CSA对CI保护框架的评论建议汇总

CSA GCR GREATER CHINA REGION cloud security alliance ®

CSA cloud security alliance ®

致谢

《CSA 对 CI 保护框架的评论建议汇总》一文由 CSA 专家编写，CSA 大中华区隐私与个人信息保护法律工作组组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组　长：原　浩

翻译组：高健凯　　贺志生　　黄鹏华　　邢海韬　　张元恺　　赵　晔

感谢以下单位对本文档的支持与贡献：北京奇虎科技有限公司

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正!

联系邮箱：research@c-csa.cn；国际云安全联盟 CSA 公众号。

《关键信息基础设施安全保护条例》施行一周年回顾：NIST 关键基础设施安全保护框架升级研讨问题引荐

2022 年 8 月 17 日，NIST 举行了一次升级关键基础设施安全保护框架（本文统称“安全框架”或 CSF）研讨会，旨在将框架从 1.1 版本升级到 2.0。全球 100 多国家的 3900 多位专家人士参加了会议建言献策。另 NIST 通过评论征集（RFI）的方式收集了 100 多家单位、个人的评论和建议，包括云安全联盟 CSA 等对框架的运行和不足提出了诸多建议。

本报告转引了 CSA 的评论建议（14 条分析建议和 3 条整体建议），适逢中国《关键信息基础设施安全保护条例》施行一周年，也期待能为中国条例的落地和进一步细化、完善有所启示或参考。

一、CSA 的分析建议

1、云安全的忽略和应通过整合云控制矩阵提升解决云安全的能力

NIST 安全框架中的五项功能框架能够帮助组织开展网络安全工作，组织可以利用这五项功能进行积极的风险管理，以降低现在和未来的风险。遵循 NIST 安全框架，将使组织更容易在未来实施（保护）时采用以 CSF 为基础的安全程序。

然而我们也认为，云安全风险被（部分）忽略，或者未从明确的通用控制角度进行解决。

如果将 CSA 的云控制矩阵添加到框架中，将有助于解决这一关键问题，实际上组织可能会发现有进一步的机会修订和完善这五项功能，以解决云安全问题。

2、使用 NIST 安全框架的当前优势和 CSA 的报告发现

组织和实体（如供应链伙伴、客户或保险公司）内部和之间的沟通是否得到改善？该框架是否允许更好地评估风险，更有效地管理风险，和/或增加管理风险的潜在方法的数量？在实施该框架后，哪些可能是改进网络安全的相关指标?如上所述，我们认为该框架不足以解决云风险。

CSA 开展了研究，并发布了“云安全联盟关于识别云计算快速采用的差距和风险的云风险管理报告”

该文件列出了五个问题，以激发讨论并促进可能的解决方案。

- 目前可用的风险管理方法是否足以管理云风险?
- 企业是否意识到云计算引入的共同责任模式，以及这些责任是否适当地反映在风险管理流程和计划中?
- 企业是否意识到云计算所带来的间接/失去控制的概念和影响，以及其对风险缓解程序的设计和验证所带来的挑战?
- 企业是否充分认识到云计算对其供应链传播的影响，以及评估和监测第三方/第四方的综合剩余风险的难度?
- 当前的治理实践是否足以有效识别、评估并向利益相关者报告相关的云风险？

风险管理应用于云计算运营时，在企业的所有流程中发挥着重要作用，对企业的整体业务改进战略至关重要。因此，这必须是一个顶层的、企业范围内的流程，而不是一个孤立的或部门性的工作。虽然不管是在云端还是在本地，风险管理的方法都是相同的，但在战术和实施上有很大的不同，这是必须要解决的问题。

有效的风险管理计划将解决与经济价值、流程改进、合规性、信息安全和隐私有关的问题，包括：

- 迁移到云所产生的新的运营安全风险
- 与未能解决云计算合规性有关的成本
- 与云计算市场增长有关的风险
- 缓解措施

3、可能阻碍组织使用 NIST 安全框架或更容易或更广泛地使用该框架的挑战（例如：资源考虑、信息共享限制、组织因素、劳动力差距或复杂性）

NIST 安全框架中一个大议题，也是我们认为的一个非常容易更新迭代的领域就是云计算。NIST 目前更偏向本地部署。问题是今天许多公司在确保云安全方面没有管理

或理解共同责任模式。事实上，许多公司甚至没有保护自己的云基础设施。相反，将 SaaS 或 PaaS 的使用外包给第三方公司，试图将风险转移给第三方，使其承担管理云的所有法律和运营责任，这往往事与愿违。在供应商、客户和第三方的责任之间虽然有明确的界限，但这些都没有明确的定义或解决方案。

