息。

依据：

- 相关社群的持续参与已经实现了“参与”目标，但无法确定信息是如何“系统地”整合的。此建议设想会有更多的公众参与到 SSR 计划中，包括框架和年度报告。这项建议并没有导致 IS-SSR 框架和年度报告的编制方式发生明显改变。
- 目前仍在针对与 ICANN 组织保持现有关系的相关社群开展外展活动，以实现“参与”目标。但是，此建议要求对其他 SSR 社群开展外展活动。
- 并没有证据表明当前的外展活动扩大了社群参与。
- 该建议特别要求制定一个更系统化的流程，以从其他生态系统参与者那里获取意见与建议。这让 SSR1 实施状态报告的最终工作成果显得不合时宜。[160]
- 实施报告表示，ICANN 员工将“支持安全团队的各种能力建设计划”。[161] SSR2 审核小组无法确定这些能力建设计划是否以及如何影响更广泛地参与到 IS-SSR 框架的制定流程中，因为 ICANN 组织已经不再更新 IS-SSR 框架。
- SSR2 审核小组无法从公共记录中找到有关能力建设计划内容以及何时执行这些计划的证据。

[160] ICANN，SSR 审核实施报告，2015 年 6 月，https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf。
[161] 同上，7。

SSR1 建议 17

“ICANN 应建立一个更具结构化的内部流程，显示活动和计划如何与 SSR 框架中的具体战略目标、宗旨和优先事项关联。”

SSR2 结论：该建议仍然适用。由于缺乏可追踪的指标，因此无法从公开可用的资料中确定实施情况。此建议并未实现其预期效果，因为 ICANN 组织不再维护 SSR 框架。

请参阅 SSR2 建议 2：对于在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理。

依据：

- 实施报告提到了 SSR1 建议 2 中的工作成果，并将此作为实施 SSR1 建议 17 的指南。但是，SSR1 建议 2 和 17 要实现的目标不同。SSR1 建议 2 要求针对与 SSR 相关的活动和职权范围定期进行公众咨询，而 SSR1 建议 17 则建议显示 SSR 相关计划如何与具体战略目标、宗旨和优先事项关联。SSR1 建议 2 的工作成果并不符合 SSR1 建议 17 的要求。
- SSR2 审阅的最新年度报告（2018 财年）列出了该财政年度的 18 项独立计划，并介绍了这些计划如何与首席技术官办公室的整体使命以及 ICANN 总体战略规划关联。然后，“年度规划”链接到描述报告期内（六个月）所完成工作的活动报告。
- SSR 年度报告和 ICANN 战略规划之间的联系尚不明确。此外，战略规划并没有提及 SSR 年度报告，而且几乎没有提到与 SSR 相关的活动。如果存在一个更具结构化的流程来显示活动和计划如何与 SSR 框架中的具体战略目标、宗旨和优先事项关联，那么这个流程并没有公开，或者没有向 SSR2 审核小组公开。但是，最新的年度报告中确定年度计划的部分确实试图将这些计划与 ICANN 的战略规划关联。
- 其他 SSR1 建议试图让 ICANN 的 SSR 活动与总体战略规划保持一致，并将这两者整合在一起。SSR1 建议 17 的实施远不能提供一个结构合理且可轻松审核的内部流程。

SSR1 建议 18

“ICANN 应对其在实施 SSR 框架方面的进展进行年度运营审核，并将此评估作为来年 SSR 框架的一部分包含在内。”

SSR2 结论：该建议仍然适用。SSR2 审核小组无法找到任何证据证明创建了内部审核流程或公开审核流程来对 IS-SSR 框架进行定期更新，因此该工作组无法确定此建议是否实现了预期效果。

请参阅 SSR2 建议 2：对于在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理。

依据：

- SSR1 建议 18 提议使用一种递归方法，即对上一年活动的审核将会影响有关未来计划的决策。SSR2 审核小组没有找到非正式或未记录的内部流程的相关证据，也没有找到证据证明对 IS-SSR 框架的实施进行了公开的年度运营审核。

SSR1 建议 19

“ICANN 应建立一个可让社群跟进 SSR 框架实施情况的流程。并且提供足够清晰的信息，以便社群可以跟进 ICANN 对其 SSR 职责的履行情况。”

SSR2 结论：该建议仍然适用。由于“足够清晰”一词缺乏明确性，因此无法全面衡量此建议。此建议并未实现其预期效果，因为社群仍无法在合理的时间范围内以公开透明的方式跟踪与 SSR 相关的活动。

请参阅 SSR2 建议 2：对于在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理。

依据：

- ICANN 组织报告称，每年发布的 IS-SSR 框架162均跟进了上一年度的框架中已承诺开展的活动的进展情况。此外，定期项目管理报告、运营规划和预算也被认为是提供 SSR 活动详细信息的工具。但是，在网站上发布年度 IS-SSR 框架似乎并不能达到为社群提供相关信息并允许其跟进框架实施情况的目的。实施文档的发布要远远落后于实施工作，因此它无法为社群提供跟进 SSR 相关活动的方法。
- 另外，SSR1 RT 似乎提供了一个示例，即建立一个公开公告板来跟进与 SSR 相关的活动，就像为实施 ATRT 的其中一项建议所做的那样。但是，目前并没有证据表明社群或公众使用此类公告板来跟进与 SSR 相关的活动。

SSR1 建议 20

“ICANN 应当更加透明地公开与实施 SSR 框架和履行 SSR 相关职能有关的组织和预算信息。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。未实现提高 SSR 相关详细信息（与组织和预算有关）的透明度这一预期效果。

