企业架构参考指南

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

云安全联盟企业架构研究工作组官网:

https://cloudsecurityalliance.org/research/working-groups/enterprise-architecture/

序言

企业数字化安全转型面临着选择、判断和组合的困扰，对组织、技术、人才、管理和业务模型等多方面的有机融合和运转构成了架构，而安全是高效的基础，二者都是竞争力。国内企业普遍在学华为、海尔、格力，同时也在吸收IBM、微软、谷歌、亚马逊等企业的成长模型。CSA编著的本指南是国外大型企业实践经验的总结凝练，是一个与时俱进的参考书。本文聚焦实践，沉淀知识，而不必全面冗长的去解读，非常适合企业管理者和IT、业务、运营、安全的负责人快速学习，定位问题，抓住要领，快速实践，企业对每一项组件的投入都可以在此架构中找到位置，找到他上层面的组、域。指南用1-2-3-4表达出每一个组件的层次，我们既可以看到1的面貌，又可以细化到2的构成和3、4的细节，是思维导图模式的简洁变形。

纵观一个企业的成长与治理，指南对企业架构建设、优化和运营实践的价值指导意义，在于他抽取、吸收了COBIT、TOGAF、ITIL、SABSA、Jericho、NIST SP 500-299、 NIST SP 500-292、ISO 27001、ISO 27002等系列框架理论的精要，从而在”云大物智移”环境下，使得企业架构的高效搭建与运行既拥有了理论框架，又有了可查找的实践行动。企业IT治理、安全治理、生产运营、应急事件处理是数字化转型基础内容，指南可服务于对安全、效率、和运营有持续优化诉求的大中小企业。本指南展开的对四个域的解构：业务运营支持服务(BOSS)、信息技术运营与支持 (ITOS) 、技术解决方案服务 (TSS) 、安全和风险管理(SRM)。可以用东方人的模式和中国人的，即“你我它”思维思考，你：是指框架中的任何组件、域，我：企业架构的需求、困难、链接方式、紧要度等，它：传递的下一站，实现企业架构期望的目标或阶段方向。

对于未来的延伸，任何一个架构都是有时效的，因为变是万物常态，运动是活力之源，企业架构的运营是指南中所提所有相关技术，组织，业务，风险应对与系统管理的多维协同，任何之一的变动延伸，都是对指南演进的新要求。本指南也为这种延伸铺垫了未来持续发挥的思路和舞台，努力为企业把技术用精，把业务做顺，把组织做通，把管理做活。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《企业架构参考指南（Enterprise Architecture Reference Guide）》由CSA研究工作组专家编写，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：程伟强　仇蓉蓉　邓　辉　伏伟任　高亚楠

贺志生　江　楠　李　钠　李　岩　李　程

林艺芳　刘　洁　鹿淑煜　沈　勇　苏泰泉

滕　伟　王永霞　吴嘉雯　吴　潇　谢　琴

杨喜龙　余晓光

审校组：陈欣炜　单美晨　何伊圣　江　楠　李　岩

刘　洁　陶瑞岩　王　阳　姚　凯

研究协调员：孙天一

感谢以下单位的支持与贡献：

北京安讯奔科技有限责任公司

北京山石网科信息技术有限公司

北京天融信网络安全技术有限公司

广东美云智数科技有限公司

华为技术有限公司

奇安信科技集团股份有限公司

三六零数字安全科技集团有限公司

三未信安科技股份有限公司

上海安几科技有限公司

上海缔安科技股份有限公司

腾讯云计算（北京）有限责任公司

长春吉大正元信息技术股份有限公司

浙江极氪智能科技有限公司

英文版本编写专家

主要作者： Jon-Michael C. Brook　　Michael Roza

贡献者： Shawn Harris　　Sunil Shanthi　　Michael Theriault

Rolando Marcelo Vallejos　　Ashish Vashishtha　　Suri Venkat

Henry Werchan

CSA团队： Sean Heide　　Stephen Lumpe (Cover)　　Jim Reavis

AnnMarie Ulskey (Layout)　　John Yeoh

总架构师： Jairo Orea

首席架构师： Dan Logan

贡献者： Richard Austin　　Ryan Bagnulo　　Charleton Barreto

Jon-Michael Brook　　Phil Cox　　Earle Humphreys

Tuhin Kumar　　Subra Kumaraswamy　　Yaron Levi

Yale Li　　Dan Logan　　Scott Matsumoto

Rajiv Mishra　　Anish Mohammed　　Price Oden

Jairo Orea　　David Sherr　　Ken Trant

Ravila White　　Vern Williams　　Rob Wilson

CSA团队： Jim Reavis　　J.R. Santos　　Kendall Cline Scoboria

Evan Scoboria　　John Yeoh

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

前言

云安全联盟企业架构工作组发布“企业架构参考指南”第2版。通过此版本，读者可以看到CSA 企业架构2.3中每个域的详细说明。

CSA企业架构是安全、身份感知云基础架构的综合方法。EAWG利用了TOGAF、ITIL、SABSA和Jericho这四种行业标准架构模型。这种方法将同类的最佳架构范例结合到云安全的综合方法。EAWG通过将业务驱动因素与安全基础设施结合，增加了企业业务模型中云服务的价值取向。CSA企业架构参考美国国家标准与技术研究所的NIST SP 500-299 和 NIST SP 500-292。

本文档汇编了现有的企业架构定义，同时，对于即将发布的EAWG版本，包括CSA云控制矩阵（CCM 3.0.1）到EA的映射以及对企业架构本身的更新，都可以参考。

感谢读者

企业架构组组长

Jon-Michael C. Brook　　John Yeoh　　Michael Roza　　Jim Reavis

企业架构概述

共同的需求产生共同的解决方案。企业架构既是一种方法，也是一组工具，使安全架构师、企业架构师和风险管理专业人员能够利用一组通用的解决方案和控制措施。这些解决方案和控制措施满足了一系列共同的要求，风险管理者必须评估内部IT安全和云提供商控制措施的运营状态。这些控制措施以安全能力形式表现出来，旨在创建一个通用的路线图，满足业务的安全需求。

业务需求必须指导架构。在企业架构中，这些要求分别来自Sarbanes-Oxley和Gramm-Leach-Bliley之类的法规、ISO-27002之类的标准框架、支付卡行业数据安全标准以及COBIT等IT审计框架驱动的控制矩阵，所有这些都包含在云服务交付模型之中，例如软件即服务（SaaS）、平台即服务（PaaS）和基础设施即服务（IaaS）。

按照这些需求，根据架构框架最佳实践定义并组织了一套安全能力。（SABSA）从业务角度定义了安全模型。信息技术基础设施库（ITIL）指定了管理公司IT服务所需的模式，以及安全地管理这些服务的安全指南。杰里科论坛指定了技术安全规范，这些规范源于传统数据中心内技术环境向解决方案跨越多个数据中心的互联网环境转变的现实，而这些数据中心中一些由企业所有，另一些纯粹用外包服务。最后，开放组架构框架（TOGAF）提供了一个企业架构框架和方法，用于规划、设计和管理信息体系架构，最终形成一个通用框架，将安全架构师的工作与组织的企业架构集成在一起。

如何使用企业架构

企业架构可用于评估改进机会、创建技术采用路线图、识别可复用的安全模式，并根据一组通用能力评估各种云提供商和安全技术供应商。

评估机会

因为云安全联盟控制矩阵映射回各种法律和监管框架的现有安全控制需求，并且因为相同的矩阵映射到架构的安全能力，为了遵守适用的法规和最佳实践框架，公司可以很容易评估自己具备哪些能力。

创建路线图

在评估组织当前能力后，可以使用参考架构根据公司作为云消费者或云提供商的业务需求来指导需要投资的能力。例如，在基于云的解决方案中，物理安全控制和能力对云消费者不太重要，但对云提供商却更为重要。此外，该参考架构能力可用于整理组织中的技术标准集合，识别是否存在多种技术实现能力相同的领域，进一步证明这些技术功能可以被整合。反之，它也可以显示公司还有哪些尚未具备的标准技术能力。

识别可复用的安全模式

由于安全模式和最佳实践是围绕参考架构构建的，因此这些模式在公司内部和公司之间的共享将因为将它们联系在一起的通用功能模型而得到增强。供应商可以根据架构中的一组能力和控制措施验证解决方案，从而使消费者能够更信任和理解供应商的解决方案。

评估云服务提供商和安全技术供应商

已定义的控制措施是用简洁明了的合同要求措辞进行书写的，几乎不需要修改就可以作为服务合同和建议邀请书（RFP）的基础。

使用定义列表

以下每个领域表（BOSS、ITOS、TSS、SRM）都会细分出所有的域、组件组、子组和容器。领域组件列中每个元素开头的连字符指明了在图表中自然理解的企业架构层次。

领域组件	定义
1 域	顶层条目，将领域划分为不同域，如 SRM 中的治理、风险与合规（GRC），或BOSS中的合规。
2 组件组	第二层条目，将域划分为子主题，例如“BOSS->合规“下的审计计划，或”SRM->治理、风险与合规“下的合规管理。
3 组件子组	第三层条目（取决于组件，容器可能在此级别）。
4 容器	架构图中的最低层元素。

CSA 企业架构

这份《企业架构参考指南(第二版) 》对应CSA 企业架构的两种表示形式。 在云安全联盟的网站有更多交互形式的内容， 并且可以深入研究各部分内容。

业务运营支持服务 (BOSS)	信息技术运营与支持 (ITOS)	技术解决方案服务 (TSS)	安全和风险管理 (SRM)

图1: 交互式 CSA 企业架构图[1]

另外一种表示形式是Visio图适用于离线参考的情况。

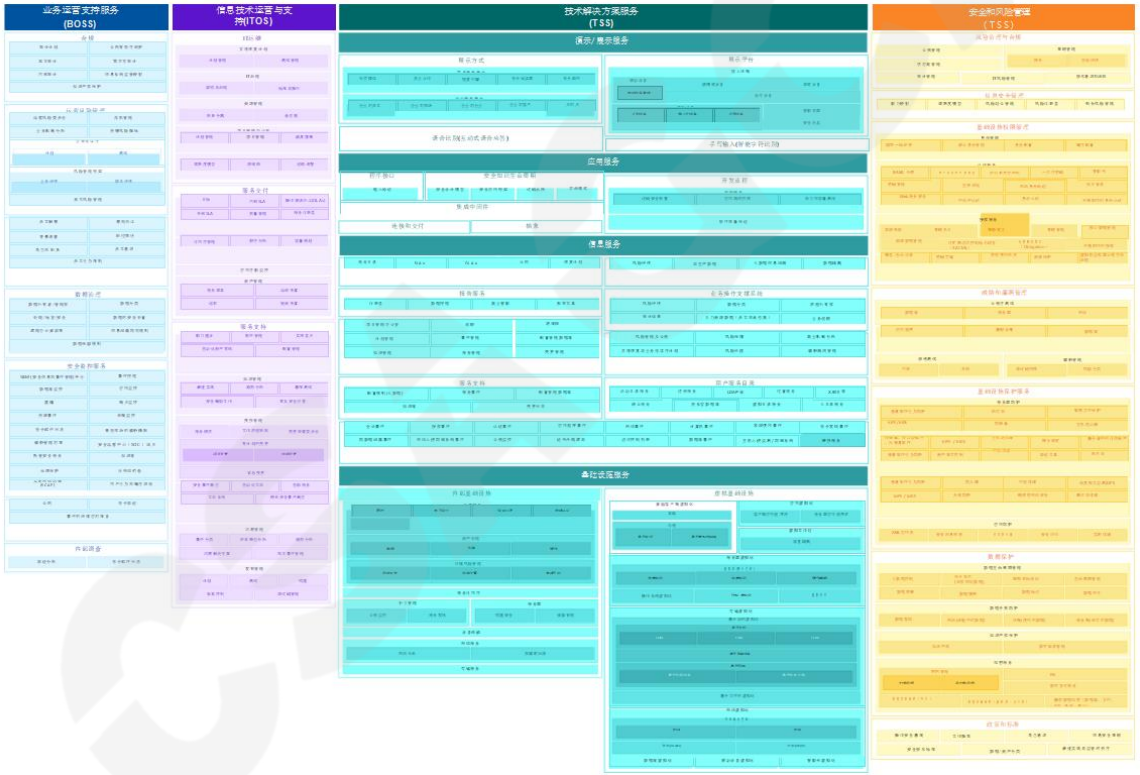

图2 企业云架构图表[2]

[1] https://ea.cloudsecurityalliance.org/index.php/explore/
[2] https://ea.cloudsecurityalliance.org/index.php/resources/

业务运营支持服务（BOSS）

业务伙伴

描述

BOSS域是对安全计划至关重要的所有公司支持的职能部门，如人力资源、合规和法务。它也是监控公司运营及其系统是否存在任何滥用或欺诈迹象的位置。

BOSS是基于最佳实践和参考框架设计的，在协调业务和将跨组织的信息安全实践转化为业务赋能因素方面颇有成效。

大多数安全架构只关注技术能力，错过了与业务建立动态协同与将被动实践转化为主动领域，从而使业务指挥中心具有提供有关信息资产和业务流程健康状况的相关信息的能力的机会。

当组织决定将服务与云提供商集成时，一个常见的问题是提供商提供的安全级别，以及在多租户模式上托管数据时的风险程度。该领域概述了除技术解决方案之外还必须考虑的因素，例如法律指导、合规和审计活动、人力资源以及侧重于预防欺诈的监控能力等方面。

BOSS组件	定义
1 合规	组织在确保了解相关法律、政策和法规并采取措施遵守这些法律、政策和法规的流程中预期实现的目标。
2 审计规划	审计规划确保配备充足的人员安排和审计，且为整体业务交付方面的一部分。
2 联系方式 权威维护	确保有关部门和关键业务合作伙伴的联系信息保持最新，以便在需要时正确无误，并强制实施企业角色级别的风险限制。
2 独立审计	独立审计能够有效地防止“自欺欺人”地确保对安全与合规相关的当前业务状态进行公正的审查。
2 第三方审计	确保所依赖的服务符合安全要求。
2 内部审计	在组织内部提供交叉检查机制。在较大的组织中，可能也会有一定程度的独立性。
2 信息系统监管映射	确保识别所有监管要求，并确保业务的合规工作考虑到这些要求。
2 知识产权保护	确保知识产权保护被确定为关键的业务驱动因素，并确保业务的合规性工作考虑到该点。
1 运营风险管理	运营风险管理从业务角度为风险评估提供了一个整体视角，使用风险管理框架有助于洞察组织面临的风险和威胁，并且该框架将提供评估、管理和

	控制整个组织不同风险的方法。 应设立运营风险委员会（ORC），定期讨论组织始终面临的威胁和合规情况。通常，该委员会的参与者由业务部门（即首席执行官、首席运营官、首席信息官、首席财务官）、合规部（首席风险官、合规官）和控制人员（审计、安全和风险管理）组成。 使用业务影响评估方法将有助于组织确定哪些流程对组织至关重要，并相应地规划以保护这些流程，确保适当的连续性计划，并使用关键风险指标衡量相关风险。 通过风险记分卡定期监控关键风险指标，集成来自安全监控服务的信息或信息服务领域整合的信息。
2 运营风险委员会	确保对所有已识别的业务风险给予运营方面的考虑。除非考虑真正的运营考量因素，否则不可能对风险进行充分的优先排序。
2 危机管理	组织有效应对危机的总体协调，总体目标是避免或最大限度地减少对组织的盈利能力、声誉或运营能力的损害。
1 业务影响分析	确保在风险管理流程中考虑业务影响，而不仅仅考虑技术方面风险。
2 关键风险指标	从管理层或执行层识别可能影响特定业务的关键风险因素是什么。
2 业务连续性	确保在风险管理流程中考虑业务连续性。不仅应解决业务连续性问题，还应解决业务恢复问题。
3 规划	准备业务连续性计划以及必要时付诸实施所需的所有步骤。
3 测试	测试业务连续性计划以确保其有效性。
2 风险管理框架	确保在业务范围内定义并记录可重复的流程。风险管理框架必须在其定义的业务环境中使用。
3 业务评估	确保对业务风险进行识别、记录，并确定适当的处理方法。
3 技术评估	确保对技术风险进行识别、记录，并确定适当的处理方法。
2 独立风险管理	由第三方进行风险评估，以从参考框架角度（即COBIT、ISO27001）、监管角度（即SOX、PCI）评估组织控制的成熟度。此类评估还可包括安全测试（黑盒、白盒、渗透测试）。
1 人力资源安全	本节重点关注与人员(员工、承包商或任何其他第三方)与组织人力资源职能互动相关的流程、最佳实践的安全和风险管理视角。
2 解雇	确保员工离职程序将离职员工在任职后滥用信息资产的风险降至最低的流程。该流程通常包括删除对电子帐户的访问、关闭VPN或外部电子邮件服务等。

