第30章

云计算安全治理

本章讲解的内容对应图 25-1 的左上部分，即云计算安全治理。

30.1 组织架构与过程模型

第 26～第 29 章主要讲述了云计算安全的技术实施。云计算安全如同传统的信息安全一样，也是技术、流程和管理(人)等多种安全要素的有机结合，本章将主要从管理和流程的角度阐述如何治理云计算安全。缺乏有效的安全治理将导致关键业务需求很难被满足，因而也很难保证云计算用户规模和云计算产品的市场竞争力。

30.1.1 组织架构

在不同领域(如医疗、金融等)，云计算安全治理方法与控制机制有很大不同。但无论是在哪个领域，在进行云计算安全治理活动前，CP 都需要有一个明晰的云计算安全的高层战略，这包含机构实施云计算安全治理要达到的总体目标及由此产生的总体需求。一个内容清晰而合理的云计算安全高层战略是构建云计算安全治理可持续运营模型的基础。

要制定高层战略，通常还需要成立一个云计算安全委员会。云计算安全委员会提供与机构业务和 IT 战略相一致的云计算安全行动指南，如云计算安全章程。在这个章程里通常会规定云计算安全治理团队以及其他与云计算安全相关的人员角色及职责。这些安全角色可能包括面向内部安全治理和外部客户安全服务的安全角色，如负责基础设施安全的人员、负责数据安全的人员、负责应用安全的人员、面向客户安全服务的人员、负责安全技术统筹实施的人员和负责安全管理的人员等；以及与服务安全治理相关的外部安全角色，如外部专家与技术顾问和终端用户等。一些角色可以合并，也可以划分得更细，这取决于云计算规模及机构整体业务战略。

需要强调一下的是，云计算安全委员会不仅要在章程里明确规定安全治理组内部安全角色及其相应职责，还要明确定义外部安全角色的职责，尤其是终端用户，虽然 CP 可能并不能完全控制其职责的实施，但应在云计算合约签订时明确告知终端用户应该负责提供的安全职责，如实施终端设备安全增强机制、采用符合 CP 要求的终端安全访问措施、加强加密密钥及证书等敏感信息保护意识等。

云计算治理要取得一个持续可运营的安全治理效果，除需要云计算安全委员会及安全治理组外，一般还需要一个云计算安全规划组。云计算安全规划组根据云计算安全委员会制定的高层战略，结合云计算安全治理组的实施建议来制定云计算安全实施规划。图 30-1 是云计算安全治理组织架构示例，它包括机构管理层、云计算安全委员会、云计算安全规划组，以及包含内部和外部人员组成的安全治理组。

云计算安全战略与云计算组织架构是云计算安全治理的输入项与基础，基于此，有助于构建一个目标明晰、过程可持续改进的云计算治理模型。

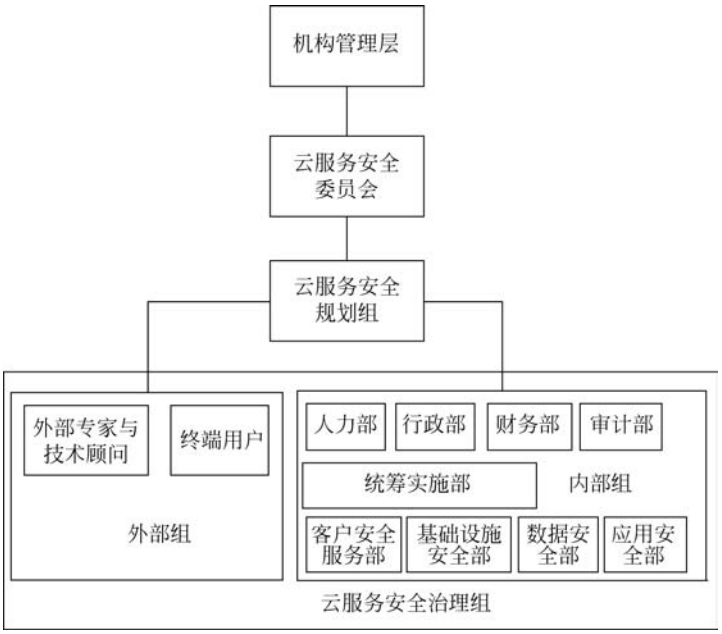

图 30-1　云计算安全治理组织架构示例

30.1.2　风险管理

云计算安全治理的过程也是云计算运营安全风险管理的过程。按 ISO 27005：2008（《信息技术－安全技术－信息安全风险管理》）对风险管理的定义，风险管理包括确定范畴、风险评估、风险处置、风险接受、风险沟通、风险监视与评审以及风险管理方法改进等，其中风险评估包括风险识别、估算与评价；风险处置包括风险降低、风险转移、风险保持与风险避免。风险管理过程通常需要对风险评估和风险处置循环进行，以获得在高风险识别与控制措施上的不断改进。

云计算环境下有效的风险识别应包含如下内容：

- 信息资产的识别，包括基础设施资产的识别、数据类型及保护级别识别、业务流程识别、应用类型识别以及数据所有权与监管责任的识别等。
- 威胁识别，包括威胁种类识别、威胁来源识别、威胁影响识别及威胁频率识别等。
- 脆弱点识别，可在组织架构、治理流程、安全相关人员、云数据中心物理环境、网络及基础资源、系统及服务配置等方面进行识别。

根据不同的云计算交付模型和部署模型，云计算环境下的风险处置（降低、转移、避免、接受）主体不同，尤其对公有云计算，由于涉及多方利益，风险处置前的沟通显得更为重要。如对公有云的 IaaS 服务、数据及应用层风险处置则由用户自己选择处理，CP 对基础资源层的风险处理需要与其相关资源的供应商及 CS 进行风险沟通后选择风险处置选项；此外，CS 可以通过选择不同的服务交付模式进行风险转移，如选择公有云的 SaaS 应用，则将数据和服务设施等风险转移至 CP。

安全风险评估为机构提供一种平衡安全控制实施与资产保护需求的重要依据。

30.1.3 过程模型

云计算是一种 IT 服务，也应遵循 ISO 27001：2005《信息技术-安全技术-信息安全管理体系要求》的 PDCA（Plan、Do、Check、Act）过程模型。云计算安全治理从规划到云计算安全治理改进形成闭环流程，云计算安全治理的过程即是云计算安全风险管理的过程。图 30-2 给出云计算安全治理过程与风险管理的关系。