请参阅 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

[162] IS-SSR 文档存档，https://www.icann.org/ssr-document-archive。

依据：

- ICANN 规划流程周期拥有三大阶段：战略规划、五年运营规划和年度运营规划和预算。[163] 这个周期的最终成果就是发布了工作成果和进展报告。正如 SSR1 实施维基页面上的实施报告所述，第一阶段工作目前已经实施，以提供与 SSR 相关规划、预算和活动有关的公共信息（如 SSR1 建议 2 中所述）；这些信息被整合到 ICANN 的 IS-SSR 框架中，并报告了 SSR 活动和支出。[164]定期发布的 SSR 活动报告可为此公共信息提供更多内容。[165] 第二阶段正在进行中，以确定在多个 ICANN 部门之间提供与 SSR 相关预算和支出有关的更详细公共信息的机制。目前，可以在“第 20 项建议”维基页面上找到 2018 财年关于此主题的公共信息。[166]
- ICANN 员工还编制了一份事后报告，其中包含与管理活动相关的预算和资源影响。[167] 截至 2020 年 3 月，未发布任何事后报告。这些报告的公共版本模板可在“第 20 项建议”维基页面上找到。
- 框架文档和年度报告中确实存在与 SSR 相关活动有关的年度报告。预算文档中有数行内容与 SSR 相关活动有关。ICANN 的定期项目管理报告中似乎并没有报告这些同类活动。实施报告表示，ICANN 会“*将 SSR 框架以及 SSR 活动和支出相关的报告整合到规划框架和流程中，以提供有关 SSR 相关规划、预算和活动的公共信息。*”[168]然而，正如 SSR1 建议 19 所述，ICANN 资产组合管理体系和 KPI 项目公告板提供的可供社群用来跟踪 SSR 相关工作的信息量非常有限。
- 2018 财年批准的预算有三个资产组合领域与 SSR 有关：标识符的发展；互联网标识符的安全、稳定与弹性；以及技术信誉。只有前两项（标识符的发展和互联网标识符的 SSR）在资产组合级别有专门的预算；但没有提供这些预算的详细信息。员工实施报告还表示，ICANN 将*“确定在多个 ICANN 部门之间提供与 SSR 相关预算和支出有关的更详细公共信息的机制”*，这表明在此方面的实施工作有望进一步开展。

SSR1 建议 21

“ICANN 应建立一个结构更加合理的内部流程，以显示组织和预算决策如何与 SSR 框架关联，其中包括基础的成本收益分析。”

163 “ICANN 规划流程”，https://www.icann.org/resources/pages/governance/planning-en。
164 SSR1 审核实施主页，https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home。
165 标识符系统 SSR 活动报告，https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en。
166 SSR1 审核实施，第 20 项建议，上次更新时间 2018 年 9 月 18 日，https://community.icann.org/display/SSR/Rec+%2320。
167 标识符系统 SSR 活动报告，https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en。
168 请参阅建议 20 的 SSR1 实施报告更新，https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2。

SSR2 结论：此建议仍然适用，并且已得到部分实施。未实现针对 SSR 相关预算决策建立一个公开透明流程的预期效果。

请参阅 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

依据：

- 在员工实施报告中，提到了 3 个工作成果：
  - 将 IS-SSR 框架和报告整合到规划框架和流程中，以提供有关 SSR 相关规划、预算和活动的公共信息。
  - 确定在多个 ICANN 部门之间提供与 SSR 相关预算和支出有关的更详细公共信息的机制。
  - 研究事后报告，其中包括与管理活动相关的预算和资源影响。
- 员工报告特别提到了一个报告模板，该模板可用于发布与受安全事件影响的预算和资源有关的信息。[169] 员工报告建议从 2018 财年开始，在每个财政年度发布一次报告。对 ICANN 网站上与 SSR 相关的页面的检查结果显示，尚未发布任何报告。框架文档和年度报告中确实存在与 SSR 相关活动有关的年度报告。预算文档中有数行内容与 SSR 相关活动有关。但是，ICANN 的定期项目管理报告中似乎并没有报告此类活动。此观察结果与 SSR1 对 SSR1 建议 20 的调查结果相同。此外，SSR 活动的预算和资源影响的相关报告似乎也从未完成，而且支持该报告的模板似乎也没有提供给公众进行审核和评议。
- ICANN 的规划流程可确保已规划和已设定预算的活动（包括那些与 SSR 相关的活动）通过具体目标确定。对于用于发布与 SSR 相关预算和支出有关的更详细公共信息的模板，目前还没有计划就其征询公众意见。现在，该模板已被财政年度的年度报告取代。

SSR1 建议 22

“随着 NgTLD 的引入，ICANN 应发布、监管并更新关于管理 SSR 问题所需组织资源和预算资源的文档。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。实施工作未实现全部的预期效果。

请参阅 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

依据：

- 在多个 ICANN 部门提供了 2018 财年 SSR 相关预算和支出的公共信息，这些信息可在以下位置找到：https://community.icann.org/x/DqNYAw。此报告每年更新一次，涵盖履行 SSR 职能所需的活动产生的直接成本，共享资源产生的直接成本，以及支持分配给 SSR 的职能产生的直接成本。此报告并未提供与新通用顶级域项目相关的资金、资源或其他活动的详细信息。