2 雇佣协议	组织与员工、承包商、第三方用户和客户之间签订的所有合同协议，在授予对数据和服务的访问权限之前，这些协议明确规定了其雇佣或服务合同的条款和条件，其中必须明确包括负责信息安全的各方。例如隐私政策、知识产权协议、可接受的使用、网站条款和条件。
2 背景筛查	人员、承包商和第三方的背景核实必须到位，并且应与根据当地法律、法规和道德规范访问的数据分类相称。
2 职位描述	工作职责的明确定义有助于确定从事该工作的人员的数据访问要求，确保职员只有最低限度的访问权限。
2 角色和职责	将工作划分为具有不同角色和职责的多个职位，允许职责分离，以确保组织流程中的适当完整性。
2 员工意识	此能力将侧重于与提供意识的流程相关的材料和工具的管理，以确保遵守监管要求、安全策略和风险管理最佳实践，从而确保组织将拥有一个安全、合规和安全的工作环境。这方面的例子包括桌面清理、灾难恢复、在线培训、PII/PHI信息保护等。
2 员工行为准则	此能力旨在管理与组织的数据、资产和服务交互的人员之间的正式协议的生命周期。行为准则必须包括从监管角度看与组织相关的预期行为、信息安全策略和风险管理最佳实践。
1 数据治理	在组织管理应用程序、服务和企业信息集成活动之间的数据时，需要有一个定义良好的治理模型，该模型概述并寻找在整个IT基础架构（包括内部和外部服务即SaaS、PaaS、IaaS、ASP或其他））中如何处理、转换和存储数据的合规性（。 数据治理中包含的流程包括数据所有权、应如何对数据进行分类、数据/资产所有者对其应用程序和服务负有的责任，以及在整个生命周期内对数据的必要控制。
2 数据所有权 管理工作	此能力为在数据的整个生命周期中与数据交互的人员管理通信、职责和相关流程。与数据交互关联的角色包括数据所有者、资产托管人、数据用户、支持服务和代表。
2 数据分类	评估信息对业务的价值，并根据数据被未经授权的个人获取对业务的影响将其分配到不同级别的流程，如(受保护的、公开的、绝密的)。
2 处理/标记/安全策略	该能力管理与数据和包含数据的对象的标签、处理和安全相关的策略、流程和通信。
2 数据安全处置	确保数据被适当销毁，以防恢复(例如，通过数字取证技术)。此类销毁的

	文件记录应落实到位，并应包括在信息生命周期管理流程中。
2 清理桌面政策	一种公司政策，确保敏感信息不会被未授权用户公开查看或窃取。
2 信息防泄露规则	此能力管理与整个组织内数据保密和保护相关的数据泄露防护和控制相关的策略、程序和业务需求。这方面的示例包括内容管理、共享文件存储库和终端视角的数据使用。
2 数据保存规则	此能力根据业务和监管角度的需要，管理与保存数据(交易信息、电子邮件、文档图像、刷卡、在线浏览历史记录)相关的策略、程序或要求，然后进行安全处置。
1 安全监控服务	与整个组织的主动式安全和风险管理态势感知相关的所有功能，以业务为重点，防止内部或外部攻击、滥用权限和数据丢失，同时保持对组织数据和访问的适当监控，无论这些服务在何处分配或管理（云、内部、托管等）
2 安全信息事件管理平台（SIEM）	安全信息和事件管理平台收集、关联、报告多个安全信息源，以保持态势感知。
2 事件挖掘	对历史事件进行统计分析，确定正常和异常行为模型。
2 数据库监控	此能力是数据库管理系统相关事件的集合，包括登录、查询、处理和管理活动。
2 应用监控	该能力是应用程序相关事件的集合，包括登录、对敏感数据的访问、处理、管理活动。
2 蜜罐	一种真实的或虚拟的系统，通过配置真实的生产系统的镜像来吸引和检测入侵者。
2 终端监控	收集与最终用户使用设备相关的事件。
2 事件关联	分析一个源中的事件并将其与相同或其他源中的事件关联以获取附加信息或检测活动模式的流程。
2 云监控	在应用程序堆栈的所有层上收集与云解决方案提供服务的使用相关联的事件。
2 电子邮件记录	监控电子邮件内容以检测数据丢失、恶意软件传播或其他基于电子邮件的威胁。
2 安全运营中心门户	由安全运营中心维护的仪表盘应用程序，提供组织安全状态的总体可见性。
2 对抗威胁管理	管理威胁和对抗策略的整个流程。
2 市场威胁情报	由分布式IDS传感器收集并由安全公司分析的网络情报。此外，这种能力可以巩固来自行业同行的威胁情报(例如，HITRUST, NSA的商业分支机构

	等)。
2 安全托管服务	为组织提供部分或全部安全运营能力的外包协议。
2 知识库	一个能够使安全运营中心高效响应事件的，有关组织基础设施和运营的知识库，
2 品牌保护	监控对组织品牌构成风险的外部实体和活动，如冒名顶替者网站、蓄意错误拼写等。
2 防钓鱼	能够检测针对组织用户的网络钓鱼攻击，如入站网络钓鱼电子邮件。
2 实时网络防护（SCAP）	安全内容自动化协议是一个持续的保障流程，可实时验证安全策略和程序的合规性。
2 用户行为与画像	有关用户的事件和信息的集合，用于分析和识别正常和异常行为模式，如特定用户或角色使用应用程序的情况。
1 内部调查	内部调查关注的是确定事实真相和政策或刑事调查的影响。这一流程涉及欺诈检测、预防和取证调查。
2 取证分析	取证分析涉及保存、识别、提取和分析与违反政策或刑事犯罪的事实问题相关的潜在证据价值项。
2 电子邮件记录	确保按照监管合规或支持诉讼的要求记录和保存所有电子邮件流量的流程和程序。
1 法律服务	当安全事件发生时，组织对法律顾问的需求至关重要。其中包括几项能力，可以帮助法律顾问领导合规活动、处理诉讼以及跟踪整个组织的预防意识。
2 合约	两个或多个当事人之间的协议，其目的是创造一项或多项法律义务。
2 电子档案查询（电子发现）	电子档案查询涉及如何识别、保存和生成对已经计划或正在进行的诉讼作出响应的数据。
2 应急响应法律准备	确保识别、收集和保存相关信息的流程和程序，支持未来有关该事件的诉讼。

示例

安全监控工具提醒分析师，客户提款交易操作的发起方是 IT 部门的工作站而不是客户联络中心。在人力资源部和法务部的帮助下进行一项特别调查显示，确定是一名心怀不满的系统管理员持续窃取公司信息。

提供的服务

合规性：合规能力的重点是跟踪内部、外部、第三方（如客户）人员行为，执行审计活动及发现相关问题。为了合规工作的顺利开展，有必要建立一个通用资料库，使组织能够跟踪和修复这些发现所概述的技术或运营差距。

审计活动包括制定审计年度计划，精简审计流程，防止重复审计。

监管映射流程将帮助组织协调和简化各种能力或流程生成的控制证据，以便存储在风险注册表（信息服务域）中。

相关组件：

- 2 审计计划
- 2 联系人/权威维护
- 2 独立审计
- 2 第三方审计
- 2 内部审计
- 2 信息系统合规映射
- 2 知识产权保护

数据治理：当组织管理应用程序、服务和企业信息集成活动之间的数据时，需要有一个定义明确的治理模型，指导包括内外部服务（即SaaS，PaaS，IaaS，ASP或其他）的整个IT基础设施中，数据的合规销毁、转换和存储。作为数据治理一部分的流程，包括数据确权，数据分类以及数据/资产所有者对其应用程序和服务的责任划分，以及整个生命周期中对数据的必要控制。

相关组件：

- 2 数据所有权/管理权
- 2 数据分类
- 2 处理/标签/安全策略
- 2 数据安全销毁
- 2 明确的桌面政策
- 2 防止信息泄露规则
- 2 数据保留规则

运营风险管理：运营风险管理从业务视角提供了风险评估的整体视角，使用风险管理框架可以洞察组织面临的风险和威胁。框架将针对组织面临的不同风险提供风险评估，管理和控制方法。

应该设立运营风险委员会（ORC）定期讨论组织长期面临的威胁和合规情况。通常，该委员会参与者按照业务人员（即CEO，COO，CIO，CFO），合规人员（CRO，合规官员）和控制人员（审计，安全和风险管理）分组。

业务影响评估方法的使用将有助于组织确定对组织至关重要的流程，并制定相应的保护计划，确保适当的连续性计划，并通过关键风险指标衡量相关风险。

可以通过风险记分卡定期监控关键风险指标，整合来自安全监控服务的信息或信息服务领域的综合信息。

相关组件：

- 2 运营风险委员会
- 2 危机管理
- 2 业务影响分析
- 2 关键风险指标
- 2 业务连续性
- 3 规划
- 3 测试
- 2 风险管理框架
- 3 业务评估
- 3 技术评估
- 2 独立风险管理

人力资源安全：如果缺乏针对人员这一最核心资产的正式控制措施、安全意识和指导方针，组织可能会经常发生安全事故和违规行为。

本节旨在确保组织制定正式程序，行为准则，人员筛选和其他最佳实践，采用了第三方云计算服务的组织更是如此。

相关组件：

- 2 人员离职
- 2 就业协议
- 2 背景审查

- 2 职位描述
- 2 角色和责任
- 2 员工意识
- 2 员工行为准则

安全监控服务：安全和可用性监控服务隶属于业务运营和支持服务，其核心任务是确保业务安全而不是聚焦于事件或硬件。通常的错误做法是未将安全功能聚焦于在流程背后的业务操作、活动和人员行为上。安全监控服务的目标应从传统的基础架构监控转变为以业务运营为中心，专注于欺诈防范，与业务战略保持一致，关注业务影响和运营需求。

组织通常只将监控活动聚焦在响应模式上，失去了成为业务合作伙伴的机会。通过使用监控服务，收集有关员工行为知识，企业可以获得流程改进的新契机。相比其他员工，有些员工比其他人更容易接触到许多机构最关键的信息，例如客户数据，信用卡信息等。如果安全监控服务侧重于这些用户及其行为，则可以防止潜在的欺诈活动。

随着监控服务开始变得不那么被动，而是更主动化，安全监控服务的重点将从内部威胁转向外部威胁。该架构概述了基于网络情报的多种能力，旨在防止威胁演变为安全事件。

相关组件：

- 2 SIEM平台
- 2 事件挖掘
- 2 数据库监测
- 2 应用程序监控
- 2 蜜罐
- 2 端点监测
- 2 事件相关性
- 2 云监控
- 2 电子邮件日志
- 2 SOC门户
- 2 反威胁管理
- 2 市场威胁情报
- 2 安全服务托管

- 2 知识库
- 2 品牌保护
- 2 反钓鱼
- 2 实时互联网工作防御（SCAP）
- 2 用户行为和侧写描述

法律服务：随着安全事件的发生，法律顾问对组织至关重要。法律顾问可指导合规工作/诉讼处理，以及跟踪和提升组织的法律风险防范意识。

本节还包括和详述了有助于提高、跟踪和管理合规性的功能。

相关组件：

- 2 合同
- 2 电子取证
- 2 事件响应的法律准备

内部调查：内部调查的作用因组织而异；一些公司让信息安全团队执行取证活动，而更成熟的公司可能会有一个专注于内部和/或外部欺诈活动的专门团队。

为了更好地协助调查人员，这些团队的能力以帮助开展安全事件响应、网络情报分析、遵守法律、安全监控、人力资源和信息安全团队管理等为导向。

相关组件：

- 2 取证分析
- 2 电子邮件日志

与其他域的关系

业务运营支持服务定义了IT运营支持服务、演示服务、应用程序服务、信息服务、基础设施服务以及安全和风险管理所要支持的高级战略要求。BOSS体现了云消费者的业务方向和目标。BOSS体现在合规目标、法律目标、人力资源要求、运营风险容忍度和安全监控服务中，这些服务是满足客户的服务级别目标和司法管辖权法定要求所必需的。

BOSS域致力于使ITOS和SRM域与业务所需的战略、能力和风险组合保持一致。

信息技术运营与支持（ITOS）

IT管理过程

ITOS就是IT部门。它是发现问题时接听电话的服务台；是在半夜里协调变更并推进实施的团队；是即便是在灾难事件发生时仍保持系统继续运行的规划与流程。

描述

ITOS概述了IT组织支持业务需求时所需的全部必要服务。该领域提供了与行业标准和最佳实践的对标（PMBOK、CMMI、ISO/ IEC 27002、COBIT和ITIL v3），从两个主要角度提供参考，使组织能够支持业务需求。

然而，技术组件之间的关系并不是与PMBOK、ISO/IEC 27002、CMMI、COBIT和ITIL v3中描述的流程接触点一一对应。

领域组件	定义
1 IT运营	IT运营定义了IT组织的组织结构和技能要求，以及一组标准的运营管理程序和实践，允许组织管理IT运营及相关的基础设施。 IT运营能力的目标是对齐业务和IT战略、项目和技术组合管理，并需要确保贯穿IT体系的架构治理。
2 灾难恢复计划（DRP ）	该文档定义了在业务中断时管理业务恢复流程所需的资源、操作、任务和数据。该计划用于在指定的灾难中，帮助恢复目标及业务。
3 计划管理	确保DRP持续获得更新以反映业务及关键功能变更的整体流程。
4 测试管理	管理对DRP进行定期测试及后续审视的整个流程。
2 IT治理	本能力涵盖了以确立决策权和责任框架为导向的所有流程和组件，并鼓励IT服务生命周期中的良好行为。
3 架构治理	一组工具，可用于开发广泛不同的架构透视图，通常集成为一个通用的架构框架。 治理流程必须包括以下元素: • 描述一种方法，用一组构建模块定义信息系统 • 展示构建模块是如何组合在一起的 • 标准列表的技术路线图 • 包含一组工具，并执行一份技术标准清单 • 提供通用词汇 确保现有解决方案和新IT服务与框架保持一致的治理流程。
3 标准与指南	此能力是对架构治理的补充，概述了所有的技术标准，以及关于如何在整个组织中使用它们的指南。这些标准应包括与组织的战略、行业

	标准、原则、可在整个组织中重复使用的模式保持一致，以及确保一致实施和采用所需的其他要素。
2 资源管理	资源管理功能能够处理将资源准确分配给IT服务交付功能的问题。它被认为是与项目管理分离的共享服务，因为相同的模式可以应用于解决操作、生产和紧急资源分配问题。资源管理包括了协助资源集中、预测和平衡的技术。其他资源管理功能则与人力资源管理解决方案的关系更为密切。该服务为BOSS领域的成本计算、预测和计划活动提供了有价值的输入。
3 职责分离	职责分离（SoD）是指一项任务需要一人以上完成，防止欺诈和错误。
3 分包商	为组织提供服务的合同所绑定的所有第三方虽然不被视为员工，但可以访问整个公司的各种资源和数据。本能力的目的是管理这些分包商，以及和人员进场及释放相关的流程。
2 项目管理办公室（PMO）	项目管理办公室（PMO）是定义和维护流程标准的部门或团体，通常与组织内的项目管理有关。项目管理办公室致力于在项目执行的流程中引进“重复经济”并使其标准化。PMO是项目管理与执行实践相关文档、指南、度量指标的来源。在一些组织中，它被称为项目集管理办公室）。
3 项目集管理	项目集管理在事件开始整个周期之后通过修复流程处理事件。项目集管理架构与服务台交互。项目集管理提供了高级的根本原因分析工具和技术，以及与信息存储库的接口，以在环境中执行趋势分析和预防服务。
3 项目管理	与项目管理办公室相关的所有流程、制品和方法，用于跟踪项目（最佳实践包括PMI知识体系等）。
3 修复	这个能力侧重于修复对企业造成影响的现有差距或问题的项目。建议使用修复仪表盘跟踪高级管理层的进度。
2 项目组合管理	本能力专注于为企业规划、跟踪、优先考虑当前和未来的项目和计划。
3 成熟度模型	比较行业最佳水平，跟踪企业的能力实践、基准和成熟度，并显示一段时间后的进展。
3 路线图	在技术组合（包括安全路线图）中变更能力及解决方案的战略方向和计划，以实现期望的未来状态（例如，持续创新、能力集成等)。这个流程必须与业务策略保持一致。
3 战略匹配	以流程为导向理解业务需求和战略，并确保信息技术和安全与风险管理战略一致，以支持路线图中的目标。
1 服务交付	服务交付功能处理对维持不间断技术服务至关重要的技术。这类服务通常包括更适合技术人员使用的服务，如可用性管理、服务级别管理、服务连续性和容量管理。