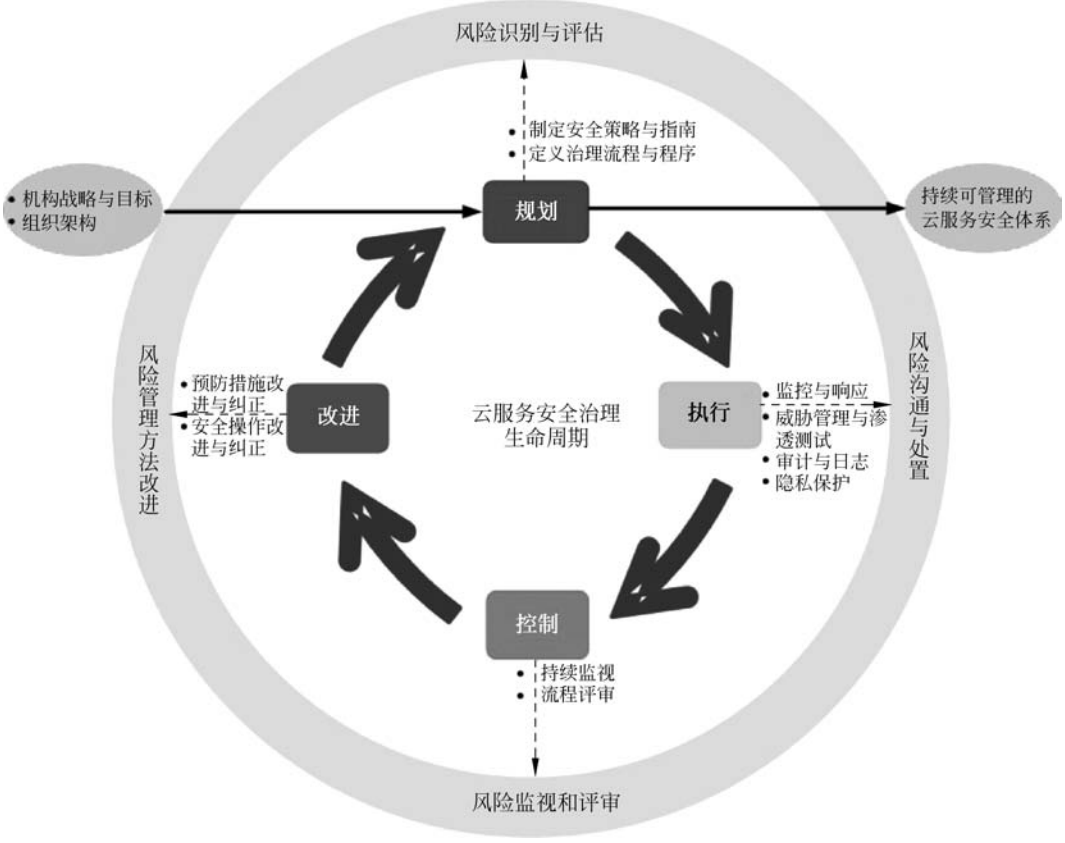

图 30-2 云计算安全治理过程与风险管理的关系

云计算安全治理过程包括四个阶段：

- 规划阶段：根据管理机构的云计算安全高层战略指导思想（输入项），由云计算安全治理组和云计算安全规划组共同制定云计算安全治理实施策略、云计算安全治理流

程与处理程序，并对安全风险进行评估等。

- 执行阶段：根据安全策略、治理流程定义以及风险评价清单实施安全操作并进行风险处置，安全操作包括安全监控与告警、安全扫描与渗透测试、变更管理、安全审计及隐私保护等。
- 控制阶段：根据安全策略、目标及既有经验评估与测量执行阶段的过程与风险管理效果，向管理层报告结果，并进行评审和持续监视。
- 改进阶段：根据内部审计及管理评审结果等信息，给出安全技术实施预防措施及安全治理操作纠正和改进建议，最终实现可持续、可管理的云计算安全治理体系。

控制和改进阶段方法具体实施请参照 ISO 27001：2005 8.1 节和 8.2 节的描述。本章后续内容主要针对规划阶段的策略制定以及执行阶段安全操作进行描述并给出实施建议。

30.2　云计算安全治理操作

30.2.1　云计算安全指南制定

国际云安全联盟（Cloud Security Alliance，CSA）发布的《云计算关键策略安全指南》（简称云计算安全指南）是 CP 关于云计算安全治理的白皮书，是满足 CP 云计算业务发展要求和相关法律法规而制定的云计算安全治理的指导文件，是对机构信息安全高层战略及目标的细化与解析。

《云计算安全指南》是指导机构员工正确操作、使用和管理云计算环境下信息资产，并保护这些资产使其拥有更好的保密性、完整性和可用性的明确指南。《云计算安全指南》是云计算安全体系防范潜在威胁的重要组成部分，这些策略在察觉并防范社会工程学攻击时尤为有效。云计算安全委员会应根据业务战略和目标制定清晰的方针指导，并通过在整个机构中颁布和维护云计算安全策略来表明对云计算安全的支持和承诺。

建立《云计算安全指南》的目的如下：

- 在 CP 机构内部与合作伙伴中建立一套云计算资产及服务安全相关的、通用的、行之有效的安全机制。
- 在 CP 内部员工与合作伙伴员工中树立起安全责任感。
- 增强云计算信息资产的可用性、完整性和保密性。
- 提高内部员工、合作伙伴员工及 CS 的信息安全意识和信息安全知识水平。

《云计算安全指南》应包含明确的目标、管理意图、职责与权限、相关术语及操作细则定义等，具体涵盖范围如下：

（1）定义与云计算安全策略和指南相关的术语。

（2）明确云计算安全策略和指南的目标。

（3）确定云计算安全策略和指南适用的信息资源及工程资源的范围。

（4）明确云计算安全治理相关组织和人员的角色与职责，以维护云计算安全和报告安全漏洞或事件。

（5）识别云计算安全风险，并评估可能发生的影响。

（6）定义变更审批流程和责任。

(7) 定义灾难恢复相关的资源、流程和责任。

(8) 定义一套从开发到运营的云计算安全控制实施标准,包括:

- 物理和逻辑访问控制。
- 事件响应与管理。
- 系统及网络配置备份。
- 周期性安全测试。
- 数据及通信加密(加密算法及密钥长度)。
- 密码标准。
- 持续性监控。

(9) 定义确保以下几方面的安全所需的处理流程和责任:

- 数据中心。
- 网络。
- 服务器和操作系统。
- 虚拟化软件。
- 数据库。
- 应用中间件。
- 代码开发和应用程序等。

(10) 指定文档的审查和修订流程。

30.2.2 安全监控与事件响应

1. 云计算环境下安全监控的意义

在云计算运营环境下,云数据中心规模庞大,应用系统多样,涉及运维及合作厂家的人员多而杂,需要有一种机制能实时可视化地记录云数据中心人员及系统的活动行为,并对安全事件提供告警。

安全监控即通过对云计算数据中心的操作人员、网络、主机及应用系统活动行为的监视,识别、记录,并统计网络、系统及应用服务的脆弱性、外部攻击与异常行为以及安全违规行为等,通过事件告警及通知机制使安全管理人员有效地监视、控制和评估网络或主机系统的运行状态,及时对安全事件进行响应,消除安全隐患或降低安全风险。

全方位的持续性监控机制和定义清晰的事件报警流程是治理良好的云计算数据中心的基础。随着云计算基础设施增长及云计算业务的不断扩展,安全监控的重要性将更加明显。在云计算环境下实施安全监控的具体意义有以下几方面:

- 发现事先无法防御的威胁:对于一些难以事先阻止或防御的攻击,安全监控则成为最后一道防线。
- 验证安全控制措施的有效性:安全控制措施通常是对安全策略的执行,其结果反映了安全控制措施实施是否正确。如果在安全事件流里出现了一些安全策略禁止的事件,则表明安全控制没有按安全策略正确实施。
- 暴露系统脆弱性:通过运行监控可以识别一些未曾发现的系统脆弱性或安全错误。
- 记录安全行为:安全监控捕获的安全事件数据合法地记录了用户或执行过程的活

动行为。

- 提供电子取证重要数据支持：在多租户云计算环境中，安全监控可以为攻击过程提供视频回放，安全事件数据则提供重要信息记录，这对于需要分析攻击过程和识别损失范围的电子取证具有非常重要的价值。

此外，通过采用一些先进的安全监控解决方案，CP 可以把安全监控作为服务对外提供。

2. 安全监控分类

安全监控通常分成两类，一类是物理监控，如视频监控、门禁、火、水及其他环境传感器、设施巡检等，这些活动通常由数据中心安全人员负责；另一类是电子监控，包括内部系统监控和威胁监控。无论哪种方式，都要有一个定义清楚的流程来确保记录了能满足安全策略要求的日志。

内部系统监控通常用于监控所有的服务器的系统补丁和防病毒补丁是否及时更新，以及 CPU 和 RAM 的利用率情况等。为提高查询效率，通常要将从这些服务器搜集到的数据存放于一个数据库中（如配置管理数据库）。

云计算环境下的威胁监控首先要从 IDS/IPS 传感器、病毒日志以及各种设备的系统日志搜集事件及报警数据。对于一些中小型数据中心可以通过人工方法收集数据，而对于一些大型数据中心，则需要利用一些工具实现自动信息收集，这些工具包括威胁关联引擎和各种各样的安全事件管理工具等，如 OSSEC、TripleWire、Splunk、Webtrends、logAnalysis 等。这些自动化工具能够减少出现在事件流中的假阳性事件数量，可以识别更复杂的攻击以及对出现故障的传感器进行报警，并可将报警分组发送并对传感器的数据进行整合关联等。

3. 云计算环境下的安全监控要求

安全监控主要用于收集环境数据、进行网络安全监控及审计日志等。在云计算环境下，安全监控的要求如下：

- 安全监控应该是一个高可用的硬件化服务设施，可通过安全方式从内部和远端进行访问。
- 安全监控要能对发生或检测到的关键安全事件以自动化方式生成告警。
- 关键告警要能通过多种方式上报并及时提醒安全管理人员。
- 安全监控审查的日志至少要能涵盖以下几种：IDS/IDP 日志、防火墙日志、用户账号日志、互联网设备日志（路由器、交换机等）、应用程序日志、Web 服务器日志、Web 应用程序防火墙日志、数据库服务器备份和恢复日志。
- 根据安全事件分级，安全人员应有多种事件响应方式，如对重要安全事件进行立即调查或处理，或仅简单浏览日志以完善告警机制等。
- 安全监控必须确保是可靠且正确的，即使事件生成和报告数据收集出现故障也要保证递交的事件是可靠的，安全日志必须符合法律及安全策略。

此外，还可以考虑一些其他扩展性功能，如允许客户对 PaaS 或 IaaS 实施入侵、异常检测，甚至允许它们发送安全事件或告警到 CP 的安全监控系统里。

最后需要提醒的是，由于 SaaS 服务面临的威胁和攻击的类型与传统的基于基础设施和物理环境的威胁及攻击有很大不同，因此，SaaS 服务机构需要扩展其传统的安全监控能力以包含对应用及数据层活动的监控，同时还需要组建一支面向云中应用安全及隐私保护等

专业领域的安全团队，以保证客户数据安全并提供应用服务的稳定性。作为参考，本章最后附部分安全告警列表。

4. 事件响应

安全监控的最终目标是对识别和检测出的安全威胁进行处理，以消除安全隐患或降低安全风险。安全监控和事件响应是两个密切联系、相互依赖的安全域，缺少任何一个环节整个安全监控将达不到预期效果。

在对安全事件进行响应之前，通常需要制定一个按安全事件严重等级区分的事件响应计划。首先给出安全事件的等级定义，并用不同的方法标识，如低、中、高或主要、次要等，并且对每个事件定义一个合理的响应。对于低级别安全事件，可以由运营人员作为日常管理活动的一部分进行处理；对于第二级别的安全事件，如机架电源故障或影响一段网络的网络故障等，除要修复此问题外，还要跟踪事件处理过程，并根据需要决定是否发起一个根本原因分析（RCA）流程，以确定原因在哪和是否需要改变策略、基础架构等以制止此类事件再次发生；对于影响大量用户或可能引发重大安全危害或影响机构信誉的最高级安全事件，做好响应计划是成功响应这类事件的关键。通常情况下，这类事件的响应不仅涉及运营人员，还可能涉及供应商及合作伙伴等，而且这类事件要求认真对待和专业处理。此外，处理过程中的证据保留很重要，如果采取的处理步骤不当，证据很容易被毁坏。

30.2.3 威胁管理和渗透测试

大多数恶意软件都是通过网络远程攻击基础设施、部件、网络服务和应用中存在的漏洞，这使得基于网络的云计算面临更大的威胁。无论是对于使用公有云模式的 IaaS 用户而言，还是对于提供 PaaS 和 SaaS 服务的 CP 而言，都需对其部署的操作系统或应用系统的脆弱性、补丁和配置管理承担主要责任，都需要一种主动式的系统或服务的脆弱性发现，修复机制可以用来降低漏洞被攻击的概率。

威胁管理即通过对系统和基础设施中可能存在的脆弱性进行主动性扫描，根据漏洞可能引发的风险大小对发现的脆弱性进行分类评估，并根据脆弱性类型进行补丁修复，以降低风险或消除安全威胁。从流程上看，威胁管理分为三个阶段：安全扫描、脆弱性评估及补丁修复。

CP 和 CS 对云基础设施的威胁管理均负有责任，这取决于 SPI 服务模型。对于 SaaS 服务而言，由 CP 负责基础设施、网络、主机、应用、存储和第三方服务的脆弱性、补丁、配置管理（VPC），SaaS 提供商需要定期评估新的漏洞，并对 SaaS 服务中涉及的所有系统软件和固件进行补丁修复。在这种服务模式下，CS 基本上对威胁管理不承担责任；而在 IaaS 服务中，CS 则需要对其管理的整个软件栈（操作系统、应用及数据库等）的威胁管理负责；另外，CS 也需要为其部署在 PaaS 平台上的应用提供威胁管理，但这些都必须是在 CS 不泄露其他用户隐私且不涉及 CP 商业机密的前提下进行，用户可以获取所需的安全配置信息以及系统运行状态信息，并在一定条件下获得部署专用安全管理软件的权利。

需要说明的是，为提高安全治理效果，通常将安全监控、威胁管理（包括配置管理）及变更管理结合在一起，以防止误报，提高事件响应效率并降低安全风险。

1. 脆弱性管理

脆弱性管理是保护主机、网络设备和应用，避免已知漏洞攻击的重要威胁管理要素。其

通过扫描网络及信息资产中存在的脆弱性并对其进行分类，以获得更有效的威胁消除或风险降低的措施，如补丁和系统升级。脆弱性评估通常与威胁发现(来自安全监控或安全扫描等)、补丁管理、升级管理过程整合在一起，以便更有效、及时地修复漏洞。