[169] SSR1 审核实施，第 20 项建议，https://community.icann.org/display/SSR/Rec+%2320。

- ICANN 组织已经研究了可在多个 ICANN 部门之间提供与 SSR 相关预算和支出有关的更详细公共信息的机制。但是，该公共信息的模板没有划分与新通用顶级域项目相关的 SSR 活动或预算。
- 很明显，与 NgTLD 团队相关的 SSR 问题的组织和预算是通过安全团队提供的，但它们也反映在新通用顶级域项目的预算和组织中（例如，域名系统稳定性专家组、EBERO、其他流程步骤等）。实施此项建议的预期结果似乎是，提高实施 IS-SSR 框架并履行与新通用顶级域项目有关的 SSR 相关职能的组织和预算信息的数量和清晰度。
- 在 ICANN IS-SSR 文档存档中，没有特定于新通用顶级域项目的文档。在 2016 年 9 月 30 日框架中，两次提到了 gTLD，一次是在“模块 A”中作为互联网生态系统中的趋势提及，另一次是在“模块 B”中作为 ICANN 总体战略规划的一部分提及。在 2013 年 3 月发布的 2014 财年 SSR 框架中，新通用顶级域项目再次被作为“趋势”提及，并被视为 GNSO 的政策驱动因素。其他唯一提到新通用顶级域项目的情况是在关于 SSR1 建议实施情况的报告章节中。

SSR1 建议 23

“ICANN 必须根据与 SSR 相关的工作组和咨询委员会的需求为其提供相应的资源。ICANN 还必须确保以客观方式达成工作组和咨询委员会所做出的决策，而不受外部或内部压力的影响。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。其预期效果是让工作组和咨询委员会以客观方式履行其职责，而不受外部或内部压力的影响，目前无法对该预期效果进行衡量。

请参阅 SSR2 建议 3：在原始 SSR1 建议的基础上，提高 SSR2 建议的 SSR 相关预算透明度。

依据：

- ICANN 组织确实向 SSAC 和 RSSAC 提供了 ICANN 技术支持员工，以协助编写文档。ICANN 组织的预算包括用于支持 SSAC 和 RSSAC 举行会议的一些资金（特别是差旅费用、酒店、餐补）；ICANN 组织向 SSR2 审核小组指出，2015 年的预算就是一个很好的例子。[170] 支持资金从未与任何正式的绩效、产出或内容评估挂钩，也从未受到任何正式绩效、产出或内容评估的制约。ICANN 认为这可以使其具有足够的独立性。事实上，尚不清楚 ICANN 或社群如何确定或评估 RSSAC 或 SSAC 的工作优先级，这在问责制方面造成了缺口，而且还导致无法评估他们是否具有“符合这两个群体需求”的资源。SSR1 原始报告包含与该建议有关的以下文本：

[170] ICANN，“通过 2015 财年运营规划和预算”，2014 年 12 月 1 日，第 77-78 页，https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf。

“在与 SSAC 的讨论中，我们发现他们对于在非常有限的时间范围内针对特定问题做出回答有时会感到有压力。这可以缩短评估问题的时间，从而获得更有针对性的建议。显然，在研究眼前的风险时，有时会对研究工作设定一个时间范围。这是不可避免的。不过，审慎的做法是，通过适当的规划确保 SSAC 和 RSSAC 能够有尽可能多的时间来提供高质量的研究工作和调查结果。”

这一观察结果反映了过去几年中的一些情况和问题，尤其是在 2018 年 10 月 KSK 轮转的背景下，当时 SSAC 努力在短时间内回应提供建议的请求，而且没有足够的数据/研究为辩论提供信息。[171] 考虑到许多当前存在和新出现的 SSR 问题，以及 SSAC 提供建议需要研究或综合先前研究的期望，ICANN 分配给 SSAC 的一小部分预算可能并不充足。SSAC 的当前结构也与“高质量研究工作”不相称，因为该组织由一组“志愿者”组成，这些志愿者大多数来自业界，并由其雇主为其参与活动的时间提供补贴，这种情况也与“不受外部压力”的描述不符。

- 因为缺乏对新通用顶级域项目成功与否的衡量标准和监控，所以这种多利益相关方方法也不是“没有外部压力”。从 CCT 角度来看，使用 CCT RT 关于 NgTLD 中 DNS 滥用的报告中的衡量标准，不可能得出新通用顶级域项目已经成功的结论。此类研究完全属于 ICANN 安全团队的职责和义务（请参阅 SSR1 建议 24）。ICANN 并未进行此类活动或为其提供资金，这可能是因为反对此类 SSR 研究活动的外部压力占据了优势。
- SSAC 运营程序文档中并没有关于管理外部和内部压力的内容，除了第 2.1.2 节“撤回和异议意见”，这意味着每个成员和委员会都会自行管理利益冲突，并且出于安全原因，所有审议都是保密的。[172] RSSAC 和 RZERC 似乎也是如此，但是在这两个组织中，由于委员会的架构所致，其中的每个人员都代表一个利益相关方。
- 一些与 SSR 相关的咨询委员会始终缺少重要的利益相关方（例如标识符滥用的受害者、学术界研究人员、执法人员、决策者）。

SSR1 建议 24

“ICANN 必须明确定义首席安全办公室团队的章程，职责和义务。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。未实现为首席安全办公室团队制定明确章程、明确的职责和义务的预期效果。

请参阅 SSR2 建议 2：对于在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理。

[171] ICANN，“首轮根区密钥签名密钥 (KSK) 轮转圆满结束”，ICANN 公告，2018 年 10 月 15 日，https://www.icann.org/news/announcement-2018-10-15-en。
[172] ICANN 安全与稳定咨询委员会，“SSAC 运营程序版本 5.1”，2019 年 2 月 27 日，第 10 页，https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf。

