面向云客户的
SaaS治理最佳实践

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

SaaS 工作组的官方永久地址

https://cloudsecurityalliance.org/ research/working-groups/saas-governance/

序言

据 Statista 预测，到 2022 年全球企业服务 SaaS 市场规模将超 1700 亿美元，SaaS 成了真正的“软件终结者”。国内 SaaS 虽然起步较晚但也已经在 2019 年进入了旺盛期，CRM、ERP、HCM、OA、财务、客服、电子签等垂直领域的 SaaS 蓬勃发展。传统软件厂商也纷纷向 SaaS 转型。尤其是新冠疫情爆发以来，很多企业不得不选择远程办公和使用线上 SaaS 应用，疫情成为 SaaS 发展强有力的助推剂。

随着 SaaS 的普及，企业软件的安全风险从传统软件转移到了 SaaS 应用。企业的云安全治理范围也从原来的 IaaS 基础设施层和 PaaS 平台层延伸到了 SaaS 应用层。因此，CSA 在发布 CAST 云应用安全可信标准与认证之后，又发布了《面向云客户的 SaaS 治理最佳实践》（以下简称《实践》）白皮书，供 SaaS 从业人员及相关的 IT 或安全从业人员参考。《实践》充分关注到了 SaaS 环境中的数据保护、SaaS 生命周期的风险以及处置等内容。而且基于安全策略、安全组织、资产管理、访问控制、加密和密钥管理、安全运维、网络安全、供应商管理、事件管理、合规等多个安全控制域为业界提供一整套用于 SaaS 治理的指南。《实践》围绕 SaaS 治理中最核心的问题“确保谁在什么场景下、拥有什么样的权限、可以访问什么数据”，并从评估、采用、使用和终止四个阶段给出了具体措施和建设，同时针对日常应用场景进行了延伸的安全考量。

随着数字化转型和数字经济发展浪潮的强势来袭，企业级 SaaS 的需求量也在与日俱增。各行业也正在大力构建新的数字生产力，发挥数字协同效应，为企业发展提供新的动力。相信通过《实践》中提出的详尽而实用的治理指引，组织及相关从业人员能够掌握 SaaS 治理的最佳方法和路线，提高 SaaS 安全治理水平，合理管控 SaaS 安全风险，切实保护 SaaS 中的数据安全。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《面向云客户的SaaS治理最佳实践》（SaaS Governance Best Practices for Cloud Customers）由CSA软件SaaS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（排名不分先后）：

组 长：郭鹏程

翻译组：陈 强 侯 俊 茆正华 王永霞 薛 琨 杨天识

审校组：陈 皓 郭鹏程 姚 凯

研究协调员：江瞿天

感谢以下单位对本文档的支持与贡献：

北京北森云计算股份有限公司 北京启明星辰信息安全技术有限公司

上海派拉软件股份有限公司 深圳市魔方安全科技有限公司

神州数码集团股份有限公司 腾讯云计算（北京）有限责任公司

英文版本编写专家

完成项目领导： Chris Hughes, Tim Bach, Michael Roza, Anthony Smith, Walter Haydock, Andreas Peter, Andrew Luhrmann, James Underwood, Alistair Cockeram, Saan Vandendriessche

完成贡献者： Bryan Solari, Sai Honig, Amit Kandpal, Jessica Shouse, Abhishek Vyas

审核： Jerich Beason, Kapil Bareja, Or Emanuel, Udith Wickramasuriya, Priya Pandey

最初的领导和贡献者： Akin Akinbosoye, Yao Sing Tao, J. R. Santos, Mickey Law, Vani Murthy, Zeal Somani, Paul Lanois, Michael Roza

CSA 全球员工： Shamun Mahmud

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。

目录

1. 引言

在云安全领域，一直以来关注的重点几乎都是对基础设施即服务（IaaS）和平台即服务（PaaS）的保护。虽然组织一般只使用2-3个IaaS提供商，但通常会使用数十到数百个SaaS产品。云客户的SaaS治理最佳实践，是SaaS治理实践的基线集合,列举并考虑了SaaS生命周期评估、采用、使用和终止等所有阶段的风险以及处理。

随着SaaS的广泛应用，组织为了应对这种新情况，必须更新网络安全覆盖的领域。

组织必须更新内部策略，包括关键事项，如服务级别协议、安全和隐私要求以及运营影响分析等。同时，应考虑组织运营安全活动受到的影响，例如职责和任务分配，以及对移动设备和远程办公的影响。信息是一种资产，在SaaS模式下，涉及到外部服务提供商时，必须考虑信息的分类、标记和存储需求。虽然SaaS提供商在共享责任模型中承担了大部分责任，但SaaS客户仍然主要负责数据治理和访问控制。这意味着需要明确谁在什么场景下，拥有什么级别的权限，访问什么数据，尤其是在零信任架构中。

组织仍然涉及对加密密钥管理和安全运营活动（如漏洞管理、备份和存储）的关键决策。组织需要确保将SaaS提供商视为第三方风险管理计划的一部分，并相应更新事件响应和业务连续性计划和流程。这一点越来越重要，因为从业务连续性的角度，SaaS通常基于远程环境提供关键功能。SaaS工作模式下，即使责任共担，组织仍然必须满足法规合规遵从性和监管要求，以保护其利益相关者及其声誉，并避免潜在的法律后果。

SaaS模式改变了组织处理网络安全问题的方式，在云厂商和云客户之间引入了共同责任模型。如果不进行相应调整，可能会造成严重后果，如泄露敏感数据、收入损失、失去客户信任和违反监管要求等。

1.1 范围

本文件:

- 提供一套用于保护SaaS环境数据的SaaS治理最佳实践基线
- 根据SaaS采用和使用的生命周期列举并考虑风险
- 从SaaS客户的角度提供潜在的缓解措施

1.2 适宜读者

- SaaS客户
- SaaS云服务提供商
- SaaS安全解决方案提供商
- 云安全专业人员
- 法务
- 网络安全主管
- IT主管
- 风险经理
- IT审计员和合规人员
- 第三方风险经理

2. 概述

软件即服务（SaaS）用户和客户应评估并减轻使用SaaS服务所带来的信息安全风险。本文档参考NIST 800-145，将SaaS定义为“通过使用供应商在云基础设施上运行的应用程序向消费者提供的能力”。在这种情况下，消费者不会管理或控制云基础设施、操作系统、关联的存储，甚至单个应用程序，特定配置或设置除外。

虽然组织选择的云计算服务和安全领域在不断发展，但有关SaaS治理和安全的指导并不多。同时，组织中的不同部门偶尔还会更多地利用SaaS服务（也称影子IT）为其关键业务流程和功能提供支持，并经常在SaaS环境中存储敏感数据。

2.1 方法

SaaS需要不同的安全治理思维。虽然与其他共享责任框架（即IaaS）的治理有一些相似之处，但SaaS部署和管理需要独特的方法。对SaaS进行适当的安全和治理，尽职调查必须从较高的层次开始，即了解SaaS应用程序的使用和功能，并深入到细节，如系统中存储的数据类型以及谁有权访问。

考虑到适当管理SaaS应用程序的使用以及可能部署的无数SaaS应用程序的独特复杂性，组织应首先寻求一个适合组织安全、业务和监管需求的框架（如NIST CSF）。该框架将帮助组织塑造安全架构所需的人员、流程和技术。

遵循广泛采用的安全框架（如NIST CSF）以及本文档中的最佳实践和建议，将有助于组织建立SaaS治理和安全流程，以降低与SaaS使用相关的风险。

2.2 结构

本文档定义了SaaS安全性的三个必要组件：流程、平台和应用程序。通过将流程安全性、平台安全性和应用程序安全性结合到一个内聚的策略中，可以实现SaaS的集成安全性。

流程安全保护程序活动的完整性，确保流程的输入和输出不容易受到损害。主要涉及管理方面，包括政策和程序，以确保与组织的流程保持一致。

平台安全性涉及平台的安全强度，即SaaS服务的基础依赖性。其中包括SaaS基础设施、操作系统及潜在供应商安全。

应用程序安全性处理SaaS应用程序本身的安全性。只有当SaaS应用程序不包含可利用的漏洞，并且实现了符合组织和供应商安全最佳实践以及法规遵从性要求的强化要求时，才能保持安全。

在SaaS模型中，有限的控制措施和可见性主要局限于流程和应用程序安全组件。SaaS消费者无法控制SaaS应用程序的平台安全组件或底层供应链。这些情况导致SaaS用户需要在其组织内拥有良好的流程安全性，并确保实现应用程序级的安全控制措施。

某些部门特定的安全控制措施通常用于满足隐私、政府或财务合规性。例如FedRAMP、NIST 800-53、HIPAA和PCI-DSS。这些需求通常属于垂直领域，适用于三个SaaS安全领域。

2.3 SaaS生命周期注意事项

如果管理得当，企业环境中SaaS应用程序的采用和使用通常遵循三个关键生命周期：评估、采用和使用。这些生命周期的常见模式如下。

很多组织对SaaS的使用快速有序增长，然而在SaaS应用程序监控方面却是落后的。这样的组织在广泛采用SaaS的同时，实施SaaS安全和治理计划，使用生命周期将是至关重要的。

2.3.1 评估

评估生命周期发生在采购之前，首先确定可由SaaS应用程序解决的业务需求。在许多组织中，这是在业务范围内的，可能涉及也可能不涉及集中采购的组织。评估生命周期通常由4个步骤组成：

- 了解用户计划使用的服务
- 市场研究
- 试点工作
- 采购决策

如果组织做出了购买决策，那么将开始生命周期中的采用阶段，部署SaaS应用程序。虽然理想情况下，相关安全和合规组织的代表会在评估阶段出席，但这些代表必须参与到采用阶段。当组织构建SaaS安全和治理计划时，这些组织“检查点”是安全团队在SaaS生命周期中的关键集成点。

2.3.2 采用

几乎所有组织的SaaS生命周期采用阶段都是一致的。它跨越了SaaS应用程序以初始形式（有时可能是一个扩展的试点项目）采购到全面部署和使用增长，一直到潜在的终止和退役的整个过程。

采用生命周期的长短各不相同，对于大型业务关键型SaaS应用程序，实际上可能是一个稳定的状态，但通常由四个步骤组成：

- **评估**：在评估阶段，云消费者评估SaaS应用程序与需求的匹配度。这通常涉及一个试点或概念验证活动，探索特性、功能和满足业务需求的能力。
- **采用**：生命周期的采用阶段是云消费者开始正式采用SaaS产品并超越试点或概念验证的阶段。这可能涉及将更敏感的数据迁移到SaaS应用程序中，以及将SaaS应用程序推广给其他业务部门使用。
- **常规使用和扩展**：可将常规使用和扩展视为维持阶段。此时，消费者通常将SaaS应用程序用于各种业务功能，并有标准的操作程序供其使用。
- **终止**：生命周期的终止阶段表示云消费者决定不再使用SaaS产品。这可能是由于各种原因，如成本、安全性或可能不再满足业务需求。消费者开始关闭SaaS应用程序的使用，减少敏感数据、账户等。

2.3.3 使用

SaaS使用生命周期有助于防范日常运营风险和安全问题，如最小权限、身份和访问管理。

SaaS使用生命周期由四个步骤组成：

- **资格**：该个人或非个人实体是否应该成为服务的用户？
- **服务开通**：需要做什么才能将此人添加到服务中，以及他们的权限是什么？
- **监控**：此人对SaaS的使用是否符合组织的预期，有无异常使用？
- **服务撤销**：如何将此人从服务中删除？

SaaS使用生命周期描述了组织如何使用CSP和SaaS服务。

了解和监控SaaS的整个使用生命周期非常重要。否则很容易将所有精力都集中在优化生命周期的一个阶段，如初始化阶段，而对企业更轻松或更迅速地实现预期结果却没有帮助。

3. 信息安全政策

SaaS客户应制定SaaS安全战略，并构建反映该战略的安全架构。一个强大的安全架构应该包括指导SaaS应用程序部署和维护的安全策略。

3.1信息安全策略

应制定有关管理SaaS服务的评估、采用、使用和终止的政策。请参阅上述常见SaaS生命周期的描述，并确保组织为每个生命周期阶段制定了全面的策略并评估控制措施。

3.1.1 评估

任何决策都应该以企业架构（architecture）的需求和流程为指导，应符合适宜环境的总体企业架构（评估产品、服务和工具及其解决的需求）。这可以防止不必要的产品、服务和工具重复。

如果确定了需求，则可以开始评估产品、服务和工具。

SaaS服务的初始评估通常会让业务、法律和安全利益相关者了解交易的风险并进行相应的处理。关键问题是“这是否与我们的风险状况和企业架构匹配？”

3.1.1.1 确定可接受风险

评估SaaS服务时，第一步是确定哪些风险与客户的风险偏好一致。SaaS应用程序可以托管在私有、混合或公有云环境中，应用程序运行在应用程序级别的专用或共享资源上（单实例、多租户）。与任何云产品、服务或工具一样，必须理解共享责任模型。

