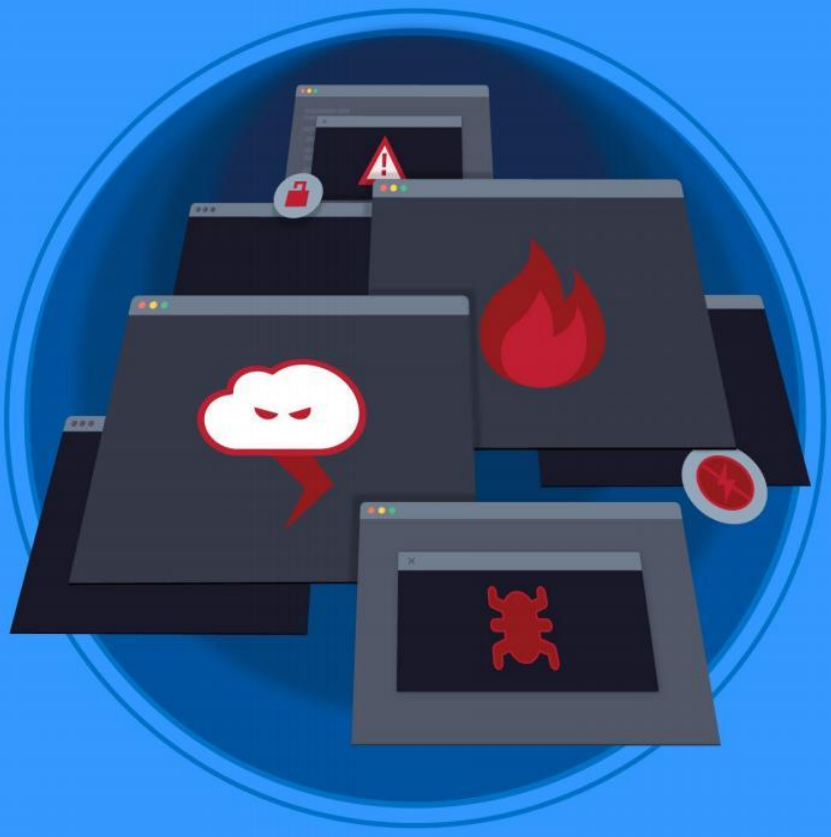
云事件响应 (CIR) 框架



CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

云事件响应工作组官网网址：

https:// cloudsecurityalliance.org/research/working-groups/cloud-incident-response/.

序言

随着云计算应用的深入，云计算在带来价值的同时，也带来了新的安全与技术挑战。随着《网络安全法》、《数据安全法》、《个人信息保护法》的相继推出，如何设计有效的纵深实时云安全防御体系成为信息安全从业者亟待解决的首要问题。其中如何制定网络安全事件应急预案、启动应急预案，网络安全信息收集、分析、通报和应急处置等成为困扰很多企业的问题。

云计算是一个与传统环境完全不同的领域，将云事件响应与传统事件响应流程区分开来的三个关键方面是治理、可见性和云的责任共享。一个好的事件响应计划有助于确保组织在任何时候都充分准备。

CSA旨在为用户提供一个广泛使用的整体框架和一致的视图，目的是为云用户提供有效准备和管理云事件后果的指南，并为云服务提供商与客户共享云事件响应实践提供透明和通用的框架。

全面的事件响应建设是任何旨在管理和降低风险的组织不可或缺的能力。许多单位由于没有可靠的云事件响应计划，在遇到云事件后出现了很多的管理与技术问题。

云事件响应架构是CSA基于《NIST 800-61》以及SANS《信息安全阅读室事件处理者手册》梳理的用于云安全的管理框架，解决企业从应急准备到应急演练的诸多问题，是企业应用云安全解决方案必不可少的参考资料。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《云事件响应（CIR）框架）（Cloud Incident Response (CIR) Framework）》由CSA工作组专家编写，CSA大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组　长：李　岩

翻译组：贺志生　蒋秋华　吴　潇

薛　琨　殷　铭

审校组：贺志生　殷　铭　李　岩　姚　凯

感谢以下单位的支持与贡献：

北京奇虎科技有限公司　北京天融信网络安全技术有限公司

中国电信股份有限公司研究院

英文版本编写专家

主要作者: Soon Tein Lim　Alex Siow　Ricci Ieong

Michael Roza　Saan Vandendriessche

主要贡献者: Aristide Bouix　David Chong　David Cowen

Karen Gispanski　Dennis Holstein　ChristopherHughes

Ashish Kurmi　Larry Marks　Abhishek Pradhan

Michael Roza　Ashish Vashishtha

审核者: Oscar Monge España　Nirenj George　Tanner Jamison

Chelsea Joyce　Vani Murthy　Sandeep Singh

Fadi Sodah

CSA 全球员工: Hing-Yan Lee Ekta Mishra Haojie Zhuang

AnnMarie Ulskey (封面设计)

特别感谢: Bowen Close

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

关于云事件响应工作组

随着当今新兴和快速演变的威胁格局，有必要建立一个考虑云中断等因素范围的整体云事件响应框架（CIR）。云事件响应(CIR)工作组(WG)的目标是开发一个全面的CIR框架，涵盖云事件的根本原因(包括安全性和非安全性) 及处理和缓解策略，目的是为云用户提供有效的详细计划，应对和管理云事件造成的后果。CIR也是一个透明和通用的框架，为云服务提供商与云客户分享云事件提供最佳实践。这个框架的发展包括云事件的必要因素，如操作失误、基础设施或系统故障、环境问题、网络安全事件和恶意行为等。

目录

1. 简介

在当今互联时代，全面的事件响应策略对于需要管理与降低风险概况的组织必不可少。许多没有可靠的事件响应计划的组织与企业在第一次遇到云事件后被粗暴地唤醒。导致重大停机的原因有很多，比如自然灾害、人为错误或网络攻击。良好的事件响应计划有助于确保组织在任意时刻都做好充分准备。然而，在基于云的基础设施和系统的事件响应策略方面，部分由于云的责任共担特性，存在诸多顾虑因素。[1]

许多政府与行业的指南中都有针对传统的本地信息技术（IT）环境制定事件响应的框架，例如《NIST 800-61r2 计算机安全事件处理指南》或SANS 研究院《信息安全阅读室事件处理者手册》。但是，当把云计算环境也考虑在内时，必须修改和完善传统事件响应框架中定义的角色和职责，以便与在不同云服务模式及部署模式的云服务提供商（以下简称：CSP）和云服务客户（以下简称：CSC）的角色和职责保持一致。

目标

本文档旨在提供一个云事件响应(以下简称：CIR)框架，针对破坏性事件的整个生命周期，为CSC提供有效准备和管理云事件的指引。它还可以作为一个透明和通用的框架，为CSP与其CSC共享云事件响应提供最佳实践。

目标读者

主要受益者是CSC。该框架指导CSC确定组织的安全需求，从而选择适当的事件保护级别。通过这种方式，CSC可以与CSP协商，或为其量身定制安全能力——提供相对清晰的安全角色和责任划分。

2. 规范性引用文件

CIR框架参考了多个业界公认的标准与框架，用于云事件的规划和准备、缓解策略和事后分析过程。

---

[1] Cloud Security Alliance, Cloud Incident Response, https://cloudsecurityalliance.org/research/working-groups/cloud-incident-response/

- CSA 云计算关键领域安全指南v4.0
- NIST 800-61r2 计算机安全事件处理指南
- ITSC技术参考（TR）62 – 云中断事件响应（COIR）
- FedRAMP 事件通信程序
- NIST 800-53 信息系统和组织的安全与隐私控制
- SANS研究院 信息安全阅读室事件处理者手册
- ENISA 云计算风险评估