依据：

- 自 2018 年以来，就不再设立首席安全办公室。然而，OCTO（首席技术官办公室）SSR 工作组处理外界关注的与 ICANN 相关的 SSR 问题，CIO 和工作组处理内部关注的安全问题，OCTO 研究团队则关注在 ICANN 有限范围和职权范围内未来面临的 SSR 风险和机遇。[173] 此工作组的网页使用一些简短术语介绍了该工作组的使命，并链接到 SSR“活动”页面。[174] 没有任何措辞提到此工作组的“章程”、“职责”或“义务”。SSR2 工作组假定此页面上列出的活动就是 ICANN 打算作为 OCTO 与 SSR 相关的职责与义务：
  - 与安全、运营和公共安全社群积极合作，收集和处理可指示 DNS 或域名注册服务运营（“DNS 生态系统”）面临（迫在眉睫）威胁的情报数据。
  - 促进或与这些社群一起参与威胁防范活动，以防御或减少对 DNS 生态系统的威胁。
  - 进行研究或分析数据以更好地了解 DNS 生态系统的运行状况和发展状况。
  - 协调 DNS 弱点披露报告 (https://www.icann.org/vulnerability-disclosure.pdf)。
  - 提供主题问题专业技能，以便就与 DNS 生态系统相关的主题（包括 DNSSEC、滥用或误用 DNS 基础设施或运营）方面，在 ccTLD 和公共安全社群中开展能力建设。
  - 协助进行 DNS 生态系统风险管理活动。
  - 与 ICANN 全球利益相关方合作团队一起，参与全球多利益相关方工作，以改善网络安全并减少网络犯罪。
- 就可供公众使用的 SSR 分析而言，OCTO 似乎并没有提供很多成果。开放数据倡议、DAAR 报告和互联网衡量标准项目似乎都是与 ICANN 组织内部相关数据有关的项目。到目前为止，尚不清楚这些工作对于 ICANN 组织旨在提供服务的更大社群能有多大帮助。

SSR1 建议 25

“ICANN 应在其风险管理框架中建立机制，确定近期和长期风险和战略因素。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。实施工作未实现全部的预期效果。

请参阅 SSR2 建议 4：对于已在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，改进风险管理流程和程序。

依据：

- ICANN 董事会在 2013 年批准了风险管理框架，并在 ICANN 第 50 届和第 51 届会议上收到了社群的意见。ICANN 组织维护着一个企业风险管理 (ERM) 公告板，该公告板列出了要监控和处理的风险，并且遵循企业风险管理框架。然而，尽管已经建立了一种机制，但是在如何将风险识别纳入相关 SSR 流程和政策方面仍缺乏明确性。

[173] ICANN OCTO，“首席技术官办公室 (OCTO)”，访问时间 2019 年 12 月 27 日，https://www.icann.org/octo。
[174] ICANN OCTO,“互联网标识符系统安全、稳定与弹性”，访问时间 2019 年 12 月 27 日，https://www.icann.org/octo-ssr。

SSR1 建议 26

“ICANN 应优先考虑及时完成风险管理框架。”

SSR2 结论：此建议仍然适用，并且已得到部分实施。鉴于“及时”一词在其意图或可接受的内容方面没有任何明确性，因此无法评估是否实现了预期效果。

请参阅 SSR2 建议 4：对于已在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，改进风险管理流程和程序。

依据：

- ICANN 董事会在 2013 年批准了风险管理框架，175并在 ICANN 第 50 届和第 51 届会议上收到了社群的意见。建议 27 的评估中涉及对此建议更详细的答复。

SSR1 建议 27

“ICANN 风险管理框架应在其 SSR 职权范围和有限使命范围内具有全面性。”

SSR2 结论：该建议仍然适用。鉴于缺乏 SSR1 对“全面性”的定义或评估的衡量标准，SSR2 审核小组无法评估此建议是否得到充分实施。ICANN 组织并未实现预期效果，即，未提供有关 ICANN 所使用的风险管理框架的全面、易于查找的信息。

请参阅 SSR2 建议 4：对于已在原始 SSR1 建议的基础上进行了扩展的 SSR2 建议，改进风险管理流程和程序。

依据：

- SSR2 审核小组讨论了 SSR1 建议 27 是否已根据员工在与 SSR1 建议 25 有关的各种问答交流期间提出的参考资料进行实施。然而，SSR2 审核小组得出的结论是，虽然此建议与 SSR1 建议 25 和 26 相关，但却是截然不同，因为它要求框架的“全面性”。SSR2 审核小组认为，如果 SSR1 建议 27 是按照 SSR1 审核小组的意图来实施的，那么它所解决的问题将与 SSR1 建议 25 和 26 可能要解决的问题相同。
- SSR1 并没有定义框架的哪些元素可以构成“全面性”，也没有定义如何评估“全面性”。在审核期间有人指出，此建议由不再在 ICANN 组织工作的 ICANN 员工实施。在这方面，并没有关于他们如何评估风险管理框架“全面性”的机构资源和完整历史记录。

[175] ICANN，“DNS 风险管理框架报告”，上次修改时间 2013 年 10 月 4 日，https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en。

- 可在几个分散的位置找到关于如何处理风险管理的公开可用信息。例如，ICANN 员工表示，董事会风险管理委员会由负责监督的 ICANN 组织高管团队组成。此外，与职能有关的风险联络人（代表每个实施风险框架的职能部门的工作人员）和管理其活动固有风险的所有组织人员，都重点关注风险管理问题；这表明 ICANN 组织的风险职能没有在战略上进行集中和协调。

SSR1 建议 28

“ICANN 应继续积极参与威胁检测和缓解，并参与分发威胁和事件信息的工作。”

SSR2 结论：此建议仍然适用，并且尚未得到充分实施。尽管 ICANN 组织已与各团体合作，以帮助检测、缓解威胁和事件并共享与之相关的信息，但其并未实现向这些指定团体之外的组织提供信息的预期效果。