根据ISO/IEC 27001，应使用风险管理方法管理信息安全。SaaS客户应首先确定SaaS服务给组

织带来的可接受风险，这构成了评估阶段的基线。可以使用不同的方法管理风险，包括国际风险管理标准ISO 31000。

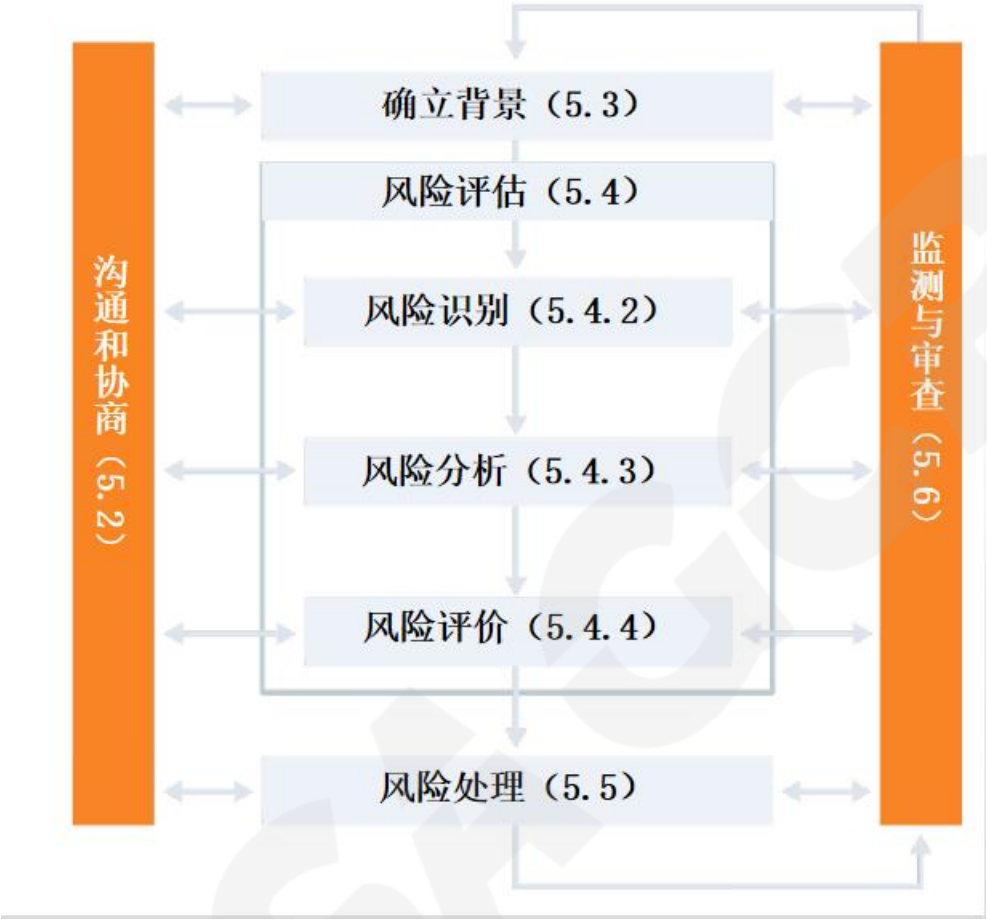

图1：ISO风险管理流程，第5条：流程

如果了解组织的风险状况，SaaS客户应该能够确定SaaS服务与组织风险管理要求的符合度。可以通过了解SaaS服务的使用情境，并考虑以下因素确定SaaS服务的风险状况：

- 数据：
  - 业务流程将存储哪些数据或需要将哪些数据提供给SaaS应用程序？
  - 直接成本（通知受影响个人的成本、股票下跌时股东的损失、竞争对手的大量涌入导致的客户流失、利润损失）和间接成本（声誉损害和错过的期货销售、网络保险成本增加、关键员工的解雇）是什么，如果存储在此SaaS应用程序中的数据的机密性或完整性受到损害，则会给业务带来隐形成本（引导员工做出

响应的成本，违规整改的成本）？

- 流程：
  - 此服务是否会影响核心或关键业务流程？
  - 如果使用SaaS服务，需要修改哪些组织策略和流程？
- 需求：
  - 哪些业务需求、法律和法规与此服务相关？

在此阶段，应评估以下方面对SaaS客户风险状况的影响：

- SaaS提供商
- SaaS服务
- SaaS提供商的供应商
- SaaS服务的使用
- SaaS客户对相关SaaS提供商应用持续监控和态势管理以缓解风险的能力

最常见的风险分析方法是经典的CIA分类：

- 保密性
- 完整性
- 可用性

有了CIA，应用程序和数据库将根据您的要求进行风险评分。

一旦建立了风险足迹，您就可以开始计算SaaS应用程序带来的风险。

计算风险的方法有很多，开发风险分析框架取决于组织需要和行业类型。

虽然可以将风险管理相关的活动转移到CSP（云服务提供商），但是**SaaS客户本身并不能将其责任外包**给CSP。SaaS客户必须始终记住，风险所有者有责任承担使用SaaS服务的风险。虽然服务提供商和消费者之间有责任分担，并且存在服务级别协议（SLA）之类的协议，但消费者最终仍然拥有风险。

3.1.1.2 安全和隐私要求

一旦确定了风险水平基线，许多云服务客户就会参与安全和隐私尽职调查。云服务客户通常会向云提供商发送评估问卷或信息请求（RFI）以供填写。

这些调查问卷询问客户希望看到的CSP实施的内部安全控制措施，通常解决有关安全和隐私的监管要求问题。

CSA STAR共识评估调查问卷等自我评估计划或第三方评估（如SOC2或FedRAMP），有助于CSP向潜在客户告知SaaS提供商的安全能力和现有做法。

自我评估或第三方报告还询问云提供商使用和披露个人信息的情况，或个人信息将在何处处理。这些项目还询问云提供商是否将信息用于自己的目的或将其披露给第三方（例如，向第三方广告商披露）。

注意数据的位置也很重要，因为可能存在数据主权要求。

第三方评估的一些关键领域包括：

- 认证和标准
- 数据保护
- 访问控制
- 可审计性
- 灾难恢复和业务连续性
- 法律和隐私
- 漏洞和漏洞利用

3.1.1.3 沟通要求

这些问卷或报告中的应答允许客户进一步完善其风险评估，并反馈到云交易的签约阶段。许多云客户为了加强其风险评估和尽职调查流程，并作为供应商管理的一部分，创建了标准的数据安全和隐私计划或条款，并包含在云合同中。

这些附表或条款的目的是多方面的，可能会产生严重后果。一个目的是解决监管问题，例如保证数据满足特定地区的监管要求。另一个是创建使云供应商遵守合理的安全标准的机制。这些附表或条款还可以约定事件响应义务，并转移因云供应商造成的数据泄露或隐私侵犯的损失风险。还可以要求在特定时间以特定方式响应数据泄露等问题，包括审计权，以及执行定期监测和控制活动的权利。

此外，必须了解CSP和消费者之间执行或管理合同的相关司法管辖区和监管框架。例如：如果您正在寻找一个SaaS平台存储或处理员工或客户PII（个人可识别信息），并且在GDPR的适用范围，

那么需要查看CSP是否存储欧盟/欧洲经济区或提供充分保护的国家的数据。如果没有，您需要了解适用的法律框架，并根据欧盟法院（CJEU）发布的Schrems II判决，确保客户服务提供商有足够的保护和补充技术控制保护数据。

总体目标是通过合同与云服务提供商无缝衔接，并尽可能降低客户的风险。

供应商管理计划中的签约流程有时会进一步细化，允许客户在与云服务提供商谈判期间针对某些条款预先建立“后备”措施。这可能包括在终止合同时如何传输数据和其他事项（例如，防止供应商锁定）。客户的法务团队和安全团队通常都会参与这些条款的谈判。

3.1.1.4 内审

客户应制定SaaS安全战略，并构建反映该战略的安全架构。SaaS客户应该记住他们负责的云共享责任模型的部分。也就是说，SaaS客户最终负责SaaS平台在设计限制内（即客户权限和责任范围内）的安全配置、管理和使用。

威胁建模和威胁分析是开发SaaS安全策略的关键。云安全联盟发布了云威胁建模，“提供关键指导，帮助确定威胁建模安全目标，设定评估范围，分解系统，识别威胁，识别设计漏洞，制定缓解和控制措施，以及措施的实施和沟通”。

SaaS客户为了应对使用SaaS平台的有效风险管理和安全控制要求，应制定一个多管齐下的安全战略，该战略适用于在此过程早期确定的SaaS应用程序的风险级别和分类。该策略可能包括以下要素：

- 了解可应用于SaaS平台的云客户适用的安全控制措施和配置（SSO、MFA、角色分配、团队/组隔离、导出日志或与安全监控解决方案集成、IP限制等），并加以应用
- 定期审查SaaS的使用情况和适用性
- 针对在SaaS应用程序或平台之外管理或部署的业务逻辑或流程进行渗透测试
- 对SaaS应用程序的配置进行持续的安全态势监控，并与组织特定的已批准/预期配置比较
- 持续监控SaaS应用程序生成的审计、事件或其他更改/活动日志，理想的情况是能够将这些日志与其他SaaS和非SaaS应用程序关联
- 持续监控对SaaS应用程序中关键数据和/或流程的访问

3.1.1.5 服务条款

未能就事件响应以及安全和法律评估权进行强有力的谈判也可能带来风险。

如果SaaS提供商违约并且影响到客户，但没有履行合同约定的违约通知和补救义务，则SaaS客户可能无法降低其法律风险并遵守监管义务。不同区域的法律和通知义务可能也有所不同；因此，在采购和合同阶段聘请专业的网络律师非常重要。

要考虑的合同控制：

- 服务级别管理
  - 服务提供商SLA与组织的SLA要求（应解决资源和支持方面的问题）
  - 业务连续性承诺：组织的RPO、RTO与MTPD
  - 事件处理和升级
- 备份的可用性
- 法律问题
  - 法律和监管要求
  - CSP和SaaS服务的管辖权、法律要求
  - 赔偿：管辖权迁移、并购
- 通知：安全、隐私、法规遵从性变更和事件
- 终止权利和流程
  - 数据可移植性（如果要迁移到其他平台，则需要考虑数据导出问题）
  - 数据删除、时间表和成功删除的书面通知
  - 外包协议终止时的退出策略

3.1.1.6 受影响的数据

使用云的一个重大风险是，失去对已传输到云的数据的绝对控制，以及外包给云的网络可用性。

例如，在更传统的IT环境中，组织有能力评估和调整其系统，使其符合适用的法规和标准。这可能包括基于组织或其客户所在地的数据驻留要求。

由于许多SaaS提供商使用位于多个司法管辖区的基础设施服务，因此在不考虑这些要求的情况下使用SaaS服务可能会增加法规遵从性风险。

SaaS客户应该能够回答以下问题：

- SaaS提供商在哪些司法管辖区运营？
- 适用哪些监管要求？
- 哪些数据将传输到SaaS服务？
- SaaS服务可以访问哪些数据？
- 对SaaS服务的数据依赖程度如何？
- 服务提供商的法律义务是什么？例如，支付提供商为了遵守反洗钱（AML）要求需要根据法律义务保留一些数据。
- 如果政府或军事实体请求访问数据，SaaS提供商会怎么做？

例如，如果SaaS应用程序中只存储非敏感数据，而不是敏感数据（例如社会保障号码或金融账户数据），则可能需要较少的供应商审查。

控制措施：

- 保密要求取决于数据价值
- 数据分类要求（如HIPAA、PCI）
- 数据和元数据控制：所有权、处理、许可
- 数据位置和主权
- 可用性要求和数据迁移

3.1.1.7 隐私

在使用SaaS提供商时，客户必须确保他们了解在该提供商中存储的数据对隐私合规的影响。SaaS客户应该了解供应商是否允许使用他们存储在SaaS应用程序中的数据（例如机器学习、匿名数据集评估等）。如果允许使用，则需要满足SaaS客户的监管和审计要求。

不断变化的监管环境本身增加了与隐私相关的法规遵从性或数据驻留违规的风险，使一些客户和某些类型数据的SaaS应用程序的部署变得复杂。国外对美国SaaS提供商存储欧洲公民数据的担忧增加了这种潜在风险。

控制：

- SaaS客户的角色与SaaS服务的角色？
  - 控制者（客户或员工的PII）
  - 处理者（控制者提供的PII）
- 隐私政策：SaaS提供商对其服务数据的权利
- 违约义务和责任
- PII数据清单、可见性
- 数据主体的“同意”管理

3.1.1.8 进行详细风险评估的步骤

1. 识别资产
2. 识别威胁
3. 识别脆弱性
4. 制定衡量标准
5. 考虑历史漏洞数据
6. 计算成本
7. 执行风险到资产的动态跟踪

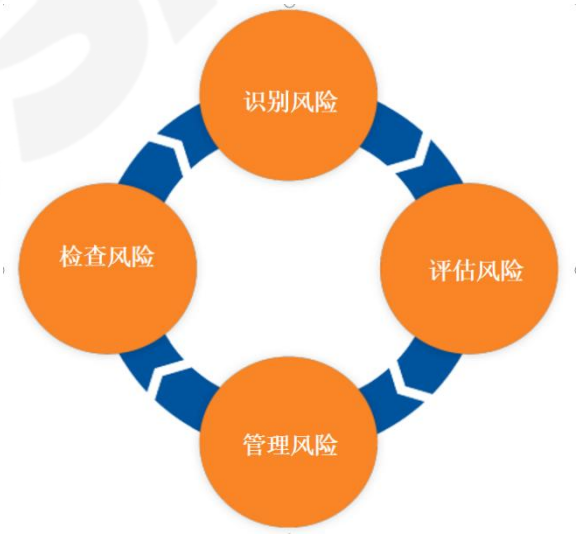

图2. 风险评估周期

3.1.1.9 识别风险

识别可能阻碍业务目标的风险领域:

- 数据、财务信息、知识产权/竞争优势的丢失
- 监管和法律规定
- 企业声誉
- 威胁、漏洞、攻击
- 事件管理
- 技术复杂性:
  - 人员专业知识
  - 财务承诺
- 第三方供应商
- 第三方审计、SOC2报告、STAR注册表等
- 人为失误

3.1.1.10 评估风险

- 定性/定量风险评估
- 治理风险合规性(GRC)
- 风险容忍度/偏好

3.1.1.11 管理风险

- 根据风险容忍度实施物理、技术、管理控制措施
- 将风险转移给第三方
- 接受风险

3.1.1.12 检查监管

- 内部、外部审计
- 风险分析

要识别风险，必须对SaaS服务和CSP进行详细的风险评估

公司资产在上云之前，应进行风险评估。风险评估的详细程度将因环境而异。例如，客户可能会决定在一个有限的用例(即沙箱、开发软件、测试CSP功能、控制等)下开始使用CSP。在这种情况下，可以进行“最小风险评估”。如果CSP的工具和特性满足CSC的业务目标，那么应该在应用正式上线之前进行更详细的风险评估。

在决定进行SaaS风险评估时，应该仔细检查三个方面：a)SaaS提供商；b)SaaS提供商的管理实践； c)SaaS应用程序的技术安全考虑事项。此表列出了需要考虑的值得关注的问题。

供应商	实践	应用程序
CSP拥有哪些认证文件？	CSP采用哪些控制措施从逻辑上限制进出不同区域的数据？	应用程序/特权账户是否被集中管理（例如，通过IAM、RBAC或账户管理工具
CSP是否经过第三方评估或审计？CSP是否可以提供SOC II类（时间段）报告（或同等类型的报告）？	CSP提供了哪些备份/恢复服务（例如，应用程序、数据、虚拟机）？	是否存在安全通道（例如，用于口令、证书、数据的安全传输）？
CSC数据是否与CSP一起存储在本地，或者CSP是否与第三方供应商签订了合同(用于基础设施托管服务)？	CSP的突发事件管理流程是什么？事件如何分类?	是否使用SSO/SAML/MFA进行安全认证?