图1显示了CIR阶段和主要参考文件之间的关系

5.1 准备和后续评审阶段	5.2 检测和分析阶段	5.3 遏制，根除和恢复阶段	5.4 事后分析阶段
CSA 安全指南V4.0	**CSA 安全指南V4.0**	**CSA 安全指南V4.0**	**CSA 安全指南V4.0**
9.1.2.1准备和后续评审	9.1.2.2 检测与分析	9.1.2.3 遏制、根除和恢复	9.1.2.4 事后分析
NIST 800-61r2	**NIST 800-61r2**	**NIST 800-61r2**	**NIST 800-61r2**
3.1准备	3.2 检测与分析	3.3 遏制、根除和恢复阶段	3.4 事后活动
TR 62	**TR 62**	**TR 62**	**TR 62**
0.1云中断风险	4.2 COIR分类	5.2 云中断中：CSC	5.3 云中断后：CSC
	5.1 云中断前：CSC	6.2 云中断中：CSP	6.3 云中断后：CSP
	6.1 云中断前：CSP		
FedRAMP事件通信程序	**FedRAMP 事件通信程序**	**FedRAMP事件通信程序**	**FedRAMP事件通信程序**
5.1准备和后续评审	5.2 检测与分析	5.3 遏制、根除和恢复	事后分析
NIST(SP)800-53 r4	**NIST(SP)800-53 r4**	**NIST（SP）800-53 r4**	**事件管理手册**
3.1选择安全控制基线	附录F-IR	附录F-IR	7 经验教训
附录 F-IR IR-1, IR-2, IR-3, IR-8	AT-2, IR-4, IR-6, IR-7, IR-9, SC-5, SI-4	IR-4, IR-6, IR-7, IR-9	8 检查清单
事件处理者手册	**事件处理者手册**	**事件处理者手册**	
2 准备和后续评审	3 识别	4 遏制	
8 检查清单	8 检查清单	5 根除	
		6 恢复	
		8 检查清单	
ENISA 云计算风险评估			
业务连续性管理，79页			

图1： 事件生命周期和规范引用

3. CIR定义

- 资产：资产是任何对组织有价值的东西。资产可以是抽象资产(如流程或声誉)、虚拟资产(如数据)、有形资产(电缆、设备)、人力资源、金钱等[2]。
- 事件：损害网络和信息系统核心服务运行的问题。
- 可报告事件：被认为具有足够重大影响的事件，根据法律或法规需要向实体外部报告。
- 事件处理[3]：针对违反安全实践和推荐实践的问题/事件采取的纠正措施。
- 事件响应计划：一套清晰的指示，帮助组织准备、检测和分析事件并从事件中恢复。
- 事件报告：报告方(云提供商或云运营商)应向国家主管部门提交报告的程序，其中包含有关事件的临时信息。
- 影响：在事件解决之前，衡量事件造成的损害程度。
- 根本原因：导致事件发生的原因(最终的根本原因)。(根本原因分析可能识别多个“因果关系”，但只有一个是根本原因)
- 威胁：威胁是任何可能对信息系统造成损害的情况或事件，其形式包括破坏、披露、数据的不当修改和（或）拒绝服务。[4]
- 漏洞：特定系统、模块或组件中的缺陷或弱点，使其容易因攻击、灾难或其他原因而受到损害。

[2] ENISA 2015, Technical Guideline on Threats and Assets, https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets
[3] NIST.SP800-61r2: Computer Security Incident Handling Guide
[4] NIST SP 800-32 under Threat NSTISSI 4009

4. CIR概述

CIR可以定义为在云环境中管理网络攻击的过程，包括四个阶段:

- 第一阶段: 准备和后续评审
- 第二阶段：检测与分析
- 第三阶段：遏制、根除和恢复
- 第四阶段：事后分析

CIR系统与非云环境的事件响应(IR)系统在治理、责任共担和可见性等多个关键方面有所不同。

治理

云中的数据驻留在多个位置，可能使用不同的 CSP。 让各个组织共同调查一个事件是一项重大挑战。对于拥有庞大客户群体的大型 CSP，这也是一种资源消耗。

责任共担

云服务客户、CSP和（或）第三方提供商在确保云安全方面都承担着不同的角色。通常，客户对其数据负责，CSP对其提供的云基础设施和服务负责。云事件响应需始终在各方之间协调。

根据所选择的云服务模式，例如软件即服务(以下简称：SaaS)、平台即服务(以下简称：PaaS)和基础设施即服务(以下简称：IaaS)， CSP和CSC之间的责任共担领域也有所不同。这个观点必须很好地理解。例如，在IaaS中，由CSC管理操作系统(OS)。因此，操作系统的IR责任也属于CSC。

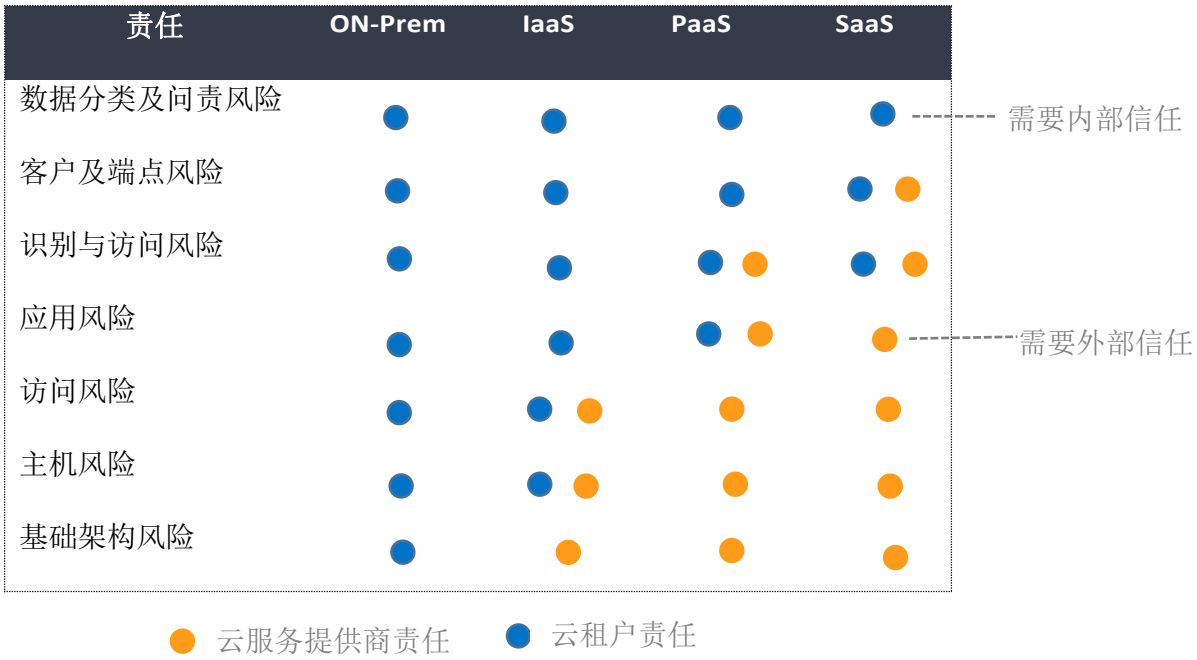


图 2：CSC和CSP共同责任风险矩阵[5]

必须详细讨论角色和治理在与CSP的合同或服务水平协议 (SLA) 中是否清晰并详细地记录。CSC不应制定或满足任何无法执行的政策。组织应该明白，他们永远不能外包治理部分或分担责任。

服务提供商多样性

组织应具有一致且定义明确的多云战略/框架，以与 CSC、CSP和（或）第三方云提供商合作。任何采用单一 CSC、CSP或第三方云提供商的“全面”战略的组织都在间接引入单点故障，要防止服务提供商端出现中断。

提供云服务的单一CSP方法可能会导致CSC/CSP一旦出现组织无法控制的故障，组织的业务可能会遭受持续中断。这种情况将严重影响业务运营，并增加业务连续性计划 (BCP) 策略无法恢复的可能性，从而导致系统性CIR事件。

