云计算

信息安全的收益、风险与建议

------精简版

ENISA

欧洲网络与信息安全

执行摘要

安全评估基于三种场景：1）中小企业向云环境的迁移，2）云计算对服务弹性的影响，3）电子政务中的云计算（如电子卫生保健）。

新的经济模式也推动了技术变革：

规模：商品化和实现经济效率的努力导致提供服务所需的硬件资源大量集中。这鼓励规模经济 - 提供计算服务所需的所有资源。

架构：最佳资源使用需要从底层硬件抽象出来的计算资源。共享硬件和软件资源的无关客户依靠逻辑隔离机制来保护他们的数据。 计算，内容存储和处理都是大规模分布式的。

最佳建议

保证客户的安全

云消费者需要确保提供者在减轻客户和提供者面临的风险（例如 DDoS 攻击）时遵循可靠的安全措施和实践。

我们已经将报告的许多建议归纳为获得云提供者安全保障保证的标准问题单：

- 评估采用云服务的风险;
- 比较不同的云提供者产品;
- 从选定的云提供者处获得保证;
- 减少云提供者的保证负担。

安全检查清单涵盖安全要求的所有方面，包括法律问题，人身安全，政策问题和技术问题。

法律建议

云计算涉及的大多数法律问题目前都将在合同评估期间（即，在不同提供者之间进行比较时）或谈判中得到解决。 云计算中更常见的情况是在市场上提供的不同合同（合同评估）之间进行选择，而不是合同谈判。 但是，云服务的潜在客户可能会选择合同可协商的提供者。

与传统的互联网服务不同，云计算的特性使标准合同条款可能需要额外的审查。合同当事方应特别关注其与安全违规通知，数据传输，衍生作品创建，控制权变更以及执法机构获取数据相关的权利和义务。 由于云可以用来外包关键的内部基础设施，并且该基础设施的中断可能会产生广泛的影响，所以各方应仔细考虑标准责任限制是否足以代表责任分配，因为各方使用云，或者基础设施的责任。

研究建议

为了提高云计算技术的安全性，我们建议优先研究几个领域。以下是我们已经考虑过的类别，并列举了完整清单中的几个特定例子：

在云中建立信任

- 不同形式的违规报告对安全性的影响
- 云端和端点之间端到端的数据机密性
- 高保证级别的云，虚拟私有云等

大规模跨组织系统中的数据保护

- 取证和取证机制。
- 事件处理 - 监控和可追溯性

相关法规的国际差异包括数据保护和隐私

大型计算机系统工程

- 资源隔离机制 - 数据，处理，内存，日志等
- 云提供者之间的互操作性
- 云计算的弹性。 云如何提高弹性？

最大安全收益

安全和规模效益：

规模越大，实施安全措施的成本越低。相同数量的安全投资能获得更好的安全收益。这包括各种防御措施，如过滤、补丁管理、虚拟机实例和虚拟化管理程序的加固等。规模化的其他好处包括：多个位置、边缘网络（交付或处理更接近目的地的内容）、事件响应的及时性、威胁管理等。

相同数量的安全投资能获得更好的安全收益。 这包括各种防御措施，例如过滤，补丁管理，虚拟机实例和虚拟化管理程序加固等。规模化的其他好处包括：多个位置，边缘网络（交付或处理更接近其目的地的内容），事件响应的及时性，威胁管理。

安全导致市场差异化：

安全性是许多云消费者的首要考虑事项;消费者将根据提供者的保密性，完整性和弹性以及声誉作为选择提供者的依据。

资源集中的好处：虽然资源的集中无疑对安全会产生不利影响[见风险]，但它具有更便宜的物理边界限制和物理访问控制（每单位资源）以及许多安全相关过程的更容易和更便宜的应用。

标准化的安全管理接口：

安全服务：大型云提供者可为托管安全服务商提供标准化，开放的接口。这为安全服务创造了更开放和更容易获得的市场。

快速智能的资源伸缩：云提供者动态资源分配使安全防御措施（例如针对 DDoS 攻击）具有明显的弹性优势。

审计和取证：通过虚拟机的专用付费取证镜像，减少取证分析的停机时间。它还可以为日志提供更具成本效益的存储。

更及时的发布更新与有效的默认安全配置：对虚拟机镜像和软件模块预先加固，包括更新最新的补丁以及进行安全设置;同时定期对虚拟基础设施进行快照，并与基线进行比较。 与传

统的基于客户端的系统相比，跨平台的平台可以更快速地发布更新，而传统的基于客户端的系统依赖于修补模型。

资源集中的优势：资源的集中会带来安全问题，但也具有明显的优势，即更便宜的物理边界限制和物理访问控制（每单位资源）以及许多安全相关过程的更容易和更便宜的应用。

最高安全风险

本文中确定的最重要的云风险类别为：

治理缺失：部分控制权转移给云提供者。 他们的 SLA 可能也不会提供相关的承诺，从而在安全防范方面留下空白。

厂商琐定：云提供者支持的接口太少，不能保证数据、应用程序和服务的可移植性。这阻碍了客户向其云提供者的迁移。

隔离失败：不同租户之间的存储、内存、路由甚至信誉分离机制的失败（例如所谓的虚机跳跃攻击）。但是针对资源隔离机制（例如，针对虚拟化管理程序）的攻击仍然较少，因为很难实施攻击。

隔离失败：不同租户之间的存储、内存、路由甚至信誉分离机制的失败（例如所谓的虚机跳跃攻击）。 但是针对资源隔离机制（例如，针对虚拟化管理程序）的攻击仍然较少，攻击者难以付诸实施。

合规风险：迁移到云可能会给云消费者获得合规或监管认证带来风险：

- 云提供者可能不能提供相关的合规证据
- 云提供者可能不允许云消费者（CC）审计。

公有云基础设施可能无法实现某些类型的合规性（例如，PCI DSS（4））。

管理平面缺陷：公有云提供者的客户管理平面可通过互联网访问，并具有对大量资源访问权限，因此会增加风险。

数据保护：云消费者（作为数据控制者）可能难以有效检查云提供者的数据处理实践，从而确保数据以合法的方式处理。

不安全或不完整的数据删除：删除云资源的操作可能不会导致真正的数据删除。在多租户和硬件资源重用的情况下，对客户来说具有比专用硬件更高的风险。

恶意的内部人员：恶意内部人员可能会造成非常大的损害。云架构需要特别注意云提供者系统管理员等高风险角色。

注意：你可以外包职责（谁来做），但你不能外包责任（问责）

目录

目标受众

本报告的目标受众是：

- 中小企业负责人;
- 欧洲决策者;
- 个人。

云计算按需服务模式，通常基于虚拟化和分布式计算技术。云计算架构有：

- **高度抽象的资源**
- **近乎实时的可扩展性和灵活性**
- **即时的配置**
- **共享资源（硬件，数据库，内存等）**
- **'按需服务'，通常采用'按需付费'记账系统**
- **程序化管理（例如通过WS API）。**

云计算 - 工作定义

本研究对云计算的定义:云计算是按需服务模式，通常基于虚拟化和分布式计算技术。云计算架构具备以下特征：

- 高度抽象的资源
- 实时的可扩展性和灵活性
- 即时配置
- 共享资源（硬件、数据库、内存等）
- '按需服务'，通常采用'按需付费'记账系统
- 程序化管理（例如通过 WS API）。

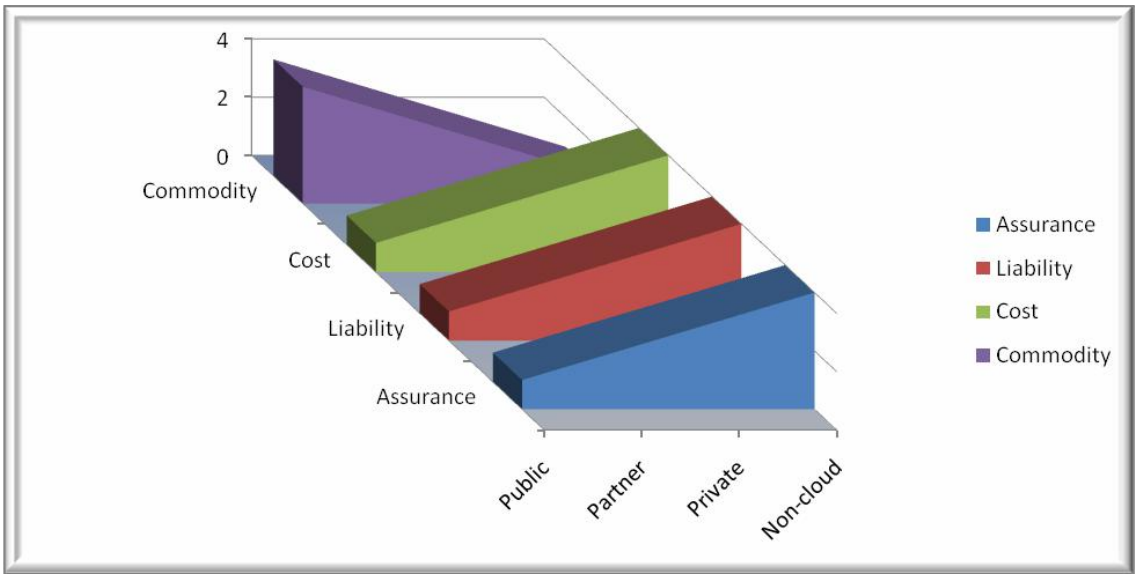
云类型：

- 软件即服务（SaaS）
- 平台即服务（PaaS）
- 基础设施即服务（IaaS）

云也可以分为：

- 公有云：公开可用 - 任何组织都可以订阅
- 私有云：根据云计算特征构建的服务，但只能在专用网络内访问
- 合作伙伴云：提供者向有限且明确定义的各方提供的云服务。

一般而言，云的商品、成本、责任和保障因下图而异



1.云计算的安全收益

简而言之，当大规模实施各种安全措施时会更便宜。 因此，相同数量的安全投入能获得更好的保护。

安全和规模效益

简而言之，当大规模实施时，各种安全措施更便宜。 因此，相同数量的安全投入获得更好的保护。 这包括各种防御措施，如过滤，补丁管理，虚拟机实例和管理程序的加固，人力资源及其管理和审查，硬件和软件冗余，强大的身份验证，基于角色的高效访问控制和联合身份管理解决方案这也改善了参与业务的各合作伙伴之间的协作网络效应。

规模化的其他好处包括：

- 多个地点：多地点、多副本，提升容灾能力。
- 边缘网络：提升服务可靠性和质量，减少局部网络问题的影响范围。
- 提高响应的及时性：更有效和高效的事件响应能力。
- 威胁管理：小公司雇不起处理特定威胁的专家。