请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理，以及 SSR2 建议 8：在与签约方的谈判中维护并展现公共利益，SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核，以及 SSR2 建议 13：对于在原有 SSR1 建议基础上扩展的 SSR2 建议，增加滥用投诉报告的透明度和问责制。

依据：

- SSR2 审核小组并没有发现任何公开可用的数据显示 ICANN 组织参与了威胁检测和缓解工作。在可行的情况下，ICANN 组织会将报告的弱点传播给负责任的外部第三方。但是，第三方有责任针对传播的威胁和事件信息采取行动。
- 并没有任何公开证据证明 ICANN 组织正在进行持续的威胁检测，也没有证据表明有人承担这一职能。但是，ICANN 社群有许多组织（开放式和封闭式）在积极地进行威胁检测，包括 SSAC、RSSAC、TLDOPS、ccNSO 事件响应工作组和 PSWG。OCTO SSR 团队与这些组织进行了协调。

附录 E：DNS 滥用趋势报告的研究数据

在不同程度与 DNS 相关的示例包括：

- 恶意软件：从 2016 年到 2018 年，被防病毒软件识别为“恶意”的唯一 URL 的数量翻了一倍多，达到了 554,159,6213[176]，从 2017 年到 2018 年，移动端恶意软件攻击几乎翻了一倍，超过 1.16 亿[177]。
- 数字证书欺诈：APWG 报告称，网络钓鱼者越来越多地使用数字证书来让攻击看起来合法，并消除浏览器欺诈检测警告。[178] 由于 ICANN 取消了对 WHOIS 的访问权限，因此 SSL 证书管理部门将不再拥有对域名注册数据的访问权限，也无法使用 ICANN 组织负责协调以验证域名所有权的域名所有权记录。PhishLabs 确定在所有网络钓鱼网站中，有一半的网站使用 SSL 加密，例如，启用 SSL 加密时，浏览器地址栏中会出现绿色锁定符号，从而让用户误认为该网站可以安全使用。攻击数量增加的部分原因是网络钓鱼者将 HTTP 加密添加到其网络钓鱼网站 – 这种技术使安全功能变得不利于受攻击者。[179]
- 网络钓鱼：APWG 报告称，网络钓鱼者会直接注册域名以实施欺诈行为，而且网络钓鱼攻击的方法也变得更为有效且难以检测。

  > *“网络钓鱼者越来越多的使用网页重定向来隐藏其网络钓鱼网站，以防被发现。当受害者单击网络钓鱼电子邮件中的链接时，重定向会让用户在访问网络钓鱼网站之前不知不觉地浏览其他网站。然后，一旦受害者提交其凭据，更多的重定向会将受害者带到另一个域。”*[180]

- 商业电子邮件诈骗：美国联邦调查局 (FBI) 互联网犯罪中心报告称，从 2016 年到 2018 年，因商业电子邮件诈骗造成的已确认全球公开的损失增加了 136%，影响了美国所有 50 个州和全球 150 个国家/地区。从 2013 年 10 月到 2018 年 5 月，FBI 记录了 BEC 导致数十亿美元经济损失，这通常涉及欺诈性域名注册，这些域名往往与目标方的其中某个域名相似。[181]

[176] AMR，“2018 年卡巴斯基安全公告：统计数据”，2018 年 12 月 4 日，https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/。
[177] 维克多 • 切比雪夫 (Victor Chebyshev)，“2018 年移动端恶意软件的演变”，2019 年 3 月 5 日，https://securelist.com/mobile-malware-evolution-2018/89689/。
[178] APWG，“APWG 2018 年第 3 季度网络钓鱼活动趋势报告”，2018 年 12 月 11 日，https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf。
[179] 艾略特 • 沃尔克曼 (Elliot Volkman)，“现在有 49% 的网络钓鱼网站使用 HTTPS”，PhishLabs 博文，2018 年 12 月 6 日，https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https。
[180] APWG 网络钓鱼活动趋势报告，https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf。
[181] “商业电子邮件诈骗：120 亿美元的骗局”，联邦调查局公共服务公告，2018 年 7 月 12 日，https://www.ic3.gov/media/2018/180712.aspx。

- 诈骗：澳大利亚竞争与消费者委员会 (ACCC) ScamWatch 报告称，在大约最近的三年时间里，诈骗造成的损失几乎翻了一番，2019 年的损失增至 1180 万澳元。[182] 用于实施网络诈骗的域名通常会侵犯品牌或企业名称。诈骗者注册这些名称时，对诈骗者可以注册的相似名称的数量几乎没有控制，而且对调查人员可以用来识别犯罪行为的信息的访问也受到了限制。
- 僵尸网络：2017 年，Spamhaus DBL 列出了 5 万个僵尸网络控制器域名，这些域名由网络犯罪分子注册和设置，其唯一目的是托管僵尸网络控制器。在这些注册的僵尸网络域名中，超过 25% 是通过单个注册服务机构 Namecheap 注册的。[183] 2018 年，Spamhaus 列出了 103,503 个僵尸网络控制器域名，增长了 106%。Namecheap 仍旧是滥用最严重的注册服务机构，该机构中注册的僵尸网络控制器域名增长了 220%。[184]
- 垃圾邮件：垃圾邮件是网络钓鱼、恶意软件和其他 DNS 相关威胁的首选提供基础结构。截至 2019 年 8 月，日均垃圾邮件发送量为 4160.4 亿。[185]

> *“无论威胁形势如何变化，恶意电子邮件和垃圾邮件仍然是攻击者散布恶意软件的重要工具，因为它们可以将威胁直接带到端点。通过应用恰当的社会工程技术组合，例如网络钓鱼、恶意链接和附件，攻击者只需袖手旁观，等待毫无戒心的用户激活他们的攻击。”* [186]