从CIR的角度处理服务提供商的多样性时，还鼓励组织在其计划中考虑数字服务主权的各个方面（例如，数据驻留、数据主权）。

[5] Microsoft TechNet 25 October 2019, Shared Responsibilities for Cloud Computing, https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

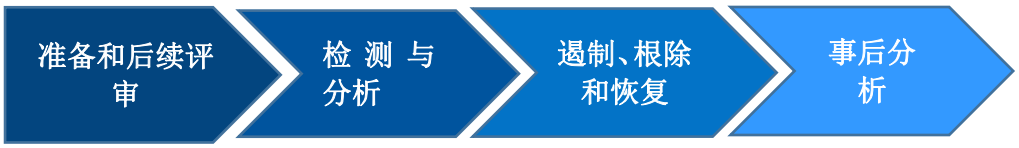
可见性

云中缺乏可见性意味着本可以迅速补救的事件没有立即得到解决，并且有进一步升级的风险。如果利用得当，云可以提供更快、更便宜和更有效的IR。CSP及其合作伙伴已经提供了许多内置的云平台工具、信息源、服务和能力，显著增强检测、反应、恢复和取证能力。在利用云架构而不是传统的数据中心模型开发IR流程和文档时，必须小心。CIR必须是主动的，架构必须能够在整个过程中抵御故障。

5. CIR架构

事件响应和管理被认为是反应性行动，最大限度地减少事件爆发的损害。它是任何信息安全计划的关键方面，如 《CSA 云计算关键领域安全指南 v4.0》[6] 的第九个域中所述，通过定义适当的事件响应流程和计划，CSC可以确保管理和控制检测到的事件。

如本文第 2 章所述，许多组织已经制定并记录了事件响应和管理框架。不同的框架有其目标和受众。该框架采用了《CSA云计算关键领域安全指南》和《NIST计算机安全事件处理指南》(NIST 800-61rev2 08/2012)中普遍接受的“事件响应生命周期”。



5.1 第一阶段：准备和后续评审

在准备阶段，有必要建立事件响应能力，以便组织做好响应事件的准备。换句话说，了解环境和“敌人”至关重要。

当事件发生时，CIR要实现以下目标：

[6] Cloud Security Alliance 2017, Security Guidance for Critical Areas of Focus in Cloud Computing v4, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

- 提供快速检测、隔离和遏制
- 最大限度地减少个人数据、专有信息和敏感信息的暴露和泄露
- 最大限度地减少对业务和网络运营的干扰
- 为适当的检索和证据处理建立控制
- 向所有受影响的各方提供事件沟通
- 提供准确的报告和有用的建议
- 保护组织的声誉和资产
- 根据经验教训教育员工
- 根据经验教训审查和改进CIR计划

要了解组织的事件响应能力，传统IR框架和CIR框架之间的关键区别之一是CSC和CSP之间存在“责任共享模型”。在传统的IR框架中，拥有系统的组织将单独对系统负责。其计算机事件响应团队(CIRT)应制定流程、程序、计划和手册处理不同类型的事件，包括安全事件。由于组织仅管理系统，因此CIRT指挥官或领导应协调、管理和监督所有受影响的系统，并从这些系统中收集必要的日志和工件。

但是，在云环境中，CSC并不是所有系统的所有者。根据采用的服务模型及其相应的责任共担模型，一些工件和日志由CSP管理。当第三方 IR 提供者参与时，CIR 计划也应将它们包括在整个过程中。这个时刻为组织提供了一个合适的机会考虑审查任何第三方 IR供应商，确保在紧急响应情况下需要时能够快速获取资源。

组织应熟悉并充分利用其CSP的业务连续性和灾难恢复功能，以便在事件中调用。因此，CSC有必要了解CSP的IR程序，并通过SLA和合同与它们保持一致。为了管理和执行这一举措，CIR计划应包括：

1. 现有环境、云架构、责任模型分析。

   a. [CSC]识别和准备要使用的云服务的清单、服务组件以及相应的服务模型和部署模型。

   b. [CSC]审核合规要求（如数据隐私和当地监管要求）并提取合规要求，如数据泄露报告时间要求。

c. [CSC]收集现有的合同和SLA，根据责任共担模型确定云架构中各方的角色和责任以及各自的义务。对角色和职责的清晰描述可防止任务重叠或忽略，以及在事件期间分配角色时浪费不必要的时间。

d. [CSC]收集不同方（内部团队、托管服务提供商、CSP或其他第三方）之间的联系方式。事件报告结构应包括联系信息，例如电话号码和电子邮件地址。

e. [CSC]从CSP处获取事件援助团队。事件援助团队包括服务台、现场支持团队和其他援助服务，例如安全运营中心或SOC。

f. [CSC]审查CSP的委派管理权限，允许CSP以与超级用户相同的权限级别访问CSC的租户。尽管CSP可以对CSC的租户实施强大的安全控制，但破坏CSP的威胁行为者可能能够访问CSC的环境。因此，CSC应验证其CSP是否需要这些委派的管理权限。如果CSP需要委派的管理权限，CSC应确保CSP实施了适当的控制措施，例如监控，从而提醒CSC潜在的滥用。CSP还应利用条件访问策略限制对CSC环境的访问（如适用）。如果CSP不需要委派的管理权限，则CSC应确保CSP已删除此权限。最后，建立CIR组织（CSC和CSP）。

g. [CSC]将收集到的联系人和已确定的组织内各方组成事件响应团队。

h. [CSC]定义CIR的组织结构，并任命事件响应指挥官、相应的系统所有者、技术响应负责人和技术协调员。根据上一步中确定的角色和职责（对现存环境、云架构和责任模型的分析），CSC可能必须指派一个技术响应领导支持在IaaS中实施的系统，或安排技术协调员沟通和收集事件的支持指标或日志。

[第二阶段：检测和分析]。确保所有云组件都由负责方处理。

2.为有效和高效的CIR响应和补救制定事件处理计划、流程和程序/自动化（CSC和CSP）。

a. 创建突发事件报告流程和流程，记录电话号码和电子邮件地址等联系信息。

b. 发布跟踪系统，记录和跟踪突发事件的状态。

c. 制定事件响应过程和程序，包括与第三方的协调和危机沟通，建立具有清晰角色和职责分离的沟通矩阵，确定升级计划，分配人员，确定程序，正式分配职责。

d. 制定流程，根据组织的变更更新CIR计划

e. 确保获得存档的经验教训，所有团队成员都可以访问这些经验教训以供参考。

f. 订阅第三方威胁情报服务，了解当前和潜在威胁的情况。

g. 通过模拟的事件场景测试CIR计划，作为员工培训的一部分；理想情况下，每年审查和更新该计划。无论这个计划的构思有多周密，如果员工没有做好充分的准备都会失败。

h. 为员工在其职责范围内的任务制定持续的培训流程，使员工具备必要的知识，以便在需要的时间作出反应。

i. 在CIR计划和程序中定义并记录CIR组织的联系人列表。联系人名单应定期更新。

3.技术层面的准备(CSC和CSP)，主动监控运行错误和恶意活动的指标。

a. [CSC]定义的角色和职责应该来自前一步（对现有环境、云架构和责任模型的分析）。CSC应该审查整个架构，确定架构中是否存在任何偏差。CSC将通过相应的内部团队在以下阶段通过责任共担模型执行事件响应过程。CSC应该从CSP中收集由CSP处理的日志和健康状态。

b. [CSC]应该将从CSP收集的日志和健康状态与CSC定义的日志和健康状态列表比较，确保收集了要分析的必要日志。CSC还应该了解从CSP中收集到的日志和工件的局限性，特别是在预期日志的可用性和保留期方面。