安全导致市场差异化

安全性是许多云消费者的首要考虑因素，客户将根据保密声誉作出购买选择。

标准化的安全管理接口

大型云提供者的安全服务通常提供标准化的开放接口，为所有客户提供服务。

根据需求动态调整防御性资源的能力对恢复力具有明显的优势。 此外，更多种类的个人资源可以以细粒度的方式进行缩放，而无需扩展所有系统资源，对突发性的业务（非恶意）峰值做出响应的成本更低。

快速智能的资源伸缩

动态资源分配使安全防御措施（例如针对 DDoS 攻击）具有明显的弹性优势。动态分配资源的能力对恢复力也具有明显的优势。 此外，资源可以细粒度的方式进行缩放，而无需扩展所有系统资源，对突发的业务峰值（非恶意）做出响应的成本更低。

审计和取证

IaaS 产品支持按需克隆虚拟机。客户可以快照实时虚拟机的镜像减少分析的停机时间。 使用 TAP 存储，可以创建多个克隆并将分析活动并行化以减少取证时间。还可以为日志提供更具成本效益的存储，使审计存储成本会变得透明。这使识别安全事件的过程更加高效。

更及时发布更新和有效的默认安全配置

与传统的基于客户端的系统相比，云平台可以更快速地发布更新，而传统的基于客户端的系统依赖于修补模型。

对虚拟机镜像和软件模块预先加固，包括更新最新的补丁以及进行安全设置;同时定期对虚

拟基础设施进行快照，并与基线进行比较。 与传统的基于客户端的系统相比，跨平台的平台可以更快速地发布更新，而传统的基于客户端的系统依赖于修补模型。

审计和SLAS促使更好的风险管理

需要量化 SLA 中各种风险场景的处罚以及安全漏洞对声誉的可能影响，激发更为严格的内部审计和风险评估程序。

资源集中的好处

资源的集中会带来安全风险，但它具有更便宜的物理资产限制和物理访问控制（每单位资源）的明显优势，以及对安全策略和控制的更简单便宜的应用。

2. 风险评估

使用场景

为了进行这种云计算风险评估，我们分析了三种使用情况：

- 中小企业对云计算的看法
- 云计算对服务弹性的影响
- 云计算和电子政务（eHealth）

风险评估过程

以下显示了风险级别作为业务影响和事件可能性情况的函数。 所产生的风险按照 0 到 8 的等级进行衡量，可以根据风险接受标准进行评估。 这个风险等级也可以映射到一个简单的总体风险等级：

- 低风险：0-2
- 中等风险：3-5
- 高风险：6-8

	事件的可能性	非常低（非常不可能）	低（不太可能）	中等（可能）	高（可能）	非常高（频繁）
业务影响	非常低	0	1	2	3	4
	低	1	2	3	4	5
	中	2	3	4	5	6
	高	3	4	5	6	7
	很高	4	5	6	7	8

3.风险

风险应该始终与整体商业机会和风险偏好相关 – 有时风险被机会补偿。

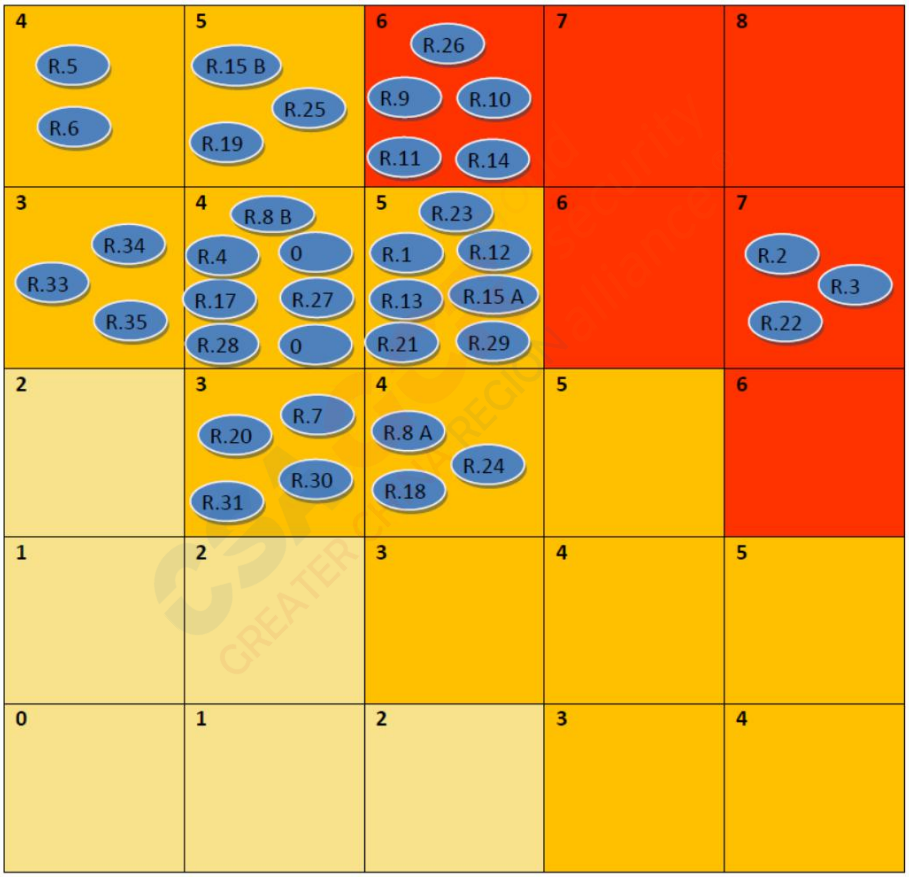
风险描述应注意的点：

- 风险应该始终与整体商业机会和风险偏好相关 - 有时风险被机会补偿。
- 在许多情况下，风险级别会随着所考虑的云架构的类型而显着变化。
- 云消费者有可能将风险转移给云提供者但并非所有风险都可以转移。

因此，使用云计算的风险应与传统解决方案（如基于桌面的模型）的风险相比较。

下图表示了风险概率和影响的分布：

可能性



影响

图 2：风险分布

评估中确定的风险分为三类：

- 政策和组织
- 技术
- 法律。

表中列出了每项风险，其中包括：

- 概率水平
- 影响程度
- 参考漏洞
- 参考受影响的资产
- 风险水平。

但是，并非所有风险都可以转移：如果风险导致业务失败，造成 严重的声誉损害或法律影响，则任何其他方都很难或不可能补偿此损害。

此外我们增加了一个比较概率和影响单元，以比较标准云计算风险和标准 IT 风险。 我们没有列入比较风险，因为它假设选择的所有风险都较高。

政策和组织风险

R.1 锁定

可能性	高	比较：较高
影响	中	比较：相等
漏洞	V13.缺乏标准技术和解决方案 V46.提供者选择不佳 V47.缺乏提供者冗余 V31.在使用方面缺乏完整性和透明度	
受影响的资产	A1.公司声誉 A5.个人敏感数据 A6.个人资料 A7.个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10.服务交付	
风险	**高**	

如果云提供者的接口的方式很少，很难保证数据和服务的可移植性（尽管有些举措确实存在，例如见（58））。 这使得客户很难从一个提供者迁移到另一个提供者，或者将数据和服务迁移到内部 IT 环境或从内部迁移。 此外，云提供者可能有动机来防止（直接或间接）客户服务和数据的可移植性。

不同类型的云琐定的范围和性质也不同：

SaaS 锁定

- 客户数据通常存储在由 SaaS 提供者设计的自定义数据库模式中。 大多数 SaaS 提供者提供 API 调用以读取（或“导出”）数据记录。 但是，如果提供者不提供现成的数据“导

出”例程，则客户需要开发一个程序来提取他们的数据并将其写入文件以准备导入另一个提供者。

- 应用程序锁定是最明显的锁定形式。SaaS 提供者通常会根据需求开发定制化的应用程序。迁移到另一家 SaaS 提供者时，拥有大量用户的 SaaS 客户可能会承担非常高的转换成本。

PaaS 锁定

PaaS 锁定发生在 API 层（即平台特定的 API 调用）和组件级别。 例如，PaaS 提供者可能会提供高效的后端数据存储。 客户不仅必须使用提供者提供的自定义 API 开发代码，还必须以与后端数据存储兼容的方式对数据访问例程进行编码。

即使提供了看起来兼容的 API，因为数据访问模型可能不同（例如关系型哈希）这些代码未必可以跨 PaaS 提供者移植。

- 因为不同的提供者提供不同的 API，所以在 API 层发生 PaaS 锁定。
- PaaS 锁定发生在运行时层上，因为“标准”运行时为了在云环境中安全运行而做了大量定制。
- PaaS 也受到数据锁定的影响，但是开发能兼容的导出程序完全是客户的责任。

在使用云基础设施时，客户端必须放弃对一部分安全性相关问题的控制权。 例如，提供者可能会禁止端口扫描，漏洞评估和渗透测试。 此外，客户加固程序与云环境之间可能存在冲突。 另一方面，提供者的 SLA 可能不会承诺提供此类服务。

此外，云提供者可以将服务外包或分包给第三方，第三方可能不提供云提供者发布的相同担保（例如以合法方式提供服务）。或者云提供者的控制权发生变化，所以其服务的条款和条件也可能发生变化。

IaaS 的锁式

IaaS 锁定取决于所使用的特定基础设施服务。 例如，使用云存储的客户将不会受不兼容的虚拟机格式影响。

- IaaS 通常提供基于虚拟机管理程序的虚拟机。软件和 VM 元数据捆绑在一起以实现可移植性 - 通常只在提供者的云中提供。
- IaaS 存储产品从简单的基于键/值的数据存储到基于策略的增强型文件存储都有所不同。功能集可能会有很大差异，存储语义也是如此。然而，应用程序级别对特定策略功能（例如访问控制）的依赖可能会限制客户对提供者的选择。
- 数据锁定是 IaaS 存储服务非常关心的问题。 随着云用户将更多数据推送到云存储，数据锁定增加，除非云提供者提供数据可移植性。

R.2 治理缺失

可能性	很高	比较：较高
影响	非常高（取决于组织） （IaaS非常高，SaaS低）	比较：相等
漏洞	V34. 不明确的角色和责任 V35. 角色定义执行不力 V21. 同步云外部的责任或合同义务 V23. SLA条款对不同利益相关者的承诺有冲突 V25. 客户无法获得审核或认证 V22. 跨云应用程序创建隐藏的依赖关系 V13. 缺乏标准技术和解决方案 V29. 存储在多个司法管辖区的数据，并且缺乏对此的透明度 V14. 无来源托管协议 V16. 无法控制漏洞评估过程 V26. 认证方案不适应云基础设施 V30. 缺乏有关管辖权的信息 V31. 在使用方面缺乏完整性和透明度 V44. 不明确的资产所有权	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付	
风险	高	

使用云基础设施时，客户端必须放弃对可能影响安全性的若干问题的控制权。 例如，可能会禁止端口扫描，漏洞评估和渗透测试。 而且，客户加固程序与云环境之间可能存在冲突（见R 20）。 另一方面，SLA 可能不会承诺提供云服务商提供的此类服务，从而在安全防范方面留下空白。

迁移到云中的某些组织为获得竞争优势或满足行业标准或法规要求（例如 PCI DSS）已做出相当大的投资。

此外，云提供者可能会将服务外包或分包给第三方（未知提供者），这些提供者可能不提供云提供者发布的相同担保（例如以合法方式提供服务）。 或者云提供者的控制权发生变化，所以其服务的条款和条件也可能发生变化。

治理和控制权的丧失可能会对组织的战略产生潜在的严重影响，从而影响到实现其使命和目标的能力。 可能导致不能遵守安全要求，缺乏机密性、数据的完整性和可用性，以及服务性

能和服务质量的下降，更不用说引入合规性的挑战了（参见 R.3).