	然而，尽管这些类别本身就足以满足ITIL服务管理指南，还有一些其他的IT规程是与服务支持和交付紧密结合的，例如项目管理和服务供应。 服务交付主要关注业务需要信息技术提供的主动和前瞻性的服务，以向业务用户提供充分的支持。它关注的是作为IT服务客户的业务。（该规程由以下流程组成，在下面的小节中进行解释。）
2 服务级别管理	本功能负责确保所提供服务水平与合同义务持续地保持一致。
3 目标	可度量的目标，用于对照服务级别协议来对服务及交付的绩效表现进行评估。
3 内部服务级别协议（SLAs）	组织内部的服务级别协议，对要交付的特定服务及对交付进行治理的绩效标准进行规定。
3 运营级别协议	必须定义运营级别协议，以支持区域或组织之间的服务级别协议(SLA)。此能力致力于从操作角度跟踪与特定SLA相关流程之间的有效集成。
3 外部服务级别协议（SLAs）	与外部实体的服务级别协议，规定要交付的特定服务及对交付进行治理的绩效标准。
3 供应商管理	本能力对管理供应商关系的流程进行治理，相关流程包括选择、审查、评估、安全和合规。通常，这些流程还包括风险评估，以及对供应商可以访问、处理、托管或查看的数据类型（考虑到他们在风险剖面）、财务及其他领域的成熟度）和连接类型进行评级。
3 服务仪表盘	所有SLA、OLA和合同都应该关联并定义关键绩效指标、关键目标指标和关键风险指标，必须定期跟踪这些指标以管理这些协议。服务仪表盘应该提供这些测量指标以助决策。
2 信息技术韧性	信息技术实体及其服务在发生意外事件（如电源中断、网络连接中断等）时能够持续提供充分服务的属性。
3 可用性管理	管理（内部和外部）用户的服务可用性的总体流程。
3 韧性分析	本流程评估组织在发生各种事件（如断电、网络连接中断等）的情况下继续提供服务的能力。
3 容量规划	容量规划确保资源和工作负载在当前和未来均是相称的。
2 应用程序性能监控	当应用程序性能度量结果（例如响应时间）超过服务水平目标时，提供告警、增量资源供应等功能。
2 资产管理	本部分管理由信息技术组织提供的配置项和服务的所有财务状况。
3 服务成本计算	该内部职能分析交付某一特定服务的应计总成本，使收入（无论是外部或内部的收款）足以支持交付该项服务。
3 运营预算编制	用于确定日常投资的规划流程，例如对现有服务、基础设施、应用程序，以及允许组织运行的其他相关因素的维护。通常来说，成本分摊流程用于在中到大型组织中分配这些成本。

3 成本分摊	此流程管理组织内某个区域或用户的IT服务消耗，并计算这些服务的相关成本，包括人员、技术和支持材料。该流程确保对总体拥有成本和每项服务的成本（即桌面支持、网络服务、安全服务等）有清晰的了解。
3 投资预算	该计划流程用于确定组织的长期投资（如新的基础设施、现有服务和基础设施的更换）新数据中心、新产品或服务、研究、应用程序开发、安全性和项目部署是否值得投入。通常，成本效益分析是投资预算流程的一部分。
1 服务支持	服务支持的重点是信息技术服务的用户，主要是确保他们能够访问适当的服务以支持业务功能。 对于业务、客户和用户来说，这是服务请求的入口点。他们通过以下方式参与服务支持： •要求变更 •需要沟通、更新 •有困难、疑问。 服务台是客户记录问题的唯一联络点。如果有直接解决方案或会造成事故，服务台将尝试解决问题。事件启动了一系列流程：事件管理、问题管理、变更管理、发布 管理和配置管理（有关详细信息，请参阅以下部分）。使用配置管理数据库（CMDB）跟踪此流程链，该数据库记录每个流程，并创建输出文档以跟踪（质量管理）。
2 配置管理	配置管理架构很容易被认为是服务交付的“主干”。配置管理架构提供基本技术支持 用于自动发现资产、许可证管理、逻辑库存、物理库存、电子软件分发和软件配置。配置管理严重依赖于称为配置管理数据库（CMDB）的信息架构组件，这是一个ITIL术语，是所有配置项的本源。 就CMDB而言，比配置项存储库（CI）更重要的是定义配置项的技术关系索引或技术元数据的概念 每个项目之间的关系。CI之间存在着多对多的逻辑关系，如软件应用程序支持服务的物理合同。
3 容量规划	确保提供服务的容量（CPU功率、网络带宽等）持续符合该服务需求的流程。
3 软件管理	应用管理活动规划、协调、测量、监控、控制和报告，确保软件的开发和维护是系统化、规范化和量化的。这包括在不同的时间点进行测量，系统地控制配置的变更，并在整个系统生命周期内保持配置的完整性和可追溯性。
3 物理资产	此流程跟踪整个信息技术组织的所有物理组件，还跟踪这些资产的所有权和保管权。
3 自动资产发现	此功能允许配置管理流程识别整个基础架构中的新资产和不断变更的资产，并维护现有的配置项清单。通常，必须有一个流程正式确定这些新资产的所有权。
3 配置管理	配置管理用于管理资产（服务器、存储阵列、网络设备等）配置的流程和步骤，确保部署的配置符合策略、标准和指导方针的规定。

2 知识管理	通常情况下，随着事件的解决和根本原因分析，大量的知识可能会丢失，当其中一些事件在一段时间内再次出现时，就会导致延迟。 知识管理流程积累了有关事件如何解决或根本原因修复的信息，一旦收集到这些信息，这些信息就会转化为常见问题或自助服务功能，用户和技术支持社区可以重用这些功能解决IT服务的问题。
3 最佳实践	制定并遵循多个组织以高效方式执行的标准方式的流程，该流程包括方法、技术或框架，这些方法、技术或框架始终显示出优于通过其他方式实现的结果，并用作基准。随着改进的发现（使用经验教训等机制），这些实践可以演变成更好的方法。 这种能力旨在作为强制性立法标准的替代品保持交付质量，并可以以自我评估或基准为基础。
3 趋势分析	从项目咨询、政策问题、最终用户培训反馈等方面分析安全方面的帮助请求，识别常见问题和知识库所需文档的新领域。
3 基线管理	确定给定的实践领域中的领导者，并将组织的实践与领导者和其他组织比较的流程。这有助于组织了解他们在知识、能力和能力方面与行业内其他组织的比较。
3 安全工作辅助	由于安全标准和模式是在整个组织中创建的，因此应该包括可以帮助员工以一致的方式遵守法规要求或安全标准的指导方针和流程。
3 安全常见问题	知识管理流程的成果之一是为员工经常提出的问题建立标准和一致的答案。此流程记录了与信息安全和合规性相关的问题。
2 变更管理	变更是一种主要的模式，充当请求、发布和配置/供应之间的中介。变更管理允许范围管理、影响分析以及变更计划。变更管理从数据维护的角度为配置管理提供了一个主要输入，使应用程序数据保持最新。
3 服务供应	实现新配置项或变更现有配置项的流程。
3 审批工作流	审查所请求变更的流程，确保适当性，并从必要的审查人员处获得继续授权。
3 变更顾问委员会（CAB）	一个跨职能团队，负责确保仔细考虑和审查环境的所有变更，尽量减少对用户和现有服务的影响。
3 计划变更	计划变更是指在需要实施之前很早就确定的变更。这些变更经过仔细考虑并充分记录。
4 项目变更	由项目产生的计划变更。项目变更是由于实施或业务需求的变更而发生的。
4 运维变更	由现有服务的持续维护活动导致的计划变更。
3 紧急变更	为修复生产服务或应用程序上的问题而生成的变更。
2 事件管理	事件管理的架构模式包括故障查询和事件分类服务。事件管理与架构的其他区域直接交互（如服务台）、间接交互（通过处理公共数据）或异步交互（作为事件管理业务流程的一部分）。事件开始于

	人类的电话事件、环境中检测到的错误（通常是来自系统管理域的事件关联的结果）或来自其他应用程序的事件消息。
3 安全事件响应	对明确的安全事件作出响应的流程和程序。
3 自动生成工单	根据事故系统自动生成事件的能力。
3 自服务	此能力允许组织中的任何人报告事件并开始事件管理流程。
3 工单	创建事件记录的流程，可在事件的整个生命周期中进行跟踪。这些事件应由唯一标识符引用。
3 跨云安全事件响应	跨云安全事件响应由于云计算的普遍性，一个安全事件可能会在多个云实例中检测到或影响到多个云实例。事件响应计划必须包括处理跨云安全事件的流程和步骤。
2 问题管理	问题管理的目标是通过分析问题以防止其再次发生，从而将问题对组织的影响降至最低。
3 事件分类	事故已经发生或正在发生无法通过一个事件表示。事件分类提供了分析和事件关联的流程，提供事件发生的评估和置信度估计。
3 根因分析	事件响应的重要组成部分，超越了事件的表面细节，确定事件的根本原因（例如，缺少的补丁可能会导致成功入侵，但根本原因分析可能会显示，该易受攻击的服务无论如何都不应该运行）。
3 趋势分析	作为根本原因分析的一部分，这一能力将使组织能够识别 某些事件或根本原因将影响整个信息技术服务。应始终跟踪所有这些趋势。也可以是评估资源使用的总体趋势、事件发生情况等的持续流程。
3 问题解决	识别配置项的适当变更和/或解决问题根本原因所需的流程，最大限度地降低再次发生的可能性。
3 孤立事件管理	对无人负责的事件的识别，以便使用适当的资源解决问题。
3 发布管理	发布管理架构是一组概念模式，支持将预生产技术资源转移到生产中。预生产包括证明特定资源 适用于技术、业务和运营环境，且不超过特定任务的风险状况的所有活动。重要的发布管理模式包括用于发布计划、发布验收和审核的模式。发布管理作为流程和技术扮演着重要的角色，为请求、变更和配置管理流程和架构提供了一个重要的控制点。
3 发布规划	作为发布管理的一部分，应制定详细的发布时间表及功能，以便将许多变更请求捆绑到单个变更日历中。
3 测试	测试与发布相关的所有变更的流程，确保它们满足要求并且不会中断现有服务。这是一个通过发布管理协调的质量保证功能。
3 构建	将源代码和配置编译成一个或多个可部署单元并交给变更管理流程的流程。
3 版本控制	跟踪源代码、配置项和文档的所有变更并为这些变更分配版本标识

	符的流程。
3 源代码管理	源代码的版本控制形式，允许对软件进行版本控制，将软件分为不同的版本，并控制对软件的访问。

示例

一名员工收到一封可疑电子邮件，她认为其中可能包含恶意软件程序。员工通知服务台。服务台会开启一个安全事件，响应团队会阻止发件人，识别其他受影响的用户，并恢复可能已经造成的任何损坏。

提供的服务

IT运营：IT运营定义IT组织的组织结构、技能要求以及标准运营管理程序和实践，以允许组织管理IT运营和相关基础设施。

IT操作功能是面向业务和IT战略的。项目和技术组合的管理确保了整个IT领域的架构治理。

相关组件:

- 2 灾难恢复计划（DRP）
- 3 规划管理
- 3 测试管理
- 2 IT治理
- 3 架构治理
- 3 标准与指南
- 2 资源管理
- 3 职责分离（SoD）
- 3 外包商
- 2 项目管理办公室（PMO）
- 3 项目群管理
- 3 项目管理
- 3 流程管理
- 3 修复措施
- 2 项目组合管理

- 3 成熟度模型
- 3 路线图
- 3 战略调整

服务交付：服务交付涉及维持不间断技术服务的关键技术。这类服务通常包括如：可用性管理、服务级别管理、服务连续性和容量管理等更适合技术人员使用的服务。

尽管这些服务类别本身就足以满足ITIL服务管理指导方针，也常于其他几个IT支持和交付服务紧密结合，例如，项目管理、服务准备和项目组合管理。

服务交付主要关注业务需要信息技术提供的主动和前瞻性服务，向业务用户提供充分的支持。它关注的是作为IT服务客户的业务。

相关组件:

- 2 服务水平管理（SLM）
- 3 目标
- 3 内部SLA
- 3 运营级别协议OLAs
- 3 外部SLA
- 3 供应商管理
- 3 服务仪表盘
- 2 信息技术弹性
- 3 可用性管理
- 3 弹性分析
- 3 容量规划
- 2 应用性能监控
- 2 资产管理
- 3 服务成本
- 3 运营预算
- 3 资源成本分摊
- 3 投资预算

服务支持:服务支持以用户为中心，主要关注确保用户能够访问适当的服务支持业务功能。

对于业务客户和用户，服务支持是服务请求的入口点。用户通过以下方式参与服务支持:

- 需求变更
- 沟通、升级请求
- 困难咨询及答疑

服务台是客户记录问题的唯一联络点。如果有直接的解决方案或自动创建事件，服务台将尝试解决问题。事件启动了一系列流程：事件管理、问题管理、变更管理、发布管理和配置管理(有关详细信息，请参阅下面的部分)。使用配置管理数据库(CMDB)跟踪这一流程链，该数据库记录每个流程并创建输出文档以供跟踪(质量管理)。。

相关组件:

- 2 配置管理
- 3 容量规划
- 3 软件管理
- 3 物理库存
- 3 自动化资产发现
- 3 配置管理

事件管理:事件管理的架构模式包括故障记录和事件分类服务。事件管理与架构的其他领域交互。形式很多样，可以是直接的，如：服务台；或间接的，如：通过操作公共数据进行；也可以是异步的，如：将事件管理作为业务流程的一部分，事件其生命周期的开始方式一般被动触发，或来自人工的电话事件、环境中检测到的错误(通常是由于来自系统管理域的事件相关性)，或通过另一个应用程序的事件消息传递。

相关组件:

- 3 安全事件响应
- 3 自动化工单
- 3 自助服务
- 3 工单流转
- 3 跨云的安全事件响应

问题管理: 问题管理在事件通过修复流程开始循环后处理事件。 问题管理架构与服务台交互。问题管理提供先进的根本原因分析工具和技术，并与信息存储库接口以在环境中执行趋势和预防服务。

相关组件:

- 3 事件分类
- 3 根本原因分析
- 3 趋势分析
- 3 问题解决方案
- 3 孤立事件管理

知识管理: 通常，随着事件得到解决并进行根本原因分析，流程中大量知识可能会丢失。从而导致事件处理效率低下，甚至其中一些事件会随着时间的推移再次出现。

知识管理流程主要关注积累根本原因、解决方案等信息。一旦收集了这些知识，就转换为用户和技术支持社区可以复用的常见问题或自助服务功能，解决常见的IT服务问题。

相关组件:

- 3 最佳实践
- 3 趋势分析
- 3 基线
- 3 安全辅助工具
- 3 安全常见问答FAQ

变更管理：变更管理是一个重要的模式，充当请求、发布和配置/供应之间的中介。变更管理允许范围管理、影响分析以及变更的调度。变更管理从数据维护的角度提供了配置管理的主要输入之一，保持应用程序数据的最新。

相关组件:

- 3 服务供应
- 3 审批工作流
- 3 变更顾问委员会（CAB）
- 3 计划变更
- 4 项目变更
- 4 操作变更
- 3 紧急变更

发布管理：发布管理架构是一组概念模式，支持将预生产技术资源转移到生产环境中。预生产

用以证明待发布资源的技术、业务和操作环境妥帖，且验证特定任务的所有活动不会超出风险范围。重要的发布管理模式包括发布计划、发布验收和审批流程。发布管理在ITOS（流程和技术集）中扮演至关重要的角色，为请求、变更和配置管理流程和架构提供了重要的控制点。

相关组件:

- 3 计划
- 3 测试
- 3 构建
- 3 版本控制
- 3 源代码管理

与其他领域的关系

使用ITOS分析服务(如数据仓库、数据集市和通用操作数据存储)是实现有效业务操作服务的关键。

- ITOS支持业务运营支持服务，以保持业务和IT之间的战略一致性。
- ITOS实现了表现、应用、信息和基础设施服务。

技术解决方案服务(TSS)

描述

IT解决方案可以被认为是一个技术栈：在顶层，实际上是用户和协议栈以及应用程序的互动。协议栈和应用程序接收到互动之后，把数据传输到底层的电脑和网络，并在此进行数据操作。四个技术解决方案领域(表现服务、应用服务、信息服务和基础设施服务)基于用于构建这些解决方案的标准多层架构。

展示层服务

与用户互动

展示层是你去网上银行时看到的网站。它是你打电话给航空公司预订系统时电话里的声音，或是你远程订购时的移动平台。

描述

展示层服务域是终端用户与IT解决方案互动的地方。展示层的安全要求将因用户的类型和所提

供服务类型而有所不同。例如，企业对消费者（B2C）网站与社交媒体网站有不同的安全问题。安全要求也将根据终端用户使用的终端类型而有所不同。

展示层服务组件	定义
1 展示模式	展示模式服务关注的安全问题因用户和服务类型差异而不同。有两个主要类型，一种是消费者服务平台，如社交媒体、协作、搜索、电子邮件和电子阅读器；另一种是企业服务平台，如企业对消费者（B2C）、企业对雇员（B2E）、企业对企业（B2B）等。
2 消费者服务平台	这个容器容纳了各种面向消费者而不是面向企业的展示模式。
3 社交媒体	一种展示模式，这种模式下平台将用户联系在一起，交换信息、照片等，以建立网络，进行一对一或小组沟通。
3 协作	一种面向协同工作的展示模式（如项目协同工作或文档协同工作）。协作应用程序共享文件，允许多个编辑者编辑文档，并经常为其参与者提供日历、任务跟踪和信息传递。
3 搜索	一种展示模式，允许用户查询单个网站或多个网站中与查询条件有关的内容。这种模式经常被用作整个互联网或网站内导航的初始形式。
3 电子阅读器	一种模拟阅读书籍或其他印刷材料的展示模式。
3 电子邮件	能够展示消息收件箱，并允许用户发送新信息或将旧信息整理到文件夹中的展示模式。通常情况下，电子邮件与日历功能和联系人管理功能结合。
2 企业服务平台	这个平台面向企业用户或者是企业的合作伙伴或者用户。
3 B2E	企业对雇员（B2E）应用允许企业的雇员处理公司的业务。
3 B2M	企业对移动（B2M）应用程序利用移动设备，如智能手机，使客户或员工能够在任何地方、任何时间与企业的系统互动。
3 B2B	企业对企业（B2B）应用允许企业批量交换常见的交易，例如采购订单、发票等。
3 B2C	企业对消费者（B2C）应用是在线企业的一种形式，允许其客户通过互联网与企业开展业务。
3 P2P	点对点（P2P）应用允许企业内的用户直接连接到对方，交换即时信息或文件。
1 展示层平台	展示层平台服务的重点是不同类型的终端，这些终端是最终用户用来与与解决方案互动的，如台式机、移动设备（智能手机、平板电脑）、便携式设备（笔记本电脑）或特殊用途设备，如医疗设备或智能电器。演示平台还包括不同的交互技术，如语音识别或手写识别，可用于与解决方案的交