c. [CSP]应通过主动扫描系统和数据中心的健康状况和网络监控，不断监控基础设施和应用程序。

d. [CSC]应定义预防措施，如具有关键操作和存储、存储备份、入侵检测系统和防御系统、文件完整性监控系统、防病毒解决方案、漏洞修复和防火墙的冗余，以及采用安全软件开发生命周期(SDLC)实践。

e. [CSC]应确定集中的日志管理和日志分析设施的位置。在许多CSC环境中，日志存储在由CSC建立的不同CSP设施和云服务器中，也可能存储在企业内部部署服务器中。应整合日志以进行有效的事件响应和分析。

f. [CSC]应定期评估脆弱性和风险，包括威胁检测能力，以改善安全态势。

g. [CSC]应维护事件分析的硬件和软件以保存日志文件，用于数字取证、恢复备份、报告编写等。[CSC]应建立一个自动化的支持机制请求协助或分发信息。CSC还应识别并准备用于云环境中事件响应的跳跃工具包。

h. [CSC]应验证内部文档包括端口列表、资产列表、网络图和当前的网络流量基线。

i. [CSC]应建立强大的业务连续性计划(BCP)并显著提高组织的运营弹性，以从突发事件中管理和恢复过来。该范围应包括CSP提供的服务。

j. [CSC]应购买可用的网络保险，可能有助于减轻云事件的潜在财务影响。[7]

k. [CSC]应该了解CSP日志记录模式，以及与企业内服务日志记录的不同。动态字段的使用可能会限制CSC在安全信息和事件管理(SIEM)解决方案中查询必要数据和创建高效警报的能力。

l. [CSC]应记录日志记录需求，因为CSP产品可能不具备在集中式SIEM中支持必要日志收集的能力。

4.沟通渠道准备（CSC和CSP）

a. [CSC]应组建公司团队，作为与CSP的所有通信的主要、唯一的联系人。

b. [CSC]与应外部各方制定危机沟通协议，如与CSP之间。沟通方法还应准备好触达组织内部或外部的关键各方，以便在事件期间顺利沟通。

c. [CSC]应确保团队应该有更新的内外部各方联系名单。紧急联系人名单应包括组织内外部的其他事件响应团队、随叫随到的工作人员信息、法律顾问、执法人员和其他重要的事件处理人员设施。

前面的列表总结了在事件响应准备阶段所产生的可交付成果清单：

[7] Wikipedia, Cyber insurance, https://en.wikipedia.org/wiki/Cyber_insurance
AIG, Cyber insurance, https://www.aig.com/business/insurance/cyber-insurance
CHUBB, Cyber Insurance https://www.chubb.com/sg-en/business/cyber-insurance.html

1. 创建一个IR计划、策略和程序。
2. 开发资产清单列表（包括云服务、服务器、帐户列表、已实施的安全防御机制、预期的日志文件和设施）。
3. 制定事件响应角色矩阵(包括CSC的CIRT和CSP中的其他参与者的角色)。
4. 事件响应演练测试计划和测试结果。
5. 事件响应弹射座椅工具箱。

5.1.1 文档编制

在整个IR过程中，组织应维护事件文件，确保有系统的记录，有效地审查事件和经验学习。组织应管理突发事件记录中的以下信息：

1. 事件的当前状态（“新的”、“进行中的”、“转发进行调查”、“已解决”等）。[8]
2. 该事件的摘要。
3. 与该事件有关的妥协指标。
4. 与原事件有关的其他事件。
5. 此事件处理者采取的操作。
6. 监管链，如适用。
7. 与该事件相关的影响评估。
8. 其他相关方（如系统所有者、系统管理员）的联系信息。
9. 在事件调查期间收集到的证据清单。
10. 来自事件处理人员的反馈。
11. 下一步计划（例如，重建主机，升级应用程序）。
12. 限制适当人员访问事件记录，因为它可能包含具有监管或合规影响的敏感信息、IP地址、被利用的漏洞、机密业务信息。

[8] NIST.SP800-61r2, Computer Security Incident Handling Guide

13. 回顾/经验教训：记录任何经验教训，如成功、改进领域、避免措施和改进结果的新程序。

5.2 第二阶段：检测和分析

5.2.1 诱因

5.2.1.1 云事件的原因

本文档中定义的云事件会损害IaaS、PaaS、桌面即服务(DaaS)、SaaS和CSP提供的相关服务的操作。云事件可能导致云中断（云服务不可用的时间）。云突发事件的原因和停机时间可分为以下几种类型：

1. 自然灾害因素（如洪水、火灾）
2. 系统问题因素
    a. 内部问题（例如，软件缺陷、硬件故障）
    b. 外部（例如，断电、电信网络连接问题）
3. 人为因素
    a. 非故意的（如人为错误）
    b. 故意（例如，政府制裁、黑客/DoS攻击、勒索软件）

5.2.1.2 事件的标志

在事故发生前，通常会有一个标志。根据美国国家标准与技术研究所(NIST)的定义，构成标志的场景包括：

- 前兆（未来可能发生事件的标志）。
- 指标（事件可能已经发生或可能正在发生的标志）。

	前兆	指标
自然灾害	恶劣天气预报	多个电源中断
系统问题	• 对多个软件服务的响应均滞后 • 显示漏洞扫描程序使用情况的Web服务器日志条目	• 多个电源中断 • 供电电源有明显的波动期 • 直流电(DC)连续升温周期 • 当针对数据库服务器发生缓冲区溢出攻击尝试时，网络入侵检测传感器发出警报
人为	• 针对组织邮件服务器的新漏洞发布。 • 来自一个团体的威胁，声明该团体将攻击该组织。	• 防病毒软件在检测到主机感染了恶意软件时发出警报。 • 系统管理员看到具有异常字符的文件名。

图3：突发事故的迹象

5.2.1.3 常用前兆和指标的来源

CSP和CSC必须要有一个系统或过程来检测这些前兆和指标，从而预防事故的实际发生。前兆和指标常用的来源包括：

1. 报警
2. 日志
3. 入侵指标(IoC)
4. 行业活动
5. 市场分析报告
6. 威胁情报报告
7. 公开可获取的信息
8. 民众
9. 社交媒体

建议通过系统收集和分析这些前兆和指标，包括系统日志、报警、SIEM、安全运维中心和综合运维中心。理想的情况是通过综合运维中心监控和关联分析各种各样的报警、日志、事件、请求和高级网络态势感知日志。所有情况下，这些收集和分析的范围必须覆盖云管理平面而不只是部署的资产。

5.2.2 分析事件判断影响

5.2.2.1 事件分析

有一部分事件信息收集的精力是判断该问题是假阳性或假阴性。如果问题判断是“假报警”[9]，那么文档（也就是工单）应该将该评估更新并关闭该问题。必须评估每个指标，确定其合法性。

事件分析的建议包括[10]：

1. 网络和系统配置管理：系统配置管理——比如基线配置——将有助于更好地识别变化。
2. 理解常规行为：实施日志审查将让分析师更好地注意趋势，比如时间轴上的趋势。异常的趋势可能表明一个事件的发生。
3. 事件相关分析：事件的证据可能从几个包含不同数据类型的日志中发现。防火墙日志中可能有源IP地址，而应用日志中可能包括用户名。
4. 运行包嗅探工具收集辅助数据：有时，指标并没有记录足够的细节使处理者能够理解正在发生的事情。如果是事件发生在网络上，收集必要数据最快的方法就是用包嗅探器捕获网络流量。
5. 采用数据分析工具来分析所有数据集：解决大量指标的一种有效策略是过滤掉往往不重要的指标类别。另一种过滤策略是只显示最重要的指标类型。但是，这种方法具有很大的风险，因为新的恶意活动可能不属于选定的指标类别之一。因此，最好可以部署数据分析工具监控所有收集的指标。

5.2.2.2 事件通知

[9] The SANS Institute, 2011, Following Incidents into the Cloud
[10] NIST, Computer Security Incident Handling Guide, SP.800-61r2