R.3 合规挑战

可能性	非常高 - 取决于PCI，SOX	比较：较高
影响	高	比较：相等
漏洞	V25. 审核或认证不适用于客户 V13. 缺乏标准的技术和解决方案， V29. 存储多个司法管辖区的数据，并且缺乏对此的透明度 V26. 认证方案不适应云基础设施 V30. 缺乏有关管辖权的信息 V31. 在使用方面缺乏完整性和透明度	
受影响的资产	A20. 证明	
风险	高	

迁移到云中的某些组织为获得竞争优势或满足行业标准或法规要求（例如 PCI DSS）已做出相当大的投资。 这种投资可能会因向云迁移而面临风险：

- 如果云提供者不能提供符合相关要求的证据;
- 如果云提供者不允许云消费者进行审计。

资源共享意味着一个租户进行的恶意活动可能会影响另一个租户的声誉。

使用公有云基础设施可能无法实现某些类型的合规性，因此云托管服务无法使用。 例如，EC2 表示客户将很难在其平台上实现 PCI 合规性。 所以 EC2 托管服务不能用于处理信用卡交易。

R.4 由于共同承担的活动造成的业务声誉损失

可能性	低
影响	高
漏洞	V6. 缺乏资源隔离 V7. 缺乏声誉隔离 V5. 高级管理人员的脆弱性
受影响的资产	A1. 公司声誉 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付
风险	**中**

资源共享意味着一个租户进行的恶意活动可能会影响另一个租户的声誉。例如，垃圾邮件，端口扫描或从云基础设施提供恶意内容可能导致：

- 一系列 IP 地址被封锁，包括攻击者和其他无辜基础设施的租户;
- 由于邻近租户的活动而被没收资源（邻居传唤）。

这种影响可能是服务提供和数据丢失的恶化，以及组织声誉方面的问题。

R.5 云服务终止或失效

可能性	N/A	
影响	很高	比较：较高
漏洞	V46. 不良提供者选择 V47. 缺乏提供者冗余 V31. 在使用方面缺乏完整性和透明度	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A9. 服务交付 - 实时服务 A10. 服务交付	
风险	**中**	

一些提供者可能因为种种原因终止一些云计算服务。这可能导致服务交付性能和服务质量的损失或恶化，以及财务损失。此外，提供者的服务失效可能会对云消费者对自己客户的履约能力产生重大影响。

R.6 云服务商并购

可能性	N/A	
影响	中	比较：较高
漏洞	V31. 在使用方面缺乏完整性和透明度	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键 A8. 人力资源数据 A9. 服务交付 - 实时服务	

	A10. 服务交付
风险	**中**

云提供者并购可能会增加战略转变的可能性，并可能使协议面临不具约束力的风险（例如，软件界面，安全投资，非合同安全控制）。 这可能导致无法遵守安全要求。 最终的影响可能会对关键资产造成破坏，例如：组织的声誉，客户信任以及员工的忠诚度和经验。

R.7 供应链故障

可能性	低	
影响	很高	比较：较高
漏洞	V31. 在使用方面缺乏完整性和透明度 V22. 跨云应用程序创建隐藏的依赖关系 V46. 提供者选择不佳 V47. 缺乏提供者冗余	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付	
风险	**中**	

云计算提供者可以将某些任务外包给第三方。 在这种情况下，云提供者的安全级别可能取决于云提供者对第三方的依赖级别。

一个典型的例子是对第三方单点登录或身份管理服务存在严重依赖性的情况。

一般来说，合同缺乏透明度可能成为整个系统的问题。缺乏透明度可能会降低客户对提供者的信任程度。

在这种情况下，云提供者的安全级别可能取决于每个链路的安全级别以及云提供者对第三方的依赖级别。

技术风险

R.8 资源耗尽（用尽或超卖）

可能性	**A**.无法为客户提供额外的能力：中	比较：N / A
	B.无法提供当前商定的能力水平：低	比较：较高
影响	**A**.无法为客户提供额外的能力： 低/中（例如，在圣诞节）	比较：N / A
	B.无法提供当前商定的能力水平：高	比较：一样
漏洞	V15. 资源使用的不精确建模 V27. 资源配置不足和基础设施投资不足 V28. 没有资源限制政策 V47. 缺乏提供者冗余	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A10. 服务交付 A11. 访问控制/认证/授权（root / admin v其他）	
风险	**中**	

云计算按需提供服务。 因此，在分配云资源时存在一定程度的计算风险，因为资源是根据统计预测分配的。 不正确的资源使用建模 ，资源配置不足，基础设施投资不足可能导致以下问题：

因此，在分配云服务的所有资源时存在一定程度的计算风险，因为资源是根据统计预测分配的。

从云提供者角度来看：

- 服务不可用性；
- 访问控制受到损害：资源耗尽的情况下可能导致“失效开放”（即故障时默认开放访问权限）；
- 经济和声誉损失：
- 基础设施超卖：资源超卖导致经济损失和利润损失。

从云消费者的角度来看，选择一个糟糕的提供者和缺乏提供者冗余可能导致：

- 服务不可用;
- 访问控制系统受到威胁：将数据的机密性和完整性置于危险之中;
- 经济和声誉损失：由于未能满足客户需求，违反 SLA，级联服务失败等。

R.9 隔离失败

可能性	低（私有云） 中（公有云）	比较：较高
影响	很高	比较：较高
漏洞	V5. 管理程序漏洞 V6. 缺乏资源隔离 V7. 缺乏声誉隔离 V17. 内部（云）网络探测将发生的可能性 V18. 可能会进行共用场所检查	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付	
风险	高	

多租户和共享资源是云的两个明确特征（注意：这不是 NIST 定义的云计算基本特征，考试的时候要注意区分）。 计算容量，存储和网络等资源均由多个租户共享。这类风险包括不同租户之间分隔存储机制的失败，内存，路由甚至信誉的失败（例如，所谓的虚机跳跃攻击）。请注意，这取决于所考虑的云模型; 私有云的可能很较低，公有云中较高。

这类风险包括共享基础设施的不同租户之间分离存储、内存、路由甚至声誉的机制失败(例如所谓的虚机跳跃攻击、SQL 注入攻击，暴露存储在同一表中的多个客户数据的攻击，以及侧信道攻击)。

R.10 云提供者恶意内部人员 - 滥用高级权限角色

可能性	中等（低于传统）	比较：较低
影响	非常高（高于传统）	比较：较高（总计） 比较：相同（对于单个客户）

漏洞	V34. 不明确的角色和责任 V35. 角色定义的执行不力 V36. 不需要知道的原则 V1. AAA漏洞 V39. 系统或操作系统漏洞 V37. 物理安全程序不完善 V10. 不可能以加密的形式处理数据 V48. 应用程序漏洞或较差的补丁管理
受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键 A8. HR数据 A9. 服务交付 - 实时服务 A10. 服务交付
风险	**高**

内部人员的恶意活动可能会对以下方面产生影响：所有类型的数据，知识产权，各种服务的机密性、完整性和可用性，因此间接影响组织的声誉，客户信任度和员工的体验。 在云计算环境这是特别重要的，因为云架构需要某些极其高风险的角色，例如云提供者系统管理员和审计员。 随着云使用的增加，云提供者的关键员工越来越成为犯罪团伙的目标。

R.11 管理平面缺陷（操作、基础设施的可用性）

可能性	中	比较：较高
影响	很高	比较：较高
漏洞	V1. AAA漏洞 V4. 远程访问管理平面 V38. 配置错误 V39. 系统或操作系统漏洞 V48. 应用程序漏洞或较差的补丁管理	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付 A14. 云服务管理平面	
风险	**中**	

公有云提供者的客户管理平面可通过互联网访问，并允许对较多资源的访问，因此会增加风险，特别是与远程访问和网页浏览器漏洞相结合时。 这包括控制多个虚拟机的客户界面，最重要的是控制整个云系统运行的云提供者界面。

公有云提供者的客户管理平面可通过互联网访问，并允许对较大资源集合（比传统托管提供者）的访问，因此会增加风险，特别是与远程访问和 Web 浏览器漏洞相结合时。

R.12 拦截传输中的数据

可能性	中	比较：较高（对于给定数据）
碰撞	高	比较：一样
漏洞	V1. AAA漏洞 V8. 通信加密漏洞 V9. 传输中的档案和数据缺乏或弱加密 V17. 内部（云）网络探测将发生的可能性 V18. 可能会进行共用场所检查 V31. 在使用方面缺乏完整性和透明度	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键 A8. HR数据 A23. 备份或归档数据	
风险	**中**	

云计算作为一种分布式架构有比传统基础设施更多的数据在传输中。 例如为了同步分布在多个物理机器之间镜像，必须传输数据。此外，有的云数据中心之间的数据传输可能没有使用VPN。

嗅探、欺骗、中间人攻击、侧信道攻击和重放攻击应被视为可能的威胁源。

此外客户的秘密信息也可能会在云中传输。

R.13 上传下载时云内的数据泄露

可能性	中等（不适用）
影响	高

漏洞	V1. AAA漏洞 V8. 通信加密漏洞 V17. 内部（云）网络探测将发生的可能性 V18. 共用场所检查可能会执行 V10. 不可能以加密形式处理数据 V48. 应用程序漏洞或较差的补丁管理
受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键 A8. HR数据 A12. 证书 A13. 用户目录（数据） A14. 云服务管理平面
风险	**中**