	互。
2 终端	终端是用户在使用IT解决方案时与之互动的设备。它们之所以被称为终端，是因为它们处于解决方案的边缘，是技术与人相遇的地方。
3 移动设备	移动设备包括智能手机、PDA和平板电脑。
4 移动设备管理	移动设备管理使企业能够管理移动终端的安全，类似于管理台式机的方式。安全功能包括锁定或擦除被破坏的设备，向设备推送软件更新，以及在允许设备连接到企业网络之前要求启用某些安全功能。
3 便携式设备	一类设备，如笔记本电脑全功能或几乎全功能的计算机，具有与台式（固定）设备相同的操作系统。
3 固定设备	不易移动且只能从一个地方使用的装置。
3 医疗设备	本架构内容中提及的医疗设备指的是一种与网络连接的设备或能够下载数据的设备，以便与病人佩戴的设备（如监测设备）进行信息交流。
3 台式电脑	台式机是典型的计算机，通常在桌上或桌下，包括CPU、显示器、键盘、鼠标和其他外围设备。
4 公司所有的	由企业购买、拥有和管理，并发放给员工使用或由客户租用的设备。
4 第三方	第三方设备由一家企业拥有，提供给另一家企业使用。
4 公共信息亭	公共信息亭是一种设备，通常是个人电脑，由多人在一个共享空间使用。
3 智能应用	主要不用于计算，但包括与网络连接以提供其状态的实时更新或被远程控制的设备。
3 安全沙箱	在自定义代码或第三方代码与基础系统之间提供信任关系抽象的隔离环境。允许应用程序在一个不影响彼此或主机操作系统的环境中运行，并允许企业拥有一个具有敏感数据的应用程序的管理安全控制区域。
1 语音识别（IVR）	语音识别可以将语音翻译成计算机输入。交互式语音应答（IVR）系统提供了用户与这个系统互动的选择菜单。
1 手写识别（ICR）	手写识别或交互式字符识别（ICR）可以将手写文本翻译成计算机输入。

示例

移动设备在本地存储的数据有跟随设备丢失的风险，而共享的公共信息亭则存在后续终端用户访问先前用户数据的风险。

提供的服务

展示模式：展示模式服务侧重于基于用户和服务类型不同的安全关注点。两大主要类型是消费者服务平台，如社交媒体、协作、搜索、电子邮件、电子阅读器和企业服务平台，如企业对消费者 (B2C)、企业对员工 (B2E)、企业对企业 (B2B) 等。

相关组件：

- 2 消费者服务平台
- 3 社交媒体
- 3 合作
- 3 搜索
- 3 电子阅读器
- 3 电子邮件
- 2 企业服务平台
- 3 企业对员工(B2E)
- 3 面向市场营销的电子商务企业(B2M)
- 3 企业对企业(B2B)
- 3 企业对消费者(B2C)
- 3 点对点（P2P)

演示平台：演示平台服务专注于最终用户用来与解决方案交互的不同类型的终端，例如台式机、移动设备（智能手机、平板电脑）、便携式设备（笔记本电脑）或特殊用途设备（例如医疗设备或智能设备）。演示平台还包括不同的交互技术，例如可用于与解决方案交互的语音识别或手写识别

相关组件：

- 2 终端
- 3 移动设备
- 4 移动设备管理
- 3 便携式设备
- 3 固定设备
- 3 医疗设备
- 3 桌面
- 4 公司所有
- 4 第三方
- 4 公共信息亭

- 3 智能家电
- 3 安全沙箱
- 1 语音识别 (IVR)
- 1 手写 (ICR)

与其他域的关系

演示服务利用安全和风险管理域对最终用户进行身份验证和授权，保护端点设备上和传输到应用程序服务域的数据，并保护端点设备本身免遭篡改、盗窃和恶意软件。

信息技术运营和支持域提供服务部署和变更终端设备，并管理最终用户遇到的问题和事件。 业务运营支持服务为终端设备、为人力资源 (HR) 以及终端用户对于技术解决方案的使用合规性战略提供安全监控。

应用服务

业务逻辑的开发与实现

将应用程序服务视为开发人员用来编写代码的流程，以及代码本身。

描述

应用程序服务是用户界面背后的规则和流程，用于为用户操作数据和执行事务。在网上银行中，这可能是从用户的帐户中扣除付款金额并向收款人发送支票的账单支付交易。除了IT解决方案的应用程序服务外，应用程序服务域还代表程序员在创建应用程序时所经历的开发流程。

应用服务组件	定义
1 编程接口	[应用程序] 编程接口 (API) 允许应用程序或服务相互通信或允许应用程序的各个部分相互通信。输入验证对于这些接口很重要，确保只提供预期的输入。缺乏这种验证可能会导致攻击者将恶意代码注入应用程序或检索比应该访问的数据更多的数据，从而产生漏洞。
2 输入验证	输入验证检查用户的输入并确定哪些输入是系统可接受的。此流程有助于提高数据质量，并允许将恶意输入注入系统。
1 安全知识生命周期	为了构建安全的应用程序，开发团队必须在开发流程中及时了解最新的威胁和适当的对策。当开发团队构建多个应用程序时，安全框架通常用于提供可重用的组件。
2 安全设计模	设计模式是解决常见技术挑战的蓝图和说明。安全设计模式侧重于身份验证、授

式	权、日志监控、单点登录等安全功能的设计。
2 安全应用框架	应用程序框架提供了一组充当应用程序基本起点的组件。框架使应用程序开发人员能够跨多个应用程序，并将工作重点放在应用程序的特定业务需求上。安全应用框架提供了扩展特定应用框架的安全组件。例如，ACEGI 安全框架成为 Spring 框架的正式组成部分，用于使用Java构建Web应用程序。
2 代码示例	代码示例提供了向程序员演示如何编写特定算法的代码片段。出于安全编码目的，示例可能包括编写不易受到 SQL 注入影响的数据库查询。
2 攻击模式	攻击模式是对恶意方使用的常见攻击的描述，程序员必须注意防御Open Web Application Security Project (OWASP) Top 10 Security Risks 描述的用于利用Web应用程序的前10种攻击模式。
1 集成中间件	集成中间件是一组工具，如服务总线和消息队列，允许应用程序在不直接对话的情况下交换信息。这些服务的安全问题包括确保在传递流程中正在交换的消息不会被读取或篡改，并且这些可靠的来源只发送这些消息。
1 开发流程	开发流程必须解决安全问题，并且同时使用源代码扫描器（可以定位代码中的常见安全漏洞）和Web应用程序漏洞扫描器（可以测试Web应用程序是否可以被黑客使用的常用技术操纵）等工具构建解决方案。
2 自助服务	自助服务能力可供开发团队独立利用，无需将工作交给另一个团队。
3 安全代码审查	从自助服务的角度来看，安全代码审查能力是指，使用源代码分析器工具读取程序的源代码以及识别容易受到众所周知的攻击模式攻击的代码区域的能力。
3 应用漏洞扫描	应用程序漏洞扫描是一项自动化能力，检查正在运行的应用程序并确定存在可以利用的弱点的区域。
3 压力和负载测试	性能和容量测试旨在各自地探明违反服务级别目标的工作负载级别，或在不违反服务级别目标的情况下可支持的最大工作负载。
2 软件质量保证	软件质量保证是测试软件和跟踪发现的缺陷的流程。作为软件质量保证流程的一部分，应测试应用程序的安全漏洞。
1 连接和交付	连接和交付服务是用来集成在应用程序之间移动消息的中间件的底层机制。这些服务还必须保护正在传递的消息，包括加密消息以隐藏其内容。
1 抽象	多个应用程序做同样的事情时通常会使用抽象的概念，这样就有了一种其他人可以理解的通用语言。虽然航空公司管理其航班的方式可能与其他航空公司不同，

	但都可能使用相同的抽象概念，以便在线旅行服务可以跨多个航空公司查找航班。这些抽象概念必须包括适当的安全机制，确保只有授权用户才能访问它们，而一个用户未经许可不能访问他人信息。

示例

开发人员正在编写一个应用程序接口 (API)，允许银行系统与其他银行交易。他使用源代码分析器扫描代码，识别出一段代码未防范非法输入而可能损坏系统。开发人员会立即变更，新 API 现在可以安全使用。

提供的服务

开发流程：开发流程必须解决安全问题，同时使用源代码扫描器等工具构建解决方案，这些工具可以定位代码中的常见安全漏洞；Web 应用程序漏洞扫描器可以测试 Web 应用程序是否被黑客使用常用技术进行操控。

相关组件:

- 2 自助服务
- 3 安全代码评审
- 3 应用漏洞扫描
- 3 压力 & 容量测试
- 2 软件质量保证

安全知识生命周期：为了构建安全的应用程序，开发团队必须及时了解最新的威胁和在开发流程中使用的适当对策。当开发团队正在构建多个应用程序时，安全框架通常用来提供可重用的组件。

相关组件:

- 2 安全设计模式
- 2 安全应用框架
- 2 代码样例
- 2 攻击模式

编程接口：编程接口允许一个应用程序与另一个应用程序通信或让应用程序的各个部分相互通信。输入验证对于这些接口至关重要，确保只能提供预期的输入。缺乏这种验证可能会导致攻击者将恶意代码注入应用程序或检索比有权访问的更多的数据，从而产生漏洞。

相关组件:

- 2 输入验证

集成中间件：集成中间件是一种类似于服务总线和消息队列的工具，允许应用程序在不直接相互连接的情况下交换信息。这些服务的安全问题包括确保在传递流程中不会读取或篡改正在传输的消息，并且确保只有可靠的来源能给他们发送消息。

连接和交付：连接和交付服务是集成中间件用于在应用程序之间传输消息的底层机制。这些服务还必须保护正在传递的消息（包括隐藏内容的加密消息）。

抽象：当多个应用程序做同样的事情时，经常使用抽象的概念，以便拥有一种其他人可以理解的共同语言。虽然航空公司可能会以不同的方式管理他们的航班，但都可能使用相同的抽象，以便在线旅行服务可以找到跨多个航空公司的航班。这些抽象必须包括适当的安全机制，以确保只有授权用户才能访问，并且一个用户未经许可不能访问另一个用户的信息。

与其他域的关系

应用程序服务利用安全和风险管理领域进行应用间的信息加密，并且对应用进行授权和认证使其能够互相交流。应用程序服务域的开发依赖于SRM的威胁与漏洞管理服务。威胁与漏洞管理服务用主要用于评估正在开发的解决方案。应用程序服务主要从展示服务域接受输入并且在信息服务域进行数据处理。它也需要基础设施服务域的服务器和网络服务。信息技术操作和支持域用于管理应用程序服务的变更。业务操作支持服务域提供安全监视服务使得管理员能够监视任何应用程序的数据异常行为。

信息服务

管理数据

通常来讲，信息服务就是在数据库中的信息存储，但有时候也是在文件中的数据存储。

描述

企业最常见的痛点之一就是内部产生的大量数据，有时候包含了很多冗余数据。（从不同维度查出的同一种威胁漏洞）。所有这些数据都需要转化为有用的信息，业务资产所有者可以使用这些信息确定优先级、制定战略和管理他们的风险组合。

本节信息的提取，转换，清除以及加载都会以通用信息模式进行，以供进行进一步分析和操作。

典型的提取、转换和加载（ETL）数据规范化、数据挖掘、平衡记分卡分析等功能将驻留在这里。

应用程序服务域通过数据管理简化所有的数据源。所有的数据存储器会分布在此，并且会提取，转化以及加载到如下地点：

- **运营数据存储：**日常以及交易信息资产将会被360°无死角监控（例如，
  应用程序和基础架构漏洞、修补漏洞、渗透测试结果、审计结果和每项资

产的控制）。

- **数据仓库：**所有历史交易将用于开发数据仓库或数据集市，可以衡量风险管理程序取得的成功。此外，该模型可用于识别整个组织的行为模式、趋势、倾向和系统性差距。

信息服务组件	定义
1 服务交付	服务交付专注于信息和通信技术（ICT）主动服务，为企业用户提供充分的支持。它专注于作为ICT服务客户的企业。
2 服务目录	服务目录是企业为其雇员和客户提供服务清单。主要包括：服务说明、履行服务的时间框架或服务级别协议、谁有权请求/查看服务、服务成本（如有）以及如何履行服务
2 服务级别协议（SLAs）	服务级别协议 (SLA) 是经客户（终端使用者）和提供服务者达成的协议。这可以是具有法律约束力的正式或非正式“合同”（例如，内部部门关系）。SLA记录了双方对服务、优先级、责任、承诺和保修的共识。 SLA可以指定服务的可用性、可服务性、性能、操作或其他属性（例如计费）的级别。“服务水平”也可以指定为“目标”和“最低”，能够让客户了解预期值（最低要求），同时提供可测量（平均）的目标值，显示组织绩效水平。在一些合约里面，会规定惩罚措施，以防不遵守SLA（但是下面所提到的内部用户除外）需要注意的是，协议只规定了消费者所接收的服务，并不是服务者怎么提供服务。 SLA通常包括：服务定义、性能度量、问题管理、客户职责、保修和灾难恢复和协议的终止。
2 运营级别协议（OLAs）	运营级别协议（OLA）定义了支持服务级别协议（SLA）的组织的内部支持组之间的相互依存关系。该协议描述了每个内部支持小组对其他支持小组的责任，包括提供服务的流程和时间框架。OLA的目标是对提供服务商的内部支持关系进行清晰、简明和可衡量的描述。
2 合同（UC）	企业与其提供服务商之间的合同规定了各方的责任以及未能满足服务级别协议的相关处罚。
2 恢复计划	恢复计划描述了中断或灾难后恢复提供服务所需的流程和流程。这些计划通常包括逐步恢复服务的步骤，同时监控每个关键的性能和系统运行状况
1 报告服务	报告服务能够以各种方式呈现数据，从顶级聚合驾驶舱到原始数据。报告服务还能够供挖掘和分析数据，并为决策者提供商业智能
2 仪表盘	仪表盘提供了信息服务各个方面的顶级视图。仪表盘通常包括聚合关键绩效

	指标（KPI）和关键质量指标（KQI）。
2 数据挖掘	数据挖掘是深入了解KPI和KQI的能力，以便找到指标结果的根本原因。实际的数据挖掘任务可以是对大量数据的自动或半自动分析，以提取以前未知的有趣模式，例如数据记录组（集群分析）、异常记录（异常检测）和依赖关系（关联规则挖掘）。这些模式可以作为输入数据的数据总结，并用于进一步的分析。例如在机器学习和可预见分析中，数据挖掘步骤可以识别多个数据组，从而通过决策支持系统可以使用这些数据获得更准确的预测结果。
2 商业智能	商业智能是指用于识别、提取和分析商业数据的技术。BI技术提供了业务运营的历史、当前和预测视图。
2 报告工具	报告工具为最终用户提供了生成报告、与其他用户共享报告以及分析信息域数据的能力。
1 ITOS	信息技术操作和支持
2 项目管理办公室（PMO）	项目管理办公室（PMO）是定义和维护流程标准的部门或小组，通常与组织内的项目管理有关。PMO努力在项目执行流程中实现标准化并引入可复制经济模式。PMO是项目管理和执行实践的文件、指南和指标的来源。
2 战略	ITOS中的战略信息表示一种商业和技术的趋势。这种趋势影响着企业，期望能力和现实能力的差距值，以及填补这种差距所需的投资。
2 产品规划图	ITOS中的路线图信息表示随着时间的推移组织能力的计划变更。
2 问题管理	将重复发生的事件作为问题管理的流程，以发现并修复根本原因，防止未来事件再次发生。
2 事件管理	从检测到审查和解决的管理流程。
2 配置管理数据库（CMDB）	配置管理数据库（CMDB）是与信息系统组件相关的信息存储库。它包含IT基础架构中配置项（CI）的详细信息。CMDB有助于组织了解这些组件之间的关系并跟踪它们的配置。CMDB记录CI以及有关重要属性和CI之间关系的详细信息。 配置管理器通常使用三个可配置属性描述CI：技术、所有权和关系
2 知识管理	组织信息和提供检索能力。例如根据以往经验快速找到问题。在信息领域中，这表示知识库中存储的有关安全常见问题解答、最佳做法和工作辅助的实际知识。
2 服务管理	服务管理是一门管理信息技术（IT）系统的学科，从哲学上讲，它是从客户的角度看IT对商业贡献的一种理论。
2 变更管理	管理IT环境中变更的生命周期的流程。