- DDOS 攻击：从 2017 年中期到 2018 年中期，分布式拒绝服务 (DDOS) 攻击增加了 40%。[187] 2018 年上半年，DDOS 最大规模攻击在全球范围内比 2017 年同期增长了 174%，2018 年 2 月，有记录以来的最大攻击 (1.7 Tbps) 袭击了北美一家主要的服务提供商。[188] 因为从企业到政府机构再到物理公共工程基础设施，这一切都依赖于与 DNS 相关的不间断服务，所以毫无节制的 DDOS 攻击的危害性变得越来越大。DDOS 攻击也变得更加复杂，而且多途径攻击现在已成为最常见的攻击。Verisign 报告称，在 2018 年第二季度记录的攻击中，有 52% 是多途径攻击。[189] 此外，物联网 (IoT) 受到的 DDOS 攻击也逐渐增多，因为这些已连接设备很容易成为攻击目标，而且数量在一直增加。2017 年已连接设备的数量为 270 亿，预计到 2020 年将达到 1250 亿。[190]

---

[182] ScamWatch，澳大利亚竞争与消费者委员会，https://www.scamwatch.gov.au/about-scamwatch/scam-statistics。
[183] “2017 年 Spamhaus 僵尸网络威胁报告”，Spamhaus 恶意软件实验室，上次修改时间 2018 年 1 月 8 日，https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017。
[184] “2019 年 Spamhaus 僵尸网络威胁报告”，Spamhaus 恶意软件实验室，未注明发布日期，https://www.spamhaustech.com/botnet-threat-report-2019/
[185] “电子邮件和垃圾邮件数据”，思科 Talos 情报小组，https://www.talosintelligence.com/reputation_center/email_rep。
[186] “思科 2018 年年度网络安全报告”，思科系统公司，2018 年 2 月，https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf。
[187] “2018 年上半年 DDOS 趋势报告”，Corero Network Security，未注明发布日期，https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html。
[188] 凯文 • 沃伦 (Kevin Whalen),“进入万亿比特时代：为更大规模的 DDOS 攻击做好准备”，2018 年 9 月 5 日，https://www.netscout.com/blog/entering-terabit-era-get-ready-bigger-ddos-attacks。
[189] “2018 年第二季度 DDOS 趋势报告：52% 的攻击采用了多种攻击类型”，Verisign 博文，上次修改时间 2018 年 9 月 27 日，https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types/。
[190] 约翰 • 英格利希 (John English)，“准备好网络以满足 IoT 期望”，NETSCOUT 博文，上次修改时间 2018 年 2 月 28 日，https://www.netscout.com/blog/getting-network-ready-meet-iot-expectations。

附录 F：关于加密技术的研究数据

椭圆曲线加密技术

椭圆曲线加密技术 (ECC) 是当前用于 DNSSEC 的 RSA 公钥加密的替代方法。该技术基于椭圆曲线理论，可用于创建更快、更小和更有效的加密密钥。[191]

根 KSK DPS 就密钥长度和密钥轮转提供了指导。但是 DPS 并没有指明更改数字签名算法的过程。美国国家安全局的最新指南建议使用 3072 位 RSA。爱德华曲线数字安全算法 (EdDSA) 似乎提供了一种优于超大型 RSA 密钥的替代方法。[192]

后量子加密技术

十年前，大多数人还没有听过量子计算，但是近几年来，它逐渐吸引了公众的注意力。在关注这一领域的人员中，部分人关注的是量子计算机的独特计算能力。美国国家科学院最近发布了一份名为“量子计算：进展与展望”的报告，得出的简要结论是，现在是时候开始为未来的量子安全做准备了。[193]

DigiCert 估计，使用传统计算技术来解析 2048 位 RSA 密钥需要花费数万亿年的时间。[194] 如果将来发明了大型量子计算机，它可能会以更快的速度在短短几个月内破解相同的密钥。在构建可能威胁 RSA 和 ECC（这两者是用于保护互联网安全的非对称密码算法）的量子计算机之前，仍然需要克服许多技术难题。

[191] 有关 DNSSEC 签名的潜在新算法的更多信息，请参阅以下 RFC：P. • 霍夫曼 (P. Hoffman) 和 W. • 维恩加德 (W. Wijngaards)“用于 DNSSEC 的椭圆曲线数字签名算法 (DSA)”，RFC 6605，DOI 10.17487/RFC6605，2012 年 4 月，<https://www.rfc-editor.org/info/rfc6605>，O. • 苏利 (O. Sury) 和 R. • 埃德蒙 (R. Edmonds)，“用于 DNSSEC 的爱德华曲线数字安全算法 (EdDSA)”，RFC 8080，DOI 10.17487/RFC8080，2017 年 2 月，<https://www.rfc-editor.org/info/rfc8080>，以及 P. • 伍特斯 (P. Wouters) 和 O. • 苏利，“DNSSEC 的算法实施要求和使用指南”，RFC 8624，DOI 10.17487/RFC8624，2019 年 6 月，<https://www.rfc-editor.org/info/rfc8624>。

[192] 伍特斯和苏利，RFC 8624，https://www.rfc-editor.org/info/rfc8624。

[193] 美国国家科学、工程和医药研究院，2019 年。量子计算：进展与展望。华盛顿特区：美国学术出版社，https://doi.org/10.17226/25196。

[194] 蒂莫西 • 霍勒贝克 (Timothy Hollebeek)，“DigiCert 关于量子的研究：美国国家科学院报告”，DigiCert 博文，2019 年 1 月 9 日，https://www.digicert.com/blog/digicert-on-quantum-national-academy-of-sciences-report/。