供应商	实践	应用程序
在故障排除、维护等方面，CSC可获得何种程度的支援?	虚拟机镜像、服务器和数据库是否定期打补丁?CSP的防病毒管理流程是什么?	应用程序/存储账户是否面向公众（开放权限）?
CSP的SLA/OLA是什么?	如何管理、存储加密密钥等?谁有访问权限?	应用程序/软件是否获得了云许可?
CSP是否提供了支持SaaS的所有第三方供应商列表?如果是，CSP是否进行背景调查并签署保密协议?	为客户提供了哪些日志记录工具？SIEM事件威胁检测工具?	软件/数据是否符合任何监管/隐私要求?
CSP能够遵守哪些标准和监管要求? CSP基于什么标准(即ISO、NIST、CIS、PCI、HIPAA、GDPR)进行基线控制?	CSP提供了哪些IDS/IPS工具?	应用程序的开发/维护需要哪些软件开发过程/工具(如DevSecOps、GitHub.、SDLC)？CSP使用了哪些工具/应用程序来支持此项工作?
CSP的底层架构是利用行业最佳实践或标准来设计或开发的吗?	CSP是否提供虚拟机加固后的镜像?它们是如何管理/执行的?	支持此应用程序需要哪些API ?CSP能提供哪些帮助?
CSP是否利用/提供云资源的自动化工具、脚本(如vm、IaC、自动修复)?	CSP是否提供控制措施以防止未经授权的数据泄露?	CSP是否支持应用程序的脆弱性/渗透测试（如有必要）?

需要说明的是，上述风险评估具体针对的是SaaS提供商及其SaaS应用程序的底层架构和实现的安全性。它不能替代对SaaS客户实施和使用SaaS应用程序的持续安全监控和风险审查。

为了正确地管理SaaS风险，必须通过不同的视角来理解和看待。只有这样，才能在一定程度上保证SaaS风险已经得到适当的识别、评估和缓解。风险评估不应被视为“一次性完成”的工作。云风险不是固定的，因此应该定期评估，并且当有重大变化时也要评估。

SaaS客户需要了解他们的解决方案的需求，然后确保SaaS提供商能够理解并满足这些需求。假设SaaS提供商无法满足客户的需求，SaaS客户有责任采取补偿措施缩小差距或选择不使用相关提供

商的服务。

3.1.1.13 云提供商审查最佳实践

- 将第三方技术服务视为组织中的一种资产
- 建立一种基于风险的第三方评估方法
- 根据整个组织的关键利益相关者的要求制定第三方评估
- 确保业务负责人参与
- 定期审查风险最高的供应商
- 发布授权供应商/应用程序列表
- 在没有商业理由和批准的情况下，要求仅使用认可的供应商/应用程序
- 考虑在整个组织中使用预先批准的供应商
- 鼓励或强制使用合规的供应商

3.1.1.14 制定政策和程序

为了安全地部署和使用SaaS应用程序，SaaS客户必须制定内部策略和流程，以持续评估和监控其SaaS应用程序的实施和使用情况。如本节前面所述，定期对SaaS提供商的技术、实践和认证进行风险审查和评估；对于SaaS客户来说，针对配置和SaaS应用程序的实际使用情况制定监控和评估方法同样重要，甚至更为重要。

这些政策至少应包括：

- 账户管理程序
- 集中式身份管理程序
- 数据和系统访问要求，例如：批准重要访问的授权，并要求对这些账户进行进一步的身份验证
- 针对服务滥用的可接受使用政策
- 在业务流程上下文中集成用户生命周期
- 数据分类和标签
- 集成到现有的服务水平、事件管理和漏洞管理流程中
- 与现有的管理机制集成、按要求创建和提升，即变更控制

与其他安全计划一样，不能把对SaaS应用配置、数据分类和数据访问的监控看作一次性的事情。SaaS比其他云技术的迭代更新更加快速，并且可以快速重新配置。SaaS客户管理员只需一个不经意的命令或按钮点击，就可以大大改变SaaS应用的安全态势，这进一步强调了对持续监控计划的需求。

3.1.1.15 配置和安全态势管理

必须对关键SaaS应用程序(根据系统中存储的数据的敏感性，或如果受到损害，可能造成的业务中断)进行持续监控。这种监控能力，最好是自动化的，应该经常运行，并能够在重大变更后临时运行;理想情况下，它们还应该能够在沙箱或预生产环境中运行，以便在生产SaaS环境中运行之前验证配置更改。

SaaS客户对关键SaaS应用程序的态势管理至少应该考虑：

- 系统设置的配置基线，特别是与以下内容相关的设置：
  - 身份
  - 身份验证和系统访问，包括MFA、SSO和地理位置或IP限制
  - 密码策略
  - 会话控制
  - 平台提供的数据防泄露和审计功能
  - 平台提供的加密和自带密钥功能
- 已安装和批准的第三方插件、集成以及OAuth或与其他云之间的连接
- 将用户分配给SaaS应用程序中的角色、配置文件、组、团队和SaaS应用程序中可以授予额外访问权限或功能的任何实体
- 配置访问授权元素和对用户的有效访问
- 可能显示敏感或特权操作的管理操作和授权日志
- 跨关键SaaS应用程序或环境的操作相关性
- 用户对关键类型的数据或记录的访问，以及确定读取（机密性）和写入（完整性）
- 离职程序

本节中的配置管理指的是配置控制。在NIST 800-53,CM-2中规定，“基线配置作为未来构建、发布或系统变更的基础，包括安全和隐私控制实现、操作过程、关于系统组件的信息、网络拓扑结构和组件在系统架构中的逻辑位置。”维护基线配置需要在组织系统变化时创建新的基线。系统的

基线配置反映了当前的企业架构。”

云的好处之一是促进了软件开发人员快速开发新功能、应用程序和服务。在目前主要SaaS应用程序中，通常包括创建和部署控制关键业务流程的少量或无代码应用程序。具有权限的用户可以快速部署和调整这些集成、工作流和应用程序。因此，这些权限对业务的潜在影响甚至更大，能够监控和提醒这些功能的错误配置或使用是很重要的。

此外，SaaS应用程序的快速配置能力和许多SaaS平台上云应用程序市场的普及，可以允许用户使用第三方(不是由SaaS客户或SaaS提供商开发的)应用程序快速扩展SaaS平台。虽然SaaS应用程序功能强大，但也会引入供应商风险评估和采购程序中的漏洞。因此，安全组织必须具备监控和告警功能，用于检测第三方应用程序与已批准的SaaS平台的未经授权的连接，这一点至关重要。

举一个例子，需要将营销自动化平台(MAP)与客户关系管理平台(CRM)集成，从而将MAP数据提供给CRM。在此场景中，需要考虑并跟踪数据流动的位置，是从MAP到CRM？还是从CRM到MAP？在这种情况下，数据流将是从MAP到CRM。

然后需要检查CRM是否有预先审核过的市场集成。通常情况下，市场集成更安全。

在此之后，将检查最佳实践指南，或者联系支持人员以获得那些最佳实践(如果无法自助获取的话)。

最后，需要分析如何确保最少特权并遵守数据最小化原则。

此外，理解如何删除连接也是必要的。

再看另一个示例，用户将其谷歌账户与第三方应用程序集成。用户主要查看第三方应用程序将获得哪些权限和范围，以及应用程序能够代表用户执行哪些操作，然后根据组织的风险偏好做出判断，用户可能需要在这方面获得安全专家的支持，还可能想知道如何撤销第三方访问权限。

在开发安全态势管理策略和规则时，SaaS客户可以利用行业最佳实践(例如:微软365的CIS基准)，与制定了基线安全策略的SaaS安全态势管理供应商合作，或者在内部努力确定适合组织的最佳实践和需求。通常，可以将这些方式结合起来制定最全面的政策。

3.1.1.16 数据安全

SaaS客户应该监控存储在SaaS应用程序中的敏感数据的访问，其方式与监控系统配置和安全状况类似。同样，由于SaaS应用程序固有的灵活性和可配置性，用户对数据的访问可能会快速变化。因此，与SaaS安全监控的其他部分一样，关键是将对数据的监控访问视为一个连续的过程，而不是一个时间点的操作。

作为任一数据安全和访问监控解决方案的一部分，SaaS客户都应该定期(或使用自动化平台特

性)对数据按敏感级别、数据类型等进行分类。这种分类，无论是在外部系统中维护还是在SaaS平台本身上维护，对于设计数据安全策略并根据该策略监控实际状态至关重要。

关于数据安全的其他注意事项，可能可以作为安全态势监测的一部分进行监测，但仍应明确定义，包括:

- 配置(和用户访问)数据导出功能和数据备份功能
- 资产、所有权和责任清单
- 限制内部和外部共享和监控系统配置以匹配安全策略
- 密码控制和要求，并对系统进行监控，以确保其配置符合预期

另一类可以应用于SaaS应用程序的安全解决方案是数据防泄露(DLP)解决方案。DLP解决方案通常与数据的访问路径一致，或者作为内置的SaaS应用程序功能，DLP提供更高级别的信息保护。DLP可以防止某些类型的文件的转移或泄露。DLP解决方案也与数据分类有关系。首先，需要对数据和文档进行分类，以便DLP解决方案能够理解分类并进行相应的监控(例如，PII、PCI)。

DLP运行主要基于关键字、短语和元数据。在DLP逻辑匹配时，它可以执行一个或多个操作，如通知用户、提醒管理员、阻止传输、删除附件和文档、编辑敏感数据，并保留数据副本以供检查/取证目的。SaaS提供商通常为其客户提供自动化处理的机制或API。当使用大量SaaS系统时，客户将选择与SaaS平台集成的DLP解决方案，以实现无缝管理。

3.1.1.17 用户意识和培训

- 为安全使用此服务制定最佳实践指南
- 强制执行数据分类和标记
- 用户了解此服务的安全事件并知道如何报告它们
- 在可行的情况下添加指导策略（例如，用户得到访问某个类别的授权服务的提示，或者记录使用替代选项的理由）
- 为坦诚的报告事件营造良好氛围

3.1.1.18 内部威胁

- 离职员工可以将SaaS数据分享给他们的个人账户，导致公司数据的泄露
- 员工在内部过度暴露敏感数据（财务和工程可以相互使用彼此的信息）
- 敏感数据分享给错误的第三方
- 未落实职责分离
- 平台配置不当导致数据泄露(例如，包含敏感数据的S3存储桶被公开暴露)
- 员工允许从系统中获取大量数据，这可能会导致他们在辞职时泄露或带走这些数据

3.1.1.19 外部威胁

- 第三方合作者可以永远访问你的公司数据
- 您的供应商与他们的供应商共享公司数据，这些供应商从未通过第三方风险评估
- 使用公司数据的第三方合作者使用个人账户，而且通常没有设置多因素身份验证
- 第三方供应商或其分包商/供应商不受监管实体保护数据的约束

3.1.2 用法

- 可接受使用政策
- 管理
- 治理

3.1.2.1 定期检查服务/供应商

- 监控存档版本发生变更的服务条款和条件
- 安全保证的有效性
- 持续的安全性能
- CSP供应商管理具有挑战性

3.1.2.2 告警

- 监控可疑的登录和数据访问
- 监控服务的使用情况和滥用情况
- 监控SLA符合性
- 监控登录和访问中的任何异常
- 监控任何有风险的组织范围内的设置变化
- 监控异常数据访问