成熟的机构通常有一个制度化的脆弱性管理流程，包括对网络环境下的各系统的脆弱性进行扫描，评估脆弱性可能给机构带来的风险并进行分级，解决风险问题的补救措施等(通常由补丁管理流程来完成)。脆弱性管理的最佳实践是安全运行人员先发布一些代码开发安全指南，并执行安全可接受性测试及相应标准，将脆弱性问题尽量在开发阶段解决。

安全扫描是脆弱性管理的基础，CP 应定期(如每周一次)进行安全扫描，以主动检查服务和应用中存在的脆弱性。安全扫描分两类，一类是端口扫描，一类是漏洞扫描。目前这两类扫描都有很多工具可用，最著名也是最常用的端口扫描工具是 Nmap。而流行的漏洞扫描工具有 Nessus(免费但不开源)、Core Impact 和 QualysGuard 和 ISS 的互联网扫描器等。在大多数情况下，可使用开源工具做内部安全扫描，使用商业解决方案以满足审计和合规需要。

端口扫描和漏洞扫描的区别往往模糊不清。端口扫描用来从远程网络位置收集有关测试目标的信息，尤其是找出每个目标主机或系统可提供的网络服务或开放的端口。而漏洞扫描用于扫描主机操作系统上已知的弱点和未打补丁的软件，以及文件访问控制和用户权限管理缺陷等配置问题。因此，端口扫描器和基于网络的漏洞扫描器的基本区别是，漏洞扫描器扫描所有系统及应用服务缺陷，包括脆弱性、访问控制缺陷和配置问题等，对于外部的恶意漏洞扫描，还会试图在目标系统上针对这些缺陷执行相应攻击；而端口扫描器只是产生可用服务的清单。

此外，设计良好的漏洞扫描器是渗透测试的一个重要工具，它为探测每个目标主机上可用的网络服务提供了必不可少的手段。漏洞扫描器可以扫描数据库记录的网络服务安全缺陷，并在目标范围内的主机服务上测试每个缺陷，这可以快速全面地发现目标系统常见的配置弱点以及未打补丁的网络服务器软件。

2. 补丁管理

与脆弱性管理类似，安全补丁管理也是保护主机、网络服务及应用、避免非授权的用户利用已知漏洞进行攻击的重要威胁管理手段，通过消除内部和外部威胁来降低机构安全风险。

补丁管理流程需要遵从变更管理框架(参考第 19 章)，其输入来自脆弱性管理。

在这种持续运营的云计算环境下进行补丁管理是非常必要也是非常重要的，以下是补丁管理的最佳实践建议：

- 所有云计算环境中运行的软件或系统所需的补丁，其开发、测试、部署及生产都需要在一个相互隔离的环境中进行。
- 在云计算环境下，必须要为网络部件、服务器、存储、虚拟化软件、应用和安全部件的软件或固件补丁管理定义一个明晰的流程。
- 必须要为漏洞修补或补偿性控制措施定义一个整合策略，策略包括从重大威胁响应到非关键性补丁处理策略等，以提高云计算的安全性或运营可靠性。

3. 安全配置管理

安全配置管理也是一个重要的威胁管理手段，可以保护主机、网络设备免受非授权用户

针对其配置缺陷进行的攻击。安全配置管理与脆弱性管理程序密切相关，是全部 IT 配置管理的一个子集。

保护网络、主机、应用的配置缺陷不受攻击需要进行安全监控，以及对关键系统和数据库配置文件的访问控制，包括操作系统配置及防火墙策略等。

4. 渗透测试

渗透测试(Penetration Test)并没有一个标准的定义，通用的说法是：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种方法。这个过程包括对系统的脆弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者的角度进行的。

渗透测试还具有两个显著的特点：一是渗透测试是一个渐进的并且可逐步深入的过程；二是渗透测试必须要采用不能影响业务系统正常运行的攻击方法来进行。

同脆弱性扫描一样，云计算环境下的渗透测试也需要定期进行。渗透测试往往需要较强的专业技巧和专业知识，云计算环境下基础设施及应用安全测试要求测试人员对虚拟化和云架构有深入理解。如果内部安全团队不具备这些能力，可以外包给有资质和能力的第三方来执行。

渗透测试和脆弱性扫描都可以发现大量漏洞，但与脆弱性测试有所区别的是，渗透测试着眼于整个云计算设施，而不仅仅是单个的服务器或部件漏洞。因此，渗透测试往往把云计算作为一个黑盒进行测试；而脆弱性测试则侧重于单个主机上系统或应用的脆弱性识别及配置缺陷等问题。

渗透测试和脆弱性扫描发现的漏洞并不是都必须或能够被修复，这些漏洞可以按关键、高、中、低进行分级。通常对于关键或高级别的漏洞需要进行修复，而对于中或低级别的漏洞，根据不同的云模型及 CP 的业务需求，可以选择接受或进行修复。对于没有被修复的漏洞需要进行残余风险评估。此外，为提高安全修复效率，对于多个相同架构的服务器的脆弱性，可以制作一个黄金镜像来对多个服务器同时进行修复。

30.2.4 变更管理

无论是云服务中的软件还是硬件，在运营过程中，通过运营中的 bug 管理、需求管理及风险控制等，CPs 需要定期优化、完善、升级对外提供的服务或用于构建服务的内部功能模块。在新版本部署到生产环境之前，需要在一个尽可能与运营环境相同的环境中进行测试。由于云服务环境是由多个离散的部件组成的，这些部件可能包括运营商级交换机、路由器、目录服务器、安全基础设施、应用服务等，因此，这种优化或升级将是一个非常艰巨的任务，尤其对于公有云而言，更不允许因升级服务或完善基础设施而导致长时间停电。

云服务变更管理即通过对云服务及其基础设施变更需求及实施流程的管理，尽可能降低变更实施风险，满足业务需求，同时提高合规性。

虽然变更管理本身并不是云服务安全治理操作内容之一，但一个没有满足安全需求或存在安全漏洞的变更申请将会导致客户数据丢失或服务中断。成功的云服务安全团队通常需要与开发团队紧密合作，并积极跟进正在开发和测试中的产品变更情况。对于一些复杂且重要的产品变更，为提供变更的自服务能力及优化安全团队的时间及资源利用，安全团队也可以创建一个标准且具有最小变更内容的安全指南。