事件响应计划需要系统地安排使得业务和服务运营影响最小化，并且在事件发生时通知相关方。事件发布应该取决于事件影响的严重程度。由于高度复杂的云环境存在大量的事件，只有那些关键和影响严重的事件才需要通知高层。CSP和CSC应将事件发布矩阵集成到双方合同和（或）SLA中。备注：CSP应该要求CSC通知CSP任何重要事件，因为这些事件可能对CSP的基础架构和运维形成威胁。

为了进行准确的报告，应从事件报告者和受影响环境（如可能）收集以下关键信息（5W）：

1. 发生了什么？用户在事件前后采取行动了吗？
2. 事件发生在哪里？被控制了吗，或者还有其它区域受到影响？非受影响区域的置信水平如何？
3. 什么时候发生的？
4. 谁发现的？谁受到或没受到影响？是如何被发现的？
5. 为什么事件会发生？事件源头或零号事件是否被发现？

5.2.2.2.1事件通知时机

通知时间至关重要。尽管需要快速处置事件，但是尽快通知利益相关方也同样重要，使得他们理解当前情况从而能够建议和采取必要行动降低事件影响。危机管理计划需要管理与服务或业务停用相关的所有事件，包括网络攻击。在事件处置的过程中，危机沟通是危机管理计划不可分割的一部分。糟糕的事件管理可能导致监管罚款、声誉受损、客户信任损失和严重的财务损失。

- 起始的事件通知应该在最开始的2-8个小时内发布给内外部关键利益相关方，使得在CSC/CSP/第三方供应商之间能够开始水平审视。
- 在最初4-48个小时内一份包括前4Ws信息的主要的事件报告应该在内部利益相关方之间分享（取决于事件的影响）。当必要情况下，外部利益相关方（CSP/第三方供应商）应该需要包含在事件调查和影响限制工作中。必要时，外部利益相关者也可能需要参与。
- CSC/CSP通常根据通用合同条款和条件在商定的时间框架内自我报告。如果此报告阈值满足要求并与总体事件管理框架一致，组织可能希望予以审查。

- 组织必须知道运营所在国家/行政区/地区监管要求。例如欧盟数据保护法（GDPR）要求公司必须在被破坏的72个小时内报告（当可行的情况下）。该要求对任何组织都有效，只要组织的目标或收集数据是有关欧盟的人们和（或）处理有关欧盟居民的个人数据。

根据上报工作流程，组织应通过商定的媒介（电话、短信、电子邮件等）快速发送通知。根据CIR计划的约定，不同严重程度的事件应上报给不同的执行和管理方。如果对业务连续性或声誉有重大影响，组织还应启动BCP和（或）危机管理计划（CMP）。

5.2.2.3 事件影响

事件影响模型必须事先建立，CSP和CSC使用该模型保障在事件评估、事件影响、通知和相应的响应活动的一致性。事件优先矩阵（也被称为“影响和应急矩阵”）来源于影响的严重程度和应急水平。必须开展快速而正确的影响评估判断损失程度。下面例子包括了CSP和CSC应该共同考虑的关键影响类型：

- 业务：业务危急的范围和水平
- 财务：停工损失或声誉损害
- 监管/法律：数据隐私和合同条款

组织必须根据忍耐度和风险偏好建立和定义合适的影响严重水平分类。根据欧盟网络安全法云安全事件报告，一个或多个参数可以评估影响水平。例如：对于一天停工和70%地理扩散，事件影响应该为“等级2/等级1”。根据这个条件，用户需要参考影响等级2和等级1类事件的控制指南。重要的是给出的值只是作为示例。水平值需要通过调整反应组织性质、优先任务和业务目标。

考虑如下因素，应急水平包括最低级别（“等级5”）到最高级别（“等级1/2”）

- 系统或服务当前是否危急？
- 是否有其它的变通办法或缓解措施？
- 有多少用户受到影响？
- 事件能否得到有效的控制？
- 事件扩散慢还是块——是否影响其它用户和系统？

- 还有其它考虑因素吗？比如，是否有潜在的法律或监管后果？

这些自评估将指导所需资源的调动和决定在要求的时间内管理和缓解事件所需的行动力度。例如，最高级影响和应急（“等级1”）的事件将对应“P1”（“优先级1”）选项。它可能是一项危机，需要触发组织危机管理计划（CMP），并发布给高层管理和（或）董事会。

组织需要采用事件分类等级供那些用于帮助用户评估影响严重程度和（或）云服务可用性对业务运营重要性的标准或指南使用。下面是基于当前云服务提供商运营趋势的一套分类策略：

优先级码=事件等级	事件影响	目标响应时间	目标解决时间
1	危急	<5分钟 24小时响应团队	<1小时
2	高	<15分钟工作时间 <2小时工作时间外对于工作时间响应团队. 否则，4-8小时，根据情况	<4小时
3	中	<15分钟 工作时间 < 2小时 工作时间外对于工作时间响应团队，否则，4-8 小时，根据情况.	<8小时
4	低	<15分钟 工作时间 <2小时 工作时间外对于工作时间响应团队，否则，4-8 小时，根据情况.	<24小时
5	很低	系统自动过滤，不需要响应	-

图4.事件响应策略

组织还希望能够开展业务影响分析（BIA）——或者针对组织界限的威胁、脆弱性和风险评估（TVRA）——和考虑购买网络保险用于缓解潜在的云事件带来的财务损失。

5.2.3 证据收集与处理

识别与调查相关的数据对于确定事件的根本原因和识别经验教训以避免重复至关重要。

识别出的数据还可以帮助支持有益的信息共享计划，以防止类似事件的发生。

请注意，由于GDPR或其他合规要求，CSP可能会限制日志的保留周期。在事件响应计划中必须理解并考虑到这些限制，因为日志可用性将影响必要的证据收集(取决于所选择的云服务)

相关数据的可能位置包括附加到虚拟实例的存储驱动器和实例的内存空间。通过利用CSP功能(例如实例快照)，CIR团队可以获得附加到事件的虚拟化存储驱动器的快照，并利用它们进行进一步的分析和发现。这些快照可以安装到数字取证调查资源，以便使用已被广泛应用的取证分析工具集进行审查。

任何收集到的证据也应该经过哈希活动过程。这有助于确保所收集到的信息的完整性，并确保数据没有从其原始来源更改。这项承诺还有助于确保有关潜在法律程序的证据的可采纳性。确保司法鉴定工作是在收集到的证据的副本(而不是经过哈希处理的原始数据) 上进行，以便法院受理。

对于网络安全事件，应采取以下步骤识别攻击主机:

- 验证攻击主机的互联网协议(IP)地址/域/电子邮件/其他信息
- 通过搜索引擎研究被攻击的主机
- 使用突发事件数据库
- 监控可能的攻击者通信通道
- 创建针对SIEM或其他工具的IoC警报，以帮助找到受攻击的主机

任何收集到的证据都应该利用哈希活动确保收集到的数据的完整性。这一过程可用于验证证据没有从其原始来源更改，并有助于确保潜在法律程序中的可接受性。

5.3 第三阶段：遏制、根除和恢复

遏制：在应对安全事件时，遏制损害的方法对于事件和组织是独一无二的。在正确识别事件后，根据事件类型列出所要采取的行动策略。遏制隔离被感染的系统。

注意:根据事件及其影响，遏制、根除和恢复可能都是同一过程的一部分。

在检测到安全事件时，遏制是必不可少的，以防止进一步的攻击者活动和系统重新进入。不受约束的活动可能会耗尽资源或增加损害。从攻击者的角度来看，典型的攻击从最初的妥协开始，然后通过下载恶意软件建立据点，升级权限，然后进行网络探索。到目前为止，攻击者可能仅限于一台机器，无法窃取数据