服务条款和条件可能会随时发生变化，导致失去控制。因此，需要使用自动化工具持续监控服务的属性。

很有必要监控配置更改并告警。

3.1.2.3 使用情况可见性

- 带有登录用户名和用户位置的身份验证日志
- 访问日志
- 审计日志
- 账户配置和撤消配置日志

3.1.2.4 持续评估并减少攻击面

- 监控服务的基本属性，进行完整性检查
- 审查控制以减少攻击向量
- 监控潜在的内部故障点

3.1.2.5 配置管理

- 监控配置更改，并在必要时发出告警

3.1.2.6 数据

- 监控对敏感数据、系统和字段的访问
- 监控管理行为
- 启用审计
- 监控备份的有效性

确保执行数据备份，更重要的是，通过备份还原来测试备份数据的可用性。

3.1.3 终止

SaaS使用的终止需要统筹和有计划的执行

SaaS服务最重要但经常被忽视的风险之一在于CSP提供的合同

传统上，组织与法律部门合作，协商服务提供商的合同条款，使其不那么“对供应商友好”，并通过让服务提供商承担财务责任减轻由服务提供商造成的任何损失。但云提供商不愿意提供通常的赔偿、责任限制或其他条款，尤其是与隐私和数据安全有关的条款。

CSP提出的最普遍的理由是，这些额外的责任和义务会威胁到价格较低的云计算模式，而且，由于CSP不知道他们的客户在云上存储了什么，他们不需要承担隔离和保护客户数据的责任。然而，CSP必须为客户提供实现这一目标的方法。

云协议中的不利条款可能会增加云客户的风险。

云客户还可能希望通过合同来限制CSP用于存储或处理客户数据的分包商。如果没有这些限制，客户可能会发现它的数据实际上是从主CSP中流转到了多个分包商。

3.1.3.1 内部流程

- 通知所有用户服务终止
- 关闭所有API访问
- 供应商替换或数据提取的指南
- 提取数据供未来使用或迁移到新的服务
- 存储在哪里，谁应该负责？
- 确保了解与所有其他系统的集成/数据流

3.1.3.2 数据保留

- 销毁备份和剩余数据/元数据(例如,系统日志、审计日志、访问日志,索引)
- 数据保留时间应满足数据分类要求
- 导出和删除财务信息
- 导出使用情况和其他报告

3.1.3.3 资产收益

- 数据/元数据的导出(例如，审计日志，访问日志，备份)
- 符合数据位置要求
- 可接受的数据格式
- 交付期、方法及访问时长

3.1.3.4 解除特定于服务的附件

- 特定服务监控
- 服务的安全监控

3.1.3.5 服务管理

- 删除所有与服务的集成
- 确保服务退役
- 确保合同结束

3.2 对信息安全政策的审查

由于技术变化频繁，因此有必要定期对政策进行审查。自上一个版本以来，可能需要增加额外的可接受的控制。这还要求SaaS操作仍然满足组织设定的最低标准。

一些解决方案提供商（如CASB）对SaaS服务提供持续的评估和评分，并提供基于这些动态分数设置告警和访问策略的功能。

4. 信息安全组织

4.1 内部组织

4.1.1 信息安全角色与责任

虽然很多人将SaaS视为外包责任，但是清晰地理解云服务客户（CSC）和云服务商（CSP）之间的角色与责任是很有必要的。当客户选择潜在云服务商，执行尽职调查时，会有助于减少想当然和误解，并且还将有助于区分云服务商和客户之间的责任。可以说，了解云服务商不负责什么比了解他们负责什么更为重要。

充分理解云服务商和客户之间的角色与责任划分（参见“共享责任模型”介绍），将会暴露出很多云客户无法控制的控制项。一般认为，对于大多数SaaS应用场景，客户负责如何授予应用和数据的访问权限。与此同时，云服务商负责其它事项（例如，SaaS客户无法控制的已知VM漏洞修复问题）。因此，云服务客户将绝大多数的安全与维护活动委托给云服务商。

SaaS解决方案的一些功能需要由客户负责。客户必须应对挑战，投入时间了解风险，并将风险减少到可接受的水平。考虑到SaaS应用接受低版本TLS协议（例如TLS1.2）的情形，客户可能禁止使用老旧版本并强制应用程序仅接受TLS1.3协议。另一个例子是可能要求使用活动目录对用户进行身份认证。

尽管如此，SaaS客户依旧需要管理与技术控制措施的组合，以保护资产和资源免受因对SaaS平台依赖而产生的安全和操作风险。下表列出云服务客户需要掌握的控制措施，请记住，实际的技术控制措施会因云服务商而异。

技术控制措施	管理控制措施
用于安全审计/日志的系统应用账号	用户/系统授权
特权账号多因素认证	用户/系统授权
特权账号的系统监控	所有特权账号拥有者的年度认证
所有账号的身份与访问管理（IAM）	经鉴别的加密密钥的所有权
加密密钥、数字证书的安全存储库	所有云计算资源/资产的库存管理
安全通讯通道（如HTTPS，SSH，SFTP）	获得网络/架构团队的批准
统一仪表盘（管理平面）管理所有云资源/资产（如SIEM，日志集成）	• 用户授权 • 指标度量 • 合规性报告
漏洞管理 补丁管理 修复加固	漏洞的分类 漏洞的通知
事件管理工具	CSP和CSC关于事件如何定义，沟通和管理达成一致性
风险管理评估工具（包括）： • 漏洞扫描 • 威胁建模 • 渗透测试	• 风险管理批准/评审 • 关键风险指标 • 与利益相关方沟通检查结果 • 知识转移

备注：请参考CSA企业架构—CCM共享责任模型，了解云客户与云服务商之间共享责任的详细清单。

4.1.2 职责分离

要落实职责分离的安全原则，控制措施必须到位。简言之，职责分离确保那些关键任务要求两个或更多的人员/实体才能完成，其目的是防止欺诈或串通。

NIST 800-145所定义的“云计算”，将“按需自助服务”列为云计算的基本特征。“按需自助服务”意味着“消费者可以单方面提供计算能力，如服务器时间和网络存储，根据需要自动实现而不需要人工交互”。换言之，“按需自服务”的特性允许云计算非常快速便捷地启动云资源和资产，而不需要最终用户具备太多专业知识。这也意味着职责分离的实施会变得非常复杂，且易于失控。

用户或应用创建/启动的云资源可能是各种形式（如用户/系统/应用的账号ID，角色和账户组）。客户必须明白这些资源可以访问云内/云外的什么资源，以及与这些 ID关联的特权，然后采取适当措施，确保这些账号执行特定任务时仅拥有最小权限。否则，可能导致某个账号具有超出预期的资源访问权限。未能实现职责分离控制的安全风险，包括未经授权披露机密/隐私信息、数据丢失、完整性受损等等。

4.1.3 与监管机构的沟通

尽管云服务商需要负责大多数维护云解决方案的任务，客户依旧对云上发生的一切负有责任。这是因为客户在签署合同时，同意“条款细则”中云服务商所提供的服务和限制。

客户应当有书面过程记录，用以标识关键利益相关方，在事故发生时或SLA/OLA（服务级别协议/运行级别协议）改变时，及时发出通知。共享这些记录给云服务商，以便他们知道发生事故时该通知谁。这些利益相关方应当清晰了解他们业务目标/成果和法律合规/监管要求。

4.1.4 与特殊利益群体的联系

云安全面临的风险每天都在变化，几乎不可能保持密切跟踪。因此强烈建议组织指定专门的人员/团队与这些特别利益群体建立/维护关系。这些群体通常跟踪最新的，或“0Day”漏洞，同样地，他们可能分享部分漏洞的可行修复方案。与特殊利益群体建立关系能节省公司的时间（比如寻找一个修复方案时）。另一个好处是，公司可以根据自身需要，选择特定利益群体（例如按行业、技术、法规）。最终，这些特殊利益群体可以提供各种最新资讯，包括新趋势、隐私、威胁、漏洞和修复方案。

4.2 移动设备和远程办公

4.2.1 移动设备策略

COVID-19（新冠疫情）产生了任何人都无法预测的影响。许多公司不得不匆忙提供居家办公方案以确保正常运转。

通过适配移动设备的Web前端，或安装在移动设备上的特定SaaS服务应用，提供基于移动设备的SaaS服务访问。这些设备形态各异，有个人/企业分派笔记本电脑，个人/企业分派移动电话，或平板电脑。没有人能确信是否会恢复到新冠之前的正常状态。因此，必须考虑开发出策略，流程以及指南，支撑安全的持续运营。

云客户必须识别出允许移动设备访问企业资源的安全风险，以下是需要考虑领域的样例：

- 谁能访问公司资源？
- 这些访问是仅限于内部员工，还是承包商和第三方供应商也能访问？
- 哪些公司资源是每个人都能访问的？
- 哪些公司资源应限制承包商/第三方提供商访问？
- 访问如何被授权- VPN，软令牌，多因素认证？
- 个人设备是否被允许访问公司资源？
- 如果允许个人设备访问公司资源，我们如何保护资源免遭勒索软件，钓鱼，欺骗等攻击行为？
- 一旦员工/承包商被授权访问，我们如何确保他们仅能访问有明确访问权限的资源？
- 访问行为如何被监控或记录？
- 我们如何确保公司的机密/秘密信息不被盗，或被转移到异地（或者给了非授权的个人或竞争对手）？
- 如果一名员工决定离开公司，应该采取哪些措施，以确保公司数据不会被离职员工带走？

除了技术控制措施，下面是一些同样需要考虑的管理控制措施（未详尽列举）：

- 安全意识培训
- 可接受使用政策
- 数据分类标准/策略
- 机密/秘密数据的处理
- 介质的管理
- 使用移动介质
- 加密（针对公司分派设备）
- 物理管控（针对公司分派设备）
- 数据保留/销毁

5. 资产管理

要从SaaS服务中获益，SaaS客户需要提供特定数据交由SaaS服务处理。因此，对于SaaS客户来说，数据的管理显得尤为重要。

5.1 资产责任

5.1.1 资产台账

SaaS客户应当能回答以下问题：

- 哪些数据会被转移给SaaS服务？
- 这些数据是如何转移的？
- SaaS服务会访问哪些数据？
- 我们依赖于SaaS服务的数据是哪些？
- 对数据是否有地理位置的要求，例如监管或客户服务要求？
- 在全组织范围内，有多少SaaS应用在使用，是否有“影子SaaS”存在？
- 客户是否能识别出不再使用的资源？那些不使用（但存活）的资源会迅速增加运行开支。

- 客户是否能便捷地识别所有云托管资源？应当具备一个公司级，集中化的资产数据库，以记录资产的所有权和管理责任。此外，还应制定一个企业范围内的标记策略和架构。资产标记使得客户方便地精确追踪云托管资源，能支持企业安全治理措施，因为它使得云资源可以按照地理位置，敏感度，法律规定，成本优化以及其它许多属性进行分类。

5.1.2 资产识别

应采取相应的流程和解决方案以持续发现和识别组织内SaaS的使用情况。可以通过以下4种方式中的一种来实现。

- 通过流程控制的方法，确保IT和安全在所有SaaS服务采购和使用之前都能了解
- 通过分析与评估来自防火墙、Web网关和云访问安全代理（CASB）的日志
- 通过使用SaaS安全态势管理解决方案
- 通过分析SaaS相关的支出报告和财务记录

5.1.3 资产归属

SaaS客户应当能回答以下问题：

- 谁为存储在SaaS服务中的数据负责？
- 谁是 SaaS的管理员？

5.1.4 可接受的资产使用方式

包括两个部分：

- 允许SaaS提供商对我们的数据做哪些处理？元数据？
- 我们的SaaS服务用户可以对数据做哪些处理？

数据与元数据的控制：所有权，处理，许可。

6. 访问控制

6.1 访问控制的业务需求

6.1.1 访问控制策略

- 评估一个人是否需要访问资源
- 识别业务需求和角色
- 基于数据分类的信息清理
- 获得安全审查和数据所有者（决策人）的批准

组织中的用户通常根据过往经验或克隆其对等角色访问权限的方式对应用程序授权。

因此，评估一个人是否真正需要一项服务的访问权限，并识别业务要求和建立角色就非常重要。

6.2 用户访问管理

身份与访问管理（IAM）的妥善管理和架构设计，对于保护云资源是不可或缺的。当人员入职时，必须考虑安全和业务需求，根据其工作角色或业务要求，将对应的用户分组、权限隔离和特权要求分配给用户。拥有适当的IAM实践有助于落实最小权限和职责分离。

6.2.1 用户注册与注销

6.2.1.1 用户访问配置

- 基于最佳实践的用户培训
- 知晓可接受的操作使用，相关策略和程序
- 根据用户访问基线创建账号
- 应作为员工入职、转岗/调岗、离职相关流程的一部分
- 只要条件允许，利用基于角色的访问并遵循最小权限
- 计费方：基于用量的分组或负责人
- 了解并设置资源限额

了解并设置资源限额，始终遵循最小权限原则。

6.2.2 特权管理

- 必须追问发起特权访问的正当理由，以确保是必需的
- 考虑使用“即时访问”，需要时才提升为特权权限，并及时恢复到非特权访问
- 拥有特权访问的用户数量应限制在最小规模

6.2.3 机密认证信息的管理

- 超级管理员账号（如租户管理员）只能用于非常特殊的用途，访问凭据的存储要有对应的安全级别，例如使用Key Vault密钥库

6.2.4 评审用户访问权限

- 需要定期审查访问权限，确保用户权限与业务需求匹配

6.2.5 移除或调整访问权限

- 确保即时账号终止
- 停止有关账号的资源付费
- 审计日志和访问日志必须与业务策略保持一致
- 如果需要进行安全审查
- 更新账号终止日志和资产库

确保审计日志按安全策略的要求进行复查和存储。

最后，当资源不再使用时，要确保计费停止。该动作应自动执行，并努力消除任何人工操作。

6.2.6 用户访问监控

- 基于基本使用情况设置监控告警
- 对可疑登录（如地点，时间）和数据访问（如批量访问）进行告警
- 遵守密码策略
- 数据丢失预防监测
- 对可疑行为和登录进行监控和告警设置，以区分内部员工与外部/承包商的访问活动
- 利用基于API的解决方案监控“静态数据”