在这方面，NIST 并没有真正处理共同责任的问题。该框架似乎假定了一种更为谨慎的工作方式。遵守 NIST 意味着组织正在设法解决自己管理的系统部分，但不幸的是可能没有对那些远程管理的部分实施任何控制。

为什么这很重要？认真对待网络安全的公司可能缺乏内部资源来开发自己的系统，所以面临着相互矛盾的解决方案。安全往往是大企业关注云计算的首要原因，但同时大企业缺乏对共同责任的理解。

CSA 云控制矩阵分解了 SSRM 以及范围适用性映射，以及典型的控制适用性和所有权。采用这种指导将极大地改进框架，并填补我们认为该框架中的一个巨大漏洞。

此外，（目前的框架）没有 NIST 认可的问责途径。我们如何知道各组织是否符合要求?英国标准协会（BSI）为 NIST CSF 创建了第一条认证途径，并在发布前的三个不同的 NIST 研讨会上进行了讨论，但认证或任何其他问责途径或有效性证明在文件中没有得到认可或鼓励。

4、NIST 安全框架的任何特征都应该（可以被）改变、增加或删除和建议的式样

这些可能包括对以下内容的增加或修改：功能、类别或子类别；层级；配置模板；参考标准、框架、模型和指南；关于如何使用网络安全框架的指导；或对关键基础设施的引用与框架更广泛的使用（另见对第 3 条的回答）。

此外，框架中的层级需要被描述为是什么，并形成一个成熟度模型。假设一个组织在各层中的定位没有任何重要的声明，这是不能接受的。

建议增加的子类别包括：

识别：资产管理（ID.AM）——具体参照第三方、外部和云应用程序和服务

ID.AM-2: ...包括云服务和 SaaS 应用的第三方服务

ID.AM-3: ...包括映射到第三方和云供应链的数据流

ID.AM-4: ...包括 IaaS 云、第三方对云的使用

风险评估——风险评估频率和节奏，如采购、采购后（评估）等。

5、对 NIST 安全框架的可用性和向后兼容性的影响

如果功能、类别、子类别等框架的结构修改或改变了，任何影响可能将转变为重大变化。这就需要一个采用框架的组织建立相应的过渡期，以免中断运营并允许系统化和有组织的过渡。

6、NIST 可以改进安全框架或使其更加完善的其他可行方式

（需要）更多关于云安全的专门指导以及认证途径。附加信息参考：CSA CCM（此参考还包括映射到多种法规和框架）；NIST 安全框架与其他风险管理资源的关系。CSA 评论（请参阅我们在供应链风险下的评论）。

7、改进 NIST 安全框架与其他 NIST 风险管理的资源

作为回复的一部分，单独使用这些资源或与安全框架结合使用这些资源同样面临益处和挑战。

这些资源包括：

- 风险管理资源，例如 NIST 风险管理框架、NIST 隐私框架，以及集成网络安全和企业风险管理（NIST 8286）。
- 值得信赖的技术资源，例如 NIST 安全软件开发框架、NIST 物联网（IoT）网络安全能力基线，以及工业控制系统网络安全指南。
- 劳动力管理资源，例如国家网络安全倡议网络安全教育（NICE）劳动力框架。
- CSF 是一个用于快速风险评估的高级框架。映射 CSF 的子类别到 8286、物联网和其他框架以允许进行更深入和更审慎的风险评估。

8、结合 NIST 的框架和使用非 NIST 的方法或框架

NIST 框架与其他自愿的、共识的框架或资源是否存在共性或冲突？NIST 与来自政府机构的其他框架、网络安全相关任务或资源是否存在共性或冲突？是否有方法改进 NIST 框架与其他框架的一致性或集成，例如像 ISO/IEC 2700、ISO/IEC TS 27110 系列

等国际标准？NIST CSF 作为高级别的框架，可以在多个类别中找到共性。但是，扩展的子类别（如问题 4 所示）和附加则需要其他参考资料和方法。CSA 的 CCM 可以将大多数（标准）引用与框架对齐，例如 ISO/IEC 27000 系列、NIST 800-53、AICPA TSP 等等。

9、框架的国际化应用

国际上有许多国家对安全框架进行适用调整的例子。继续使用将重点放在互操作性、安全性、可用性和弹性上的网络安全的国际标准，可以提升创新和竞争力，同时使组织能够更容易和有效地整合新技术和服务。鉴于这种重要性，NIST 应该考虑哪些步骤来确保任何更新都能增加安全框架的国际化使用?