接下来，攻击者可以通过在少量其他机器上安装不同的恶意软件横向移动并建立持久性。这使得恶意软件的检测风险很低，同时提供了重新进入网络的方法。攻击者现在已在系统中建立起来，并将开始执行他们的任务。

一旦发现事件，受影响的组织应执行预定义的CIR计划（在“第一阶段：准备”中所述），例如使系统下线、隔离系统和限制连接。最重要的是不要通过盲删消除威胁，因为这就破坏了CIR计划修订所需的取证证据。遏制措施为制定补救策略提供了时间。遏制的一个重要部分是决策(例如，关闭系统，断开与网络的连接，删除API密钥，禁用用户名)。通过预先确定的事件遏制策略和程序，这种决定要容易得多。在定义和记录策略和程序时，IR团队应该利用方案手册和操作说明简化任务。

各组织应在处理突发事件时确定和定义可接受的风险，并制定相应的战略。遏制策略因事件类型而异。例如，包含电子邮件传播的恶意软件感染的过程与基于网络的DDoS攻击响应完全不同。组织应针对每种主要事件类型制定单独的遏制策略，并将标准明确记录下来以便制定决策。

确定适当策略的准则包括：

- 业务影响
- 潜在的资源盗窃和损害
- 需要保存证据
- 服务可用性(例如，网络连接，提供给外部各方的服务)
- 实施策略所需的时间和资源
- 战略有效性（如部分控制、全面控制）
- 遏制方法的持续时间、复杂性(例如，4小时内删除的紧急解决方案，2周内删除的临时解决方案，永久解决方案)

- 资源可用性(特别是技术专长)
- 备份/副本/快照的可用性和完整性
- 沙箱/蜜罐环境的可用性

适当的遏制策略的最终目标是限制攻击者的行动，并在尽可能短的时间内防止进一步未经授权的访问或感染，同时最大限度地减少服务中断。适当的策略将防止进一步的损害发生，同时保留调查所需的证据。

5.3.1 选择遏制策略

在某些情况下，一些组织将攻击者重定向到沙盒(一种类似蜜罐的遏制形式)，以便监视攻击者的活动(通常是为了收集额外的证据)。IR团队应该与其法律顾问讨论该策略，确定其可行性。

组织不应该实施其他替代方法监视攻击者的活动(沙箱除外)。如果一个组织检测到系统被破坏，并允许这种破坏继续下去，那么如果攻击者使用被破坏的系统攻击其他系统，那么该组织可能要承担责任。

延迟的遏制策略是危险的，因为攻击者可能升级未经授权的访问或危及其他系统。另一个潜在的问题是，一些攻击可能会在遏制后造成额外的损害。例如，一台已被入侵的主机可能会运行一个定期发送给另一个主机的恶意进程，当事件处理程序试图通过断开受感染主机与网络的连接控制事件时，后续的ping就会失败。

由于出现故障，恶意进程可能会覆盖或加密主机硬盘上的所有数据，即使主机已经与网络断开连接，处理程序也不能假定该主机不会受到进一步的破坏

5.3.2 根除与恢复

根除：消除问题。这包括最大限度地减少损失、信息被盗和服务中断，以及消除威胁。根除步骤可能是必要的，可恢复所有受影响的系统的操作水平。必须消除威胁、感染或损害，使系统恢复到可操作的水平。这可能需要清理磁盘，删除受影响的代码和用户账户。

恢复：包括安全、及时地恢复计算服务[11]。恢复过程将系统修复到原始的或增强的状态。

[11] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/

此过程通过应用补丁、重建系统的密钥文件、重新安装应用程序、更改密码和从备份中恢复文件，将其返回到生产过程中。

5.4 第四阶段 事后分析

CIR流程的最后一个阶段是事后分析。这一关键阶段的目标是评估企业和CSP团队如何处理和管理事件，改进未来的事件处理程序。评估的基础是审查事件数据和包含“经验教训”[12]的事后报告。要回答的关键问题是：哪些方面可以做得更好?这种反馈应该转化为新的对策，并返回到第1阶段。

5.4.1 事件评估

对事件特征的分析可以在最低限度上指出安全弱点和威胁、云配置弱点以及事件趋势的变化。这些数据可以作为反馈循环添加到风险评估过程中，可能导致选择和实施额外的控制措施、流程和预防措施。

客观的事后分析还将帮助团队使用收集到的信息衡量CIR过程的总体有效性。

问题可能包括：

- 如何回应的？
- 优势和弱势是什么？
- 从中学习到了什么？

如果事件数据被正确地收集和存储，应该突出IR团队的几个成功度量(或至少是活动)。

5.4.1.1 事件评估指标

还可以收集突发事件数据，确定是否随着时间的推移而存在显著的趋势。这些模式可能会更多地揭示团队在一个确定的持续时间内所做的事情，以及是否有改进（例如，事件数量的减少）或值得增加关注的领域（例如，与安全相关的事件的激增）。在被监管的行业中，组织机构通常必须向监管机构和管理层报告这些信息——尤其是重大事故。CSC应及时、准确和完整地收集必要的数据，以满足这些要求。

---

assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

[12] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

应收集流量日志或其他流量日志等数据，以便审查未经授权的访问或可疑的流量。

收集到的事件数据应该包含以下信息的指标(性能指标):

- 平均检测时间(MTTD)：发现安全事件的平均时间。从事件开始到团队意识到这一点需要多长时间？ 这与攻击者停留时间（攻击者渗透到检测点之间的时间）直接相关。
- 平均确认时间 (MTTA)：安全操作员响应系统警报所需的时间。MTTD 衡量的是攻击者被注意到之前的时间，而 MTTA则侧重于衡量安全操作员响应安全警报和开始分析的时间。
- 平均恢复时间 (MTTR)：使系统恢复运行状态所需的时间（与第 3 阶段相关）。
- 平均遏制时间 (MTTC)：检测、响应、消除和从事件中恢复所需的平均时间。 MTTC可以通过将所有范围内事件的 MTTD、MTTA和MTTR 相加除以范围内事件的数量计算。该指标被认为是一个关键指标（关键绩效指标，或KPI），因为它显示了事件响应团队的组织程度。MTTC升高表明某些子流程在事件响应期间不是最佳的。较低的MTTC表明团队组织良好。
- 威胁指标，例如DDoS攻击时的Gbps或Tbps。
- 威胁行为者TTP（策略、技术和程序）。这些包括网络钓鱼和账户操纵。更多示例可在 MITRE 的 ATT&CK® Cloud Matrix 中找到[13]。

5.4.1.2 事件分类

严重性和紧急性分类(H/M/L)可能会在检查后发生变化。

危及个人身份信息 (PII) 或个人健康信息 (PHI) 的机密性/完整性以及为大量客户提供服务的高严重性事件可能会产生重大的财务影响。示例包括：

- 确认违反 PII/PHI
- 生产系统的成功根级别妥协
- 金融恶意软件

[13] MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques
https://attack.mitre.org/matrices/enterprise/cloud/

- 导致严重中断的拒绝服务攻击

中等严重性事件表示尝试（可能不成功或尚未成功）违反PII或可用性/财务影响有限的事件。示例包括：

- 疑似PII泄露
- 有针对性地尝试破坏生产系统
- DoS 攻击导致有限的系统降级或其他性能问题
- 低严重性事件不会影响 PII、可用性或对企业或客户的财务影响。 示例包括：
- 尝试破坏非重要系统（例如，登台/测试实例）
- 涉及特定员工的事件
- DoS攻击对客户没有明显影响

5.4.2 事件总结报告

事件结束后，管理事件的CIR团队应使用从先前阶段和事件评估收集的数据撰写正式的事后报告 (AAR)。这项任务在事后阶段至关重要，应在课程仍然新鲜时尽快执行。如果延迟，关键细节可能会丢失或遗忘——可能会对未来的事故预防产生重大影响。CIR团队应在事件结束后的两周内将AAR提交给关键利益相关者。[14]必须制定适当的对策并由（高级）管理层验证。最好使用正式批准的报告模板创建AAR，确保报告始终符合预期标准。