1 服务支持	服务管理是一门管理信息技术（IT）系统的学科，从哲学上讲，它是从客户的角度看IT对商业的贡献的一种理论。
2 配置规则（元数据）	此配置项包含如何部署特定配置的元数据变更。
2 服务事件	支持IT操作的服务的信息。包括部署、变更和维护事件。事件可以基于超过阈值的关键性能指标、网络警报、设备指标。
2 配置管理数据库（CMDB）	配置管理数据库（CMDB）是与信息系统所有组件相关的信息存储库。它包含了IT基础设施中的配置项的细节信息。 CMDB有助于组织了解这些组件之间的关系并跟踪它们的配置。CMDB记录CI以及有关重要属性和CI之间关系的详细信息。配置管理器通常使用三个可配置属性描述CI：技术、所有权和关系
2 知识库	知识库包含关于已知模式、流程和流程的信息。
2 变更日志	从安全角度来看，监视变更日志并将其与配置管理变更比较并检测到环境中的未经授权的变更。
1 数据治理	数据治理体现了组织中的数据质量、数据管理、数据策略、业务流程管理和风险管理的融合。
2 风险评估	风险评估从参考框架角度（即COBIT、ISO27001）、监管角度（即SOX、PCI）衡量组织控制的成熟度。
2 非生产数据	为了在非生产环境中测试和开发，应生成测试数据，以避免在控件较少的环境中托管实时数据。当必须使用实时数据时，应屏蔽或标记以消除包含的个人信息的标识。
2 信息泄漏元数据	附加到关键信息块上的元数据，用于标记以供数据泄漏预防工具检测。
2 数据隔离	数据隔离是确保数据在多租户环境中隔离的流程和控制，因此每个租户都可以访问自己的数据，并且只能访问自己的数据
1 BOSS	业务操作支持服务（BOSS）
2 风险管理	风险评估从参考框架角度（即COBIT、ISO27001）、监管角度（即SOX、PCI）衡量组织控制的成熟度。
2 数据分类	描述数据业务价值的流程，将数据分为公开、私有、机密等类别，以指导数据处理流程。
2 进程所有权	有关业务流程以及负责监督和操作这些流程的责任方的文件。
2 审计结果	关于通过审计流程发现的组织控制措施中的具体差距的文件。
2 人力资源数据	有关组织员工和承包商的信息，可用于各种流程，包括访问控制、业务连续

	性规划、数据治理和背景检查。
2 业务战略	业务目标的文档，可用于确定支持业务的信息技术和安全战略.
2 风险管理	风险管理是识别、评估和确定风险优先级，然后协调和经济地应用资源，最小化、监控和控制不幸事件的概率以及影响。
2 治理、风险与合规(GRC)	治理、风险与合规描述了一个完整的管理方法，高级主管通过这套方法指导和控制整个组织，这个方法使用管理信息和曾计划管理控制结构。治理行为确保传递给执行层的关键信息是足够完整、精确和及时以保证制定的管理决策是恰当的，并提供了控制机制以确保管理层的战略、方向和指令被系统有效地执行。 风险管理是一个流程集，通过这些流程管理部门鉴别、分析风险，并对有可能对组织业务目标有负面影响的分享做出恰当的处理响应。 对风险的处理响应取决于感知到的风险严重性，响应行为包括控制风险、避免风险、接受风险和把风险转移给第三方。 而组织日常例行管理广泛的风险(比如技术风险、商业/金融风险、信息安全风险)，外部合法和监管合规风险是本节重点讨论的关键话题 合规意味着遵守规定的要求。在组织层面，需要管理部门鉴别出所有使用法规要求(比如法律条文、监管法规、合约、策略和政策)，评估当合规的状态，评估风险和违规的潜在成本以及达成合规的预计开支，并因此发现并启动必须的正确合规动作，并对其排列优先级。
2 风险评估(RA)	对风险评估的结果和范围进行文档记录。
2 业务影响评估(BIA)	业务影响评估信息有关于业务流程或者其数据不可用、丢失或被盗后对组织的影响
2 灾备恢复(DR) 和业务可持续性计划(BC P)	对恢复IT运营的灾备恢复计划和在计划或非计划宕机时确保企业连续服务的业务可持续性计划进行文档记录。
2 供应商风险评估（VRA）	对组织相关第三方供应商造成的风险之评估结果进行文档记录。
2 威胁漏洞管理(TVM)	有关威胁、漏洞管理测试、渗透测试以及合规测试的信息。
1 用户目录服务	用户目录服务这个系统负责存储、组织目录中用户的信息并提供对这些信息做访问操作的能力。目录允许根据给定的用户ID做搜索，用户ID有可能关联多种不同类型的数据。

2 活动目录服务	活动目录服务是网络管理和安全的中心位置。活动目录负责一个Windows网络域类所有用户和机器的身份验证和授权，对网络类所有的机器做安全策略的分配和强化以及在网络计算机上安装和更新软件。
2 注册服务	注册服务目录服务在IT基础设施内可用还有他们应该如何服务的元数据。
2 轻型目录访问协议资源库	轻量级目录访问协议资源库组织用户和用户组信息成为一个层级的组织结构。
2 位置服务	有关资产、资源、设施和人的物理位置的地理定位信息。
2 X.500目录服务协议资源库	X.500目录服务协议资源库根据面向电子目录服务的X.500系列计算机网络标准存储层级化的条目组织结构。
2 数据库管理系统资源库	数据库管理系统用来存储用户账号以及把他们的数据以表的形式存储在数据库中。
2 虚拟目录服务	虚拟目录服务聚合多个目录为一个统一视图，该视图将用户应用视为单个目录。
2 元目录服务	提供一个或多个目录服务或数据库的数据流以导入或维护这些数据源的同步性。
1 安全监控	这个模块将BOSS中的信息源集中在一起-安全监控服务。
2 会话事件	表示用户与计算机资源之间的交互开始和结束的事件。
2 授权事件	表示对给定主体访问给定客体的可访问性策略决策结果的事件。
2 身份认证事件	表示一个成功或不成功的验证用户凭证的事件。
2 应用事件	在应用内被认为是对安全监控有用的事件，比如访问受保护数据或者执行欺诈交易。
2 网络事件	在应用内被认为是对安全监控有用的事件，比如访问受保护数据或者执行欺诈交易。
2 计算机事件	被服务器、桌面计算机或其它终端设备所产生的事件，包括启动、关机、配置变更和系统错误。
2 特殊权限使用事件	表示对系统做管理变更的事件，一般意味着会影响系统的保密性、可用性、和完整性。
2 电子取证事件	电子取证事件意味着保留数据用于法律和调查目的。
2 数据泄露防御事件	当特权数据被截获并流出组织之外时触发数据泄漏防御事件。
2 网络入侵防护服务事件	网络入侵防护服务事件(NIPS)意味着入侵企图的来源和目标信息。

2 合规性监控	对当前配置和期望配置基线的对比信息。
2 身份凭证注销列表	身份凭证注销列表是一个已注销凭证的列表，所以这些凭证不能再被信任。
2 访问控制列表	访问控制列表表示访问主体被授予的访问或改变系统内客体的权限。
2 数据库事件	数据库事件表示数据库管理系统内的事件包括登录、事务和管理性变更。
2 主机入侵检测系统-主机入侵防御系统（HIDS-HIPS)	主机入侵检测系统(HIDS)可以检测到视图攻陷资源保密性、完整性和可用性的行为。主机入侵防御系统包括没有直接人介入的前提下采取防御措施。
3 安全事件数据转换服务	安全监控事件数据的转换和规划化以便于将数据挖掘和事件关联。

示例

管理员创建用户帐户时，用户标识和密码存储在用户目录中。当用户登录系统时，显示登录日期和时间的日志会存储在安全监控数据库中。

提供的服务

用户目录服务:所有身份验证和授权存储库都分配到本部分，简化用户目录的技术占用。

相关组件:

- 2 活动目录服务
- 2 注册服务
- 2 LDAP存储库
- 2 位置服务
- 2 X.500存储库
- 2 联合服务
- 2 数据库管理系统（DBMS）存储库
- 2 虚拟目录服务
- 2 元目录服务

安全监控数据管理:与安全监控相关的所有数据都被分配到本部分，考虑以下几个主要的组:

外部监控:品牌保护、蜜罐、网络爬虫防护和网络智能。

内部监控:SIEM相关数据、趋势、行为模式和取证信息。

执行报告:平衡记分卡、执行仪表盘和ODS(风险注册)。

威胁和漏洞管理数据 - 应用程序合规、补丁、配置健康检查、基础架构、应用程序和漏洞。

相关组件:

- 2 会话事件
- 2 授权事件
- 2 身份认证事件
- 2 应用程序事件
- 2 网络事件
- 2 计算机事件
- 2 权限使用事件

- 2 电子发现事件
- 2 数据泄露防护（DLP）事件
- 2 网络入侵检测系统（NIPS）事件
- 2 合规性监控
- 2 证书吊销列表（CRL）
- 2 访问控制列表（ACL）
- 2 数据库事件
- 2 主机入侵检测系统（HIDS）-主机入侵防御系统（HIPS）
- 2 转换服务

服务交付数据管理:关注与整个公司的信息技术服务管理相关的结构或非结构化数据。这包括服务级别管理、可用性管理、灾难恢复和服务接收方。在考虑这些服务的相关成本时，应进行成本效益分析。

相关组件:

- 2 服务目录
- 2 服务级别协议（SLA）
- 2 运营级别协议（OLA）
- 2 合同
- 2 恢复计划

服务支持数据管理:与面向整个公司的业务提供服务相关的所有数据都将属于本部分。这包括与服务台、事件管理、配置管理、问题管理和知识管理相关的信息。

相关组件:

- 2 配置规则(元数据))
- 2 服务事件
- 2 配置管理数据库(CMDB)
- 2 知识库
- 2 变更日志

数据治理数据管理：随着应用程序和信息技术服务在整个组织中的推广和管理，本部分将在整个软件开发生命周期中存储证据和适当的合规性数据。

相关组件:

- 2 风险评估
- 2 非生产数据
- 2 信息泄露元数据
- 2 数据隔离

风险数据管理:与信息安全技术能力相关的所有信息都将存储于本部分，包括数据治理、应用程序安全和数据泄露防护等有助于改善收集到的每个信息资产风险状况的信息源。

相关组件:

- 2 治理、风险与合规（GRC）
- 2 风险评估（RA）
- 2 业务影响分析（BIA）
- 2 灾难恢复（DR）和业务连续性（BC）计划
- 2 供应商风险评估（VRA）
- 2 威胁漏洞管理（TVM）

ITOS数据管理: 本部分将包含与IT组织的战略和典型运营相关的数据，例如质量管理、项目管理办公室（PMO）、企业架构合规性、业务和信息技术协调，以及在支持业务需求时如何将所有这些服务转化为协议。

相关组件:

- 2 项目管理办公室（PMO）
- 2 战略
- 2 路线图
- 2 问题管理
- 2 事故管理
- 2 配置管理数据库（CMDB）
- 2 知识管理
- 2 服务管理
- 2 变更管理

BOSS数据管理：与业务运营支撑服务领域相关的所有数据源都分配到本部分。

相关组件:

- 2 风险评估
- 2 数据分类
- 2 流程负责人
- 2 审计结果
- 2 人力资源数据(员工和承包商)
- 2 商业战略

报告服务：所有用于生成运营报告、决策制定、平衡记分卡、仪表盘的工具，及其他将不同的数据源和数据模型转化为对业务有用的信息和对风险管理战略的适当支撑(运营和战略)的能力，都将在本部分。

相关组件:

- 2 仪表盘
- 2 数据挖掘
- 2 商业智能
- 2 报告工具

与其他域的关系

信息服务域为应用程序和展示服务域提供上下文支持。信息技术运营和支持域管理其他域需要定期实施的应用程序服务变更和部署流程。业务运营支持服务域管理信息服务应用程序的安全监控。业务运营支持服务（BOSS域）监控应用程序正在执行的活动是否有任何异常行为。

基础架构服务

不同于基础设施即服务(IaaS)，基础设施服务可以看作是由能在任何标准数据中心内看到的一排排计算机、网线、电源、冷却通风口和灭火管道提供的基本能力。这些能力包括虚拟化、计算、存储和网络；设施和环境；以及物理安全和访问限制。基础设施服务也可以参考设施、硬件、网络和虚拟环境。

描述

基础设施服务是分层的基本核心能力，支持其他架构领域的高层面能力。这些层面包括虚拟机、应用程序、数据库，以及网络和物理硬件和设施。

由于它们提供了一个基础，基础设施服务对于云服务的终端用户大多不可见。例如，客户可能会被要求尽职调查，确保云设施提供物理安全以匹配他们使用云服务的风险特征，但除此之外，他

们会忽略如何实施物理访问控制的操作细节。

基础架构服务组件	定义
1 内部基础架构	内部基础架构服务主要涉及云服务提供商为支持云用户实际看到的虚拟化服务使用的物理资产。在许多方面，这些服务是最底层的，对终端云用户也是最不可见的，尽管它们是支撑云服务可靠和安全运行的基础。例如，如果没有良好的设施安全，对手就没有必要对云服务进行网络攻击，因为只要走进设施，拔掉服务器或网络连接就可以了。
2 设施安全	涉及在云计算设施中运用的安全控制，确保云基础设施的物理组件有一个安全和可靠的操作环境。例如：包括适用于物理访问的控制、环境控制等。
3 受控物理访问	限制对设施及其内容的物理访问的安全控制措施。
4 围栏	拒绝或限制对设施或其部分的物理访问（例如，在设施和道路之间设置柱子，禁止车辆进入）。
4 电子监控	对连续观察一个地区以检测入侵情况，记录进入情况并监测运动。
4 安全巡逻	由人或动物看守定期巡视，阻止和发现非法活动，并核实其他安全控制的状况（例如，核实门是否锁好）。
4 物理认证	通过物理手段验证所声称的身份的流程（例如，保安人员验证身份证上的照片与提供照片的人相符）。
3 资产处理	管理实物资产所涉及的流程和程序（例如，库存控制、位置管理等）。
4 数据	各种事物以任何形式的数字表示（SNIA词典）。
4 存储	一种记录数据并支持检索的功能（SNIA词典）。
4 硬件	一般来说，用于提供基础设施服务的物理设备（例如，一台服务器、一台路由器等）。
3 环境风险管理	评估和控制基础设施周围环境产生的风险的一般流程（例如，估计备用发电机厂的规模，以便在公用事业电力损失时提供电力的连续性）。
4 物理安全	关注减轻对设施及其员工的物理威胁（例如，灭火设备和定期消防演习）。
4 设备位置	将设备安置在适当的地点所涉及的流程和程序（例如，将关键的网络设备安置在有冗余电源、温度控制等的安全房间内）。
4 电源冗余	提供多种电力来源，确保在失去公共电力的情况下继续运行。
可用性服务	关注确保基础设施组件的可用性，匹配服务级别目标。这个层次的控制措施包括在地理上分散的站点之间的数据镜像、冗余组件和它们之间的切换流程。
2 补丁管理	关注确保所需的软件修复在基础设施内以受控和及时的方式应用，包括清点

	基础设施中实际存在的服务（操作系统、应用程序、嵌入式软件等），确定特定修复的适用性，并监测基础设施，确保所需的修复实际存在并安装。
3 合规监测	为确保提供服务符合适用的政策和监管框架而进行的处理和程序，可以通过定期审计或持续监测实现。
3 服务发现	为假定适当的补丁已经安装，识别实际存在的服务（相对于那些被记录为存在的服务）的流程和程序，。
2 服务器	关注安装在物理服务器上的软件镜像，以及用于确保安全构建这些软件镜像的控制措施，以及如何管理这些镜像。
3 安全构建	保证符合安全策略的标准软件镜像。
3 镜像管理	在一个基础设施内管理软件镜像集合的流程和程序。
2设备维护	关注确保物理基础设施设备得到适当的维护，以保证持续运行。例如，定期检查、清洁和更换空气过滤器，在发现退化时主动更换部件等。
2 网络服务	关注管理网络环境所带来的安全风险。这一层面的控制措施包括适当的网络隔离（例如，组织A使用的资产对组织B不可见）并提供基本的网络服务，如准确和可追踪的时间标准。
3 网络隔离	确保网络结构与基础设施内建立的风险域相匹配的流程和程序（例如，对外的服务器与内部服务器所处网段相互独立）。
3 权威时间来源	确保在基础设施内使用可追踪的标准时间源（例如，服务器时间与时间源同步，以便在事件响应期间将一台服务器上发生的事件与另一台服务器上发生的事件联系起来）。
2 存储服务	关注基础设施中物理存储的提供、迁移和数据清洗。这一层次的控制措施保证了存储在需要时是可用的，其冗余/可靠性要求符合服务要求，等等。
1 虚拟基础架构	虚拟基础架构继承了一些与物理基础架构中存在的相同服务。例如，必须为虚拟服务器安全地构建和管理软件镜像，这些虚拟服务器托管在物理服务器提供的虚拟化平台上。然而，对于虚拟化基础架构本身也有独特的要求。
2 桌面客户端虚拟化	关注如何创建、展示和管理传统桌面的虚拟实例。
3 本地	在终端上安装和管理但与终端的其余部分隔离的虚拟机或应用程序沙箱。管理可以是集中的，但虚拟机在终端设备（平板电脑、PC 等）上本地运行。
3 远程	通过网络交付的虚拟机，而不是本地安装在设备上。
4 基于会话	任何设备的远程桌面展示，该展示由一个远程终端控制。
4基于虚拟机虚拟桌面（VDI）	与演示服务器集成的虚拟桌面，用于控制访问和管理多个用户。