国际上适用的调整有用更新包括在（数据）主权和隐私权的身份类别覆盖中增加数据保护元素，因此保护类别可能需要包括使用中的数据保护。例如：

识别：管理（ID.GV）：

ID.GV-3 包括隐私义务，但没有涵盖（数据）主权或数据位置的子类别。

保护：数据安全（PR.DS）：

保护使用中的数据

10、应考虑纳入 NIST 的在线信息计划的参考资料

该计划旨在定义 NIST 和行业资源以及文件、产品和服务元素与 NIST 各种文件之间的标准化关系，如 NIST 安全框架、NIST 隐私框架、信息系统和组织的安全和隐私控制（NIST SP 800-53） 、NTST 安全软件开发框架以及 NIST 物联网（IoT）网络安全能力基线。

就 CSA 而言，云控制矩阵（CCM） /共识评估倡议问卷（CAIQ）是云安全领域控制措施和评估问题的框架。CCM 还将云安全控制措施映射到 50 多个行业法规/框架（包括 NIST 800-53、FedRAMP 和 CSF），并对可审计性和实施性进行更新。这些是 CSA 安全、信任、保障和风险（STAR）计划的一部分，用于云供应商评估。

11、网络安全供应链风险管理与改善供应链网络安全的国家倡议（NIICS）

在供应链风险管理的网络安全方面，NIICS 面对的最大挑战是什么?NIST 如何在其

目前关于供应链安全工作的基础上，包括源于总统行政令（EO14028）的软件安全工作，来增加对技术产品、设备和服务的信任和保证?

除了建立软件材料清单（SBOM）外，还需要建立云服务的 SaaSBOM。数据识别和保护的部分数据流可以知道 SaaS 和其他第三方应用程序的云供应链组件。参见 CSA 作为 SaaSBOM 考虑的参考。

12、管理供应链中与网络安全有关风险所需的方法、工具、标准、指南或其他资源

NIST 欢迎在狭义的领域（如硬件或软件保证或保证的服务，或具体的服务）对此类资源的投入。潜在的低风险、高回报的资源可以在不同的学科、部门或利益相关者之间得到促进；以及在大规模和极度困难的领域更广泛地利用。

13、其他差距，以及开源的考虑

在现有的网络安全供应链风险管理指南和资源中是否观察到差距，包括它们如何适用于信息和通信技术、操作技术、物联网和工业物联网?

此外，NIST 的软件和供应链指导和资源是否适当地解决了与开放源码软件相关的网络安全挑战?是否有其他方法、工具、标准、指南或其他资源需要 NIST 考虑，以实现整个软件供应链的更大保障，包括开源软件?

就 CSA 而言，除了 CSA 针对云的 CCM 指南外，CSA 还开发了用于物联网环境中的安全控制矩阵：CSA IoT 控制矩阵（物联网安全控制矩阵）。开源软件和云的漏洞也在全球安全数据库中统一跟踪。

14、框架和网络安全供应链风险管理指南的整合

是否以及如何将网络安全供应链风险管理的考虑因素进一步整合到更新的 NIST 安全框架中，或者是否以及如何由 NIST 制定一个新的和单独的专注于网络安全供应链风险管理的框架？这些都可能是有价值的和更合适的（讨论）。

二、CSA 的整体建议

在为 NIST 安全框架提供指导和框架修改方面，有关的风险管理考虑整体概述如下：

1、目前的框架虽然针对关键基础设施，但没有提供指导或讨论：当该框架应用于指定

的关键基础设施部门而非真正的关键部门时，如何校准组织的风险容忍度（def） 以及相应的风险偏好（def）。从风险的角度来看，确定关键部门的推论是该组织对风险的容忍度低于非关键部门。因此，应该提高安全控制、政策和程序的强度，以最大限度地减少暴露和成功攻击的风险和可能性。这对组织如何设计企业风险管理计划（ERMP）至关重要。企业风险管理计划能够确保组织的关键部门适当地处理和加强控制，以达到降低组织的风险容忍度的需求。