变更管理流程如图 30-3 所示。特别需要说明的是，上文中描述的配置管理及补丁管理在实施流程中也需要遵循变更管理框架。

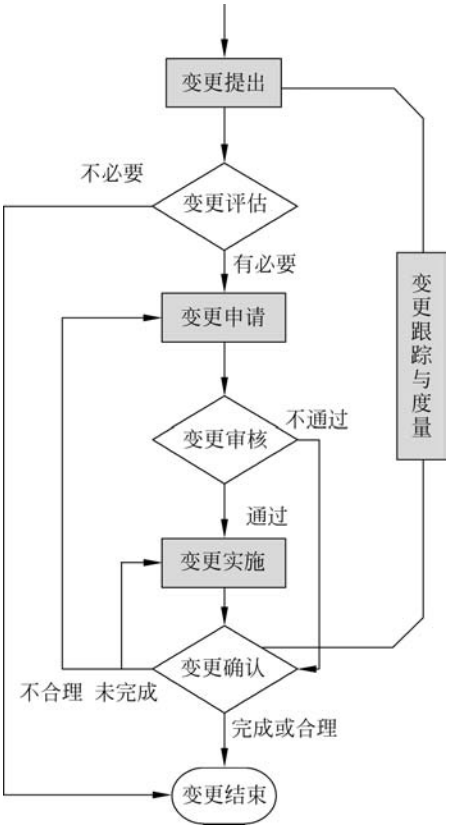

图 30-3　变更管理流程

30.2.5　安全审计与日志

云计算是一种构建体系复杂及用户群体多样的生态环境。在这种环境下，即使在相关的基础服务设施或系统内都实施了一定的安全保护机制（如访问控制和加密等），并且也在整个云计算环境中采取了一定的云计算安全治理措施，如安全监控、威胁管理和渗透测试等，但仍然不能保证某些基础设施或应用系统不会遭到破坏或攻击，以及一旦采用的这些安全防御体系被突破我们还能做什么。另一方面，作为面向广大用户群体提供服务并受到监管机构监管的云计算提供商，除了事前预防和事中监控的安全措施外，还必须要有一种能够提供事后追查和事后取证的机制，这种机制即是安全审计。安全审计一方面能及时发现预先定义的攻击性行为，另一方面也为法律或监管部门调查取证提供重要线索。此外，安全审计对于 CP 的业务恢复也具有重要意义，因为只有弄清系统是怎么遭到攻击的，才能更快地恢复系统或服务。从这些意义来讲，云计算环境下的安全审计如同飞机上使用的“黑匣子”。

安全审计是指识别、记录、存储、分析与网络和系统安全行为相关的信息的过程。安全审计是计算机和网络安全的重要组成部分，也是评判一个系统是否真正安全的重要标准。在云计算环境下，面向系统和网络的安全审计至少要实现以下几方面的安全目标：

- 跟踪或监测系统中的异常事件。
- 确认并保持系统活动中每个人的职责。
- 确认并重建已发生的安全事件。
- 评估损失。
- 提供有效的灾难恢复依据。
- 提供阻止不正当使用系统行为的依据。
- 提供网络安全案件侦破证据。

ISO/IEC15408 在“信息技术安全性评估通用准则 2.0 版”中对安全审计定义了一套完整的功能，包括安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计事件存储、安全审计事件选择等。在云计算环境下，安全审计系统应跟踪所有服务层次产生的与安全相关的事件，包括系统事件、安全事件、网络事件、应用事件以及其他事件等。图 30-4 所示是安全审计系统框架。

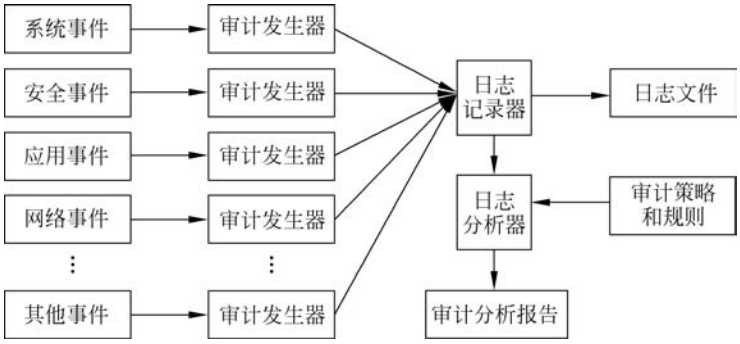

图 30-4 安全审计系统框架

安全审计有两种实施情况：

- 内部审计：是应内部治理需要而做的，如为彻底审视云计算安全治理状况，这通常由云计算治理安全组织架构中的审计部门来负责实施。
- 外部审计：通常由监管部门的合规检查或客户的合规性要求而做，多由外部代理或顾问来实施。目前外部审计情况居多。

此外，无论是内部安全审计还是外部安全审计，以下都是进行安全审计的实施步骤。

- 第一步：定义审计的范围和目标。创建一个主列表，列出审核应该包括的工作。大多数情况下，如果以前做过同样或类似的工作，都会有一些可以借用的模板或范例。
- 第二步：差距分析。主要是检查目前的状况、分析需要做多大改进，评估有多大风险和任务的紧急性等。
- 第三步：实施和部署解决方案。一旦知道了差距，下一步是针对每一个问题找到解决方案，并按照一定的优先级实施解决方案。

此外，对审计师的资质要求和人员选择也很重要。对于外部审计来说，很多时候组织没有权利去选择审计师或安全评估人员。由于目前阶段很多审计师对云和虚拟化技术还不是很熟悉，如果机构可以选择的话，强烈建议选择一个对云计算技术和安全都有一定了解的审计师，可以从询问这些人员关于 IaaS、PaaS、SaaS 相关术语的熟悉程度作为一个评判的起点。

本节重点阐述了云计算安全治理可采取的一些关键措施，包括制定安全策略、监控安全事件、管理风险与变更、记录安全日志等，这些多属技术领域范畴。下面将要讲解的云计算业务的隐私保护不仅涉及技术的范畴，更多会涉及法规政策及管理制度的范畴。

30.3 隐私保护

30.3.1 云计算环境下隐私保护的概念

随着互联网的普及与推广，近年来通过互联网来披露、公开或传播他人隐私行为的方式及事件已越来越多，如通过“人肉搜索”就可直接探测个人隐私信息，将例如家庭住址、年龄、身份证号等隐私信息轻而易举地挖掘出来。而随着互联网经济的快速发展，这种通过网络传播个人隐私信息的事件呈扩大化，侵权形式也更加多样化，侵权手段更为智能化，危害结果日趋严重化。

在讨论云计算环境下隐私保护问题之前，先看看什么是隐私。隐私的概念最早由美国法学家沃伦(Samuel D. Warren)和布兰德斯(Louis D. Brandeis)于1890年在《哈佛法律评论》发表的一篇文章《论隐私权》中提出，后得到全球各界人士的普遍认同。它是指自然人自身所享有的与公众利益无关的且不愿他人知悉的私人信息，这是隐私的普遍定义。对于基于网络的隐私，法学界至今还没有形成统一的看法。有的学者认为网络隐私是指自然人在网络上的个人数据信息、隐私空间以及任何与个人网络活动有关的信息。网络隐私权保护即禁止他人非法知悉、侵扰、传播或利用的权利。由于网络环境的开放性、虚拟性、交互性、匿名性等特点，使得基于现实环境的一些隐私权保护手段在网络环境中变得难以实施。