2 应用程序虚拟化	删除应用程序与承载它的服务器之间的连接。消费者将访问应用程序实例不考虑应用程序驻留的地点或内容。
3 客户端应用程序流	应用程序流解决方案的终端组件。客户可以是平板电脑、手机、智能设备。
服务器应用程序流	应用流解决方案的服务器端组件，负责向多个客户端交付内容。
2 虚拟工作区	云提供商定义的虚拟化基础架构的模板定义了虚拟基础设施实例的特性，如主机数量、网络分段、存储和安全元素。对于高可用性，可以在实例或云提供商之间复制工作区，以提供用于故障转移目的的冗余功能。
3 垂直隔离	垂直隔离了工作区的所有虚拟化组件，例如使用细节、通信、内存或数据，这些组件可能不会在工作区之间泄漏。
2 服务器虚拟化	关注虚拟服务器的创建、访问和管理。此级别的控件确保服务器配置正确，包括正确的软件镜像等。
3 基于主机虚拟机	物理主机可以虚拟化其各种组件和功能，提供多个机器、应用程序等的虚化。
4 全虚拟化	包括处理器、存储和网络功能在内的完全虚拟化的环境或结构。可作为物理机器的一部分或跨多个物理机器提供。
4半虚拟化	虚拟操作系统，其中客户操作系统的源代码修改为专门作为客户操作系统而不是作为原始硬件目标操作系统的二进制等效物运行。
4 硬件辅助	支持给定处理器架构中用于虚拟机管理程序（hypervisor）执行（通常通过提供支持在客户实例之间切换等的专门指令等）。
3 操作系统虚拟化	具有虚拟工作空间的功能，可以根据客户需求安装不同的操作系统。
3 TPM虚拟化	受信任的平台模块可以存储软件认为攻击者无法变更的代码签名或密钥。此功能是指虚拟化的TPM实例。TPM由受信任计算组(Trusted Computing Group)定义。
3 虚拟内存	一种操作系统特性，使用物理内存和后备存储(通常是磁盘)的组合创建虚化有更大的内存空间可用。为了获得良好的性能，它依赖于局部性原则，该原则假设程序的地址空间(工作集)在任何时间点实际上都只有一小部分在使用。
2 存储虚拟化	关注如何创建、分配和管理虚拟化存储。这既包括“基于块的”存储，如SAN(存储区域网络)，也包括“基于文件的”虚拟化，如NAS(网络附加存储)，无论是否由文件服务器提供或设备。这个级别的控制确保存储足够满足需求，适当地隔离和保护，并且其性能符合服务级别协议（SLA）中指定的概要文件。
3 基于块的虚拟化	块级设备级别的虚拟化（例如，主机带有虚拟磁盘设备）。
4 基于主机	虚拟化文件系统可能由服务器提供（例如提供多个文件共享的文件服务器）。

5 逻辑设备管理器（LDM）	逻辑设备管理器(LDM)。在功能上类似于逻辑卷管理（LVM）的Microsoft Windows功能。
5 逻辑卷管理（LVM）	逻辑卷管理(LVM)。允许将多个物理磁盘分组到主机查看的单个逻辑卷中
5 协议逻辑单元号（LUN）	SCSI协议的逻辑单元号（LUN)的首字母缩写，通常用作一个术语，指通过SAN提供给主机的块设备。
4 基于存储设备	存储设备控制器可以允许虚拟化磁盘卷(例如，硬件RAID控制器将多个物理卷或列的部分分组到单个主机可见的RAID-5阵列)。
4 基于网络	文件系统级别的虚拟化（即主机带有虚拟文件系统）。
5 设备	由专用硬件设备（例如 NAS 文件服务器）提供的基于网络的可视化。
5 交换	更复杂的存储区域网络架构，包括连接主机和LUN的交换网络。交换式SAN可以基于光纤通道，也可以基于以太网光纤通道(FCoE)或ISCSI。
3 基于文件的虚拟化	更高级别的文件视图，使文件在很大程度上独立于其呈现方式。例如，一个消费者会访问我的预算（mybudget.global），而不管它是驻留在NAS设备、SAN还是物理服务器上
2 网络虚拟化	关注提供适当的虚拟网络服务。此级别的控件可确保虚拟网络实现适当的隔离（见上面的"分段"）、所需的连接和适当的访问控制。
3 网络地址空间	在虚拟工作空间中定义网络地址以创建独立于物理主机的虚拟网络分段的能力。
4 互联网协议第4版（IPv4）	IPv4是互联网协议（IP）的第四版，是互联网和其他分组交换网络中基于标准的互联网工作方法的核心协议之一。IPv4是1982年在SATNET上部署的第一个版本，1983年1月部署在ARPANET上。尽管正在部署后续协议 IPv6，但IPv4仍然负责大部分互联网流量的路由。
4 互联网协议第6版（IPv6）	IPv6是互联网协议（IP）的最新版本，该通信协议为计算机提供互联网网络和路线流量的识别和定位系统。IPv6由互联网工程专责小组（IETF）处理期待已久的IPv4地址耗尽问题。
3 外部虚拟局域网（VLAN)	虚拟局域网是一组主机（前提是在云端，本地主机、云中主机、云间主机或混合主机）。它们具有一组通用的需求，就是不管它们的物理位置如何，就像连接到同一个广播域一样通信。
3 内部虚拟网络接口(VNIC）	虚拟网络接口是一种虚拟网络接口，提供与实际接口相同的介质访问控制（MAC）接口。
2 数据库虚拟化	数据库虚拟化是对数据库层的解耦，数据库层位于应用程序堆栈中的存储层和应用层之间。数据库层的虚拟化允许扩展硬件资源，以便在应用程序和用

	户之间更好地共享资源，屏蔽查询程序中数据库的物理位置和配置，并支持更可伸缩的计算。
2 移动设备虚拟化	移动设备虚拟化允许组织测试不同移动设备的新技术的兼容性。
2 智能卡虚拟化	允许用户将本地智能卡虚拟化的方法和系统，以便可以远程连接到服务器并与服务器交互，就像本地智能卡物理连接到服务器一样。

示例

云位于物理位置的某处，即数据中心。通过采用围栏、摄像头、保安人员、陷阱和门卡激活等措施对这些数据中心进行物理保护。通过连接多个互联网服务提供商的线路、停电时的发电机以及多台计算机在一台计算机出现故障时执行相同的工作来确保基础设施的可用性。

提供的服务

基础设施服务

基础设施服务主要涉及云服务提供商为云用户提供虚拟化服务的物理资产。在很大程度上，这些服务是最低级别的，对最终云用户也是最不可见的。尽管如此，它们却是云服务可靠和安全运行的基础。例如，如果没有良好的设施安全性，攻击者就没有必要对云服务发起网络攻击。只需拔掉服务器或网络连接即可。

设施安全：涉及云计算设施中应用的安全控制措施，确保云基础设施的物理组件有一个安全可靠的操作环境。例如，适用于对物理访问和环境控制的限制。

相关组件:

- 3 受控物理访问
- 4 围栏
- 4 电子监控
- 4 安全巡逻
- 4 物理认证
- 3 资产处理
- 4 数据
- 4 存储
- 4 硬件
- 3 环境风险管理

- 4 物理安全
- 4 设备位置
- 4 电源冗余

服务器：涉及安装在物理服务器上的软件映像以及用于确保这些软件映像的安全构建以及如何管理这些映像的控制措施。

相关组件:

- 3 安全构建
- 3 镜像管理

存储服务：涉及基础设施中物理存储的配置、迁移和清理。 此级别的控制可确保存储在需要时可用，且其冗余/可靠性要求与服务要求匹配。

网络服务：涉及管理网络环境带来的安全风险。此级别的控制包括适当的网络分段（例如，组织A使用的资产对组织B不可见）和提供基本网络服务（例如，准确且可追溯的时间标准）。

相关组件:

- 3 网络分段
- 3 权威时间源

可用性服务：涉及确保基础设施组件的可用性，匹配服务级别目标。此级别的控制措施包括地理上分散的站点、冗余组件之间的镜像数据，以及它们之间的切换。

补丁管理：涉及确保在基础设施内以受控和及时的方式应用所需的软件修复程序。包括盘点基础设施中实际存在的服务（操作系统、应用程序、嵌入式软件等）以确定特定修复程序的适用性，以及监控基础设施以确保存在并安装所需的修复程序。

相关组件:

- 3 合规监控
- 3 服务发现

设备维护：涉及确保物理基础设施设备得到适当维护以确保持续运行。 包括定期检查、清洁和更换空气过滤器，以及在检测到性能下降时主动更换组件。

虚拟基础设施服务

虚拟基础设施继承了物理基础设施中已有的一些服务。例如，必须为运行于物理服务器之上，安全地构建和管理托管在在虚拟化平台上的虚拟服务器中的软件镜像。此外，虚拟化基础设施本身也有独特的要求。

桌面“客户端”虚拟化：涉及如何创建、显示和管理传统桌面的虚拟实例。

相关组件:

- 3 本地
- 3 远端
- 4 基于会话
- 4 基于虚拟桌面基础架构

存储虚拟化：涉及如何创建、分配和管理虚拟化存储。无论是由文件服务器还是设备提供的存储，包括“基于块”的存储（例如，SAN（存储区域网络））和“基于文件”的虚拟化（例如， NAS（网络附属存储））。通过采用特定的控制确保存储满足要求、充分隔离和保护，并且其性能符合服务级别协议中指定的配置文件。

相关组件：

- 3 基于块的虚拟化
- 4 基于主机
- 5 逻辑磁盘管理
- 5 逻辑卷管理
- 5 逻辑单元号
- 4 基于存储设备
- 4 基于网络
- 5 设备
- 5 交换
- 3 基于文件的虚拟化

服务器虚拟化：涉及创建、访问和管理虚拟服务器。 此级别的控制措施可确保服务器配置正确，以及正确的软件镜像和管理程序。

相关组件:

- 3 虚拟机(基于主机)
- 4 全虚拟化
- 4 半虚拟化
- 4 硬件辅助
- 3 操作系统虚拟化
- 3 可信平台模块虚拟化

- 3 虚拟内存

网络虚拟化:涉及提供适当的虚拟网络服务。此级别的控制可确保虚拟网络实施适当的隔离（请参阅上面的“分段”）、所需的连接性和适当的访问控制。

相关组件:

> - 3 网络地址空间
> - 4 互联网协议版本4(IPv4)
> - 4 互联网协议版本6(IPv6)
> - 3 外部虚拟局域网（VLAN)
> - 3 内部虚拟网络接口卡(VNIC）

与其他域的关系

基础设施服务提供了许多核心组件和功能，用于支撑架构其他部分所提供的功能。例如，如果基础设施的基础级别没有良好的物理安全性，那么在安全和风险管理领域提供更高级别的治理在很大程度上是毫无意义的。信息技术运营与支持（ITOS）领域下的服务交付和支持同样取决于基础设施级别提供的性能和可靠性保证。

安全和风险管理（SRM）

保护数据和管理风险

安全和风险管理一般指通过使用密码、防火墙和加密技术等，定义策略并根据这些策略审计系统的用以保护计算机系统和数据的流程。大多数人在想到网络安全时，都会想到使用渗透测试和工具测试系统中的脆弱环节。

描述

安全和风险管理领域提供了一个组织的信息安全计划的核心组成部分，保护资产和检测、评估、监测运营活动中的固有风险。其功能包括身份管理和访问控制、治理、风险管理与合规（GRC）、政策和标准、威胁和漏洞管理以及基础设施和数据保护。

基础设施服务组件	定义
1 治理、风险管理与合规（GRC）	云计算中治理和企业风险管理的基本问题涉及适当的组织结构、流程和控制的识别及实施，保持有效的信息安全治理、风险管理和合规性。GRC包括、整合和协调诸如公司治理、企业风险管理和公司遵守适用的法律法规等活动。

	组件包括： a. 合规管理（确保遵守所有内部信息安全策略和标准） b. 供应商管理（确保服务提供商和外包商遵守适用所有权和保管权的预期的和合同规定的信息安全策略） c. 审计管理（强调需要改进的地方） d. IT风险管理（确保所有类型的风险可以被识别、理解、沟通、接受、修复、转移或规避） e. 策略管理（维护支持创建、实施、异常处理和支持业务需求框架的组织结构和流程） f. 技术意识和培训（以提高选择和实施有效技术安全机制、产品、流程和工具的能力）
2 合规管理	分析所有指定的内部信息安全策略、控制标准和程序的合规性。
2 策略管理	安全策略是安全计划的主要目标。策略管理努力维持这样一个组织结构和流程，支持代表业务需求的创建、实施、异常处理和框架。
3 例外	误差包括当无法满足或只能部分满足的情况下对常用策略给予例外。通过这种方式，信息安全团队意识到一种不合规定的场景，因此可以了解相关风险并监控异常情况。有时异常是有时间限制的，并定期审查以评估风险及实施修复计划。
3 自我评估	一种由所有者/用户而非第三方分析/评估风险或合规性的工具和流程。
2 供应商管理	确保服务提供商和外包商遵守适用所有权和保管权概念的预期的和合同规定的信息安全策略
2 审计管理	独立审计师必须能够核实系统是否符合安全策略。为此，系统和流程必须确保将安全相关事件记录在防篡改的审核日志中。
2 IT风险管理	信息风险管理是将风险暴露和风险管理能力与数据所有者的风险承受能力结合的行为，为信息技术资源提供决策支持的主要手段，旨在保护信息资产的机密性、完整性和可用性。确保所有类型的风险可以被识别、理解、传达、接受、纠正、转移或避免。IT风险管理可以查看合规性管理活动的输出，以协助组织评估整体安全态势，并与确定的风险目标保持一致。
2 技术意识和培训	提高选择和实施有效技术安全机制、产品、流程和工具的能力。
1 信息安全管理	信息安全管理的主要目标是实施适当的措施，尽量减少或消除与安全相关的威胁和漏洞可能对组织产生的影响。衡量标准包括能力成熟度模型（随着组织经验和知识的增加，确定组织从不成熟状态到几个成熟度级别的发

	展阶段）、能力映射模型（描述企业为实现其目标所做的工作，并促进业务模式和支持业务需求的技术基础设施之间的紧密关系，从而形成业务和IT都能理解的观点）、安全架构形式的路线图（为服务于单个业务计划的单个项目提供了指南）以及风险组合（登记、监控和报告已识别的风险）。安全管理和风险管理的仪表盘用于衡量和报告决策的有效性，并帮助组织做出新的决定，以保持和提高这种有效性。修复残余风险的分析和计划也是整体风险管理框架的一部分。
2 能力映射	信息安全计划的能力可以通过安全服务目录描述，该目录是一些发布给企业的IT组织文档的更大目录的一部分。这些能力可以通过描述业务如何实现其目标的方式映射，并促进业务模式和支持业务需求的技术安全基础设施之间的紧密关系，从而形成业务和IT都能理解的观点。
2 成熟度模型	随着组织经验和知识的增加，确定组织从不成熟状态到几个成熟度级别的发展阶段。COBIT定义了一个能力成熟度模型，有六个成熟度级别：不存在、初始、可重复、已定义、管理和优化。
2 风险组合管理	信息安全计划的范围和章程的阐述包括，诸如声誉、公司治理和监管、公司社会责任和信息保证等重点领域。组合可以根据需要改变，与业务目标保持一致，并对不断变更的威胁环境和不断发展的法律和法规保持相关性和响应性。
2 风险仪表盘	以图形方式衡量和报告潜在、固有和残余风险的水平以及控制措施的有效性，帮助组织了解威胁和漏洞，并做出基于风险的决策以维持或提高控制措施的有效性。
2 残余风险管理	在理论上或应用上实施缓解控制后，为了提高控制有效性并最终将风险降到可以接受的水平，修复仍然存在的信息安全风险的分析和计划。
1 授权管理基础设施	权限管理基础设施通过身份管理、身份验证服务、授权服务和权限使用管理等身份和访问管理功能，确保用户拥有执行其职责和职责所需的访问控制措施的权限。此安全规则使合适的人员能够在合适的时间以合适的理由访问合适的资源，解决了关键任务的需求，确保在日益异构的技术环境中对资源的适当访问以及满足日益严格的合规性要求。 这种安全实践对于任何企业都是至关重要的工作。 权限管理基础设施的技术控制集中于身份提供、密码和多因素身份验证、策略管理等。 它也越来越与业务挂钩，需要业务技能而不仅仅是技术专长。