要在大型量子计算机方面取得进展，就必须跟踪物理量子比特或“量子比特”计算机数量的扩展比率和错误率。错误率非常重要，因为它们会显著影响生成逻辑量子比特所需的物理量子比特的数量。物理量子比特是代表 0 或 1 的单个量子系统；然而，即使在接近绝对零度的温度下，物理量子比特也容易通过与环境不可避免的相互作用而产生错误。多个物理量子比特可以组合成单个逻辑量子比特，而且附加的量子比特可用于检测和纠正这些错误。研究人员甚至还没有产生一个逻辑量子比特，尽管他们在朝着这个目标迅速取得进展。一旦逻辑量子比特可用，跟踪逻辑量子比特的数量将成为要跟踪的衡量标准。

行业标准组织也在为未来的后量子算法做准备。最有名的活动是 NIST 后量子加密项目，世界各地的研究人员均参与到此项目中，以开发不容易受到量子计算机攻击的新加密原语。[195] 可以预料，该项目将需要花费数年的时间才能将生成的算法进行标准化。

与此同时，研究人员一致认为基于哈希的签名具有后量子安全性。互联网研究任务组 (IRTF) 已在其加密技术论坛研究小组 (CFRG) 中指定了这些签名算法，这些算法使用较小的私钥和公钥，且计算成本较低。[196] 然而，由于签名的数量非常大，而私钥只能产生有限数量的签名，尽管这些算法当前可用，但这两种特性使得基于哈希的签名在 DNSSEC 环境中不受欢迎。

[195] 国家标准与技术研究院 (NIST) 信息技术实验室计算机安全资源中心，“后量子加密技术”，创建日期 2017 年 1 月 3 日，更新日期 2020 年 11 月 23 日，https://csrc.nist.gov/projects/post-quantum-cryptography。
[196] IRTF，加密技术论坛研究小组，https://irtf.org/cfrg。

附录 G：了解 SSR2 建议与《ICANN 2021-2025 财年战略规划》和《ICANN 章程》的关系

相关《ICANN 章程》

《章程》第 1.2.(a)(i) 节和第 1.2 (a) (ii) 节，以及第 27.1(c)(i)(B) 节关于“保持并增强对 DNS 的管理以及 DNS 和互联网运营的稳定性、可靠性、安全性、全球互用性、弹性和开放性：”

《章程》第 3.6(a) 节 – 协助董事会审议和报告“其决策对全球公益的实际影响（如果有），包括讨论对 DNS 的安全性、稳定性和弹性的实际影响。”

《章程》第 12.2(b) 节和第 12.2(c) 节 – 与安全与稳定咨询委员会，特别是与根服务器系统咨询委员会紧密合作，并确保 ICANN 董事会和 ICANN 组织充分执行其批准的建议。

《章程》附录 G-1，第 1.1(a)(i) 节中提到的有关 gTLD 注册服务机构和 gTLD 注册管理机构的主题、问题、政策、程序和原则包括：“为提高互联网、注册服务机构服务、注册管理机构服务或 DNS 的互用性、安全性和/或稳定性，必须采取统一或协调的解决方案的问题”以及“顶级域名 (TLD) 注册数据库的安全性和稳定性”。

相关的战略规划目标和宗旨

摘自 ICANN《2021-2025 财年战略规划》。[197]

1.增强域名系统和 DNS 根服务器系统的安全性。

- *1.1 通过与利益相关方合作来强化 DNS 协调性，提高相关各方维护 DNS 安全性与稳定性的共同责任意识。*
- *1.2 协同 DNS 根服务器运营商，加强 DNS 根服务器运营治理。*
- *1.3 加强与相关硬件、软件和服务供应商的合作沟通，识别和缓解 DNS 安全威胁。*
- *1.4 增强 DNS 根区密钥签名和分发服务及流程的稳健性。*

2.战略宗旨：提高 ICANN 多利益相关方治理模型的效果。

- *2.1. 增强 ICANN 自下而上的多利益相关方决策制定流程，确保及时有效地完成相关工作和政策制定。*

[197] ICANN《2021-2025 财年战略规划》，https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf。

2.2 支持并提升利益相关方主动、明智且有效的参与。
2.3 保持并增强开放性、包容性、问责制，以及透明度。

3. 战略宗旨：与相关方协调并合作，不断发展唯一标识符系统，以继续满足全球互联网用户群的需求。

3.1 提高社群对普遍适用性、IDN 实施和 IPv6 的认识，鼓励人们做好相关准备，促进互联网领域的竞争、消费者选择和创新。
3.2 加强与相关方的互动沟通，以此改进对影响互联网唯一标识符系统安全性、稳定性与弹性的新技术的评估，并提高对新技术的响应能力。
3.3 继续行使并增强 IANA 职能，实现卓越运营。
3.4 通过新的 gTLD 轮次，为互联网唯一标识符系统的持续发展提供支持；按照 ICANN 流程，以审慎负责的态度，对这个新的 gTLD 轮次提供资金支持，并加以妥善管理和风险评估。

4. 战略宗旨：解决影响 ICANN 使命的地缘政治问题，维护统一、全球互用的互联网。

4.1 进一步开发早期预警系统（例如，ICANN 组织的《立法和监管发展动态报告》），确定并积极应对属于 ICANN 职权范围内的全球性机遇和挑战。
4.2 继续与互联网生态系统内部和外部的各方构建联盟，提高人们对 ICANN 使命的认识，增进全球利益相关方参与政策制定。