在云计算环境下，只要用户愿意，任何可以存放在本地机器的数据都可以存放在云上，包括邮件、健康档案、财务信息、约会计划、广告策划、商业计划、演示文档、图片、视频，等等。在云计算环境下，首先要保护这些存放的数据隐私信息，如不允许第三方在未经同意的情况下存储或读取用户云上存储的邮件信息等；其次还要保护发生在云环境下的用户操作行为的隐私性，如用户访问的站点应不允许用于商业目的收集；更重要的是，用户个人相关信息不允许共享给与用户云计算使用无关的他人。因此，概括起来，云计算环境下的隐私保护最主要的目的是防止CP恶意泄露或出卖用户隐私信息或机密数据，或者搜集用户数据进行分析以挖掘用户隐私信息，例如分析用户潜在有效的盈利模式，或者通过两个公司之间的信息交流推断他们之间可能有什么合作等。

对基于网络提供服务的云计算环境而言，由于用户数据控制权的转移及安全边界的消失，用户个人隐私信息及数据隐私保护问题，尤其是服务端隐私保护问题将变得更加突出，用户对云计算下的个人隐私信息及数据隐私保密性担忧已成为阻碍用户使用云计算的最大障碍之一。按Ponemon研究所及TRUSTe公司所做的“2008年隐私保护最受信任的公司调查”结果，隐私保护是如今电子领域里市场竞争的关键因素之一。调查认为云计算的消费者愿意和一个他们可以信任的CP建立业务关系。因此，对云中个人隐私及数据安全提供保护无论是对CP还是CS都具有重要意义。

30.3.2　云计算环境下的隐私数据

在云计算环境下，个人及数据隐私保护强调的是个人存放在云上的数据、云计算环境下的用户访问行为(如访问的站点)或双方签约相关信息(如身份证号码等)等不允许非授权访问或非正当原因的收集、使用与披露，最终目的是保护客户个人隐私信息及机密数据，并防御各种欺骗行为，如身份盗窃、垃圾邮件、钓鱼等。为便于阐述云计算环境下的隐私保护对策，先来看一下云计算环境下哪些信息是用户的隐私信息。

云计算环境下的用户隐私信息可以分成两块：一块是与用户使用云计算相关的数据，叫用户数据(User Data)；另一块是用于唯一识别、联系、定位个人或与其他信息一起可唯一识别个人的数据，即用户可识别信息(PII)，也叫个人数据(Personal Data)。

用户数据是从客户收集的信息，包括：

- 任何直接从客户处收集的数据，如通过用户界面输入的信息。
- 任何间接从客户处获得的信息，如文档中的元数据。
- 任何关于用户使用行为的数据，如日志和历史等。
- 任何与客户系统相关的数据，如系统配置、IP地址等。

个人数据可能包括以下几种：

- 联系人信息：姓名、邮件地址、电话、邮寄地址等。
- 身份信息：身份证、社交号码(SSN)、驾驶证、护照、医保卡、指纹、营业执照等。
- 人口特征：年龄、性别、种族、宗教信仰、性取向、犯罪记录等。
- 职业信息：工作头衔、公司名称、所属行业、从事专业等。
- 健康信息：健康计划、健康历史、保险情况、遗传信息等。
- 财务信息：银行存款、信用卡或借记卡账号、购买记录、信用卡消费记录等。
- 在线行为：IP 地址、Cookies、Flash Cookies、登录凭证等。

需要强调的是，对于企业用户而言，上述的用户数据是以一个公司为实体的隐私信息，也属于个人隐私信息保护范畴。

上述用户数据和个人数据，尤其是个人数据，CS 通常并不是在使用云计算的情况下提供给 CP，如身份证信息和营业执照等信息通常是在签订合约时提供，或在生成订单时提交给 CP。这些信息均与用户使用云计算系统时存储在云上的其他业务数据有很大的不同，需要针对其不同的特点采取不同的保护措施。

30.3.3 云计算环境下隐私数据保护对策

从上述关于用户隐私信息的数据类别来看，用户的隐私信息涉及范围较广，从业务数据到用户输入访问信息，从用户个人特征信息到用户在线行为信息等，因此，对于云计算环境下的用户隐私信息的保护，仅仅依靠单一手段如数据加密是远远不够的，需要有一套完备的隐私保护体系，涉及多个层面，以下仅从法律、技术、监管、约束机制四方面分析其对策。

1. 完善立法及相关的法规制度

云计算环境下保护隐私信息最好的实践就是要有法律做保证，许多国家已经颁布相应法律来保护其个人隐私，如加拿大的个人信息保护和电子文档法案(Personal Information Protection and Electronic Documents Act，PIPEDA)、欧盟委员会的数据隐私保护指示、瑞士联邦数据保护法案(the Swiss Federal Data Protection Act，DPA)、瑞士联邦数据保护法令(the Swiss Federal Data Protection Ordinance)等。在美国，个人隐私权利还要受到行业相关管制法案的保护，如健康保险责任法案(Health Insurance Portability and Accountability Act，HIPAA)、金融服务法案(The Gramm-Leach-Bliley Act，GLBA)和美国联邦通信委员会客户专属网络信息规定(FCS Customer Proprietary Network Information rules，CPNI)等。第 31 章将会对上述部分规约进行介绍。

目前，国内现行法律对用户信息隐私的保护还比较滞后，还无专门针对网络环境下的用户隐私保护的体系化的法律或法规，更没有针对云计算环境下的用户隐私信息保护的相关法律或法规。要适应云计算环境下的用户隐私信息保护需求，我国乃至全球的立法机关都应加快加强用户隐私信息保护方面的相关立法，明确云计算环境下用户隐私信息的保护内容及流程，建立一套完善的用户隐私信息保护体系。

2. 运用数据安全保护及隐私增强技术

对于存放在云上的用户数据其隐私信息保护主要采用数据加密、安全认证、访问控制、数据屏蔽等技术。需要说明的是，在保护云中存放的数据及其所包含的隐私信息方面，数据

加密能较好地解决无意或恶意带来的隐私信息泄密问题。此外，双因子增强认证方案为云中数据访问认证提供更好的安全保护。

关于隐私增强技术（Privacy Enhancing Technologies，PETs），目前业务还无统一的定义，学界认可的说法是，PETs 是指任何可以用来保护或增强个人隐私信息安全的技术，包括数据加密技术，智能卡和可信任的令牌环，增强型便携式客户端设备，分布式应用，面向对象的封装（数据与方法的紧耦合），基于 XML 的消息（基于格式与规则的紧耦合），用于分布式数据与处理的 Web 服务架构，更细粒度级的断言、隔离认证、授权与属性以及零知识证明技术等。

3. 设立政府监管机构

除了法律对隐私信息违规行为的制裁和增加安全技术实施外，云计算服务下的用户隐私信息保护更多依赖相关机构的有效监管。设立以政府为主导的可信的第三方监管机构，不仅可以为云计算环境下的用户隐私信息保护提供公平、可靠、权威的监督与管理，还可定期对云计算提供商的服务可用性、安全技术实施与安全治理进行审计、评估等。

此外，监管机构还可以在 CS 与 CP 双方间的服务等级协议（Service Level Agreement，SLA）履行过程中起到很好的监督与制约作用。SLA 是明确云计算相关各方权利与责任的合约，一方面可以较好地保证云计算的质量；另一方面，SLA 也确定了双方的经济关系与赔偿机制。监管机构应该根据 SLA 的要求，对云计算涉及的多方进行监督，保证用户和服务提供商的权利和利益。一旦出现违反 SLA 的行为，监管机构应该协助权益受到损害的一方要求侵权实体提供合法的赔偿。