2 身份管理	通过监督一个身份的整个生命周期，确保可信身份可用于身份验证、授权和访问管理。
3 域唯一识别符	在计算机软件中用作标识符的唯一参考号（例如GUID、32个字符的十六进制字符串、用于Microsoft的通用唯一标识符标准的实施）
3 联合身份管理	指一种基于新标准的目录服务方法，简化和确保了用户对网络资源的访问，能够在各种安全域之间建立信任关系，实现身份验证、授权和隐私断言的传递。
3 身份配置	创建、维护和停用存在于一个或多个系统、目录或应用程序中的用户对象，响应自动化或交互式的业务流程。
3 属性配置	创建、维护和停用存在于一个或多个系统、目录或应用程序中的用户属性，响应自动化或交互式的业务流程。
2 认证服务	一种确定人或物是否有身份/内容符实的功能/API/流程。
3 SAML令牌	安全断言标记语言（SAML）令牌是一个基于XML的开源标准数据格式，在当事方之间交换身份验证和授权数据。
3 基于身份认证的风险	一种非静态身份验证系统，考虑了请求访问系统的代理的概况（IP地址、用户代理HTTP标头、访问时间等），确定与该交易相关的风险概况。然后使用风险概况确定挑战的复杂性。较高的风险概况会带来更大的挑战，而静态用户名/密码可能足以应对较低风险的情况。基于风险的实施允许应用程序仅在风险级别合适时才向用户挑战额外的凭据。
3 多因子认证	一种依赖于两个或多个要素的组合进行身份验证形式。常见形式有“something you have” （例如智能卡）、“something you know”（例如密码或PIN码）和“something you are”（例如物理指纹或键盘的动作节奏）。
3 一次性密码（OTP）	一次性密码 (OTP) 是一种在短期内有效的密码（例如，只有一次登录会话或交易），旨在避免与传统静态密码相关的几个缺点。生成 OTP的最流行的方法之一是身份验证服务器和客户端之间的时间同步。OTP实现通常用于双因素身份验证解决方案中，用户输入pin作为算法中的变量，该算法生成身份证据，发送给执行代理以确定身份是否有效。
3 智能卡	智能卡（又称微处理器卡、芯片卡或集成电路卡）传统上采用的是一种带嵌入式集成电路的袖珍卡。智能卡通常用于双因素身份验证解决方案，用户输入pin，智能卡上的操作系统使用pin发布身份证据，如数字证书或允许私钥签署身份令牌（该令牌发被送给一个确定身份是否有效的执行代理）。
3 密码管理	明确多个密码策略、定义密码组合规则、维护密码历史记录、限制密码、

	配置密码有效期、创建密码规则等流程。
3 生物特征识别	生物特征识别是指通过一个或多个固有的生理或行为特征识别唯一人的方法。 生物特征被认为是身份的一种形式，用于身份认证和访问控制。
3 网络认证	认证服务为用户（或设备）提供登录到网络的方法、协议及其他便利（例如，SSO）。
3 单点登录（SSO）	一种访问控制功能，用户登录一次即可获得对许多其他系统的访问权限，而无需在每个系统上再次登录。Kerberos是SSO单点登录的一种实现方式。
3 服务安全	基于简单对象访问协议（SOAP）灵活且功能丰富的扩展，可将安全性应用于web服务。该协议规定了如何对消息实施完整性和保密性，并支持各种令牌格式的通信，如SAML、Kerberos和X.509。
3 中间件认证	对用户永远不会直接看到的应用程序/服务/组件的身份认证。
3 身份验证	通过使用生理和行为特征或权威机构签发的派生文件鉴定其身份的流程
3 开箱即用（OTB）认证	一种通过身份提供商的服务在应用程序中实现用户登录功能的方法，无需自定义身份认证代码。
2 授权服务	一种功能、API或流程，有助于对操作系统/应用程序/服务/数据的受限区域进行访问控制，并允许管理员限制用户或设备对特定功能的访问。
3 权限审查	检查现有的用户和角色访问授权是否恰当的流程
3 策略执行	授权服务中的一个阶段，在此阶段批准或拒绝访问请求。
3 策略定义	授权服务中的一个阶段，描述对资源的访问流程或细粒度访问控制及约束。
3 策略管理	用于集中化的策略创建、存储和管理的流程或平台。
3 主体数据管理	管理与访问控制决策主体相关的所有属性的能力。这些主体可以是用户、机器或服务。授权决策可能需要考虑关于主体的许多属性，包括角色、位置、与帐户的关系、其他主体等。
3 资源数据管理	授权通过为应用程序信息资源同时提供访问和保护，在数据管理中发挥着关键作用。
3 可扩展访问控制标记语言（XACML）	可扩展访问控制标记语言是一种用XML实现的声明性访问控制策略语言。
3 角色管理	角色代表一组权限和特权，角色管理确保角色被正确定义为仅包含所需的权限和特权，并充分地分配给实体。
3 义务	在XACML中，义务是指从策略决策点到策略执行点的指令，用于指示在授予访问权限之前或之后必须完成哪些操作。

3 开箱即用（OTB）授权	一种允许从应用程序外部进行授权的方法，例如，通过提供授权插件。这使得开发人员能够避免创建自定义访问控制的费用和权衡。OTB授权解决方案可以提供全功能授权，包括完整的RBAC模型、策略存储、用户界面、内置应用程序组支持、规则和查询支持、集成系统审计和性能优化。
2 特权使用管理	特权账户一般包括用于安装、配置、操控管理操作系统、应用程序和数据库的管理帐户，如管理员。特权用户管理系统可以通过对特权账户管理，实现对敏感信息资源的访问控制。健壮管理的特征包括：集中化、策略驱动、自动化、细粒度和可审计。
3 键盘/会话日志	获取与实体交互的详细记录的方法（在单个击键级别或与实体交互级别）
3 密码保管	一种基于软件的解决方案，可安全存储和管理多个密码。
3 特权使用网关	根据工作负载上的使用特权为会话授予/拒绝连接的网关。
3 资源保护	防止滥用计算机资源。
3 Hypervisor 合规性与治理	基于与Hypervisor管理员相关联的角色和用户进行特权管理和监控的能力。这还包括管理云环境中的虚拟网络、服务器和应用程序。
1 威胁和漏洞管理	该规程涉及核心安全，如漏洞管理、威胁管理、合规性测试和渗透测试。漏洞管理是一项复杂的工作，在这项工作中，企业跟踪其资产，监视、扫描已知/新出现的漏洞，并通过修补软件、变更配置或部署其他控制措施减少资源层的攻击面。威胁建模和安全测试也是有效识别漏洞活动的一部分。该规程旨在通过漏洞扫描、虚拟补丁以及安全测试和响应的其他方面，主动检查运行云的基础设施，以应对新的安全威胁。
2 合规性测试	合规性测试确定对信息安全策略、标准和控制程序的遵从程度。例如是通过扫描检测虚拟机和物理机上是否存在要求的补丁与更新。
3 数据库（DBs）	对数据集合进行合规性测试，该数据集合经过组织以便使其内容易于访问、管理和更新。
3 服务器	针对软件程序或运行该程序的计算机进行的合规性测试为在同一计算机或网络上的其他计算机上运行的客户端软件提供特定类型的服务。
3 网络	针对由通信路径互连的一系列点或节点进行合规性测试。网络可以与其他网络互连并包含子网络。
2 漏洞管理	识别、分类、修复和缓解漏洞的周期性实践（通常在软件中）。
3 应用程序	为帮助用户执行特定任务而设计的计算机软件。例如企业软件、会计软件、办公套件、图形软件和媒体播放器等。
3 基础架构	一个共享、不断发展、开放、标准化和异构的安装基座，以及支持信息的

	创建、使用、传输、存储和销毁的所有人员、流程、程序、工具、设施和技术（也称为信息基础设施）。
3 数据库（ DB）	见数据库（前文）
2 渗透测试	一种通过模拟恶意外部人员（不具有访问组织内系统的权限）和恶意内部人员（具有一定级别的访问权限）的攻击评估计算机系统或网络安全性的方法，也可简称为“渗透（pentest）”。
3 内部	关注可能由内部人士发起的攻击。与远程攻击者相比，该攻击者可能具有某种形式的访问权限，并且已经能访问内部网络。内部人员还可以对有价值数据的位置有更多的了解。
3 外部	重点关注远程攻击者访问内部网络的能力。这种形式的渗透测试旨在通过利用外部暴露的设备（包括服务器、客户端、应用程序和无线接入点）访问位于内部网络中的数据。
2 威胁管理	威胁管理主要关注可能危及数据保密性、完整性和可用性的威胁、威胁源和威胁代理。威胁管理可以利用威胁分类法提供结构，威胁管理也有助于整体风险评估流程。
3 源代码扫描	使用静态代码分析工具识别软件中安全缺陷的方法。
3 风险分类	用于识别、捕获和分类已知威胁的分类法。SABSA威胁建模框架中使用的一个示例定义威胁域(人员、流程、系统、外部事件)和基于经验和观察的威胁类别。
1 基础设施保护服务	基础设施保护服务保护服务器层、端点层、网络层和应用层。该规程使用传统的纵深防御方法确保数据容器和管道的安全。基础设施保护服务的控制通常被视为预防性技术控制措施，如入侵检测/防御系统（IDS/IPS）、防火墙、反恶意软件、白/黑名单等。它们在防御大多数传统或非高级攻击时具有较好的成本效益。
3 恶意软件行为防护	基于事件识别恶意软件行为的能力。例如，一封附带有针对性恶意软件的入站电子邮件通过安全虚拟机过滤，识别负载何时会触发非典型性活动。
3 白名单	由于某种原因而被提供特定特权、服务、流动性、访问或认可的实体的列表或登记册。
3 敏感文件保护	保护敏感信息不被管理员读取或修改的能力，这些管理员可以访问文件系统，但没有权限读取某些文件中的受保护数据。此外，还能够监视敏感文件的变更，以便审核对其进行变更或读取的人员。
3 主机入侵检测（防	主机入侵检测系统(HIDS)可以检测到试图破坏机密性、完整性或资源可用性

御）系统（HIPS/HIDS）	的行为。主机入侵防御系统(HIPS)包括在没有直接人工干预的情况下采取预防措施。
3 反病毒	请参阅反病毒、反垃圾邮件、反恶意软件。
3 主机防火墙	保护终端的一种形式是使用个人防火墙，通常是控制与计算机之间的网络通信的应用程序，基于作为规则集实现的安全策略允许或拒绝通信。终端防火墙不同于通常放置在网络上并为终端提供服务的防火墙设备。
2 终端	用户使用的计算设备（如台式机、平板电脑、智能手机）。
3 反病毒、反垃圾邮件、反恶意软件	用于预防、检测和删除恶意软件的软件程序，恶意软件包括但不限于计算机病毒、计算机蠕虫、特洛伊木马、垃圾邮件、间谍软件和广告软件。
3 HIPS/HIDS	基于主机的入侵检测是一种检测试图破坏主机或终端上资源的保密性、完整性或可用性的行为的能力。基于主机的入侵防御包括在没有直接人工干预的情况下采取预防措施。
3 主机防火墙	在单台主机上运行的一种软件程序或功能，只能限制进出该主机的网络活动
3 介质封禁	也称为可移动介质锁定，一种阻止用户访问可写入设备（如USB闪存棒和CD/DVD-RW驱动器）以防止数据泄漏的控制措施。
3 基于硬件的可信资产	具有硬件可信根的资产（例如带有TPM芯片的计算机）。
3 恶意软件行为防护	基于事件识别恶意软件行为的能力。例如，一封附带有针对性恶意软件的入站电子邮件，将通过使用安全虚拟机过滤，识别负载何时会触发非典型性活动。
3 资产库存控制	为组织的物理和数字资产提供管理控制和问责制。在云计算和虚拟化场景中，当试图以传统跟踪物理机的方式盘点虚拟机时，会产生挑战。
3 内容过滤	基内容过滤技术是基于对访问内容的分析来允许或阻止访问，而不是通过来源或其他条件。它在互联网上广泛用于过滤电子邮件和网络访问。
3 取证工具	确保授权方可获得适当的工具和流程，促进与调查相关的相关数字工件的识别和保存(例如，违反政策、电子发现请求或刑事调查)
3 白名单	白名单是一种过滤形式，创建一个列表注册授予访问权限或受欢迎签名的实体。当使用白名单时，默认为“拒绝所有”，过滤器中枚举的条目除外。白名单通常在更容易（或用更短的列表）识别什么是被许可的而非什么是不被许可的情况下使用。
3 恶意软件行为防护	基于事件识别恶意软件行为的能力。例如，一封附带有针对性恶意软件的

	入站电子邮件通过使用安全虚拟机过滤，识别负载何时会触发非典型性活动。
3 防火墙	防火墙是一个或一组基于一系列规则来允许或拒绝网络传输的设备，并常用于保护网络免于被未授权访问的同时允许合法的网络流量通过。许多个人计算机操作系统包含软件防火墙，防止来自公网的威胁。许多在网络之间传递数据的路由器都包含防火墙组件
3 内容过滤	内容过滤技术是基于对访问内容的分析而不是通过来源或其他条件允许或阻止访问。此技术广泛用于过滤电子邮件和相关的网络访问。
3 深度报文检测（ DPI）	深度报文检测 (DPI)（也称为完全数据包探测和信息提取、深度包检测) 是一种计算机网络数据包过滤形式，在数据包通过检测点时检查数据部分（也可能包括数据包头），主要检测不合规的协议、病毒、垃圾邮件、入侵或事先定义好的标准，确定数据包是否可以通过或是否需要路由到其他地址，或收集统计信息。
3 网络入侵防御（检测）（NIPS / NIDS）	网络入侵防御包括在没有直接人工干预的情况下采取防御措施。网络入侵检测是能够检测试图破坏网络上资源的机密性、完整性或可用性的行为的能力。
3 无线保护	保护通过无线媒体传输的数据，包括802.11 Wi-Fi、蜂窝和蓝牙。典型的保护方法是使用各种的加密手段，例如利用TKIP或AES的Wi-Fi保护访问 (WPA)。
3 链路层网络安全	数据保护可以应用于OSI第2层数据链路层。网络交换机是第2层通信的关键组件，容易受到CAM表溢出、VLAN跳跃、生成树协议操作、MAC地址欺骗和ARP等攻击。缓解措施包括在交换机上配置端口安全、修改VLAN配置、路由器端口上的ACL配置和802.1X。
3 黑名单过滤	黑名单是一种过滤机制，主要是通过创建列表记录禁止访问或不受欢迎的签名的实体。使用黑名单时，除了过滤器中明确列举的那些条目，其他默认值是允许的。通常在更容易确定不应允许哪些实体，即禁止列表更短时使用。
3 XML设备	用于保护、管理和调解XML流量的专用网络设备。它们最普遍地在面向服务的架构中实现以控制基于XML的Web服务流量，并且越来越多地在面向云的计算中实现，帮助企业将内部部署应用程序与外部云托管应用程序集成。XML设备通常也称为SOA设备、SOA网关、XML网关、云代理。
3 安全消息传递	当将敏感数据被发送到公司网络外时，启动服务器层面的防御机制，以符

	合HIPAA、GLBA和SOX等合规要求
3 应用防火墙	一种防火墙的形式，用于控制应用程序或服务的输入、输出和/或访问。 它通过监视并可阻止不符合防火墙配置策略的输入、输出或系统服务调用运行。
3 安全协作	一种用于保护协作服务（例如 SharePoint）的技术或解决方案，将访问权限扩展到移动办公的员工、合作伙伴、供应商甚至客户。
3 实时过滤	一种跟踪使用模式和信息的控制，例如根据策略可实时访问或屏蔽某些站点。
1 数据保护	在信息时代，数据是一种资产。但是，大多数数据只有在受到保护时才有价值。数据保护需要覆盖全数据生命周期的各阶段、数据类型和数据状态。数据生命周期包括创建、存储、使用、传输、共享和销毁等阶段。 数据类型包括非结构化数据（例如文字处理文档）、结构化数据（例如数据库中的数据）和半结构化数据（例如电子邮件）。数据状态包括静态数据 (DAR)、传输中数据 (DIT)（又名动态数据、飞行数据）、和使用中的数据 (DIU)。 数据保护控制包括数据生命周期管理、数据防泄露（DLP）、通过数字权限管理的知识产权保护以及密钥管理和PKI/对称加密等加密服务。
2 数据全生命周期管理	数据生命周期管理包括以下六个阶段：创建、存储、使用、共享、归档和销毁。尽管显示为线性进展，但一旦创建，数据可以在各个阶段之间不受限制地流动，并且在可用期间内可能不会经历所有阶段。
3 元数据控制	控制底层数据附带的元数据类型（例如，由文字处理应用程序生成的文档修改记录的维护文档元数据，不应该与文档一起发布）
3 电子签名（非结构化数据）	电子签名表明某人采用数码数据的内容，或者声称编写了消息的人就是本人。 这最常用于非结构化数据。
3 数据去标识化	通过使用数据屏蔽等方法从数据集中删除识别信息的流程，最常用于保护个人隐私。数据去标识化还可用于保护组织，例如统计调查中包含的企业，或其他信息，例如矿物或考古发现或濒危物种的空间位置。
3 生命周期管理	用于管理数据从创建到使用、存档到最终销毁的整个生命周期的政策、流程和程序
3 数据屏蔽	在数据存储中隐藏（屏蔽）特定数据元素的流程。 它确保敏感数据被替换为实际可用但不真实的数据，目标是敏感数据在授权环境之外不可用。
3 数据模糊	通过某种形式的混淆（例如加密）保护字段或数据记录的一种方法。例如，可以在源代码中使用数据混淆技术来防止应用程序的逆向工程。还有一些