6.3 系统和应用访问控制

6.3.1 信息访问限制

- 遵循SaaS客户的企业安全策略，通过身份验证的用户仅限于从许可设备上访问 SaaS应用存储的信息。鉴于某些应用程序的特性（如与外部合作的应用），这种严格的访问限制不可行，可采用类似反向代理的其它方案，提供细粒度访问控制。
- 可采用基于API的解决方案以保护静态数据，执行适当的共享与DLP策略（例如，有个人可识别信息的任何文档如果分享到外部域，将自动恢复到仅限于内部用户访问）。考虑到SaaS应用面向互联网，只要有可能，应当根据许可IP范围或位置限制访问范围。
- 一旦访问，SaaS应用保存的信息会被下载。应该开发适当的安全策略，以确保信息下载到符合企业安全策略的受许可设备。
- 能够区分出经过批准和未经批准的SaaS应用实例是非常重要的，还要应用相应的使用策略。
- 对任何第三方的基于API 的访问都需要经过适当的检查才能获得批准，并在满足业务要求后撤销。
- 如果SaaS服务商需要访问SaaS客户的数据，应该通知客户，由客户评估请求并最终决定批准或拒绝。

6.3.2 安全登录程序

- 不能使用基本认证（Basic Authatication），该方式本身就不安全
- 如果可能，SaaS应用程序应使用商用的身份服务，启用单点登录SSO以保障安全地登录
- 如果没有SSO，SaaS应用程序应强制密码复杂度和确保未泄露（例如在网站https://haveibeenpwned.com/进行验证），且密码不能与公司密码相同
- 考虑到SaaS应用程序向互联网开放，要确保用户身份真实性，应启用多因素认证
- 符合企业安全策略，仅允许用户通过许可设备登录SaaS应用程序
- 如果安全登录失败，任何密码重置过程都应自助完成

6.3.3 密码管理系统

- 如果可能，SaaS应用程序不应管理密码，而是通过IdD（身份提供商）启用SSO认证
- 针对SaaS应用本地密码验证的情况，密码存储应遵循OWASP指南

密码还应被存储在Key Vault密钥库，或类似的用于保护访问机密性、完整性和可用性的安全设备。

需要注意，密码是一种“凭据”。为了方便讨论，“凭据”的形态包含加密密钥、数字证书，或令牌Token。如果云服务客户不能管理密钥，那么强烈建议使用Key Vault密钥库或类似安全方案保障密钥的机密性、完整性和可用性。

6.3.4 使用特权实用程序或第三方插件

- 不应该允许以编程方式进行基本身份验证
- 应通过mTLS（双向TLS）验证访问者的身份
- 首选基于令牌的身份验证（OAuth 2.0）
- SaaS API应仅在指定的IP范围内可用
- 建立安全库并以加密格式存储特权凭据
- API的密钥应安全存储，并且只能通过HTTPS传输
- SaaS应用程序应该能够撤销访问密钥和令牌授权
- 应定期审查用于特权程序访问的身份
- 审查用户对第三方应用程序的许可
- 监控第三方应用程序的活动

6.3.5 程序源代码访问控制

- SaaS提供商应限制对源代码的访问
- 对产生源代码的开发管道或环境的访问控制也应仅限于SaaS提供商
- 源代码不应向不受SaaS提供商控制的程序或系统提供后门访问，也不应向SaaS消费者提供源码访问
- SaaS消费者创建的任何源代码以及备份应只被他们自己访问
- CSC应记录一个流程，描述要实施的安全门，以及在使用CI/CD管道时会触发安全审查的事件。安全门是一种评估软件安全风险的安全策略。在软件进入下一阶段前，必须审查和批准所有软件代码

7. 加密和密钥管理

7.1 SaaS环境中的数据安全

使用SaaS服务时需要考虑的最关键的方面之一是存储在该服务中的数据的安全性。在此运营模型中，供应商承担了应用程序安全的大部分责任。然而，正如共享责任模型所认为的那样，数据是云消费者的责任。

为了确保传输并存储到SaaS提供商的数据是安全的，客户在与这些供应商接洽时应考虑数据的加密以及对加密密钥的管理。无论何时从安全的内部位置移动数据，客户组织都有意外或恶意暴露数据的风险。确保正确的加密和密钥管理意味着，即使确实发生了对数据的不正当访问，在不先对数据解密的情况下，数据将无法使用。

本节回顾了客户组织可以采取的步骤，以确保使用管理良好的加密密钥对存储在SaaS提供商中的数据进行充分加密。

7.1.1 共享责任模式

虽然使用SaaS服务将管理和维护应用程序的一些责任从客户组织转移到了供应商，但一些责任仍将由客户承担。这些责任包括SaaS服务中数据的管理和安全以及其中的访问模型。

责任		SaaS	PaaS	IaaS	本地On-Prem
责任始终由客户承担	信息和数据	●	●	●	●
	设备 (移动端和PC端)	●	●	●	●
	账户和身份	●	●	●	●
责任因类型而异	身份认证和目录基础设施	●●	●●	●	●
	应用	●	●●	●	●
	网络控制	●	●●	●	●
	操作系统	●	●	●	●
责任转移至云提供商	物理主机	●	●	●	●
	物理网络	●	●	●	●
	物理数据中心	●	●	●	●

● 云提供商负责　● 云客户负责　●● 共享责任

7.2 加密SaaS提供商共享的数据

如上所述，任何时候从安全的内部位置移动数据，都有意外或恶意泄露的风险。缓解此风险的最佳方法可能是确保数据在传输到SaaS提供商或从SaaS提供商传输时以及存储在SaaS提供商系统中时加密。这包括确保应用程序和物理资源内的正确加密，这是SaaS提供商的责任。

7.2.1 需要考虑的问题和领域

需要加密的级别和需要存放的位置取决于对传输数据的理解和SaaS提供商的通用做法。在确定数据所需的保护级别时，应考虑以下问题：

7.2.1.1 供应商问题

- 供应商是否提供共享数据的精细控制（例如，仅在内部共享、与选定合作伙伴共享还是与所有人共享等）
- SaaS提供商是否在传输过程中提供数据加密？
- SaaS提供商是否提供静态数据加密？
- SaaS提供商是否支持端到端加密？
- SaaS提供商支持哪些加密算法和传输协议？
- SaaS提供商是否为每个客户提供唯一的加密密钥（单租户）？
- SaaS提供商是否有关于其关键管理程序的文档？
- SaaS提供商是否允许使用客户管理的加密密钥？
- SaaS提供商是否能够识别和/或屏蔽（遮掩）敏感数据？
- 当需要将生产数据复制到沙盒环境时，SaaS提供商是否支持假名化或修改（重新编辑、替换、删除等）？
- SaaS提供商是否为用户提供了标记敏感数据或字段的机制？

7.2.1.2 内部问题

- 上传到SaaS提供商的数据是否包含任何敏感细节？
  - 敏感数据可能包括类似个人可识别信息 （PII）或由您的数据隐私和合规需求定义的其他元素。
- 如果数据公开，对客户组织有何影响？
- 对组织的关键管理实践是否有信心？
- 内部流程是否支持端到端加密？

7.2.2 传输加密

数据从一个位置移动到另一个位置时被视为“传输中的数据”，这包括从客户组织传输到SaaS提供商的数据，反之亦然。配置多个互操作层时，数据安全性最强；因此，在数据传输过程中，安全性通常认为较低，因为用于保护数据的层较少。

为了保护传输过程中的数据，建议确保在所有数据传输中使用安全的加密网络协议。在编写本文时，最佳加密网络协议是传输层安全（TLS）1.2版或更高版本（首选TLS 1.3）。为了提升安全级别，TLS协议使用对称加密（使用相同的密钥加密和解密数据）和非对称加密（使用数学上相关的公钥和私钥加密和解密数据）的组合。这种组合的加密方法增强了所传输数据的机密性和完整性。

TLS 1.3删除了TLS 1.2中的一些影响性能的步骤，同时又不牺牲安全性。TLS 1.2和1.3的TLS握手和密钥交换过程示例如下：

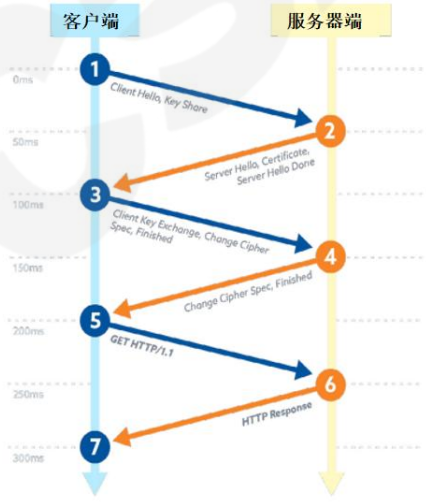

图 3. TLS 1.2（完整握手）

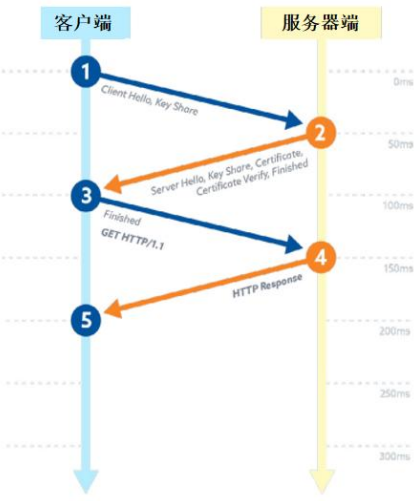

图 4. TLS 1.3（完整握手）

7.2.3 静态加密

如果数据在应用程序、网络或系统中不移动，则视为“静态”。如果数据在“静态”期间没有充分的保护，对SaaS提供商托管设施进行不当访问的攻击者可以公开（或泄露）这些数据或将其用于牟利。对静态数据加密可确保即使存储数据的硬件被盗，数据也不可用。

数据也可以在应用程序中加密，确保只有SaaS消费者能够看到他们的数据（因为他们是唯一可以解密数据的人），从而在多租户SaaS提供商环境中提供了一个边界。

加密的类型和强度取决于数据分类。如果存储的数据被视为公共数据，则可能不需要像敏感数据那样严格的加密。因此，客户组织应在向SaaS提供商存储数据之前做如下审查：

- 数据泄露的业务影响分析（BIA）
  - 为了确定数据是否需要在静态下加密，组织应执行BIA，以了解数据公开后的影响。
  - 另外应考虑CSP的其他安全组件，如访问管理，以确定数据泄露的风险.
- 静态加密服务的可用性
  - 并非所有SaaS提供商都将免费提供静态数据加密服务。了解购买（或获取）静态加密所需的许可模型。
- 静态备份数据加密的可用性
  - 虽然许多SaaS提供商将提供一种静态加密形式，但这并不总是适用于数据备份。确保对活动存储的数据和备份数据进行加密。
- 加密磁盘加密vs文件加密
  - 了解提供的静态加密类型。例如，使用磁盘加密方法虽然是一种合理的控制，但主要用于在磁盘或系统被盗时提供保护。
  - 作为一种更为常见的情况，使用文件加密可以保护单个文件和数据在不适当的访问情况下不被窃取。
- 用于加密静态数据的加密算法和密钥长度
  - 确保静态数据的加密方法满足CSC的需要。NIST 800-57第1部分：密钥管理建议（参考表2）详细说明了基于算法和密钥长度的加密强度。

7.3 客户管理加密密钥 vs 供应商管理加密密钥

通常，使用客户管理的加密密钥比供应商提供的加密密钥更安全。然而，是否使用供应商管理的加密密钥取决于两个因素。首先，供应商是否允许使用客户管理的密钥？并非所有供应商都支持使用你的加密密钥。其次，确保存储在供应商中的数据是否能达到使用你自己密钥同等级别的风险缓解水平，或者使用供应商管理的密钥的风险是否可以接受？

例如，使用供应商管理的加密密钥的风险水平取决于以下几个方面：

- 供应商是否提供有关如何创建和管理加密密钥的信息？
  - 在大多数情况下，供应商不会共享其环境中加密密钥的创建和生命周期管理背后的详细信息。
  - 为了更好地了解供应商的密钥创建和管理实践，建议要求提供他们系统中数据在传输和使用时如何加密的文档
- 存储在供应商系统中的数据有多敏感？
  - 例如，被定义为公共级别的数据在使用其加密密钥时可能几乎没有风险。
- 组织是否有良好的加密密钥管理实践？
  - 除了供应商的安全之外，通过密钥管理提供的保护还取决于您的组织保护密钥材料的能力。如果您的组织在实践方面与供应商相比还不成熟，那么使用供应商管理的密钥可能最适合您。

7.4 加密和密钥管理的未来状态

未来考虑的领域:

- 硬件安全模块即服务 (HSMaaS)
  - 有时也称为“云HSM”，这是一种通过SaaS提供的HSM产品创建和管理加密密钥的方法。
  - 经FIPS验证的HSMaaS提供商，如Fortanix、Microsoft，其他提供商的使用率正在增加。
- 隐私增强加密 (PEC) 方法