这与之前的风险相同，但适用于云提供者和云消费者之间的数据传输。

R.14 数据的缺失或无效删除

可能性	中	比较：较高
影响	很高	比较：较高
漏洞	V20.敏感的介质	
受影响的资产	A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键 A12. 证书	
风险	**中**	

云中的数据可能超过安全策略中指定的生命周期。 可能不能执行安全策略指定的过程，因为只有通过销毁存储数据的磁盘才能完全删除数据。 云资源删除操作可能不会导致真正的数据擦除。 如果需要真正的数据擦除，必须执行特殊程序。

其次，这可能不被标准 API 支持（或根本不支持）。

如果使用有效加密，那么风险级别会较低。

有几种不同的情况，云消费者的资源可能会被其他方以恶意方式使用，从而产生经济损失。

R.15 分布式拒绝服务（DDOS）

可能性	客户：中	比较：较低
	提供者：低	比较：N / A
影响	客户：高	比较：较高
	提供者：非常高	比较：较低
漏洞	V38. 配置错误 V39. 系统或操作系统漏洞 V53. 过滤资源不足或配置错误	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A9. 服务交付 - 实时服务 A10. 服务交付 A14. 云服务管理平面 A16. 网络（连接等）	
风险	**中**	

R.16 经济拒绝服务（EDOS）

可能性	低
影响	高
漏洞	V1. AAA漏洞 V2. 用户配置漏洞 V3. 用户解除配置漏洞 V4. 远程访问管理平面 V28. 没有资源限制政策
受影响的资产	A1. 公司声誉 A2. 客户的信任 A9. 服务交付 - 实时服务 A10. 服务交付
风险	**中**

云消费者的资源可能以恶意方式被其他方使用，并且具有经济影响：

- 身份盗用：攻击者使用客户的账号和资源以谋取私利或为了经济损害客户。
- 云消费者没有对付费资源的使用设置有效限制。
- 攻击者使用公共信道来占用客户的计量资源，例如 DDos。

R.17 加密密钥的丢失

可能性	低	比较：N / A
影响	高	比较：较高
漏洞	V11. 糟糕的密钥管理程序 V12. 密钥生成：用于随机数生成的低熵	
受影响的资产	A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键 A8. HR数据 A12. 证书	
风险	**中**	

这包括向恶意方泄露密钥（SSL、文件加密、客户私钥等）或密码。这些密钥的丢失或损坏，可能被用作未经授权的身份验证，破坏抗抵赖能力（抗抵赖通过数字签名实现，依赖私钥的保密性）。

R.18 进行恶意探测或扫描

可能性	中	比较：较低
影响	中	比较：较低
漏洞	V17. 内部（云）网络探测将发生的可能性 V18. 可能会进行共同住所检查	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A9. 服务交付 - 实时服务 A10. 服务交付	
风险	**中**	

恶意探测或扫描以及网络映射是对资产的间接威胁。它们可以用于在攻击者收集信息。可能会影响服务和数据的机密性、完整性和可用性。

R.19 服务引擎损坏

可能性	低
影响	很高

漏洞	V5.管理漏洞程序 V6 缺乏资源隔离
受影响的资产	A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键A8. HR数据 A9. 服务交付 - 实时服务 A10. 服务交付
风险	**中**

每个云架构都依赖于高度专业化的平台，该平台位于物理硬件资源之上，并在不同的抽象级别管理客户资源。 例如，在 IaaS 云中，这个软件组件可以是虚拟化管理程序。 在某些情况下，服务引擎由云平台提供者和开源社区开发和支持。 它可以由云计算提供者进一步定制。

云提供者必须明确规定客户必须采取的最低限度行动的职责分工。

像任何其他软件层一样，服务引擎代码可能存在漏洞，容易受到攻击或意外故障。 攻击者可以通过从虚拟机（IaaS 云），运行时环境（PaaS 云），应用程序池（SaaS 云）或通过其 API 遭受黑客攻击。

对服务引擎进行黑客攻击可能有助于避免不同客户环境之间的隔离（越狱）并获得对其中包含的数据的访问权限，以透明的方式监控和修改其内部的信息，或减少分配给他们的资源，导致拒绝服务。

R.20 客户加固程序与云环境之间的冲突

可能性	低
影响	中
漏洞	V31. 在使用方面缺乏完整性和透明度 V23. SLA条款与不同利益相关者的承诺相冲突 V34. 不明确的角色和责任
受影响的资产	A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键
风险	**中**

云提供者必须明确规定客户必须采取的最低限度行动的职责分工。

提供者应进一步明确其隔离机制并提供最佳实践指南，以协助客户保护其资源。

客户必须意识到并承担自己的责任，因为如果不这样做，他们的数据和资源将面临更大的风险。

客户必须意识到并承担自己的责任。云消费者可能会不恰当地认为云提供者负责并正在确保其数据安全。云消费者必须

明确他们的责任并遵守它们。

云提供者本质上负责提供多租户环境，因此不同安全需求的客户之间可能会产生冲突，并且这种冲突会随着租户的数量和需求差距的增加而恶化。云提供者必须能够通过技术、政策和透明度来应对这些挑战。

法律风险

R.21 传唤和电子取证

可能性	高
影响	中
漏洞	V6. 缺乏资源隔离 V29.在多个司法管辖区存储数据，并且缺乏对此的透明度 V30.缺乏有关管辖权的信息
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付
风险	高

如果由于执法机构或民事诉讼的传票而没收了实体硬件（15），物理硬件的共享意味着更多的客户有可能披露他们的数据给不需要的各方（16），（17），（18）。

R.22 管辖权变更的风险

可能性	很高
影响	高
漏洞	V30. 缺乏有关管辖权的信息 V29. 在多个司法管辖区存储数据，并且缺乏对此的透明度

受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付
风险	高

客户数据可能在多个司法管辖区保存，其中一些可能具有很高的风险。如果数据中心位于高风险国家，数据可能会被地方当局强制搜查、披露或扣押。合法的硬件扣押可能会影响执法目标以外的很多客户，这取决于数据的存储方式(19)、(20)。

R.23 数据保护风险

可能性	高
影响	高
漏洞	V30. 缺乏有关管辖权的信息 V29. 在多个司法管辖区存储数据，并且缺乏对此的透明度
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付
风险	高

云计算为云消费者和提供者带来了一些数据保护风险。

- 云消费者(作为数据控制器的角色)很难有效地检查云提供者进行的数据处理，从而确保数据是以合法的方式处理的。一些云提供者确实提供了他们的数据处理的信息。一些国家还提供了关于数据处理和数据控制的认证，例如 SAS 70。
- 可能存在数据安全漏洞，但云提供者未及时通知客户（数据控制器）。
- 云消费者可能会失去对云提供者处理的数据的控制权。
- 云提供者可能会收到其客户（数据控制器）非法收集的数据。

R.24 许可风险

可能性	中	比较：较高
影响	中	比较：较高
漏洞	V31. 在使用方面缺乏完整性和透明度	
受影响的资产	A1. 公司声誉 A9. 服务提供 - 实时服务 A20. 证明	
风险	中	

许可条件（如按用户授权协议）和在线许可检查在云环境中可能无法使用。与所有知识产权一样，如果没有受到适当合同条款的保护，云上的原创作品可能面临风险。

不是云中特有的风险

我们确定了以下不是云计算环境特有的威胁，在评估云系统的风险时应予以仔细考虑。

R.25 网络中断

可能性	低	比较：一样
影响	很高	比较：较高
漏洞	V38. 配置错误 V39. 系统或操作系统漏洞V6. 缺乏资源隔离 V41. 业务连续性和灾难恢复计划缺乏或未经过检验	
受影响的资产	A9. 服务交付 - 实时服务 A10. 服务交付	
风险	**中**	

最高的风险之一！ 可能使成千上万的客户同时受到影响。

R.26 网络管理（网络拥塞/ 连接中断/未优化的网络）

可能性	中	比较：一样
影响	很高	比较：较高
漏洞	V38. 配置错误 V39. 系统或操作系统漏 洞V6. 缺乏资源隔离 V41. 业务连续性和灾难恢复计划缺乏或缺乏经验	

受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A9. 服务交付 - 实时服务 A10. 服务交付 A16网络（连接等）
风险	高

R.27 篡改网络流量

可能性	低
影响	高
漏洞	V2. 用户配置漏洞 V3. 用户解除配置漏洞 V8. 通信加密漏洞 V16. 无法控制漏洞评估过程
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A9. 服务交付 - 实时服务 A10. 服务交付
风险	中

R.28 特权升级

可能性	低	比较：较低
影响	高	比较：较高（对于云提供者）
漏洞	V1. AAA漏洞 V2. 用户配置漏洞 V3. 用户解除安置漏洞 V5. 管理程序漏洞 V34. 不明确的角色和责任 V35. 角色定义的执行不力 V36. 需要了解的原则不适用 V38. 配置错误	
受影响的资产	A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键A8. HR数据 A11. 访问控制/认证/授权（root / admin v其他） A13. 用户目录（数据）	
风险	中	

R.29 社会工程攻击(假冒)

可能性	中	比较：一样
影响	高	比较：较高
漏洞	V32. 缺乏安全意识 V2. 用户配置漏洞 V6. 缺乏资源隔离 V8. 通信加密漏洞 V37. 物理安全程序不完善	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A3. 员工忠诚度和经验 A4. 知识产权 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 关键A8. HR数据 A11. 访问控制/认证/授权（root / admin v其他） A12. 证书	
风险	中	

R.30 操作日志的丢失或损坏

可能性	低	比较：较低
影响	中	比较：相同（对于客户）
漏洞	V52. 缺乏对日志收集和保留的策略或不当程序 V1. AAA漏洞 V2. 用户配置漏洞 V3. 用户解除安置漏洞 V19. 缺乏取证准备 V39. 系统或操作系统漏洞	
受影响的资产	A21. 操作日志（客户和云提供者）	
风险	中	

R.31 安全日志的丢失或损坏（取证调查的操作）

可能性	低	比较：较低
影响	中	比较：相同（对于客户）
漏洞	V52. 缺乏对日志收集和保留的策略或不当程序 V1. AAA漏洞 V2. 用户配置漏洞 V3. 用户解除安置漏洞 V19. 缺乏取证准备 V39. 系统或操作系统漏洞	
受影响的资产	A22. 安全日志	
风险	中	

R.32 备份丢失、被盗

可能性	低	比较：较低
影响	高	比较：相同（对于客户）
漏洞	V37. 物理安全程序不完善 V1. AAA漏洞 V2. 用户配置漏洞 V3. 用户解除配置漏洞	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A8. HR数据 A9. 服务交付 - 实时服务 A10. 服务交付 A23. 备份或归档数据	
风险	中	