	技术含量低的解决方案，比如用油墨印花涂抹纸质文件上的敏感信息。
3 数据打标	数据标签是通常作为元数据形式分配给一条信息的关键字或术语，有助于描述一个项目，并有助于通过浏览或搜索再次找到。
3 数据标记	数据标记是一种在数据中植入易于识别的对象用以检测和跟踪被抓取、抄袭和盗窃的数据的最终位置，或是使用虚假记录破坏数据的价值的方法。例如，通过在电话号码数据库中插入奇怪名称的记录，如果该虚假记录出现在竞争对手的数据库中，则真正的发起人/所有者可以识别该记录。
2 数据防丢失（DLP）	DLP是指执行通过策略以确保知识产权和客户信息等关键数据不会从企业内泄露到非预期方的保护系统。包含发现和分类敏感数据，根据内容和上下文形成定义和管理策略，监控和执行数据移动路径，以及报告、审计和记录数据泄漏事件的一组策略。
3 数据发现	扫描和分类保存在网络、端点和服务器中的数据。
3 网络（传输中的数据）	请参阅传输中的数据加密（在本例中为 DLP）
3 端点（使用中的数据）	请参阅使用中的数据加密（在本例中为 DLP）
3 服务器（静态数据）	请参阅静态数据加密（在本例中为 DLP）
2 知识产权保护	防止滥用和不当披露知识产权的活动（例如应用流程或技术控制措施）。
3 知识产权	是基于创造成果经特定程序被法律所承认的权利的统称。根据知识产权法，所有者被授予如音乐、文学和艺术作品；发现和发明；以及单词、短语、符号和设计等无形资产的专有权。常见的知识产权类型包括版权、商标、专利、工业设计权和某些司法管辖区的商业秘密。
3 数字版权管理	DRM是硬件制造商、出版商、版权所有者、企业和个人用来限制使用数字内容和设备的访问控制技术的术语。这个词至少有两种含义。一种是指支持1998年《跨世纪数字版权法》(Digital Millennium Copyright Act，或称《数字千禧著作权法》)的技术，保护受版权保护的媒体、维持版税并确保艺术的控制措施。另一种则适用于企业权限管理技术，这些技术试图使安全控制措施更贴近企业数据本身，通常是在指加密及元数据中携带的访问控制信息。
2 加密服务	一组加密功能（例如，编码和解码、加密和解密），计算机应用程序可以使用这些功能实现安全解决方案（例如，强用户身份验证或安全电子邮件）。例如，在Microsoft Windows中，加密服务提供程序 (CSP) 是实现 (CAPI) 的

	软件库。
3 密钥管理	密钥管理涵盖密钥从始至终的整个生命周期，包括生成、通信和分发、存储、输入和安装、检查有效性、使用、变更活动密钥、归档、销毁、密钥操作和使用的审计、密钥备份和恢复，以及紧急储备钥匙。
4 对称密钥	也称为对称密码密码，双方必须使用相同的密钥加密和解密。在对消息解密之前，双方必须共享加密密钥。
4 非对称密钥	也称为非对称密码，加密密钥和解密密钥是分开的。在非对称系统中，每个人都有两把钥匙。一个密钥，即公钥，是公开共享的。第二个密钥，即私钥，不应与任何人共享。
3 公钥基础设施（PKI）	公钥基础设施 (PKI) 是创建、管理、分发、使用、存储和撤销数字证书所需的一组硬件、软件、人员、策略和程序，支持商业社区中的所有使用公钥密码的参与者 . 组件包括注册机构和证书机构。PKI是一个典型的分层模型，由根证书颁发机构、注册机构和证书颁发机构组成。
3 签名服务	一种提供电子编码消息的软件程序或功能，该消息对文档和签名者都是唯一的，并将两者绑定在一起。数字签名确保签名者的真实性。 签名后，对文档所做的任何变更都会使签名无效，从而防止签名伪造和信息篡改。
3 使用中的数据加密（内存）	“使用中的数据”（在内存、交换、处理器缓存或磁盘缓存等中的数据）的加密。
3 传输中的数据加密（临时的/永久的）	传输中的数据加密（临时的/永久的）
3 静态数据加密（数据库、文件、SAN、桌面、移动设备）	“静态数据”（记录在存储介质上的数据）的加密。
1 策略与标准	安全策略是企业安全架构逻辑抽象的一部分。它们源自基于业务需求的风险，存在于多个不同级别，包括信息安全策略、物理安全策略、业务连续性政策、基础设施安全策略、应用程序安全策略和总体业务运营风险管理策略。安全策略是业务的状态体现，指什么样的业务应该用怎样的安全手段以及需要多少投入。政策通常应该说明要做什么，同时避免涉及特定的技术解决方案。安全标准是组件级别的抽象，需要确保许多不同的组件可以集成到系统中。有许多国际公认标准机构的安全标准，如 ISO、IETF、IEEE、ISACA、OASIS 和 TCG。还可以在操作安全基线、工作指南、最佳实践、监管要求的相关性和基于角色的意识方面提供指导。对信息分类并将策略与

	生成的数据类别关联是安全处理策略及其实施的一种方法。
2 运维安全基线	基线列举了一个可以进一步专业化的符合策略的起点（例如，转移到生产流程可能包括一个基线配置，该配置要求所有默认用户/密码、SNMP社区名称等变更它们的默认值，然后设备才能用于生产。如果设备需要额外的加固，例如部署在DMZ中，则将应用进一步的专业基线）。
2 工作指南	又名标准操作程序或手册，通过存储信息或指令提供给用户，指导他们正确执行任务。在实际应用中，当用户需要了解信息或流程时，可以在需要时快速查阅，为用户提供具体、简洁的信息，从而降低个人的记忆成本。在执行某些严格依赖步骤顺序的情况下，是一种有效减少问题发生的方法。
2 基于角色配置	政策与给定角色的关联。例如，用户可以被指定为“本地用户”，并且数据传输等功能可以配置为仅对“本地用户”角色可用，而对具有“移动用户”角色的用户不可用。
2 信息安全策略	指导组织信息安全操作的管理意图的广义声明。策略是通过标准和程序实现，并且可以通过审计验证其合规性。
2 技术安全标准	规定必须如何实施特定的安全技术控制措施（例如，安全策略可能要求对特定类别的数据进行静态加密，而安全技术标准可能指定加密必须使用FIPS 140-2 认证的 AES-256） .
2 数据/资产分类	将所涉及信息数据分为若干类，并为每个分类配置一组安全策略的实现方法。服务器和终端等资产也可照此进行分类定义。在特定情况下，数据只能在具有相同分类级别的计算机上处理或存储。
2 监管要求与最佳实践	最佳实践与强制性监管要求的映射关系。如果监管要求需要加密某种类型的数据（例如，HIPPA中的PHI），那么供应商的最佳实践文档将与监管要求相关联，以显示满足合规的最佳实践。

示例

在家工作的员工必须使用其密钥卡上的一次性密码令牌登录公司的VPN。 正在构建的新网站经过了公司安全策略合规性测试。 如果硬盘加密，窃贼就无法读取被盗的笔记本电脑上的数据。

提供的服务

治理、风险管理与合规：GRC涵盖、整合和协调公司治理、企业风险管理和公司遵守适用法律法规等活动。组件包括合规管理（确保遵守所有内部信息安全策略和标准）、供应商管理（确保服务提供商和外包商遵守预期的和合同规定的信息安全策略，应用所有权和托管概念）、审计管理（突出需要改进的领域）、IT 风险管理（确保所有类型的风险都被识别、理解、传达，并被接受、修复、

转移或避免）、策略管理（维护组织结构和流程，支持代表业务需求的战略的创建、实施、异常处理和管理），以及技术意识和培训（提高选择和实施有效技术安全机制、产品、流程和工具的能力）。

相关组件：

- 2 合规管理
- 2 策略管理
- 3 例外
- 3 自评估
- 2 供应商管理
- 2 审计管理
- 2 IT风险管理
- 2 技术意识和培训

信息安全管理：“信息安全管理”的主要目标是实施适当的措施，最大限度地减少或消除与安全相关的威胁和漏洞可能对组织产生的影响。衡量标准包括：“能力成熟度模型”（确定组织的发展阶段，从不成熟的状态到随着组织获得经验和知识而达到的几个成熟度级别）；“能力映射模型”（描述企业为实现其目标所做的工作，以及促进业务模型和支持业务需求的技术基础设施之间的强关联，从而形成业务和 IT 都可以理解的视图）；安全架构路线图（为服务于特定业务计划的特定项目提供指导）和风险组合（已识别的风险被登记、监控和报告的地方）。使用安全管理和风险管理仪表盘衡量和报告决策的有效性水平，并帮助组织做出新的决策，保持和提高安全的有效性。对残余风险进行修复的分析和计划，也是整体风险管理框架的一部分。

相关组件：

- 2 能力映射
- 2 成熟度模型
- 2 风险组合管理
- 2 风险仪表盘
- 2 残余风险管理

权限管理基础设施：“权限管理基础设施”通过“身份和访问管理” (IAM) 功能（例如身份管理、认证服务、授权服务和权限使用管理）确保用户具有执行其职责所需的访问权限。此安全规则使合适的人员能够在合适的时间出于合适的原因访问合适的资源。它满足了确保在日益异构的技术环境中访问适当资源的关键任务需求，并满足日益严格的合规性要求。

“权限管理基础设施”的技术控制措施侧重于身份配置、密码、多因素身份验证和策略管理。

这种安全实践对任何企业都是一项至关重要的工作。由于它与业务越来越保持一致，因此需要同时具备业务能力，而不仅仅是技术专长。

相关组件：

- 2 身份管理
- 3 域唯一标识符
- 3 联合身份管理
- 3 身份配置
- 3 属性配置
- 2 认证服务
- 3 令牌
- 3 基于风险授权
- 3 多因子认证
- 3 一次性密码（OTP）
- 3 智能卡
- 3 密码管理
- 3 生物特征识别
- 3 网络认证
- 3 单点登录（SSO）
- 3 服务安全
- 3 中间件认证
- 3 身份核实
- 3 开箱即用（OTB）的身份认证
- 2 授权服务
- 3 权限审查
- 3 策略执行
- 3 策略定义
- 3 策略管理

- 3 主体数据管理
- 3 资源数据管理
- 3 可扩展访问控制标记语言（XACML）
- 3 角色管理
- 3 必要操作指令
- 3 开箱即用（OTB）的授权
- 2 特权使用管理
- 3 键盘/会话日志
- 3 密码保管库
- 3 特权使用网关
- 3 资源保护
- 3 Hypervisor合规和治理

威胁和漏洞管理：这个领域涉及核心安全，例如漏洞管理、威胁管理、合规性测试和渗透测试。漏洞管理是一项复杂的工作，企业跟踪其资产、监控和扫描已知漏洞，并通过软件补丁、变更配置或部署其他控制措施，尝试减少可利用的攻击资源。威胁建模和安全测试也是有效识别漏洞的一部分活动。

相关组件：

- 2 合规测试
- 3 数据库
- 3 服务器
- 3 网络
- 2 漏洞管理
- 3 应用程序
- 3 基础架构
- 3 数据库
- 2 渗透测试
- 3 内部

- 3 外部
- 2 威胁管理
- 3 源代码扫描
- 3 风险分类

基础设施保护服务：“基础设施保护服务”保护服务器、终端、网络设备和应用程序层。该领域使用传统的纵深防御方法确保容器和数据管道的健康。“基础设施保护服务”通常视为预防性技术控制措施，例如 IDS/IPS、防火墙、反恶意软件、“白名单”、“黑名单”等。它们在防御大多数传统或非高级攻击方面相对具有成本效益优势。

相关组件：

- 2 服务器
- 3 恶意软件行为防护
- 3 白名单
- 3 敏感文件保护
- 3 主机入侵防护系统/主机入侵检测系统（HIPS / HIDS ）
- 3 反病毒
- 3 主机防火墙
- 2 终端
- 3 反病毒、反垃圾邮件、反恶意软件
- 3 主机入侵防护系统/主机入侵检测系统（HIPS / HIDS ）
- 3 主机防火墙
- 3 介质锁定
- 3 基于硬件的可信资产
- 3 恶意软件行为防护
- 3 资产库存控制
- 3 内容过滤
- 3 取证工具
- 3 白名单

- 2 网络
- 3 恶意软件行为防护
- 3 防火墙
- 3 内容过滤
- 3 深度报文检测（DPI）
- 3 主机入侵防护系统/主机入侵检测系统（NIPS / NIDS）
- 3 无线防护
- 3 链路层网络安全
- 3 黑名单过滤
- 2 应用程序
- 3 XML应用机
- 3 安全消息传递
- 3 应用防火墙
- 3 安全协作
- 3 实时过滤

数据保护：在信息时代，数据是一种资产。 但是，大多数数据只有在受到保护的情况下才能保有价值。“数据保护”需要涵盖数据生命周期的所有阶段、所有的数据类型和数据状态。 数据生命周期阶段包括数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁。数据类型包括非结构化数据（例如文字处理文档）、结构化数据（例如数据库中的数据）和半结构化数据（例如电子邮件）。数据状态包括静态数据 (DAR)、传输中数据 (DIT)（也称为“运动中的数据”或“飞行中的数据”）和使用中的数据 (DIU)。 数据保护控制包括数据生命周期管理、数据泄漏预防、通过数字权限管理的知识产权保护，以及密钥管理和 PKI/对称加密等密码服务。

相关组件：

- 2 数据生命周期管理
- 3 元数据控制
- 3 电子签名（非结构化数据）
- 3 数据去标识化
- 3 生命周期管理

- 3 数据屏蔽
- 3 数据模糊
- 3 数据打标
- 3 数据标记
- 2 数据防泄露（DLP）
- 3 数据发现
- 3 网络（传输中的数据）
- 3 终端（使用中的数据）
- 3 服务器（静态数据）
- 2 知识产权保护
- 3 知识产权
- 3 数字版权管理
- 2 加密服务
- 3 密钥管理
- 4 对称密钥
- 4 非对称密钥
- 3 公钥基础设施（PKI）
- 3 签名服务
- 3 使用中数据加密（内存）
- 3 传输中数据加密（临时的、永久的）
- 3 静态数据加密（数据库、文件、SAN、桌面、移动设备）

策略和标准：安全策略是“企业安全架构”逻辑抽象的一部分。它们源自基于风险的业务需求，并存在于多个不同级别，包括信息安全策略、物理安全策略、业务连续性策略、基础设施安全策略、应用程序安全策略以及总体业务运营风险管理策略。安全策略是获取了企业安全要求的陈述，指定什么类型的安全以及应该采用多少安全措施保护业务。策略通常说明应该做什么，同时避免提及特定的技术解决方案。安全标准是组件级别的抽象，需要确保许多不同的组件可以集成到体系中。

来自标准机构的国际公认的各个方面的安全标准包括 ISO、IETF、IEEE、ISACA、OASIS 和 TCG。其他还可以提供指导的形式包括操作安全基线、工作辅助指南、最佳实践、监管要求的相关性和基

于角色的意识等。处理安全策略及其实施的一种方法是对信息进行分类，并将策略与产生的数据类关联起来。

相关组件：

- 2 运维安全基线
- 2 工作辅助指南
- 2 基于角色的配置
- 2 信息安全策略
- 2 技术安全标准
- 2 数据/资产分类
- 2 监管要求与最佳实践

与其他域的关系

SRM 为 “IT 运营和支持”提供安全环境。 ITOS能力和功能方面的安全，对于支持业务的IT服务的交付至关重要。SRM 是“业务运营支持服务”下“运营风险管理”的关键组成部分，安全风险是组织商业智能(BI)的关键数据点，商业智能提供了做出合理业务决策所需的信息。“人力资源”通过对员工的高度关注支持 SRM。SRM提供“身份和访问管理服务”，这些服务是向用户展示数据的先决条件。保护传输、存储和使用中的数据是“应用服务”处理和操控数据的关键基础。 SRM依赖“基础设施服务”提供的核心组件和功能，包括设施的物理安全和补丁管理。