2、目前的 NIST 框架没有识别也没再讨论与采用和/或使用基于云的服务和平台有关的技术和其他风险。当务之急是认识到、并衡量此类"固有风险"，以及将其纳入组织的风险登记（册），以确保建立相关的和适当的控制、程序和流程，有效管理所有引入的云风险。

3、以下给出旨在识别和讨论组织采用云计算相关的大量固有风险（的示例）。

云组件	风险因素
云战略	缺乏统一的云计算战略，或与其他战略不一致。 供应商或客户缺乏/集中风险。 针对云的管理效率低下。 缺少执行战略的技能和经验。
共享服务模式（与责任分担模式）	订阅公有云供应商的服务，将使客户立即暴露在一个新的管理模式下。这种模式在云客户和云提供商之间分配了各种角色和活动。 云客户有责任创建必要的实践和措施，以验证云提供商的正确表现。SRM 模式下的服务质量、违约或赔偿责任也应在合同中预先约定。
丧失对技术资产的控制或访问（能力）	在除私有云部署外的云模式中，客户失去了对所有物理技术资产的自治和访问。这可能会大大降低客户直接控制相关技术资产性能的能力。 此外，还直接影响到保证和持续监控的概念。同样， CSF 中也提到了这些要求，但在基于云的环境中，需要额外的指导。
网络安全	一旦上云，云生态系统立即将组织暴露在来自全球各地威胁者的无法衡量的威胁和风险之下。 在 NIST CSF 最初发布时，这种规模的风险（相对）不存在的，并（在当时）也不以云服务为目标。

数据治理	数据是许多基于云的产品和服务背后的“货币”（资产）。设计不当的实践和方案会导致糟糕的业绩、合规和监管的罚款和处罚，以及声誉和信任的破坏。
业务	运作的弹性和一直在线将成为组织的必要性。如果不符合要求，就会导致业务失败。 在基于云的生态系统中，业务弹性和恢复成为一个关键问题，虽然 CSF 中有这些概念，但没有指导如何在基于云的环境中实现和测试。
遵从（法律）	完全遵守所有相关客户的（可适用）法律是一项预期的服务，但对持续符合的验证难达到和保持。 应该为任何 CSF 的更新制定相关的指导和要求，特别是供应链风险，因为合现性可能需要境外 CSP 为基于外国法律法规和/或要求提供服务。
配置错误	据 Gartner 估计，到 2025 年，超过 99%的云计算故障与客户的错误配置和错误管理有关。NIST CSF 的更新提供了一个理想的机会来加强框架，以减少这些预计的失败率，并制定指导和准则，使客户能够更有效和高效地管理他们的云服务提供商的组合。
事件响应与处置	当不存在对技术资产的控制和访问时，制定一个有效的事件响应(IR) 和管理计划可能具有挑战性和成本压力。 NIST 的事件管理框架应号 CSF 紧密结合。NIST 计划的准备阶段需要大量的前期工作和协调，因为临时获取信息和分析以处理潜在的违规行为和补救真实的违规行为可能需要在自动化、监控和报告方面进行大量投资。
供应商的选择与监测	这一因素在范围、规模和执行方面都具有重要意义，并与从传统技术平台向基于云的服务的迁移成正比。 获取技术服务的便利性与确保所有云供应商得到适当审查的潜在困难相结合，使 NIST CSF 有理由提高管理这种风险所需的严格程度。这对关键基础设施部门的云供应链管理尤为重要。在任何 NIST 框架的更新中，这一领域都需要予以重大关注。
绩效管理	失去对成功所需的资产/资源的直接控制和获取，会带来新的和难以管理的风险。 依靠合同和支持性条款和条件来管理结果和绩效，对许多组织而言可能需

	要新的技能和能力。
员工学习	缺乏有经验的人员，是许多组织实现和保持成功的一个重大挑战。 需要对现有人员的继续培训与赋能，为业务和服务质量带来新的风险。

（相关基础概念，暂略）