R.33 未经授权进入场所（包括对机器和其他设施的物理访问）

可能性	非常低	比较：较低
碰撞	高（要有非常高的影响，它应该是目标攻击（指向特定的机器等），否则影响应该很大。	比较：较高
漏洞	V37. 物理安全程序不完善	

受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A8. HR数据 A23. 备份或归档数据
风险	中

由于云提供者将资源集中在大型数据中心，虽然物理边界控制可能更强大，但违反这些控制措施的影响也更大。

R.34 计算机设备失窃

可能性	非常低	比较：较低
影响	高	比较：较高
漏洞	V37. 物理安全程序不完善	
受影响的资产	A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A8. HR数据 A17. 物理硬件	
风险	中	

R.35 自然灾害

可能性	非常低	比较：较低
碰撞	高	比较：较高
漏洞	V41. 业务连续性和灾难恢复计划缺失或未经测试恢复计划	
受影响的资产	A1. 公司声誉 A2. 客户的信任 A5. 个人敏感数据 A6. 个人资料 A7. 个人数据 - 至关重要 A8. HR数据 A9. 服务交付 - 实时服务 A10. 服务交付 A23. 备份或归档数据	
风险	中	

一般来说，与传统基础设施相比，云在面临自然灾害时风险较低，因为云提供者默认提供多个冗余站点和网络路径。

4.脆弱性

以下漏洞列表不能包括所有脆弱性，但足够我们分析使用。它包含云特有的和一般信息安全漏洞。

V.1 AAA 脆弱性

- 认证，授权和记账系统漏洞可能会导致未经授权的访问，特权升级，无法追踪资源滥用和一般安全事件等，方法如下：
- 客户对云访问凭证的不安全存储：
- 角色不足;
- 存储在临时机器上的凭证。

此外，由于企业应用程序暴露在互联网上，因此云计算使用基于密码的身份验证将不能满足安全需求，需要更强或双重身份验证来访问云资源。

V.2 用户供应（开通）漏洞

- 客户无法控制供应（开通）过程。
- 客户身份在注册时未得到充分验证。
- 云系统组件（时间和配置文件内容）之间的同步延迟。
- 制作多个未同步的身份数据副本。
- 凭证很容易被拦截和重放。

V.3 用户撤消供应（注销）漏洞

用户注销以后凭证可能仍然有效。

V.4 远程访问管理平面

客户端系统和浏览器的漏洞可能会对管理平面产生威胁。

V.5 高级管理员的脆弱性

虚拟机管理程序对攻击者非常有吸引力。控制了虚拟化管理程序就意味着可以控制每一个虚机。

通过利用虚拟机管理程序漏洞实现的典型场景是所谓的“虚机逃逸”，其中一个例子是“云爆发”。 另一种情况是“虚拟机跳跃”：攻击者先控制一台虚拟机，然后利用虚拟机管理程序漏洞进一步控制在同一宿主机上的其他虚拟机。

V.6 缺乏资源隔离

一个客户的资源使用可能会影响另一个客户的资源使用。

IaaS 云计算基础设施主要依赖于多个虚拟机共享物理资源。虚拟化管理程序的漏洞可能导致未经授权访问这些共享资源。

IaaS 云中使用的虚拟机管理程序提供了丰富的 API，云提供者使用这些 API 来开发向客户公开的专有管理，供应和报告界面。 管理程序安全漏洞可能导致未经授权访问客户信息。 与此同时，此级别的漏洞可能允许攻击者操纵云设施内的资产，引发拒绝服务（例如，关闭正在运行的虚拟机），数据泄露，镜像模板篡改，数据损坏或直接经济损失（例如复制和启动许多虚拟机副本）。

最后，缺乏强制执行服务条款（ToS）或更具体的服务级别协议（SLA）的工具（如服务质量（QoS）或分布式资源调度（DRS）产品）可能允许某一个客户独占云设施，从而影响其他客户的可用性和性能。

V.7 缺乏声誉影响隔离

一个客户的活动会影响另一个客户的声誉。

V.8 通信加密的脆弱性

这些漏洞涉及通过中间人攻击读取传输数据的可能性，如弱认证、自签名证书等。

V.9 文档和数据在传输中缺乏加密或使用弱加密

未加密的传输中的数据，保存在档案和数据库中的数据，未装载的虚拟机映像，取证镜像和数据，敏感日志以及其他静态数据都可能处于危险中。

使用加密技术会极大地影响效率。 这意味着，在未来很长一段时间内，云消费者必须信任云提供者。

V.10 以加密格式处理数据的不可能性

尽管加密静态数据并不困难（比如使用同态加密技术），但商业系统都无法做到在加密的状态下处理数据。这意味着云消费者必须信任云提供者。

V.11 糟糕的密钥管理流程

云计算基础设施需要管理和存储许多不同类型的密钥; 例如包括会话密钥、文件加密密钥、识别云提供者的密钥对、识别客户的密钥对，授权令牌和撤销证书（29）。 由于虚拟机没有固定的硬件基础设施，而且基于云的内容往往分布在不同的地理位置上，因此将硬件安全模块（HSM）存储密钥应用于云环境变得更困难。 例如：

- HSM 必须受到严格的物理保护（防盗，窃听和篡改）。 这使得它们很难在分布式的云体系结构中使用（即地理分布和高度复制）。
- 由于用户和云密钥存储之间的通信通道以及所使用的远程认证机制的安全性降低，通过互联网访问的密钥管理接口也更容易受到攻击。
- 需要验证自身的新虚拟机必须以某种机密的形式实例化。 这些机密的分布可能会带来

可扩展性问题。

- 撤销分布式架构中的密钥成本也很昂贵。

V.12 密钥生成：随机数生成的低熵

标准系统映像，虚拟化技术和缺乏输入设备的组合意味着系统比物理随机数生成器具有更低的熵;也就是说一个虚拟机上的攻击者可能能够猜测其他虚拟机上生成的加密密钥，因为用于生成随机数的熵源可能相似。

V.13 缺乏标准技术和解决方案

缺乏标准意味着数据可能会被提供者“锁定”。 如果提供者停止运营，这是一个很大的风险。

V.14 无来源的托管协议

缺乏资源托管意味着如果 PaaS 或 SaaS 提供者破产，其客户将不受保护。

V.15 资源使用的不精确建模

云服务特别容易受到攻击导致资源耗尽，因为它们是按统计数据提供的。 虽然许多提供者允许客户预先预留资源，但资源调配算法可能会因以下原因而失效：

- 不准确的资源使用建模，这可能导致超额预订或超额配置（反过来，导致云提供者资源浪费）。
- 资源分配算法失效。
- 资源分配算法使用作业或分组分类失效。
- 整体资源配置失效（与临时过载相反）。

虽然许多提供者允许客户预先预留资源，但资源调配算法可能会因以下原因而失败：

不准确的资源使用建模，这可能导致超额预订或超额配置（反过来，导致云提供者浪费资源）。

V.16 不可控的脆弱性评估过程

不对端口扫描和漏洞测试进行限制是一个很重要的漏洞。

V.17 内部（云）网络探测

云消费者可以对内部网络中的其他客户执行端口扫描和其他测试。

V.18 执行共享场所检查的可能性

利用缺乏资源隔离的侧信道攻击，攻击者可以确定哪些客户共享哪些资源。

V.19 缺乏取证准备

提供者可能不具备足够的取证准备和支持能力。 例如，SaaS 提供者可能不会对客户提供访问日志。IaaS 提供者可能不提供取证服务，如最近的虚机和磁盘映像。

V.20 敏感介质数据擦除

物理存储资源的共享意味着敏感数据可能泄漏，因为传统物理设施的数据销毁策略在云环境无法使用。

V.21 同步外部责任或合同义务

云消费者通常不知道服务条款分配给他们的责任。 即使在双方的合同条款中明确规定不承担责任时，仍存在将归档加密等活动的责任归于云提供者的倾向。

V.22 跨云应用程序产生隐藏的依赖性

隐藏的依赖关系存在于服务供应链中，当涉及到的第三方、分包商或客户与服务提供者分离时，云提供者体系结构不支持从云继续操作。反之亦然。

V.23 对不同利益相关者冲突的 SLA 条款

SLA 条款也可能与其他条款或其他提供者的条款所作的承诺相冲突。

V.24 SLA 条款包含过高的商业风险

考虑到技术故障的实际风险，SLA 可能会给提供者带来太多的业务风险。从客户的角度来看，SLA 可能包含有害的条款-例如，在知识产权领域，SLA 可能指定云提供者对存储在云基础设施上的任何内容具有权利。。

V.25 消费者无法对云提供者进行审计或认证

云提供者无法为客户审计提供任何保证。例如云提供者可能正在使用未经认证的开源虚拟化管理程序或其定制版本（例如 Xen（38））。

V.26 认证方案不适用于云基础设施

没有任何云特定的控制，这意味着安全漏洞可能会被忽略。

V.27 基础设施资源配置不足和投入不足

基础设施投入需要时间。 如果预测模型失败，云提供者服务可能会长时间失败。

V.28 没有资源上限策略

如果提供者不支持资源配额限制，可能会产生问题。

V.29 数据在多个司法管辖区的存储和缺乏透明度

通过边缘网络和冗余存储镜像传输数据，客户不能知道数据实时的存储位置。 这可能在不知情的情况下违反法规，特别是当没有提供存储管辖权的明确信息时。

V.30 缺乏关于司法辖区的信息

数据可能存储在高风险司法管辖区或在这些区域进行处理，它们很容易被强制没收。 这会使云消费者束手无策。

V.31 缺乏完整性和透明度的使用条款

不是云特有的漏洞

下面这些漏洞并非特定于云计算，但在评估云系统时应予以仔细考虑。

V.32 缺乏安全意识

云消费者并不知道他们在迁移到云时可能面临的风险，尤其是那些由云特定威胁（即失控，

提供者锁定，用尽的云提供者资源等）所产生的风险。

V.33 缺乏审查过程

由于云服务提供者可能存在非常高的特权角色，由于涉及资源规模大，对具有此类角色的工作人员风险状况的缺乏或不充分审查是一个重要的漏洞。

V.34 角色和责任不明确

这些漏洞涉及云提供者组织中角色和责任的归属不明确

V.35 对角色定义执行不力

如果云提供者未能分离角色，可能会导致权限过大，从而导致大范围的系统受到攻击。

V.36 没有遵循“需知原则”