    - 一组技术，用于在维持功能的同时最大限度地减少系统收集的个人或敏感数据量。
    - 为了维护通用服务，SaaS提供商可能不支持使用PEC技术，因为他们需要更多的定制和与用户系统的交互来实现结果。
    - NIST提供了博客帖子和一个项目来审查PEC技术，并围绕这些技术制定标准和要求。
- 同态加密
    - 涉及对使用中的数据加密，同时仍允许通过位级加密/解密对数据操作。与传统方法相比，速度非常慢。
    - PEC方法的需求文档，包括同态加密，仍在由ISO和NIST等组织通过开放联盟领导开发。
- ‘机密计算’ 或 安全飞地
    - 使用硬件特性来保护云数据安全，使用中可通过从其他并发工作负载中隔离和处理数据。
    - NIST有可用的文件草案，提供有关云计算和边缘计算的保密计算技术的进一步信息。
- 后量子密码技术（PQC）方式
    - 可能至少在8年以后。
    - 2016年的NIST内部报告（IR）8105指出，到2030年，能够在数小时内破解2000位RSA的量子计算机可能已经存在。
    - NIST和其他组织，已经有项目在推进后量子加密标准的制定，其中一些组织公开呼吁提交和反馈。

8. 操作安全

8.1 操作程序和职责

8.1.1 记录的操作程序

SaaS产品的灵活性使得有必要了解组织将如何使用此类产品。

- 访问控制 - 参见访问控制章节
- 变更管理
- 容量管理
- 环境隔离
- 终止 - 参见终止章节

8.1.2 变更管理

添加SaaS产品应经过深思熟虑，太随意的添加到组织的生态系统可能会导致问题。因此，应实施强有力的变更管理流程。SaaS产品的变更往往很小而且很频繁。通常，用户可能看不到这些变更。然而，下游系统可能会受到影响。

重要的是要确定变更是否会影响组织的安全态势。此类变更可能需要组织修改其他系统。需要审查重大变更（通常是版本变更），并将其作为变更管理流程的一部分。

此外，SaaS产品通常考虑在特定的操作范围内使用。SaaS应用程序业务功能的后期更改、使用量的增长或使用复杂性的变化可能会导致需要重新考虑与使用SaaS应用程序相关的安全注意事项。建议管理员定期审查SaaS应用程序的使用情况，确保初始安全审查的范围与当前的使用范围相匹配。这将确保维护SaaS应用程序的最新安全模型。

8.1.3 容量管理

SaaS产品的使用可能对用户数量有许可限制。监控产品还可能限制被监控或附属的账户数量。根据用户或账户的数量，可能存在定价差异。在提高容量之前，需要考虑了解需求。

8.1.4 开发、测试、运行（生产）环境隔离

与内部开发的系统一样，有必要进行环境分离，以防生产数据从经批准的生产系统中泄漏。预计SaaS供应商将不断改进其系统。改进、升级或更新应该在具有非生产数据的非生产环境中测试。SaaS供应商应提供证明，证明不仅存在单独的环境，而且非生产数据也驻留在这些环境中。

此外，应持续评估这些SaaS应用程序的配置，以确保维护安全的环境。识别安全设置中的错误配置、跨用户数据访问、第三方集成等可以降低发生数据泄漏的风险。应在“过渡到产品（staging to product）”工作流（即产品研发工作流）涉及的环境中进行安全审查，以便在安全问题影响生产环境之前被及时识别。

8.2 防止恶意软件

8.2.1 恶意软件控制

恶意软件保护的大部分责任在于SaaS提供商，然而，在SaaS用户/管理员的控制下，仍然存在一些传播恶意软件的媒介。这些用户控制的媒介包括客户自定义的静态文件托管和附件，这些文件托管和附件可以由使用SaaS应用程序/特权用户的组织员工上传，或者由普通公众上传（如果SaaS应用程序提供面向公众的门户）。

SaaS管理员及其安全组织应进行典型的威胁建模练习，了解SaaS部署的面向公众的功能中存在哪些内容上传功能（如果有的话）。要注意面向公众的内容或文档上传系统，它们旨在存储或传输SaaS应用程序内部的，或特权用户将下载到企业设备上以其他方式查看的文件。

在评估其SaaS部署和配置时，客户应该熟悉SaaS平台的内置功能。很多都具有标准化的恶意软件和病毒扫描功能，可以标记或阻止潜在的恶意上传。应对SaaS系统的配置进行评估和监控，以（1）最大限度地减少可上传的外部控制内容的类型和数量，（2）确保启用内置保护和文件类型限制。

8.3 备份和高可用

8.3.1 信息备份

在大多数SaaS应用程序中，在基础设施或应用程序层出现故障时，管理数据备份、冗余和故障转移的责任由SaaS提供商承担。这是合理的责任分配，因为SaaS客户没有直接访问数据库、创建故障转移实例/副本等的能力。客户对数据的访问通常仅限于SaaS平台支持的API，这通常是创建和管理数据备份的低效方法。如果发生灾难性数据丢失事件，SaaS平台提供商将负责恢复数据。因此，当管理SaaS部署时，信息备份并不像在IaaS或其他部署那样重要，客户在较低级别上控制部署即可。

也就是说，SaaS客户仍然需要考虑信息备份方面的问题。如果在SaaS应用程序的预期/允许使用参数范围内无意或恶意删除数据(即恶意参与者使用支持的删除流程、API端点等删除数据和/或记录)，SaaS提供商将不负责提供备份并从备份中恢复。作为客户管理SaaS应用程序的经验之谈。如果平台按照设计的方式运行，即使配置是不安全的或不正确的，SaaS提供商也没有责任补救。

为了减轻SaaS客户的此类风险，部署持续配置和数据访问监控至关重要，以帮助确保不会向任何可能导致数据丢失事件的用户授予无意或过高的访问权限。这可能包括管理数据访问，以便正确授予用户最小权限，以及监控系统配置，确保逻辑删除或数据保留设置允许轻松恢复数据。最后，如果SaaS提供商尚未在平台上提供“回滚”或“备份”解决方案，SaaS客户应考虑是否提供额外的，基于平台外的API数据备份解决方案，为关键数据提供额外的冗余。

除了备份数据外，CSC还应实施快照策略。NIST标准800-125将快照定义为“…运行图像状态的记录，通常捕获图像与当前状态之间的差异。例如，快照将记录虚拟存储、虚拟内存、网络连接和其他状态相关数据的更改。快照允许挂起虚机系统并随后恢复，而无需关闭或重新启动虚机。许多（但不是所有）虚拟化系统都能打快照。”快照的一个好处是，与从备份执行恢复相比，可以更快地恢复图像/数据。

8.3.1.1 高可用

许多SaaS提供商在与SaaS客户的合同中定义了SLA和OLA，如果他们不能满足合同要求，通常会有服务承诺支持。也就是说，考虑到SaaS应用程序的需求，SaaS客户可以选择不同的冗余选项。不应该仅仅因为它是SaaS，就认为它总是可用的，并且应该探索可用的备选方案，同时考虑到业务对SaaS应用程序可用性问题的影响。

8.4 日志和监控

8.4.1 事件日志

与安全团队可能更习惯使用的基础设施、IaaS、PaaS 或应用程序日志相比，SaaS 部署的事件和访问日志记录具有明显的挑战。从使用SaaS应用程序日志的安全组织的角度来看，由于安全组织无权访问运行SaaS应用程序的硬件或软件的底层日志的事实，因此存在重大限制。

在极少数情况下，SaaS提供商可能会通过手动请求流程提供更详细和（或）更原始（更接近应用程序源）的日志。但是，由于这些选项所涉及的时间延迟、过程成本和财务成本，因此不能视为SaaS日志监控最佳实践的一部分。

对于监控SaaS应用程序安全的安全组织，更为复杂的是，SaaS应用程序日志输出没有行业标准的公认格式。像用户登录这样的常见操作在不同SaaS应用程序之间的日志消息格式和内容方面可能会明显不同，这给希望跨SaaS应用程序关联日志和活动的安全组织带来了挑战。

日志交付的及时性也会给希望使用SaaS事件日志作为事件检测手段的安全组织带来挑战。日志条目只有在经过SaaS提供商处理并在API或其他交付设施中提供以供最终用户自动访问后，才能供SaaS应用程序用户使用。从事件发生到事件日志可用性的SLA规定可以是几分钟到24小时，取决于SaaS提供商。

这些复杂性给使用SaaS事件日志作为监控SaaS应用程序中的安全性和活动的唯一机制带来挑战，但这并不能消除监控SaaS事件日志作为整体SaaS安全解决方案一部分的价值。使用SaaS事件日志的安全组织应该确保开发或部署以下功能：

- 从SaaS应用程序或提供商处获取日志的自动化程度和频率应该更高
- SaaS 日志首先应标准化为跨SaaS应用程序的通用格式，然后再传送到 SIEM 或其他日志存储解决方案。 这使安全团队能够有效地监控SaaS应用程序的活动
- 包含用户信息（如用户名或用户 ID）的事件、审计、活动和其他的日志条目应标准化为企业身份，以便同一个人在不同SaaS应用程序中的不同用户账户可以关联
- 每个SaaS应用程序的操作和日志条目可用性的预期、平均和最大延迟应记录在案，并将由使用日志系统的安全运营团队理解

8.4.2 日志信息的保护

8.4.2.1 管理员和操作员日志

许多SaaS 应用程序，尤其是那些具有显著复杂性的应用程序，都有单独的日志记录或审计工具来监控高权限用户所做的系统级配置更改。该系统可能被称为“审计跟踪”、“设置日志”或类似名称。在许多情况下，这会是与标准访问和事件日志相比在逻辑上独立的数据结构，并且可能需要不同的 API 或访问方法检索。

这些日志对于SaaS 事件监控至关重要，由于它们表示特权、经过身份验证的操作，可能会对SaaS应用程序的安全状况产生重大影响。此日志子集应遵循本文档“事件日志记录”部分中概述的所有最佳实践。

此外，监控SaaS应用程序的安全团队应该熟悉这组日志中最受关注的操作类型，并考虑部署可以监控这些日志的安全自动化技术，并提醒安全团队注意特权用户（即SaaS 管理员）所做的影响安全的更改。监控SaaS生态系统中这些预定义的“高风险”活动旨在减少检测时间，这有助于减少与SaaS数据泄漏相关的损害。

8.5 技术漏洞管理

确定SaaS 应用程序的所有者，并将这些所有者与安全功能联系起来。在大多数组织中，SaaS安全属于企业安全团队的责任。 但是，一些组织将SaaS安全定义为应用程序安全或第三方风险问题。无论谁负责，确定SaaS应用程序的所有者、了解每个SaaS应用程序的业务用例，然后定义漏洞管理的责任都至关重要。

跨SaaS应用程序控制安全性可能是一项重大挑战。例如SaaS 客户可能无法缓解发生在SaaS提供商基础设施中的已知漏洞。但是，大多数SaaS安全问题（以及相关的云安全问题）都发生在客户共享责任范围内。

这些共享责任包括管理SaaS应用程序的设置和配置，确保它们符合安全最佳实践。根据 NIST CSF、ISO 27001或NIST 800-53等标准审查策略配置，是降低不合规或不安全配置环境风险的有效做法。

考虑SaaS应用程序接受弱TLS加密套件的情况。 客户的策略可以强制其所有用户在与该SaaS的连接上使用安全性更强的加密套件，从而减轻此漏洞，直到最终解决为止。此外，需要考虑管理员关闭关键安全防护机制（如 xss 防护）以便于为用户提供更流畅的体验。在这种情况下，管理员应该通过对这种错误配置的持续监控机制得到告警，并修复问题。

8.5.1 技术漏洞管理

SaaS安全只有通过IT应用程序所有者、企业安全团队和技术领导者之间的跨职能协作才能最有效地得到改善。IT 应用程序所有者必须负责问题的补救，而安全人员必须负责分类和跟进，确保在组织内商定的唯一SLA范围内补救。必须与组织接受的SLA保持一致，并像对待任何其他安全域一样遵循。

如云安全联盟博客文章“构建SaaS 安全计划：快速入门指南”中所述，“了解哪些SaaS应用程序属于对哪些团队很重要，因为一旦您确定了问题，就需要与正确的业务团队沟通以解决它们。不可避免的是，业务关键型 SaaS工作流中可能存在一些最紧迫的安全问题。

因此，应急响应团队需要迅速采取行动，清点所有安全漏洞，把它们映射到所有者，并对每个发现的风险做出基于严重性的决策，以便他们能够首先解决最重要的问题。”

8.6 信息系统审计注意事项

8.6.1 信息系统审计控制

SaaS提供商可能不受客户的信息系统审计控制。但是，客户需要（通常通过法规）确保 SaaS 提供商具有可接受的控制措施。这可以通过自我证明或第三方证明。

虽然自我证明可能是法律要求的最低审查，但也是了解现有安全控制是否有效运行的最不可靠的方法。同样，仔细阅读第三方审查结果至关重要，并且要重点关注以下方面：

- 评估范围- 读者可能会发现参与的第四方不包括在评估范围内，包括额外的IaaS、PaaS、SaaS或其他第四方解决方案。如果是这种情况，了解供应商管理/第三方风险政策、清单以及所进行评估的范围和深度将会非常重要。
- 测试和报告方法 - 选择放弃现场审查并选择依赖第三方评估（ISO27001，SOC2 Type II）应由熟练且全面的审核人员考虑和评估，最好具有行业认可的证书，也最好具有实施纵深防御战略的丰富经验。
    - 第三方评估应让读者相信SaaS技术和安全人员接受了访谈，阅读了安全策略文件，收集了样本并进行了测试。
    - 评估员的专业水平也可以从报告语言中推断出来。应摒弃对控制语言的简单重述，以及不存在或不可靠的测试方法。

这可以通过在合同中加入条款，要求SaaS提供商遵循特定可接受标准的条款来实现（例如，CSA 的 CCM 、FedRamp、NIST、ISO），并提供对这些标准的认证，并定期审查证明控制有效性的证据。