4. 建立云计算环境下用户隐私信息使用约束机制与流程

由于监管审计或法律查证等需要，仍然存在将涉及云用户隐私信息的数据提供给第三方的可能。在这种情况下，无论宏观环境或安全技术实施对用户隐私信息提供多大保护，最终的用户隐私信息保护还需要云计算提供商与用户间有一个严格而规范的用户隐私信息使用的约束机制与流程来保证，这可能包括：

- 用户隐私信息收集前的正式声明：根据监管或法律等要求需要收集、使用、持有、分布、传输用户隐私信息的公司或提供商必须对数据拥有者提供一个清晰而明确的正式声明，声明中必须如实说明收集用途、期限、执行实体等信息。
- 隐私信息拥有者的确认：隐私信息拥有者必须提供一个清楚而正式的确认函，用于表明同意收集、使用、持有、披露、传输和保护用户隐私数据。
- 用户隐私信息收集：必须要有一个符合相关法规、规范和监管政策的用户隐私信息收集、使用和传输应用系统。
- 用户隐私信息的使用：用户个人数据只能用于与上述声明中陈述一致的目的。
- 用户隐私信息的安全：必须要采取合适的安全措施（如加密）来确保个人数据在传输、存储及使用过程中的安全性。
- 用户对隐私信息的管理权：隐私信息拥有者对个人数据有浏览及更新权，而对个人数据访问仅受限于相关的授权人员。
- 用户隐私信息的持有：必须有一个合适的流程（收集、使用与销毁等）来确保个人数据仅限于实现商业目的或法律限定的期限内持有。

- 用户隐私信息的处置：过期或不用的个人数据必须采用安全且妥当的方式进行销毁处理，如使用加密盘销毁或碎纸器。

最后需要强调的是，无论是 CP 还是 CS，都将得益于更透明的云计算风险管理体系，更公平标准化的云计算使用条件，以及更健全的法律保护和监管环境。下面将以金融业的电子支付运营为例说明云计算安全运营治理过程。

30.4 案例：金融业的电子支付运营安全

30.4.1 需求分析

从广义上讲，电子支付是一种云计算服务，它是指电子交易的当事人（包括消费者、商家、金融机构或第三方支付服务提供方）使用安全电子支付手段，通过网络进行货币支付或资金流转的活动。电子支付已成为电子商务发展过程中最重要的一个环节。但在目前社会整体信用度欠缺、相关法律法规对电子支付的权利和义务界定尚不清晰的情况下，电子支付存在密码管理、网络病毒、木马、网络钓鱼等安全问题。调研数据表明，在不愿意使用电子支付的网民当中，有高达 70% 的人是因为担心交易与资金的安全。

针对电子支付的各种不同的安全性要求，需要从技术实施、法律规范、运营治理等多个方面来保障电子支付数据的保密性、数据的完整性、交易者身份的确定性以及交易的不可否认性。

从技术上看，目前在电子商务界，已开发出相应的技术措施，较为成熟的有加密、访问控制与安全认证、防火墙、入侵检测、漏洞扫描等技术；国际上也已经形成了一些比较成熟的安全机制或协议，如基于信用卡交易的安全电子交易（Secure Electronic Transaction，SET）协议、用于接入控制的安全套接层（Secure Socket Layer，SSL）协议、Netbill 协议、安全 HTTP（S-HTTP）协议、安全电子邮件协议（如 PEM、S/MIME 等）、用于公对公交易的 Internet EDI 等。

从法律上看，由于网络特殊的跨国性交易特性，除需要从业者的自律规范，更需要通过各国有关银行或金融的相关法规加以规范。

对于电子支付服务而言，相对于技术和法律两个层面，运营安全治理显得尤为重要，因为支付服务更强调支付信息的保密性、支付流程的严谨性、支付过程的可追溯性，因此，支付提供方的组织架构的合理性、安全治理操作的完备性以及对客户隐私的保护对保障消费者账户等金融信息的安全至关重要。

30.4.2 设计考虑

X 公司是一家国内领先的独立第三方支付企业，主要为各类企业及个人提供安全、便捷和保密的综合电子支付服务。根据国家金融服务领域的相关政策法规，X 公司基于 ISO/IEC 27001 安全管理体系建立了信息安全管理架构，用于支持与保障公司业务发展目标，保证为客户提供优质的支付服务，并确保服务的安全、稳定、便捷、合规。

为此，X 公司在技术层面针对不同安全层次实施了分层次的管理：物理环境安全管理、网络安全管理、主机安全管理、系统安全管理、数据安全管理、业务持续性管理、支付流程安

全管理。更重要的是，X 公司建立了明确的安全管理组织与方针以及严密的安全监控措施，以保障安全管理措施能够被有效落实，并与公司安全管理及业务目标保持一致。

30.4.3　安全运营治理实施

30.4.3.1　运营组织架构

（1）信息安全目标。信息安全管理必须从公司业务目标与需求出发，确保支持业务的信息资产具备有效的内部控制，通过持续改进机制防范风险事件，实现公司信息安全目标。安全目标主要包括以下几项：

- 保密性：确保任何非授权主体无法访问或使用信息资产。
- 完整性：确保信息资产的准确与完整，防止未授权的修改。
- 可用性：确保授权主体在需要时能够访问及使用信息资产。
- 可靠性：确保相关信息资产在规定条件内能完成规定功能。
- 不可抵赖性：确保行为各方在行为发生后无法否认。
- 问责性：确保所有信息资产都有明确的部门与岗位对其负责。
- 合规性：遵循法律法规、合约责任及公司规章制度。

（2）安全管理组织。图 30-5 所示为 X 公司电子支付服务运营保障组织架构。公司最高管理层为公司信息安全负责，并给予充分、明确的支持与指导，提供必要的资源保障，创造积极的内部环境。公司任命了信息安全管理层代表，设立了专职的安全中心、内部审计部以及各业务部门的安全管理岗等，保证安全管理有充分的组织支持。