这是有关角色和责任的特殊情况。 不应对缔约方进行不必要的数据访问。 否则就构成了不必要的风险。

V.37 不适当的物理安全程序

这包括：

- 缺乏物理边界控制（入口的智能卡认证）；
- 缺乏对易受窃听的关键资产的电磁屏蔽。

V.38 配置错误

这类漏洞包括：安全基线和加固程序的应用不充分，人为错误和未经培训的管理员。

V.39 系统或操作系统的脆弱性

V.40 不受信任的软件

V.41 缺乏业务连续性和灾难恢复计划，或缺乏经过测试的灾难恢复计划

V.42 资产清单缺失，不完整或不准确

V.43 资产分类缺失，贫乏或不充足

V.44 资产所有权不明确

V.45 项目需求的识别不充分

其中包括缺乏对安全性和法律合规性要求的考虑，没有系统和应用程序用户参与，业务需求不明确或不足等。

V.46 可选提供者太少

V.47 缺乏提供者冗余

V.48 应用安全漏洞或安全补丁管理缺失

这类漏洞包括：应用程序代码中的错误，提供者和客户之间的补丁程序冲突，未经测试的补丁程序的应用，浏览器中的漏洞等。

V.49 资源消耗的脆弱性

V.50 由提供者违反 NDA（保密协议）

V.51 数据丢失责任（云提供者）

V.52 缺乏日志收集或保存的政策或程序

V.53 资源过滤不足或错误配置

5.资产

资产		所有者[参与人员或]	价值感知 [规模：非常低 - 低 - 中等 - 高 - 非常高]
A1.公司声誉		云消费者	**很高**
A2.客户的信任	包括商誉，可以通过投诉来衡量	云消费者	**很高**
A3.员工忠诚度和经验		云消费者	**高**
A4.知识产权		云消费者	**高**
A5.个人敏感数据	（如欧洲数据保护指令中所定义的）	提供者 / 云消费者	**非常高（因为它包括谁在使用家庭护理系统的数据）**
A6.个人资料	（如欧洲数据保护指令中所定义的）	提供者 / 云消费者	**中（运营价值）/ 高（损失的价值）**
A7.个人数据 - 至关重要	（根据欧洲数据保护指令包含在“个人数据”类别中的所有数据，并被组织或公司分类或重视	提供者 / 云消费者	**高（运营价值）/ 高（价值如果丢失）**
A8.HR 数据	除了数据保护要求之外，从操作的角度来看，这些数据是相关的	云消费者	**高**
A9. 服务交付 - 实时服务	所有那些时间紧迫的服务需要的可用性水平接近 100%	提供者 / 云消费者	**很高**
A10. 服务交付		提供者 / 云消费者	**中**

A11. 访问控制 访问控制/身份验证/授权（root / admin v 其他）		提供者 / 云消费者	**高**
A12. 凭证	进入系统的患者和工作人员	云消费者	**很高**
A13. 用户目录（数据）	如果目录失效，那么没有人进来	云消费者	**高**
A14. 云服务管理平面	这是管理通过云提供的所有服务的管理平面（基于 web 或远程 shell 等）。	提供者 / 云消费者	**很高**
A15. 管理接口 API		提供者 / 云消费者	**中**
A16. 网络（连接等）	包括云内和云外的连接	提供者 / 云消费者	**高**
A17. 物理硬件		提供者 / 云消费者	**低（取决于你丢失多少）/中（如果被盗和未受保护可能是严重的）**
A18. 物理建筑		提供者 / 云消费者	**高**
A19. 云提供者应用程序（源代码）		提供者 / 云消费者	**高**
A20. 认证	ISO，PCI-DSS 等	提供者 / 云消费者	**高**
A21. 操作日志（客户和云提供者）	这些日志用于维持和优化业务流程并用于审计目的	提供者 / 云消费者	**中**
A22. 安全日志	用作为安全漏洞和取证的证据	提供者 / 云消费者	**中**
A23. 备份或归档数据		提供者 / 云消费者	**中**

6.建议和关键信息

本节包含主要建议和关键信息：

- 信息保障框架 - 一个标准的问题清单，可用于云消费者从云提供者处获取安全保证
- 法律建议
- 研究建议。

信息保证框架

介绍

本报告最重要的建议之一是设计的一套保证标准：

1) 评估采用云服务的风险。
2) 比较不同的云提供者。
3) 从选定的云提供者处获得保证。
4) 减少云提供者的保证负担。大量客户要求对其基础设施和政策进行审计。这会给安全人员造成严重的负担，同时也会增加进入基础设施的人数，这就大大增加了由于滥用安全关键信息、盗窃而受到攻击的风险。云提供者需要通过建立一个处理此类请求的明确框架来处理关键数据或敏感数据等。

这部分建议提供了一系列问题，组织可以要求云提供者确保自己充分保护他们的托管信息。

这些问题旨在提供最低基准。 因此，任何组织都可能具有基准范围内未涵盖的其他特定要求。

责任部门

关于安全事件，需要在客户和提供者之间对安全相关的角色和责任有清晰的定义和理解。

下表显示了客户与提供者之间预期的责任分配。

	用户	提供者

内容的合法性	全部责任	根据电子商务指令(1)及其解释的条款免除的中介责任。
安全事件（包括数据泄露，使用账户发起攻击）	根据合同条件对其控制下的内容负责尽职调查	对其控制下的事物负责尽职调查
欧洲数据保护法律地位	数据控制器	数据处理器（外部）

责任分工

关于安全事件，需要在客户和提供者之间对安全相关的角色和责任有清晰的定义和理解。下表显示了典型和合理的责任分工。

软件即服务

顾客	提供者
• 遵守关于收集和处理客户数据的数据保护法 • 身份管理系统的维护 • 身份管理系统的管理 • 认证平台的管理（包括强制密码策略）	• 物理基础设施（设施，机架空间，电源，冷却，布线等） • 物理基础设施安全和可用性（服务、存储、网络、带宽等） • 操作系统补丁管理和强化程序（还要检查客户加固程序和提供者安全策略之间的任何冲突） • 安全平台配置（防火墙规则，IDS / IPS调整等） • 系统监控 • 安全平台维护（防火墙，主机IDS / IPS，防病毒，数据包过滤） • 日志收集和安全监控 •

平台即服务

顾客	提供者

• 身份管理系统的维护 • 身份管理系统的管理 • 认证平台的管理(包括强制密码策略)	• 物理基础设施(设施，机架空间，电源，冷却，布线等) • 物理基础设施的安全性和可用性(服务器，存储，网络带宽等) • 操作系统补丁管理和加固程序(还要检查客户加固程序和提供者安全策略之间的任何冲突) • 安全平台配置（防火墙规则，IDS / IPS调整等） • 系统监控 • 安全平台维护(防火墙，主机IDS / IPS，防病毒，包过滤) • 日志收集和安全监控

基础设施即服务

顾客	提供者
• 身份管理系统的维护 • 身份管理系统的管理 • 认证平台的管理（包括强制密码策略） • 客户操作系统补丁和加固程序的管理（也检查客户加固程序和提供者安全策略之间的任何冲突） • 访客安全平台的配置（防火墙规则，IDS / IPS调整等） • 访客系统监控 • 安全平台维护（防火墙，主机IDS / IPS，防病毒，包过滤） • 日志收集和安全监控	• 物理基础设施（设施，机架空间，电源，冷却，布线等） • 物理基础设施的安全性和可用性(服务器，存储，网络带宽等) • 主机系统（管理程序，虚拟防火墙等）

云消费者对 IaaS 的安全性负责，他们应该考虑以下几点：

IAAS - 应用程序安全

IaaS 应用程序提供者将客户虚拟实例中的应用程序视为“黑盒”，因此对于客户应用程序的

操作和管理完全不可知。 整个'堆栈' - 客户应用程序，运行时应用程序平台均由客户自己管理。

以下是与安全应用程序设计和管理最佳实践有关的简要清单和说明：

- 云部署的应用程序必须针对互联网威胁模型进行设计
- 他们必须设计或嵌入标准安全对策，以防范常见的网络漏洞（OWASP top 10）。
- 客户有责任更新他们的应用程序，因此必须确保他们有适当的补丁策略。
- 客户不应该试图使用自定义的身份验证，授权和审计（AAA）实现，因为如果执行不当，可能会变得脆弱。

由于这个原因，必须注意到客户必须承担保护其云部署应用程序的全部责任，这一点非常重要。

总之：企业分布式云应用程序必须运行许多控制措施以保护主机，用户访问权限和应用程序级别控制。此外许多主流厂商（如 Microsoft，Oracle，Sun 等）都会发布有关如何确保其产品配置的全面文档。

方法论

本文档的关键部分基于 ISO 27001/2（42），（43）和 BS25999（44）标准中的控制类别。 这些章节中的细节来源于标准以及行业最佳实践的要求。 在整个过程中，我们只选择了与云提供者和第三方外包商相关的那些控制。

注意事项

以下部分的问题是一些常见控制。 它并不是详细的清单; 同样，某些问题可能不适用于特定的实现。 因此，该清单应作为共同控制的基线，如有需要应该寻求更细致的资料。

值得注意的是，虽然有可能将许多风险转移给外部提供者，但转移风险的真正成本却很少能真正转移。 例如，导致未经授权披露客户数据的安全事件可能会导致提供者蒙受经济损失，但消费者信心的负面宣传和损失以及潜在的监管处罚（PCI-DSS）将由最终客户感承担。也就是说转移商业风险是可能的，但最终风险始终存在于最终客户。

对风险评估结果-特别是缓解投资的数量和类型-作出的任何反应，都应根据本组织的风险偏好以及遵循任何特定的减轻风险战略而失去的机会和节省的资金来决定。

云消费者还应该执行他们自己的特定于上下文的风险分析。

风险评估应该是一项常规活动，而不是一次性事件。

政府需要注意

以下控制措施主要针对中小企业。它们也可能对政府有用，但有以下条件。在任何政府机构的信息分类方案中，应仔细考虑所使用的云的特性。

- 公有云使用-即使提供者对以下调查表作出了积极的答复-除了最低保证级别的数据之外，其它的数据不建议使用。
- 对于更高级别的数据保证，本报告中建议的检查清单也是有效的，但应补充附加检查。
- 提供者是否提供透明信息并完全控制所有数据的当前物理位置？ 高监管数据通常受到位置限制。
- 提供者是否支持使用符合要求的数据分类方案？
- 提供者提供什么保证，客户资源是完全隔离的（例如，不共享物理机器）？
- 假设客户之间不共享物理机器，在重新分配机器之前，存储器，内存和其他数据记录能否完全擦除。
- 提供者是否支持双因素身份验证？
- 提供者是否持有 ISO 27001/2 认证？ 认证的范围是什么？
- 提供者使用的产品是否具有 CC 认证？ 在哪个级别？ 产品的保护配置文件和安全目标是什么？