云安全联盟提供基于云控制矩阵（CCM）版本 4 的审计指南。这些指南旨在促进和指导 CCM 审计。根据 CCMv4.0 控制规范向审计员提供了一套评估指南，旨在提高控制实施的可审计性并帮助组织更有效地实现合规性。这些指南在本质上既不详尽，也不具有规范性质。它们代表了评估建议形式的通用指南。审计师将需要定制描述、程序、风险、控制和文件，并根据评估范围内调整组织和服务的审计工作计划，解决审计的具体目标。

9. 网络安全管理

在SaaS服务消费背景下，网络安全的治理或与数据流安全相关的控制已分为两个不同的领域；由SaaS提供商拥有和操作的控制措施以及SaaS使用者可能需要考虑的控制措施。

跨两个域的关键网络控制可以概括为传输中的数据加密、对指定资源的授权和数据传输控制。

这里介绍了实现网络安全的零信任网络访问ZTNA和安全访问服务边缘SASE方法。

9.1 SaaS提供商网络控制

服务消费者应与SaaS提供商确认有效的TLS证书用于外部连接和微服务的内部保护。证书应该来自知名的、受信任的证书颁发机构，而不是自签名的。

此外，服务消费者应设法确认在SaaS平台内的离散服务组件之间使用加密的程度。

SaaS 提供商可以通过零信任网络访问策略在最低特权的基础上控制网络数据流。SaaS提供商可以利用网络流量异常检测功能作为检测控制。

9.2 SaaS消费者网络控制

服务消费者在评估与SaaS提供商相关的安全状况和风险时应考虑以下网络安全控制。

由于与SaaS提供商的连接可能会遍布公共互联网，通过TLS 1.2及以上版本保护传输中的数据是关键的安全控制。

访问SaaS服务可能会为不良行为者提供机会，通过将数据上传到不受SaaS消费者控制的账户泄露数据。可以使用云访问安全代理（CASB）和租赁通道身份验证控制这种风险。

还应考虑数据丢失预防（DLP）控制；这些可能部署在网络或其他层，具体取决于对有效载荷数据的访问。

服务消费者在构建与SaaS提供商的网络连接时应考虑可用性要求，例如冗余互联网线路和容量规划。

SaaS 消费者应考虑使用受保护的DNS(通常是基于SaaS的服务)控制DNS流量。

现代网络架构可能会利用出站互联网访问的分流，从而导致本地分支机构互联网流量激增。SaaS消费者必须考虑在客户直接使用SaaS服务的情况下应用上述控制。

安全访问服务边缘（SASE）模型可以通过充当SaaS消费者和提供商之间的策略执行点促进这种控制状态。

10. 供应商关系

10.1 供应商关系中的信息安全

SaaS 产品几乎总是建立在第三方服务之上，包括由供应商直接管理和维护的服务以及第四方IaaS、PaaS 和SaaS 产品。与传统的客户管理软件部署不同，SaaS消费者通常很难理解相关产品的完整依赖项集。因此，对于那些运营SaaS产品的人来说，构建其业务运营所依赖的技术的综合模型至关重要。

与传统的客户管理软件部署一样，可以为SaaS产品(也称为 SaaSBOMs)开发软件物料清单(SBOM)提供这样的模型。现有的标准CycloneDX可以促进包含SaaS组件的SBOM的创建。对这些表示的评估可以让组织识别其技术供应链中的已知漏洞，并允许更快速地修复。

除了开发和维护组成给定SaaS产品的组件的实时情况外，组织还应该为使用这些组件制定内部风险管理策略。同样，组织应与CSP协商合同条款，以确保产品的安全性。最后，外部认证制度可以帮助风险管理分析和决策，但使用SaaS服务的组织不应仅仅依赖它们。

10.1.1 供应商关系的信息安全政策

所有依赖外部方来保障其业务运营的企业（几乎是现代经济中的每一个公司）都应该有第三方风险管理政策。除了与组织有直接关系的第三方之外，这些外部方本身也将与第四方建立关系和依赖关系网络，因此需要制定第三方风险管理政策。

除了组织所依赖的其他技术外，此策略还应针对SaaS产品。至少，这样的策略应明确以下内容：

- 与第三方的每种关系（及其所有固有的第四方风险）在组织内的单一责任角色或职位。
- 要求提供关于依赖第三方产品或服务的业务运营的关键性评估，最好是定量评估。
- 评估事件影响第三方的可能性以及此类事件影响组织业务运营的方法，考虑到上面确定的关键性。这可以包括但不限于使用以下内容：
    - 外部审计和安全审查（有关详细信息，请参阅认证保证部分）
    - 供应商安全评分/评级工具
    - 直接的技术尽职调查，包括由客户组织进行的审计、渗透测试或对供应商的产品或基础设施使用自动扫描工具
- 基于上述确定的风险阈值，如果第三方超出此范围，将触发第三方（合同规定）、组织本身（通过一些补偿控制）或两者采取补救措施的要求。
- 组织内有权接受上述风险的单一责任角色或职位，以及用于记录和证明接受此类风险的透明流程

10.1.2 解决供应商协议中的安全问题

与供应商的协议应要求采取各种措施确保其SaaS产品的安全可靠运行。SaaS提供商可以代表不同规模和复杂程度的组织，他们的产品可能对组织具有不同程度的重要性。因此，可能有必要为各个供应商量身定制协议。此类合同可以包括：

- 服务级别协议（SLA），不仅针对产品的可用性（也称为“正常运行时间”），还针对数据的机密性和完整性。例如，为了达到激励目的，组织可能会要求供应商同意为每条被恶意行为者暴露或破坏的特定类型的记录支付预定费用。
- 要求组织进行外部审查（如审计、渗透测试等）并提供审查结果。。
- 要求基于对风险的客观评价，在给定的时间内解决供应商产品中的漏洞或提供缓解措施。
- 如果供应商发现组织可以对其应用采取补偿控制以降低漏洞的严重性或被利用的可能性，则应要求供应商在特定时间段内通知组织。
- 要求供应商与组织合作调查和补救已影响或可能影响组织数据机密性、完整性或可用性的事件。
- 要求供应商告知数据中心位置和拒绝不合规位置的权利。

与供应商谈判的组织应谨慎考虑自己的风险管理能力，避免在合同中添加不切实际的条款。例如，要求供应商将其网络、系统或软件中发现的任何漏洞通知组织的要求可能会导致一连串的告警，而这些告警对于组织基本上是无用的。

10.1.2.1 外部认证

外部认证是指受信任的外部组织证明供应商满足特定要求的过程。此类认证可以在对CSP进行风险评估时提供帮助，并有助于澄清提供商对其控制措施的声明以及提供商的实际安全状况。话虽如此，审查外部证明应该是对全面广泛的第三方风险管理计划的补充，而不是替代。

并非所有的认证和审计报告都是相同的，相同的报告类型覆盖的范围也不相同。 ISO/IEC 27001等认证表明CSP已按照规定的一组控制措施建立了信息安全管理基线。

然而，SOC2鉴证是基于审计师对提供商遵守控制措施能力的评估。而且，与 ISO/IEC 27001 不同的是，SOC2 报告本身并不是“认证”。基于正在审查的认证标准（由提供商选择），审计师会对提供商是否满足这些标准的要求发表四种意见之一。审计师报告还将记录供应商声称已实施的控制措施的任何异常情况。许多供应商会声称他们“符合 SOC2标准”，这不是审计会给出的结果。如果您正在查看SOC2报告，请务必检查：

- 考虑了哪些 TSP 标准（安全性、机密性、可用性、处理完整性和隐私）。
- 报告类型是什么
  - SOC2 类型 1 – 说明服务组织的基于TSC的系统和控制设计。该报告描述了当前的系统和控制措施，对围绕这些控制措施的文件进行了审查。所有管理、技术和逻辑控制的设计考虑都在特定时间点进行验证。
  - SOC2类型 2 – 说明服务组织的系统已经设计并应用了相关控制，以及这些控制是否有效。 SOC2 类型 2审计通过收集并分析至少六个月的证据来进行，以查看系统和现有控制是否按照服务组织管理层的描述运行。通常 SOC2 类型 2 报告需要在签署 MNDA（双方保密协议） 的情况下共享。
  - SOC3 – 这是与 SOC2类型 2 报告类似的可公开共享的报告。
- 请务必阅读独立审计师的评论部分。审计师会说明哪些领域不合规。这可以让您了解SaaS提供商是否按照他们在政策和程序上的规定进行了落实。

无论您查看CSP的哪些报告，密切关注认证/审计的范围和业务实体或证明。范围应涵盖正在考

虑或使用的SaaS服务，业务实体应为将与之签订合同的实体。例如，一些供应商可能会提供其服务运行所依赖的IaaS供应商而不是要审计的内部控制的SOC2报告。这虽然有助于分析第四方风险，但此类报告并不能替代提供商本身的审计。

同样，有必要查看报告以确定是否涵盖组织将依赖的整个产品，而不仅仅是包含应用程序所使用的数据中心/IaaS云资源。

以下是SaaS客户在评估CSP的安全性时可以使用的部分鉴证报告、认证和证明清单：

- 综合
  - 美国注册会计师协会（AICPA)- SOC2
  - 国际标准化组织（ISO)/国际电工委员会（IEC）-27001
  - HITRUST -通用安全框架（CSF)
- 政府资助
  - 美国 - FedRAMP
  - 新加坡 - SS584
  - 欧盟 - 通用数据保护条件（GDPR）
- 专注于云安全
  - 云安全联盟 - STAR
  - ISO/IEC - 27017
- 专注于金融交易
  - BSI Kitemark - 安全数字交易
  - 支付卡行业 - DSS
- 注重隐私
  - ISO/IEC - 27018

11. 事件管理

11.1 云安全事件管理

许多组织都坚持云优先战略。尽管这通常是一个更受业务驱动的决策，但这些组织必须意识到，必须审查、调整和采用相应的基础信息安全流程和程序。这其中的关键文件之一是安全或网络事件响应（IR）计划。作为健全的安全治理的一部分，应审查现有的 IR 流程和程序，并且应该纳入企业利用的所有云服务和部署模型。

有关云事件响应和各个阶段的更多详细信息，强烈建议查阅 CSA的云事件响应框架。

11.2 SaaS事件响应责任和程序

将数字信息资产转移到云端并不能完全转移责任或问责制（尽管可以通过明确的托管合同协议约定例外情况）。最后，资产的所有者全权负责对其云资产（及资产上的数据）的审慎管理，以应对暴露的风险。在三种云服务模型中，SaaS模型与其他模型（即PaaS和IaaS）相比，提供了最全面完整的功能。如CSA的安全指南 v4 第20页所述 - 对于 SaaS，云提供商负责几乎所有层的安全。云服务客户 (CSC)只能管理对应用程序（包括客户端设备）的身份和访问、应用程序的信息清除，以及r提供商支持的某些数据加密设置（如自带密钥）。 CSC无法控制虚拟化、网络和边界安全。互联网安全中心的共享责任模型如下图所示，供参考：

责任	本地On-Prem	IaaS	PaaS	SaaS	FaaS
数据分类和责任	●	●	●	●	●
客户端和端点保护	●	●	●	●●	●●
身份和访问管理	●	●	●●	●●	●●
应用级访问控制	●	●	●●	●●	●●
网络访问控制	●	●●	●	●	●
主机基础设施	●	●●	●	●	●
物理安全	●	●	●	●	●

● 云客户的责任　● 云提供商的责任　●● 共享责任

在这种模式中，一些技术责任会被转移， 因此，云客户有必要明确地与云服务提供商签订符合企业安全要求和标准基线的合同协议。CSC在采购阶段可以参考利用《CSA共识评估调查问卷》。如前所述，CSC 无论何种关系，仍然具有保护企业信息和资产的责任。 控制权可以转移，但责任不能转移。

必须更新客户的事件响应计划，以纳入这些技术限制，并维护关键CSP联系人清单。安全和非安全事件的服务级别协议必须通过合同协议达成。

11.3 阶段 1：准备

如参考的CSA云事件响应框架所述，事件管理的准备程度与组织对（网络）安全事件的反应方式直接相关。在SaaS服务方面，必须对企业（经批准的）SaaS环境有一个清楚的了解. 在采购过程应审查每个SaaS服务，并包括可靠的第三方风险分析，以符合公司风险容忍度、监管和行业合规要求。任何未受CSC直接（技术）控制的已识别风险必须进行评估，如有必要，应通过合同约束来降低风险.