事故报告应包含以下内容：

- 事件的日期和时间
- 事件结束的日期和时间
- 事件范围
- 报告事件的人的姓名
- 受影响人的组织和业务单位
- 事件描述

[14] SANS Institute 2021, Incident Handler's Handbook, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

- 受影响的云系统和提供商/本地资源（硬件、软件、位置）和各自的 SLA
- 业务服务所有者和CSP联系人（如果适用），包括事件管理期间涉及的CSP参与者（如果适用）
- 事件分类（严重性分类）
- 公司/客户影响分析
- 解析度
- 建议
- “经验教训”部分，用于确定成功和需要改进的地方，以制定增强的响应以防止未来发生事件

在撰写报告时，请考虑以下要素：

- 回顾事件的时间轴和任何CIRT和CSPCIRT的观察结果。
- 在“5个为什么”(或“5W”)技术的支持下进行彻底的根本原因分析，识别和审查所有导致事件的因素。
- 优先考虑补救步骤，减少未来再次发生事件的可能性。
- 使用AAR作为新团队成员的培训材料，传达更有经验的团队成员如何应对事件。
- 集中和索引AAR（按分类级别），并为每个事件生成后续报告。在处理类似的未来事件时，报告是有价值的参考。
- 审查沟通渠道（CSP<->CSC）并在必要时更新。
- 审查取证能力并确定“云跳跃工具包”中是否缺少任何元素[15]。
- 查看事件中确定的与可利用的安全漏洞、敏感数据详细信息或影响PII/PHI的其他详细信息相关的数据。
- 查看违规通知时间表（例如，GDPR）和流程。
- 对于CSC，在事件响应期间审查提供的提供商支持，并评估是否需要调整合同以促进增强的提供商支持。

[15] CSA Security Guidance For Critical Areas of Focus In Cloud Computing v4.0, section 9.1.2

通常认为有必要在向高层管理人员报告信息后向更广泛的公众发布报告，促进跨企业的事件信息共享。这种透明度有助于同行更好地识别和控制风险。

5.4.2.1 经验教训

处理安全事件的最后一步是确定学到了什么。如果在与人员、流程或技术相关的事件响应过程中发现差距，则必须加以解决。结束事件的人员必须确保对安全事件进行回顾性审查——这项工作被称为“经验教训”。使用“经验教训”帮助修改和巩固CIR计划。每个IR团队都应主动发展以反映新的威胁、改进的技术和经验教训[16]—改进未来的响应行动。

安全指南：特别注意数据收集限制并确定如何解决未来的问题。由于云数据位于多个位置（并且可能具有不同的 CSP），因此以下注意事项对流程的这一阶段提出了挑战：

- 与从各种第三方提供商（互联网服务提供商）获取和协调事件数据收集相关的挑战
- 来自第三方提供商的资源依赖（可能是由于来自其客户端池的依赖大小）。

以下建议的问题可以帮助CSC提出自己的查询：

- 服务层的哪些部分有问题？对受影响的应用程序和用户有何影响？
- 问题持续了多长时间，在什么时间？
- 问题原因是否已知？
- 学到了什么可以防止或减轻这一事件的发生？
- 应该采取什么行动？
- 从安全角度看，有什么可疑之处吗？
- 提供商或经纪人提供事件支持（如果适用）的效果如何（或多快）？
- 用于法医证据收集的范围内技术的识别程度如何？
- 是否有人——或者自动监控或其他扫描系统——检测到远程连接上的未经授权的访问或可疑流量？ 从事件发生之时起，整个事件生命周期中的角色和责任是否清晰？

[16] NIST.SP.800-61r2 Computer Security Incident Handling Guide

- 这些技术是否引起了警觉？
- 以前的“低级”事件能否与根本原因联系起来？

5.4.3事故证据保留

在“第2阶段检测和分析”期间收集的所有已识别证据必须根据企业适用的法律、法规、行业或合同义务的要求予以保留。为以下三 (3) 个目的保留证据：

- 监管合规要求（即审计日志、警报生成、活动报告和数据保留的特定级别和粒度）。数据保留可能不是受提供商影响的标准服务协议的一部分。
- 法律：支持对破坏PII/PHI或企业系统的起诉。
- 风险管理：反映和重新评估新的威胁策略和技术。
- 培训：为了促进团队更好地为未来的事件做好准备，将适应性事件学习纳入其中。[17]

企业取证模型必须能够促进所需的证据保留期限和所使用的技术。根据之前的 CSA 指南。[18]CSC应与CSP合作评估事件处理。在云环境中保留数字取证证据必须视为CSP和CSC之间的集成模型。[19]

6. 协调和信息共享

要解决事件响应方面的责任共担模型的复杂性，需要云用户和CSP进行大量且多样的主动投资。有效地使用这些投资对于确保高效和有效的CIR至关重要。所有云利益相关方应该共同制定CIR的短期和长期目标。长期目标的一些例子包括建立/持续增强框架，让受影响的用户参与进来以减少损失和制定业务恢复方法的战略。

提供者和用户之间的沟通路径应该适当建立。应该为任何受影响的用户提供定期更新，减少损失并制定业务恢复方法的战略。有效的协调和沟通不仅仅是向客户报告。

由于云计算的共享特性，一次攻击通常会同时影响多个组织。因此，事件信息共享在

[17] Incident Response Teams – Challenges in Supporting the organizational Security Function, Ahmad, Hadgkiss & Ruighaver 2012; Shedden, Ahmad & Ruighaver 2011 https://www.sciencedirect.com/science/article/pii/S0167404812000624?via%3Dihub

[18] CSA Security Guidance For Critical Areas of Focus In Cloud Computing v4.0

[19] An integrated conceptual digital forensic framework for cloud computing, Martini and Choo https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X

帮助相关组织防范相同威胁方面是互惠互利的。CSA运行云网络事件共享中心(CloudCISC)[20]，方便参与的CSP之间共享事件数据。

与关键合作伙伴、其他部门的IR团队和执法机构的协调大大增强了CIR的能力。这种沟通应该从一开始就建立起来——在计划阶段，并在必要时在整个CIR过程中保持。

下面的信息图举例说明了组织在发生危机时为确保有效沟通所经历的各个阶段[21]

准备	确定沟通团队	选择沟通渠道	给目标听众的消息
CCMP:事件管理计划	首席市场官	内部和外部邮件	监管机构
维护RACI矩阵或线性责任图	沟通领导	致传媒新闻稿	董事会
建立作战室	主题专家	董事会报告	劳动力
网络空间危机桌面演习	公司秘书	监管报告	第三方
RACI：负责、负责、咨询和知情		股东会议	客户
		IVR服务 通知/通过区域办事处/分公司网络进行简报	保险公司
		网站	执法机构
		社交媒体	渠道合作伙伴
		客户支持	债权人
			股东

图5：有效的危机沟通阶段

6.1 协调

6.1.1协调关系

所有利益相关者应该共同努力，明确彼此在云安全事件期间的角色和责任。传统上，这些角色与共享责任模型中的职责紧密联系在一起。例如:

- PaaS或SaaS应用的平台或服务层发生的安全事故应由CSP驱动;
- 对于PaaS应用程序，发生在应用层的安全事件应该由CSC驱动;

[20] More information on CloudCISC: https://cloudsecurityalliance.org/research/working-groups/cloudcisc/

[21] REBIT Cyber Crisis Communications Playbook https://rebit.org.in/playbooks-and-presentation/cyber-crisis-communications

- 发生在IaaS基础设施云平台层的安全事件应该由CSC和CSP共同驱动，以确定它是源于CSC的环境还是CSP的环境。

通常，所有事件都需要 CSC和CSP之间密切合作，有效地管理事件。

利益相关者应该主动识别此类事件场景以及他们的角色和职责。他们还应该确定在事件发生时使用的沟通渠道(例如，电子邮件、视频/电话会议细节)，以便利益相关者知道如何有效地共享信息。