信息保证要求

人员安全

人员安全评估与大多数评估一样，需要在风险与成本之间寻找平衡。

- 您有哪些政策和程序对 IT 管理员获得系统访问权限进行控制？ 这些应该包括：雇用前背景检查（国籍、身份、工作经历和参考资料，犯罪记录等）。
- 不同的数据存储位置或应用程序运行位置对应不同的策略？
    - 例如，一个地区的招聘政策可能与另一个地区的不同。
    - 各地区的做法需要保持一致。
    - 敏感数据可能与适当的人员存储在一个特定区域中。
- 你为全体员工开展了哪些安全教育课程？
- 有没有一个持续评估的过程？
    - 评估的频率如何？
    - 访谈

- 安全访问和特权审查
- 政策和程序审查。

供应链保证

以下问题适用于云提供者将一些操作分包给第三方(例如，SaaS 提供者将底层平台外包给第三方提供者、云提供者将安全服务外包给托管安全服务提供者、使用外部提供者对操作系统进行身份管理等)，还包括具有实体或远程访问云提供者基础设施的第三方。 它是假设整个问题单可以递归地应用于第三方云服务提供者。

- 定义服务交付供应链中外包或分包的服务，这些服务对于您的运营的安全性（包括可用性）至关重要。
- 详细说明用于确保第三方访问您的基础设施（物理和/或逻辑）的过程。
- 你是否审核你的外包商和分包商，多久审核一次？
- 外包商承诺的 SLA 条款是否低于您向客户提供的 SLA？ 如果没有，您是否有提供者冗余？
- 采取了哪些措施来确保和维持第三方服务水平？
- 云提供者能否确认安全策略和控制措施是否适用于（第三方）提供者？

操作安全

预计与外部提供者的任何商业协议都将包括所有网络服务的服务水平。然而，除了定义的协议外，最终客户还应确保提供者采用适当的控制措施，以减少未经授权的信息披露。

- 详细说明您的变更控制程序和政策。
- 定义远程访问策略。
- 提供者的系统维护操作是否有文件化的记录？
- 开发，测试和生产环境是否隔离？
- 定义主机和网络控制。这些应包括对外部标准的认证细节（如 ISO 27001/2）。
- 指定用于防范恶意代码的控件。
- 部署的安全配置只允许执行授权的移动代码和授权功能
- 详细的备份策略和程序。

审计日志既可用于事件调查; 也可以用于故障排除。 为了达到这些目的，最终用户需要确保提供这些信息：

- 提供者能否详细说明审计日志中记录的信息？
  - 该数据保留了多长时间？
  - 是否有可能在审计日志中对数据按租户进行细分？
  - 采用了哪些控制措施来保护日志免遭未经授权的访问或篡改？
  - 用什么方法检查和保护审计日志的完整性？
- 如何对日志进行审计？ 对于日志审计行为本身的日志如何记录？
- 是否使用 NTP 服务器同步系统时钟，并提供准确的审计日志时间戳？

软件保证

- 定义用于保护操作系统和应用程序完整性的控件。
- 如何验证新版本是否有风险（后门，特洛伊木马等）？
- 遵循什么实践来保证应用程序的安全？
- 是否进行了软件渗透测试以确保它不包含漏洞？ 如果发现漏洞，那修复过程是什么？

补丁管理

- 提供补丁管理程序的详细信息。
- 您能否确保补丁管理流程涵盖云交付技术的所有层面 - 即网络，操作系统，虚拟化软件，应用程序和安全子系统？

网络体系结构控制

- 定义用于减轻 DDoS（分布式拒绝服务）攻击的控制。
  - 纵深防御（深度数据包分析，流量控制，数据包黑洞等）
  - 您是否有针对“内部”（源自云提供者网络）攻击以及外部（源自 Internet 或客户网络）攻击的防范？
- 使用什么级别的隔离？
  - 用于虚拟机，物理服务器，网络，存储（例如存储区域网络），管理网络和管理支持系统等。
- 当公司与服务提供者分离时，该体系结构是否支持从云中继续操作（反之亦然）（例如，是否存在对客户 LDAP 系统的严重依赖性）？
- 云提供者使用的虚拟网络基础设施是否保护提供者和/或最佳实践的特定标准（例如，MAC 欺骗，ARP 中毒攻击等是否通过特定的安全措施配置来防止）？

主机架构

- 提供者是否确保默认情况下虚拟机镜像被加固？
- 加固的虚拟镜像是否受到未经授权的访问？
- 提供者能否确认虚拟化映像不包含认证凭证？
- 主机防火墙是否运行，是否只支持虚拟实例中服务所必须的端口？
- 基于主机的入侵防御服务（IPS）能否在虚拟实例中运行？

PAAS - 应用程序安全

一般来说，PaaS 服务提供者负责平台软件堆栈的安全性，本文档中的建议是确保 PaaS 提供者在设计和管理其 PaaS 平台时考虑安全原则。 通常很难从 PaaS 提供者那里获得关于如何保护他们的平台的详细信息 - 但是以下问题有助于评估他们的产品。

- 要求提供多租户应用程序隔离的信息 - 需要对隔离措施进行高级描述。
- PaaS 提供者如何确保仅限于您的企业用户和您拥有的应用程序访问您的数据？
- 平台架构采用“沙箱” - 提供者是否确保 PaaS 平台沙箱受到新的漏洞影响？
- PaaS 提供者应该能够提供一组安全功能（在客户端之间可重复使用） - 这些功能包括用户认证，单点登录，授权（特权管理）和 SSL / TLS（通过 API 提供）？

SAAS - 应用程序安全

SaaS 模型规定提供者管理交付给最终用户的整套应用程序。 因此 SaaS 提供者主要负责确保这些应用程序的安全。 客户通常负责操作安全流程（用户和访问管理）。

以下问题有助于协助评估其产品：

- 提供了哪些管理控制，并且可以使用这些控制来为其他用户分配读写权限？
- SaaS 访问控制是否精细，可以根据贵组织的政策进行定制？

资源配置

- 在资源过载的情况下（处理，内存，存储，网络）？
    - 在配置失败的情况下，提供了有关分配给我的请求优先级的信息？
    - 服务水平和需求变化是否有交付时间？
- 你的资源能扩展到多少？ 提供者是否在最短时间内提供最大可用资源保证？
- 你可以多快地扩展规模？ 提供者是否在最短时间内提供补充资源的保证？
- 处理大规模资源使用的过程是什么（如突发的高并发流量）？

身份和访问管理

以下控制适用于云提供者的身份和访问管理系统（受其控制的系统）：

授权

- 是否有任何账户对整个云系统具有完整权限，如果有，能执行哪些操作（读取/写入/删除）？
- 具有最高权限级别的账户如何进行身份验证和管理？
- 最重要的决策（例如，同时释放大规模资源）是如何被授权的（单一或双重的，以及组织内部的角色）？
- 是否将任何高特权角色分配给同一个人？ 这种分配是否会破坏职责分离或最小特权原则？
- 你使用基于角色的访问控制（RBAC）吗？ 是否遵循最小特权原则？
- 如果有的话，管理员权限和角色会发生什么变化，以便在发生紧急情况时可以进行应急访问？
- 对于客户是否有'管理员'角色？ 例如，客户管理员是否能添加新用户（但不允许他更改底层存储！）？

身份供应（开通）

- 在注册时对用户账户的身份进行了哪些检查？ 是否遵循任何标准？
- 根据所需资源是否存在不同级别的身份检查？
- 什么流程用于撤销身份凭证？
- 是否在整个云系统中同时提供凭据和取消配置，或者是否存在跨多个地理分布位置取消配置的风险？

个人数据管理

- 哪些数据存储和保护控制适用于用户目录（例如 AD，LDAP）并对其进行访问？
- 用户目录数据是否能以可互操作的格式输出？
- 了解云提供者访问客户数据符合基本的“需知”原则吗？

密钥管理

对于云提供者控制下的密钥：

- 是否有安全措施来控制读写这些密钥？
- 是否有适当的安全控制措施来使用这些密钥来签名和加密数据？
- 应对重大密钥损害事件的预案是否到位？ 例如，密钥撤销列表。

- 密钥撤销是否能够处理多个站点的同步问题？
- 客户系统映像是受保护或加密的吗？

加密

- 加密可以在多个地方使用 - 它在哪里使用？
    - 传输中的数据
    - 静态数据
    - 处理器或内存中的数据？
- 用户名和密码？
- 对于应该加密的内容以及不应该加密的内容，是否有明确的策略？
- 谁拥有访问密钥？
- 密钥如何保护？

认证

- 需要高度保证的操作使用哪种形式的认证？ 这可能包括登录管理平面，创建密钥，访问多用户账户，防火墙配置，远程访问等。
- 双因素身份验证是否用于管理基础设施内的关键组件，如防火墙等？

凭证损坏或被盗

- 您是否提供异常行为检测？
- 发生盗窃客户凭证时有哪些规定（检测，撤销，行为证据）？

提供给云消费者的身份和访问管理系统

以下问题适用于云提供者为云用户使用和控制提供的身份和访问管理系统：

身份管理框架

- 该系统是否允许一个联合身份管理基础设施，它既可用于高安全级别(必要时使用一次性
- 密码系统)，也可用于低安全级别(例如用户名和密码)？
- 云提供者是否可以与第三方身份提供者互操作？
- 有没有单点登录的能力？

访问控制

- 客户端凭证系统是否允许分离角色和责任以及多个域？
- 您如何管理对客户系统映像的访问 - 并确保凭证和密钥不包含在其中？

认证

- 云提供者如何向客户标识自己（即，是否存在相互认证）？
  - 当客户发送 API 指令时？
  - 当客户登录到管理平面时？
- 您是否支持联合身份验证机制？

资产管理

确保提供者维护硬件和软件（应用）资产的最新列可以用于检查所有系统是否都使用了适当的控制。

- 提供者是否有自动化的方法来清理所有资产？
- 是否有客户在特定时间段内使用的资产列表？

在最终客户部署需要额外保护的数据时（即认为敏感），将使用以下问题。

- 资产是按照敏感性和重要性分类的？
  - 如果是，提供者是否在具有不同分类的系统
  - 具有不同安全分类的系统的单个客户之间是否采用适当的隔离机制？

数据和服务的可移植性

为了理解与提供者锁定相关的风险，应考虑这些问题。

- 是否存在用于从云端导出数据的文档化程序和 API？
- 提供者是否为云中存储的所有数据提供可互操作的导出格式？
- 就 SaaS 而言，API 接口是否标准化？
- 是否有任何关于以标准格式导出用户创建的应用程序的规定？
- 是否有数据导出到另一个云提供者的流程 - 例如，客户是否希望更改提供者？
- 客户端是否可以执行自己的数据提取以验证该格式是否具有通用性并且能够迁移到其他云提供者？