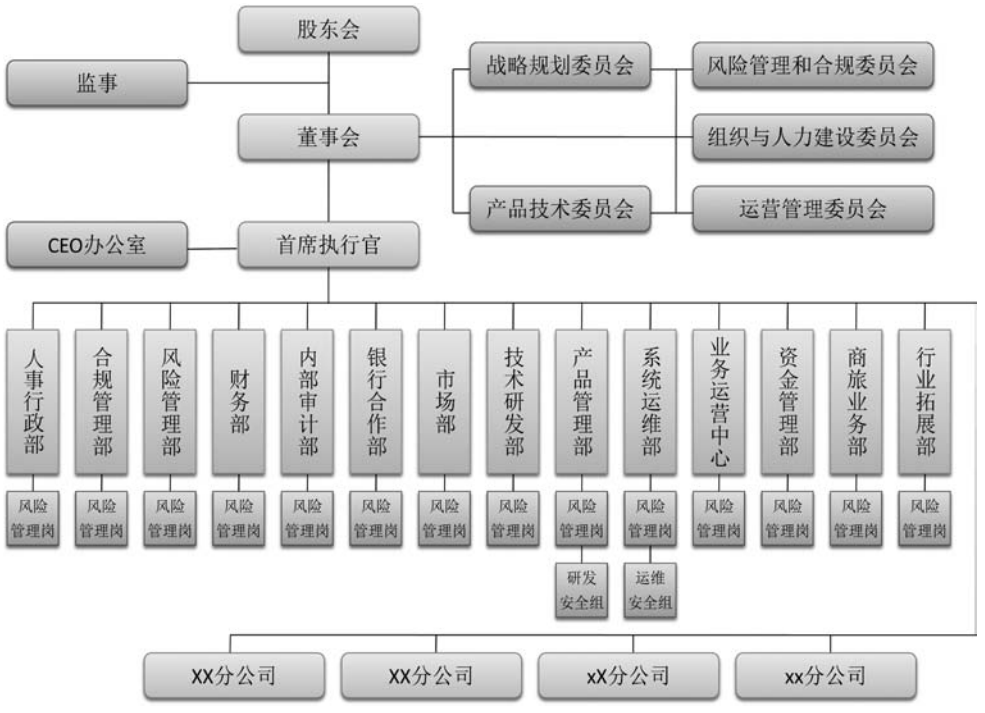

图 30-5　X 公司电子支付服务运营保障组织架构

(3) 风险为导向的管理方法。安全管理必须以风险为导向,通过对信息资产的识别,分析评估相应的风险,并且根据风险水平实行相应的处置策略与内部控制措施,兼顾成本与效果的平衡,最终使风险水平控制在可以接受的容量内。

(4) 持续改进机制。安全管理体系通过有效的自我评估、内部审计、ISO/IEC 27001 认证机构审计以及管理评审活动,及时识别内部控制缺陷,实施纠正和预防措施,不断完善信息安全管理体系。

(5) 技术与管理并重。X 公司在信息安全管理体系建设过程中,坚持技术为手段,管理做保障,两者缺一不可,一方面提升信息安全管理中的技术应用水平,另一方面持续加强信息安全管理流程与内部控制的落实。

30.4.3.2 安全运营监控

X 公司对电子支付服务的整个运行过程进行了全年 7×24 小时专人严密监控,监控主要包括服务可用性监控、交易正确性监控、产品服务监控、安全性监控等内容,涉及范围包括用户应用异常、用户交易异常、入侵检测、已知攻击检测、传输过程中数据窜改、峰值异常、网络异常等,其目标是对系统与产品事故进行及时预警、发现和处理,防止事故影响扩大,维护系统的稳定性,并对事故行为进行分析汇总,以建立相应预防措施,保障用户交易顺畅及用户账户安全可靠。

系统监控通过探针形式实现,监控探针形式包括实时可用性探针、交易正确性探针、产品合规性探针。其中实时可用性探针由生产系统主动汇报自己的生命特征,把生命数据放入监控数据库,通过监控控制台显示报警;交易正确性探针可以用生产程序每步双检测(DOUBLE CHECK)的方式来做,一旦异常,报警通知,也可以事后交易数据合规检查的方式来报警;产品合规性探针可以通过 SQL 查询统计的方式来监控报警。探针的数据获得后存放到监控数据库,控制台对每种业务的监控做好规则配置,一方面作为报警规则,另一方面也作为显示报警的依据,方便监控人员监控跟进。当监控发现问题时,某些报警出现后可以通过自动规则触发修复命令,系统自动修复,修复后再报告修复完毕,以便事后检查。监控过程如图 30-6 所示。

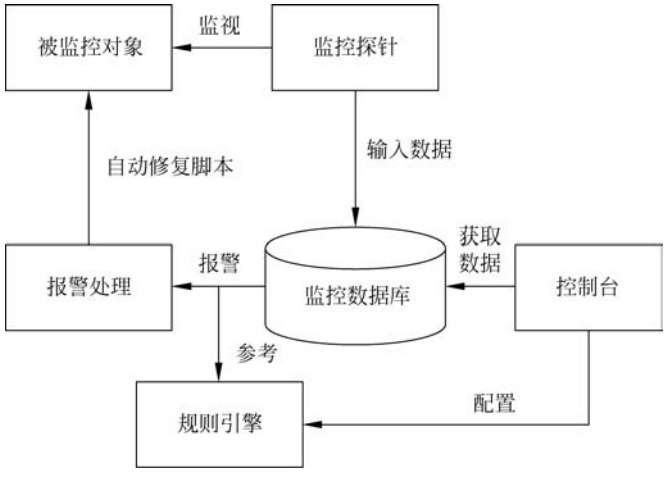

图 30-6 电子支付运营过程中的监控

除上述从技术层面的安全监控实施外，X公司还根据中国人民银行公布的《支付机构反洗钱和反恐怖融资管理办法》中的相关要求，建立了正式的反洗钱内部控制制度，对商户身份识别、身份资料和交易记录保存、可疑交易报告、反洗钱融资调查等环节进行了明确规范。同时，X公司还启用了反洗钱可疑交易监控系统，对商户可疑交易进行实时监控，防止商户通过该公司的服务进行任何非法交易。

30.4.4　成效评估

X公司严格遵守金融服务领域的相关政策法规，以安全合规为前提，积极推进各类创新型金融服务的发展和应用。目前，X公司正在与超过180万家商业合作伙伴，共同创造信息化金融服务的巨大价值。仅2011年，X公司的交易量总额就突破了12 000亿元人民币。

30.5　本章小结

云计算安全治理是云计算安全在生产环境下安全运营的重要保证，一方面验证了安全技术实施策略的有效性，另一方面也是发现云计算在构建中遗留的安全问题并进行修复的重要环节。

云计算安全治理本身是一个不断改进、逐步提升治理效果、降低安全风险的过程。在此过程中，云计算安全治理策略为云计算安全治理过程提供了指导方针与实施指南，从安全治理目标、管理意图、职责与权限、相关术语及操作细则定义等方面规划云计算安全治理内容。

安全监控与事件响应、威胁管理、渗透测试、安全审计、日志及隐私保护是云计算安全治理的主要控制措施。安全监控对云计算运行环境的安全状态提供全局性监视机制，其提供的安全告警或安全事件是云计算运行过程进行事件响应的重要依据。事件响应按预先定义的安全级别进行相应的安全事件处理，以降低安全风险或消除安全隐患。威胁管理则从“点”的角度提供了对网络及应用系统的脆弱性检查与修复机制，增强了系统的主动安全性，降低了网络或系统被攻击的风险。渗透测试基于“黑盒测试机制”对云计算整体环境进行测试，以主动发现可能存在的漏洞与风险。

在云计算环境下，安全审计和隐私保护既是监管和法规的要求，也是云计算提供商内部安全治理的需求。安全审计不仅为事后取证、业务恢复提供重要依据，定期的审计也可让CP提前发现可能存在的安全隐患，避免安全风险。隐私保护是一个相对复杂的云计算安全保护问题，它不仅依赖于与立法、技术、监管等宏观外部环境，更依赖于云计算提供者与消费者之间相互作用的微观内部环境。