利益相关者沟通：沟通建议应基于不同的第一反应者可能性(例如，CSP作为第一反应者vs.云用户作为第一反应者)。

6.1.2 共享协议和报告要求

一旦利益相关者确定了角色和责任，在合同协议中正式确定这些关系至关重要。协议应该包括针对所有利益相关者的保密协议(NDA)，以便他们能够机密地共享信息(包括企业最敏感的信息)。试图与外部组织共享信息的组织应该在开始协调工作之前咨询法律部门。讨论之前，可能会有一些合同或其他协议必须落实到位。

组织还应该考虑任何现有的报告要求，例如与信息共享和分析中心(ISAC)共享事件信息或向更高级别的CIRT报告事件。

6.2 信息共享技术

所有利益相关者必须能够识别威胁并与关键利益相关者共享安全信息。通常，所有利益相关者对于发现或共享事件关键信息以及评估其能力的最优方法并没有明确的方向。

客观地，必须评估共享技术以确定减少利益相关者负担的有效性，同时确保互联互通和弹性。即使是最小的组织也必须保持与同行和合作伙伴共享事件信息的能力，实现积极的结果。

组织应该在整个事件响应生命周期中而不是等到事件完全解决才共享信息。

信息共享是实现跨组织协调的基本要素。

1. 点对点模式
2. 部分自动化
3. 安全注意事项

6.3 粒度信息共享

组织还必须权衡信息共享的好处和共享敏感信息的缺点。企业应该只与适当方面共享必要的数据。理想情况下，所有利益相关者都应该有一份NDA，为敏感和专有信息提供合同保护。

6.3.1 业务影响信息

云安全事件既是业务问题，也是IT问题。云安全事件可能会导致一系列负面业务影响，例如财务损失（例如，服务不可用、失去合规认证导致无法开展业务、事件响应成本）、声誉影响（失去客户信任）、商业秘密披露、知识产权盗窃、敏感数据泄露或其他问题。

业务影响信息只有在向有意确保受影响企业任务的组织报告时才有用。在很多情况下，除非有明确的价值主张或正式的报告要求，IR团队应避免与外部组织共享业务影响信息。然而，在某些情况下，由于监管和法律要求，组织可能被迫公开共享这些信息。

业务影响信息描述了事件在任务影响、财务影响等方面对组织的影响。至少在摘要级别上，此类信息通常报告给更高级别的IR协调团队，用于传达事件的损害估计。

业务影响信息只有在向对确保发生事件的组织任务有一定兴趣的组织提出报告时才有用。在很多情况下，除非有明确的价值主张或正式的报告要求，IR团队应避免与外部组织共享业务影响信息。

6.3.2 技术信息

由于CSP服务于许多客户，因此攻击者经常使用相同的弱点攻击多个CSP客户。一旦CSC/CSP提取了有关攻击或新兴威胁的技术细节，就可以分发这些数据以增强对特定攻击的防御。

在当今的数字经济中，速度和效率至关重要。对于那些负责保护网络免受攻击的人来说，网络罪犯的行动速度可能令人担忧。该行业必须与行业同行共享更多安全情报，以便更好地保护并且适应不断演变的威胁。在企业通过收集内部指标获得价值的同时，也可能会通过分析从合作伙伴组织收到的指标以及共享内部指标以供外部分析和使用中获得额外价值。如果组织收到有关其未看到的事件的外部指标数据，则可以在事件开始时使用该指标识别事件。类似地，组织可能会使用外部指标数据检测由于缺乏捕获特定指标数据的内部资源而没有意识到正在发生的事件。组织还可以从与外部组织共享内部指标数据中受益。

技术指标数据有助于组织识别实际事件。然而，并非所有从外部来源收到的指标数据都属于接收该数据的组织。外部数据有时可能在接收组织的网络内产生误报，并对不存在的问题造成不必要的资源分配。

组织应尽可能多地分享见解。然而，可能存在安全和责任方面的原因，决定了为什么组织可能会隐瞒被利用漏洞的详细信息。

技术指标数据有助于组织识别实际事件。然而，并非所有外部源指标数据都与接收该数据的组织有关。在某些情况下，这些外部数据会在接收组织的网络中产生误报，从而为不存在的问题分配不必要的资源。

6.3.3 CSP仪表盘

CSP应该为用户提供一个可自定义的自助仪表盘，通知有关事件的信息，以便客户了解最新情况。这些仪表盘通常用于传达影响大量客户的事件。CSP还应支持配置选项，自定义云警报并创建个性化仪表盘，以分析相关事件、监控云资源影响、提供指导和支持，以及共享详细信息和更新。这些仪表盘可以设计为有关云资源的唯一事实来源，并且应该让用户更清楚地了解可能有影响的任何问题。

6.4 桌面演练和事件模拟

除了少数进步组织之外，大多数企业很难通过具体的“真实世界”经验为安全事件做好准备。这些现实的演练引入了无害的（但真实的）安全漏洞，并模拟外部利用以评估这些组织的准备情况。在此类活动中，一个小型的组织团队会意识到该演练。对于其他人而言，不存在演练。这是一起真实的安全事件。

这就是桌面演练的价值所在，一个纯粹的模拟攻击场景和一次安全事件准备活动。桌面演练通过指导参与者完成对模拟事件场景的响应过程，帮助组织考虑各种安全事件场景并为潜在的网络威胁做好准备。这种经验为参与者提供了实践培训，然后可以突出IR流程中的缺陷。

任何组织都应该能够执行桌面演练（而不是在需要复杂技术和操作能力的客户环境中引入bug）。此外，与“真实世界”模拟相比，桌面演练所需的资源要少得多。

桌面演练有助于改善整体事件响应态势，以及团队在事件发生时的集体准备和决策过程。演练从IR计划开始，并根据该计划衡量团队表现。由于大多数组织都没有做好应对云安全事件的准备，因此制定执行良好的IR计划至关重要。

7. 总结

> 引用本杰明·富兰克林的话说，“没有做好准备，就做好了失败的准备。”

在很多方面，这种观点都击中了关注网络攻击威胁的组织的痛处。组织应充分了解事件响应过程及事件响应能力，为任何潜在事件做好准备。

本文探讨了CIR框架以及有效响应事件所需的准备工作。它可以作为CSC在破坏性事件的整个生命周期中准备和管理云事件的首选指南，还为CSP和CSC共享云事件响应实践提供了一个透明、通用的框架。

我们分四个阶段介绍了CIR框架（加上最后一节涵盖协调和信息共享）。

准备工作涉及云事件之前所需的策略和行动。有效的事件响应计划包括组建CIR团队（CIRT）、战略规划和准备、程序开发、技术准备和沟通计划创建。

检测和分析涵盖了云事件的各种迹象和可能的原因，以便及早发现。为了确定根本原因，讨论了多种方法。早期事件通知的速度(以及基于业务影响的相应解决时间)也是CSP/CSC考虑的重点。

遏制、根除和恢复解释了在进行调查和取证时选择正确策略阻止攻击者进一步破坏系统的重要性。

事后分析过程识别人员、流程或技术方面的差距，并将其转化为必须在准备阶段吸取的“经验教训”。这一结束阶段的关键目标是改进未来的事件处理。为了提高企业的安全能力，审查CSP的事件/取证支持（如适用）、支持事件分析的可用技术工具、参与者使用的TTP以及进行取证调查至关重要。

协调和信息共享部分描述了云威胁的复杂性如何要求利益相关者协调和共享安全信息以减轻损失。

总之，该框架将有助于指导CSC确定其安全需求和适当的事件保护级别。此外，CSC可以使用本指南与CSP和（或）第三方协商，确定各方的能力和责任共担。