业务连续性管理

提供连续性对于一个组织很重要。 尽管可以设置服务级别协议，详细说明系统可用的最短时间，但还有一些额外的考虑因素。

- 提供者是否维护一个详细记录中断的影响的方法？
    - 什么是服务的 RPO（恢复点目标）和 RTO（恢复时间目标）？ 根据服务的重要性详细说明。
    - 信息安全活动是否在恢复过程中得到适当解决？
    - 发生中断时，与最终客户的沟通渠道是什么？
    - 在处理中断时，团队的角色和责任是否明确？
- 提供者是否将恢复的优先级进行分类。
- 存在哪些与恢复过程相关的依赖关系？ 包括提供者和外包合作伙伴。
- 如果主站点不可用，切换到备用站点的最短时间是多少？

事件管理和响应

事件管理和响应是业务连续性管理的一部分。 此过程的目标是将突发事件和潜在干扰事件的影响控制在组织可接受的水平。

要评估组织为降低信息安全事件发生的可能性或减少信息安全事件负面影响的能力，应向云提供者询问以下问题：

- 提供者是否有正式的流程来检测，识别，分析和响应事件？
- 这个过程是否经过演练？在演练期间能否确保相关支持组织中的每个人都知道事件处理期间（事件和事后分析过程中）的流程和角色？
- 检测能力如何构建？
    - 云消费者如何向提供者报告异常情况和安全事件？
    - 提供者允许客户选择第三方 RTSM 服务(在适当情况下)干预其系统或与云提供
- 商协调事件响应功能的设施是什么？？
    - 是否有实时安全监控（RTSM）服务？ 服务是否外包？ 哪些的指标和服务被监控？
    - 您是否提供（根据请求）关于安全事件的定期报告？
    - 安全日志保留多久？ 这些日志是否安全存储？ 谁有权访问日志？
    - 客户是否可以在虚拟机映像中部署 HIPS / HIDS？ 是否有可能将客户的入侵检测和预防系统收集的信息整合到云提供者的 RTSM 服务或第三方的 RTSM 服务中？
- 如何定义严重性级别？
- 如何定义升级程序？ 升级程序何时涉及云消费者？
- 如何记录事件并收集证据？
- 除了身份验证，计账和审计之外，还有哪些控制措施可以防止恶意内部人员的活动？
- 提供者是否向客户提供虚拟机的取证镜像？
- 提供者是否收集事件度量和指标。

- 哪些内容服务提供者可以公开？
- 提供者多久测试一次灾难恢复和业务连续性计划？
- 提供者是否收集 SLA 满意度数据？
- 提供者是否执行服务台测试？ 例如：
  - 身份假冒测试：通过电话请求重置密码的人真的是他说的那个人吗？还是所谓的“社会工程”攻击。
- 提供者是否进行渗透测试？ 多久测试一次？ 在渗透测试期间实际测试的是什么？
- 提供者是否执行漏洞测试？ 多久测试一次？
- 修补漏洞（修补程序，重新配置，升级到更高版本的软件等）的过程是什么？

物理安全

与人员安全一样，由于 IT 基础设施受第三方控制（如传统外包），因此出现许多潜在问题，但物理安全漏洞可能会对多个客户（组织）产生影响。

- 您可以向客户提供有关该场所物理安全性的什么保证？
  - 除授权 IT 人员之外，谁拥有对 IT 基础设施无陪同（身体检查）访问权限？
    - 例如，清洁工，经理，“人身安全”员工，承包商，顾问，提供者等。
  - 访问权限多久审查一次？
    - 访问权限多久撤销？
  - 您是否定期评估安全风险并评估边界？
    - 频率是什么？
  - 你是否定期进行风险评估，包括邻近建筑物等？
  - 您是否控制或监控访问安全区域的人员（包括第三方）？
  - 你有什么样的政策或程序来安装，卸载和安装设备？
  - 交付物（如设备等）是否在安装前检查风险？
  - 数据中心中是否有最新的实物资产清单？
  - 网络电缆是否通过公共访问区域运行？
    - 你使用铠装电缆还是管道？
  - 你是否经常巡查建筑以寻找未经授权的设备？
  - 是否有任何场外设备？
    - 如果有是如何保护的？
  - 您的员工是否使用可以访问数据中心的便移动设备（例如，笔记本电脑，智能手

机）？

- 这些如何保护？

- 采取了哪些措施来控制访问卡？
- 有什么过程或程序在需要时销毁旧介质或系统？
  - 数据覆盖？
  - 物理破坏？
- 设备从一个地点移动到另一个地点的授权流程是什么？
  - 你如何识别具有授权的工作人员的（或承包商）？
- 设备审核多久进行一次，以监控未经授权的设备移除？
- 多久进行一次检查以确保环境符合适当的法律和法规要求？

环境控制

- 哪些程序或政策可以确保环境问题不会导致服务中断？
- 你用什么方法来防止火灾，洪水，地震等造成的损害？
  - 在发生灾难时，将采取哪些额外的安全措施来保护物理访问？
  - 主站和备用站点都有这些措施吗？
- 您是否监控数据中心的温度和湿度？
  - 空调或监控？
- 你是否保护你的建筑免受雷击？
  - 包括电气和通讯线路？
- 发生电源故障时是否有独立的发电机？
  - 他们能运行多久？
  - 有充足的燃料供应吗？
  - 有备用发电机吗？
  - 你多久检查一次 UPS 设备？
  - 你多久检查一次发电机？
  - 你有多个电力提供者吗？
- 所有公用设施（电力，水等）都能够支持您的环境吗？ 这种重新评估和测试的频率是什么？
- 你的空调能够支持你的环境吗？
  - 它多久测试一次？

- 你是否遵循制造商推荐的维护计划？
- 您是否只允许授权的维护或维修人员进入该场所？
    - 你如何检查他们的身份？
- 当设备被送去维修时，数据是否先从其中清除？
    - 这是如何完成的？

法律要求

云提供者服务的客户和潜在客户应考虑到各自在遵守监管框架方面的国内和国际义务，并确保适当遵守任何此类义务。

客户应该向云提供者询问的关键法律问题是：

- 云提供者位于哪个国家/地区？
- 云提供者的基础设施是否位于同一个国家或不同的国家？
- 云提供者是否会使用基础设施位于云提供者之外的其他公司？
- 数据位于何处？
- 合同条款和数据的管辖权是否分开？
- 是否将任何云提供者的服务分包出去？
- 是否将任何云提供者的服务外包？
- 客户和客户的客户提供的数据将如何收集，处理和传输？
- 在合同终止时发送给云提供者的数据会发生什么变化？
-

法律建议

目前，云计算涉及的大部分法律问题将在客户评估合同，用户许可协议（ULA）和 SLA 期间得到解决。中小企业可以在市场上提供的不同合同之间作出选择，而一个更大的组织则可以通过谈判协商合同。

由于云计算的性质，某些标准合同条款可能值得进一步审查。应特别注意与以下方面有关的权利和义务：安全漏洞通知、数据传输、衍生作品的创建、控制权的变更和执法实体对数据的访问。

考虑到各方对云的使用情况，责任的标准限制是否充分地代表了责任的分配。

以下列出了客户在评估 SLA，ToUs，ULA 和其他云服务协议时应特别注意的领域：

a) 数据保护：应该注意选择一个处理器，该处理器提供足够的技术安全措施和组织措施来管理要执行的处理，并确保遵守这些措施

b) 数据安全：应注意强制性数据安全措施，如果合同未解决这些义务，则可能导致云提供者或客户受到监管和司法措施的约束。

c) 数据传输：应注意提供给客户的信息

d) 执法访问：每个国家都有对执法访问数据的独特限制和要求。 客户应注意提供者提供的关于数据可能存储和处理的司法管辖区的信息，并评估可能适用的司法管辖区产生的任何风险。

e) 保密和不公开：应审查与此问题有关的责任和义务。

f) 知识产权：在 IaaS 和 PaaS 的情况下可以存储知识产权，包括使用云基础设施创建的原始作品。云消费者应确保合同尽可能尊重他们对任何知识产权或原始作品的权利，同时不影响所提供的服务质量。（例如，备份可能是提供良好服务水平的必要部分）。

g) 风险分配和责任限制：在审查各自的合同义务时，各方应该强调那些对他们构成重大风险的义务，包括货币补救条款或赔偿义务，以防另一方违反该合同义务。 此外，任何涉及责任限制的标准条款都应该仔细评估。

h) 控制权变更：透明度涉及云提供者在控制权变更的情况下继续履行合同义务的能力，以及撤销合同的任何可能性。

研究建议

在云中构建信任

- 云计算安全性度量标准;
- 安全投资回报（ROSI）：云计算可以提高安全投资回报率;
- 不同形式的检举行为对安全的影响;
- 提高透明度同时保持适当的安全级别的技术：
  - 标记，例如位置标记，数据类型标记，策略标记
  - 隐私保护数据来源系统，例如通过系统端到端追踪数据;
- 云端及以外的端到端数据机密性：
  - 加密搜索（长期）
  - 加密处理方案（长期）
  - 云中社交应用的加密和保密工具
  - 云中的可信计算，例如虚拟机堆栈的可信引导序列;
- 高保证级别的云，虚拟私有云等;

- 将基于云的信任扩展到基于客户端的数据和应用程序。

大规模跨组织系统中的数据保护

以下领域需要进一步研究云计算：

- 数据销毁和生命周期管理
- 完整性验证 - 云中的备份和归档及其版本管理
- 取证和取证机制
- 事件处理 - 监控和可追溯性
- 争议解决和证据规则
- 相关法规的国际差异，包括数据保护和隐私
    - 促进多国云基础设施顺利运作的法律手段
    - 自动化手段，以缓解不同司法管辖区的问题。

大型计算机系统工程

- 大型分布式计算机系统内的深度安全性;
- 云中的安全服务 - 安全技术的去边界化;
- 资源隔离机制 - 数据，处理，内存，日志等;
- 云提供者之间的互操作性;
- 避免提供者锁定；

- 将数据，应用程序的接口标准化 - 以便每个操作系统都可以开发相应的客户端接口;
- 资源（带宽和主机）大规模弹性供应和分配;
- 云平台内的可扩展安全管理（策略和操作程序）：
    - 自动执行安全和数据保护策略
    - 确保提供者的安全操作流程 - 实施治理流程;
- 云计算的弹性 - 如何提高云的弹性：
    - 在客户端使用云架构（边缘网络，p2p 等）
        - 聚合多个客户端网络
        - 基于客户端的冗余和备份;