5. 战略宗旨：确保 ICANN 的长期财务可持续性。

5.1 实施五年财务规划，为五年运营规划提供支持。
5.2 制定可靠且可预测的经费规划。
5.3 管理运营及其成本，以优化 ICANN 活动的效果并提高效率。
5.4 确保根据 ICANN 环境的复杂性和面临的风险，持续设立、实现并维护 ICANN 储备金标准。

序号	建议	战略宗旨和目标
1	完成所有相关 SSR1 建议的实施工作。	战略宗旨 1、2 和 3
2	SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理	战略宗旨 1、3 和 4
3	SSR2 建议 3：提高 SSR 相关预算的透明度	战略宗旨 1、2、3 和 5；以及战略目标 2.1 和 3.4
4	SSR2 建议 4：改进风险管理流程和程序	战略宗旨 1、2、3、4 和 5

5	SSR2 建议 5：遵守适当的信息安全管理系统和安全认证规定	战略目标 1
6	SSR2 建议 6：SSR 漏洞披露和透明度	战略宗旨 1、2、3 和 4；以及战略目标 1.1、1.2、1.3 和 4.1
7	SSR2 建议 7：改进业务连续性和灾难恢复流程和程序	战略宗旨 1、3 和 4；以及战略目标 1.1、1.4 和 3.3
8	SSR2 建议 8：在与签约方的谈判中维护并展现公共利益	战略宗旨 1 和 3；以及战略目标 1.1、1.2、1.3 和 1.4
9	SSR2 建议 9：监督并强制实施合规	战略宗旨 1、2 和 3；以及战略目标 2.1
10	SSR2 建议 10：明确滥用相关术语的定义	战略目标 1
11	SSR2 建议 11：解决 CZDS 数据访问问题	战略宗旨 3；以及战略目标 3.2
12	SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核	战略宗旨 1、2、3、4 和 5
13	SSR2 建议 13：提高滥用投诉报告的透明度和问责制	战略宗旨 1 和 3；以及战略目标 2.1
14	SSR2 建议 14：制定临时规范，提高基于证据的安全性	战略宗旨 1；以及战略目标 1.1
15	SSR2 建议 15：启动 EPDP 以提高基于证据的安全性	战略宗旨 1；以及战略目标 1.1
16	SSR2 建议 16：隐私要求和 RDS	战略宗旨 1、3 和 5
17	SSR2 建议 17：衡量域名冲突	战略宗旨 1、3 和 4；以及战略目标 3.4
18	SSR2 建议 18：为政策辩论提供信息	战略宗旨 1、3 和 4；以及战略目标 3.2
19	SSR2 建议 19：完成 DNS 回归测试套件的开发工作	战略宗旨 1；以及战略目标 1.1、1.2、1.3 和 1.4
20	SSR2 建议 20：用于指导密钥轮转的正式程序	战略宗旨 1、2 和 4；以及战略目标 1.4
21	SSR2 建议 21：提高与 TLD 运营商的通信安全性	战略宗旨 1；以及战略目标 3.3
22	SSR2 建议 22：服务衡量标准	战略宗旨 1、2、3、4 和 5；以及战略目标 1.1、1.2、2.1、3.2、3.4 和 4.1
23	SSR2 建议 23：算法轮转	战略宗旨 1 和 3

24	SSR2 建议 24：提高 EBERO 流程的透明度和改进端到端测试	战略宗旨 1；以及战略目标 1.2

附录 H：公众意见分析

SSR2 审核小组创建了一个电子表格，用于记录其对公众意见的响应以及因公众意见而产生的更改。该文件可在 SSR2 维基页面的审核小组文档和草案页面上找到，或者可以使用下面的链接直接下载。

Excel：
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191048/Public%20Comment%20Feedback%20-%20March%202020.xlsx

PDF:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191042/Public%20Comment%20Feedback%20-%20March%202020.pdf

附录 I：情况简报

ICANN 组织会按季度发布情况和费用简报，按月发布参会情况并更新重要事件。上述文件将对社群如何使用审核小组的资源和如何安排审核小组的时间引入透明度和责任制。

情况简报记录了审核小组成员的出席情况、与专业服务和参加面对面会议差旅费相关的费用以及重要事件和参会情况。

定义如下：

专业服务：审核小组使用独立专家服务的预算标准可参阅章程的第 4.6 (a)(iv) 节的相关规定。审核小组还可招募和选择独立的专家来根据审核小组的请求提出建议。根据章程的第 4.6 节的相关规定，ICANN 将为这些专家每次的审核支付合理的费用和开支，额度应与为每次审核指定的预算一致。在运作标准中规定了审核小组如何与独立专家合作并考虑其建议的指导准则。

差旅：审核小组参加面对面会议的批准差旅费数额。差旅支出示例包括但不限于以下方面：机票、酒店、每日费用报销、会场开会支出、视听/技术支持以及餐饮。这些花费包括审核小组和 ICANN 组织支持活动相关差旅的费用。

ICANN 组织支持：ICANN 组织为支持审核小组的工作而签约外部服务的批准预算数额。

目前已支出预算：金额包括自审核小组开始工作到最近一个季度末的季度费用。

已承诺使用的服务：
1.差旅：为参加批准的面对面会议估算的费用。
2.专业服务：包括已签署合同中将提供或将开具发票的服务。

这些服务通常用于合同方提供的与员工无关的支持服务。总计

目前已使用和已承诺使用总额：这是截至最近一个季度末的“目前已支出预算”和“已承诺使用的服务”相关金额的总和。“已承诺使用的服务”相关金额不包含“目前已支出预算”金额。剩余预算：这是“已批准预算”和“目前已使用和已承诺使用总额”之间的差额。可以通过以下链接访问情况简报存档文件：https://community.icann.org/x/S7zRAw。