CSC必须了解该服务在供应链风险和业务目标连续性方面的重要性（机密性、完整性和可用性的评估）除此之外，对于任何采购的SaaS服务，必须记录关键利益相关者（业务、技术（IT/IT安全））的联系人列表，并添加到集中的企业资产数据库中，并告知事件响应者（或CSIRT的任何其他成员）。

根据偏好，必须编写针对SaaS场景的剧本，匹配适用于此服务模型的威胁/滥用场景。如果SaaS提供商违反了条款，则可以准备沟通方案，以通知公司（内部/外部）利益相关者。即使影响尚未明确或完全形成，也可以发布声明，主动通知客户/合作伙伴。每个SaaS服务应具有集中存储的参数或标签（即CMDB），这将有助于决定应执行何种类型的沟通（即租户是否管理个人客户数据？）。

11.4 阶段 2：检测和分析

因为客户（CSC）只负责保护数据和访问数据，此类SaaS环境中的大多数事件将由CSP检测。CSC应通过利用身份提供商的身份验证信息和SaaS服务访问日志密切监控未授权访问。 CSC完全负责检测数据外泄或侦察活动（即利用蜜罐）。因此，CSC必须始终致力于将任何SaaS服务与企业身份平台集成，包括多因素身份验证。其次，CSP发出的告警应与标准CSC事件响应流程相结合。最好通过自动接收告警和分配适当的优先级实现自动化，取决于SaaS服务的业务关键性。如果CSP支持，则应将日志发送到CSC SIEM或IDS解决方案。

此外，利用已建立的SaaS CSP干系人合同援引协议中商定的网络条款并获得必要的支持以分析任何潜在的违反保密性、完整性或可用性的行为仍然至关重要。最后，CSP的参与对调查取证至关重要。

11.5 阶段 3：遏制、根除和恢复

与之前的所有阶段一样，CSC在响应行动中会受到限制。CSC只能做到：基于原始IP限制对其租户的访问（Allowlist，注意：并非所有SaaS提供商都支持此功能），撤消用户或账户访问（包括oAuth权限、密钥轮换、多因素令牌等），以及轮换静态数据加密密钥，等等。

在恢复方面，请求CSP提供必要的支持以调用CSC数据备份和恢复计划至关重要。这可以通过CSC利用第三方备份工具或通过请求CSP支持恢复租户数据来实现。

11.6 阶段 4：总结改进

永远不要错过重要的改进机会；回顾所吸取经验教训，是健全IRP的关键最后一步。审查整个事件，以确定计划中哪些要素可以改进。它可以是技术性的，也可是管理性的（如缺少与SaaS提供商的合同协议或缺少过程中的步骤）。关键问题可能是：

- 是否及时发现事件，或者是否可以改进？（指标和日志）
- 是否得到了供应商的必要支持？（合同/SLA）
- 是否及时通知利益相关者（合规和沟通）

事后的总结报告应作为经验教训直接反馈到第1阶段，并帮助CSC更好地管理（SaaS）事件。理想情况下，事件后分析应该仅仅回顾时间线和事件，更应该是一个学习过程。这方面的一个很好的例子是“根因分析（how we got here）”或“howie”流程，该流程最初由Jeli、Netflix、Slack和自适应容量实验室（Adaptive Capacity labs）共同创建，虽然并不是严格以安全为中心。

或者，必须评估某些事后信息是否对同行或其他CSP有利。可以向利益相关者发布公告消息（参见2021 11月16日谷歌云宕机的示例）或利用CSA的云网络事件共享中心（CloudCISC）。请参阅CSA云事件响应框架第6章，指导信息共享和协调。

12. 合规性

12.1遵守安全策略和标准

使用SaaS应用程序存储和处理敏感数据必须按照所有相关的内部和外部适用合规标准和安全政策进行评估，评估方式和严格程度与公司所有其他系统相同。值得注意的是，这意味着应根据SaaS应用程序中包含的数据的类型和敏感性以及其他相关风险因素（如：风险记录的数量、组织的依赖性和连续性）对SaaS应用程序进行分类和评估。

合规的组织至少必须了解、记录和监控：

- SaaS应用程序中的相关数据分类
- 广泛访问SaaS应用程序的用户类型
- 哪些类型的用户可以访问SaaS应用程序中哪些类别的数据
- SaaS应用程序中的访问控制
- SaaS应用程序提供的任何审计功能
- 与SaaS消费者相关的合规框架的任何适用合规性评估或认证

特别重要的是要注意使用中的任何SaaS应用程序，这些应用程序可能既包含敏感和/或法规遵从性相关数据，又向外部用户（非员工/非特权）开放访问门户或其他访问入口。这些SaaS应用程序需要额外的审查和监控，因为错误配置可能会导致违反合规性要求。例如，向匿名的互联网用户或未经授权的用户泄漏数据。

虽然在许多组织中，SaaS应用程序的合规性评估和认证是根据需要进行的，通常是每季度或每年进行一次，但更好的做法是建立一个自动化、连续的监控系统，满足安全和合规需求。一般来说，建立持续监控系统的前期工作等于验证单个合规周期的合规性所需的工作。连续监控系统既可以减少未来法规遵从性周期中的工作量，又可以减少系统可能不符合法规的时间，使其成为一项值得长期投资的项目。连续监控系统还促进了近实时的法规遵从性保证，而不是传统的基于快照的评估活动。

部署此类连续监控解决方案通常需要：

- 确定哪些SaaS应用程序与每个合规框架相关并在其范围内。
- 确定每个相关SaaS应用程序中哪些用户组或群组在合规范围内。
- 将相关合规框架所需的特定于SaaS应用程序的设置和访问控制映射到它们满足的框架的元素。
- 利用基于软件的工具，促进SaaS应用程序的自动连续监控和报告活动。

一旦这些工作完成并有了持续监控解决方案，确保SaaS应用程序及其数据始终符合所有相关的内部标准和外部合规框架就变成了一个自动化的过程。这种连续监控可用于根据需要生成合规制品（如监控数据或结果），从而验证SaaS应用程序是否符合要求，以及是否在给定的时间段内符合要求。

请求定制保留时间最好在合同阶段协商。如果购买SaaS解决方案是为了完成定制任务，那么何时可以从SaaS解决方案中永久删除已处理的数据？如果SaaS解决方案有保留数据的法律义务，是否可以每隔一段时间将处理后的数据传输到离线存储？通过请求自定义保留时间，可以显著降低风险。

12.2 遵守法律和合同要求

12.2.1 适用法律和合同要求的识别

请参阅“供应商关系”一节中的“解决供应商协议中的安全问题”。

12.2.2 知识产权

云客户必须审查并理解CSP使用其平台的“条款和条件”。在某些情况下，服务提供商可能保留访问客户数据的权利。服务提供商还可以就某些任务与第三方供应商签订合同。这也会导致外部公司访问云客户数据的可能性。

12.3 信息安全审查

利用如上所述的持续监控工具和实践，可以促进组织SaaS使用的信息安全审查活动。这些审查可以包括合规性评估、遵守组织和行业安全最佳实践以及实施充分的安全保护等活动。信息安全审查还应包括评估组织SaaS库存的活动，以确定潜在的未经批准的SaaS使用情况。

13.CASB的功能和发展方向

云访问安全代理CASB是随着SaaS服务的发展而出现的一类服务，其功能聚焦影子IT（即：使用的服务未经公司IT部门批准，因此不受其保护）的可见性、监控和控制。包括以下主要功能：

- 风险洞察：最初的用例是分析客户出口设备日志以及与单个云服务相关的风险专有数据，以共享洞察，如：
  - 客户环境中的云服务总数；
  - 高风险服务的占比（例如，远程桌面控制、协作应用程序等类别）；
  - 上传到高风险云服务的数据量；
  - 利用公司信用卡获得的任何云订阅，确定要购买的未经批准的应用程序。

这种可见性对于商业决策者来说是前所未有的。当然，下一个问题是关于控制现在可见的风险。

- API：此模式利用API实现额外的可见性和控制。例如，常见用例是列出下载最大数据量的顶级用户，撤消任何外部方对公司某个数据子集的访问等。在此模式下采取的所有策略操作都几乎是实时的
- 内联：这种模式提供了最全面的覆盖范围，通过将应用程序流量引导到CASB云，解析流量的模式检测上传、下载等特定活动，应用细粒度策略，而不是传统的允许或阻止策略。一个常见的例子是，对于中等风险的云应用程序，只允许下载不违反数据保护策略的数据。

另一类服务是SaaS安全态势管理（SSPM），它通过根据预先构建的符合行业标准（如CIS或NIST）的策略配置文件持续监控SaaS应用程序，从而简化和自动化SaaS应用程序的配置管理。错误配置会迅速触发警告，用户甚至可以在问题被利用之前自动修复。

这几类服务将继续发展并可能融合到一个称为安全服务边缘（SSE）的新服务中。对这种演变的详细分析超出了本文的范围，但这是云和SaaS安全从业者应该持续关注的问题。

14. 结论

很明显，SaaS的使用正在加速。随着这种加速，企业运营和利用云产品的方式受到了广泛的影响。也就是说，与传统的云安全不同，SaaS的细微差别需要更多的关注和解决。这包括组织如何处理信息安全策略、访问管理和访问控制。由于数据不再由消费者控制，因此围绕加密和密钥管理的考虑变得至关重要。网络安全决策可能会对消费者访问SaaS服务的方式以及从提供商到SaaS消费者的潜在连接产生影响，无论是在内部部署还是在云中。SaaS还代表着一个复杂的供应链，通常不仅包括SaaS供应商，还包括底层云或托管提供商。必须重新审视事件管理和业务连续性实践，因为SaaS产品在业务运营中发挥的作用越来越大。

虽然SaaS为企业提供了巨大的机会改变其运营方式、使用创新能力并减轻与创建和维护应用程序相关的许多运营负担，但并非没有安全隐患。未能解决这些问题可能会增加与SaaS相关的安全事件的潜在风险和后果。

15. 参考文献

Cloud Security Alliance. (n.d.). *Security, Trust, Assurance and Risk (STAR)*. CSA. Retrieved May 20,2022, from https://cloudsecurityalliance.org/star/

Cloud Security Alliance. (2017, July 26). *Security Guidance for Critical Areas of Focus in CloudComputing v4.0*. CSA. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Cloud Security Alliance. (2021a, May 4). *Cloud Incident Response Framework*. CSA. https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/

Cloud Security Alliance. (2021b, June 7). *Cloud Controls Matrix and CAIQ v4*. CSA. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Cloud Security Alliance. (2021c, June 7). *STAR Level 1: Security Questionnaire (CAIQ v4)*. CSA. https://cloudsecurityalliance.org/artifacts/star-level-1-security-questionnaire-caiq-v4/

Cloud Security Alliance. (2021d, July 29). *Cloud Threat Modeling*. CSA. https://cloudsecurityalliance.org/artifacts/cloud-threat-modeling/

Cloud Security Alliance. (2021e, December 8). *CCMv4.0 Auditing Guidelines*. CSA. https://cloudsecurityalliance.org/artifacts/ccm-v4-0-auditing-guidelines

International Standards Organization. (2020, December 16). *ISO/IEC 27001:2013*. ISO. Retrieved May20, 2022, from https://www.iso.org/standard/54534.html

International Standards Organization. (2021, April 15). *ISO/IEC 27002:2013*. ISO. https://www.iso.org/standard/54533.html

International Standards Organization. (2022a, February 4). *ISO 31000:2018*. ISO. https://www.iso.org/standard/65694.html

International Standards Organization. (2022b, May 4). *ISO/IEC 27000:2018*. ISO. https://www.iso.org/standard/73906.html

16. 定义

云访问安全代理(CASBs) 。内部部署或基于云的安全策略执行点，位于云服务消费者和云服务提供商之间，用于在访问基于云的资源时合并和插入企业安全策略。CASB整合了多种类型的安全策略执行。比如身份验证、单点登录、授权、凭据映射、设备分析、加密、令牌化、日志记录、告警、恶意软件检测/预防等[1]。

软件即服务(SaaS)。 提供给消费者的能力是使用提供商在云基础设施上运行的应用程序。可以通过瘦客户端界面（如web浏览器）或程序界面从各种客户端设备访问应用程序（比如基于web的电子邮件服务）。消费者不管理或控制底层云基础设施，包括网络、服务器、操作系统、存储，甚至是单个应用程序功能，但需要管理特定于用户的应用程序设置，虽然这些设置功能可能是很有限的[2]。

软件物料清单。 一种正式记录，包含构建软件中使用的各种组件的详细信息和供应链关系。软件开发人员和供应商通常通过组装现有的开源和商业软件组件来创建产品。SBOM列举产品中的这些组件[3]。

SaaS安全态势管理 (SSPM)。提供对基于云的SaaS应用程序（如Slack、Salesforce和Microsoft 365）的自动连续监控，最小化风险配置，防止配置漂移，并帮助安全和IT团队确保合规。

安全服务边缘(SSE)。保护对web、云服务和私有应用程序的访问。这些功能包括访问控制、威胁保护、数据安全、安全监控，以及通过基于网络和基于API的集成执行的可接受使用控制。SSE主要以云服务的形式提供，也可能包括内部部署或基于代理的组件。

[1] https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokerscasbs
[2] https://csrc.nist.gov/glossary/term/software_as_a_service
[3] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations cybersecurity

17.缩略词

AICPA - 美国注册会计师协会

API - 应用程序接口

CASB - 云访问安全代理

CIA - 保密性、完整性、可用性

CCM - 云控制矩阵

CSA CCM - 云安全联盟云控制矩阵

CSA STAR - 云安全联盟安全、信任、保证和风险

CSC - 云服务客户

CSP -云服务提供商

DLP -数据防泄露

FedRAMP - 联邦风险和授权管理计划

HIPAA - 健康保险携带和责任法案

HITRUST-健康信息信托联盟

IaaS - 基础设施即服务

IEC - 国际电工委员会

ISMS - 信息安全管理体系

ISO - 国际标准化组织

NIST - 美国国家标准与技术研究院

MTD - 最大容许宕机时间

OTP --一次性口令

PaaS - 平台即服务

PCI -支付卡行业

PII - 个人可识别信息

RFI - 信息请求

RTO -恢复时间目标

RPO - 恢复时间点目标

SaaS - 软件即服务

SASE - 安全访问服务边界

SBOM - 软件物料

SIEM - 安全信息与事件管理

SLA - 服务级别协议

SOC1 - 服务组织控制1

SOC2 - 服务组织控制2

SSE - 安全服务边界

SSPM -SaaS安全态势管理

TLS - 传输层安全协议

VM - 虚拟机

ZTNA - 零信任网络架构