白皮书
服务器

SUSE® Manager 如何帮助您实现合规

目录 页码

您为何需要合规计划 2
合规标准：SOX、HIPAA 和 PCI 2
IT 需要关注哪些合规问题 3
SUSE Manager 帮助组织遵守法规要求的 10 种方法 4
摘要 5

SUSE
We adapt. You succeed.

您为何需要合规计划

在法制环境中，由于法规的数量不断增加，以及企业普遍不够了解需要怎么做才能遵守新旧法规，合规性日益成为需要重点关注的一个业务问题。

合规性是指遵守规定的准则、规范或法规。通常是指遵守萨班斯法案 (SOX) (2002)、健康保险便携与责任法案 (HIPAA) (1996) 或支付卡行业 (PCI) (2004) 标准等法规。

但是，联邦重要法规的数量在不断增多。2012 年，美国独立社区银行家协会在国会听证会引述说，过去三年中高级主管在合规问题上投入的时间增长了四倍。随着法律对公司业务的管制越来越多，合规成本将继续增长，不合规风险和对此的担忧也随之增加。因此，法规风险可能对企业的收益产生严重影响。

在法制环境中，由于法规的数量不断增加，以及企业普遍不够了解需要怎么做才能遵守新旧法规，合规性日益成为需要重点关注的一个业务问题。不合规的代价可能很高，例如公司的员工和高管可能遭受罚款和监禁。（安然事件便是一个警钟。）这些处罚可能导致公司停业，或者严重扰乱公司为客户提供产品和服务的能力，进而使公司出现生存问题。

如果不制定合适的策略并采用技术以智能方式自动实施和管理这些策略，便无法解决当今法制环境的复杂性、法规对组织的影响以及不合规处罚等问题。许多首席合规官 (CCO) 仍然在缺乏适当技术的情况下尝试管理公司的大部分合规计划。他们需要 IT 支持。IT 可以提供一些必要技术，但不是所有必要技术。但是有一款软件产品可以显著减少与合规相关的时间和成本，这就是 SUSE® Manager。下面详细介绍主要法规以及 IT 如何帮助组织实现合规。

合规标准：SOX、HIPAA 和 PCI

三种最常见的合规标准是 SOX、HIPAA 和 PCI。美国的许多上市公司需要遵守至少其中一种法规，具体取决于公司的业务类型。下面概述了这些法规的要求以及 IT 在满足这些要求时的角色，以便于您了解合适的系统管理工具如何帮助公司遵守法规要求。

SOX 法规要求

SOX 的作用是通过管制手段来确保财务信息的保密性和完整性，以此增加投资者对上市公司财务报告过程的信心。SOX 适用于在美国上市的公司，但是也具有国际适用性，因为许多大型外国公司也在美国股票交易所交易。为了符合 SOX 法规，公司必须定期进行外部审计，以评估管制措施是否到位，从而确保信息准确并能真正反映公司的财务状况。

SOX 是针对安然公司和世通公司的财务丑闻而颁布的。它是为了保护股东和公众免受企业会计错误和欺诈行为的影响。联邦证券交易委员会 (SEC) 负责管理 SOX 法规。SOX 规定了企业应该保存哪些记录以及保存多长时间，例如影响企业财务的任何记录。任何人如果故意破坏、更改或伪造业务记录，将被处以罚款和/或监禁。

尽管 SOX 并未直接针对 IT，但是明显暗指 IT，因为大部分财务信息都是通过 IT 控制和管理的计算机系统进行传送。这意味着 IT 必须确保财务信息不能被未授权人员更改或查看，同时

又能供授权人员按需使用。SOX 涉及 IT 方面的具体要求包括信息的保密性、完整性、可用性、审计和记录以及变更管理。

HIPAA 法规要求

HIPAA 确立的联邦法规要求医生、医院和其他的医疗保健供应商在处理医疗记录和医疗病人帐户等受保护电子健康信息 (ePHI) 时，必须满足特定的基本标准。HIPAA 法规的基础概念是数据库的拥有者不一定是数据库所含信息的拥有者。

遵从 HIPAA 法规的组织必须确保记录拥有者：

- *可以访问自己的记录，有权请求纠正错误*
- *事先了解其信息将被如何使用*
- *相关人员在 ePHI 被用于营销目的之前授予明确许可*
- *有权询问和要求医疗组织采取合理措施来保护个人与组织之间的沟通隐私性*
- *有权向合适的主管部门提交与隐私相关的正式投诉*

HIPAA 涉及 IT 方面的具体要求包括信息的保密性、完整性、可用性、审计和记录以及鉴定。

PCI 法规要求

PCI 法规是基于 VISA、MasterCard、American Express 和 Discover 这四家卡服务商各自创建的安全计划的一种标准。PCI 建立了一套全面的全球性安全标准，规定了所有的商户和服务供应商如何存储、传送或处理任何主要的卡服务商提供的持卡人信息。

为了验证是否符合 PCI 法规，必须通过审计来确认是否充分满足这些安全标准。根据商户分类的不同，需要进行季度和年度合规审计。一个组织处理的交易越多，该组织需要管控的风险就越高，满足 PCI 标准的重要性也就越大。其目的是保护持卡人信息，实施强有力的访问控制措施，并且定期监视和测试网络。

保密性和鉴定是 PCI 标准的首要目标，旨在保护消费者信用卡信息。信用卡信息通常经过多个中介机构从个人传送到信用卡公司。因此，采取加密措施并确保只有授权的系统或机构有权访问敏感的帐户信息至关重要。记录和审计是 PCI 合规第二重要的方面。

IT 需要关注哪些合规问题

SOX、HIPAA 和 PCI 法规最重要的要求是信息的保密性、完整性、可用性、鉴定、审计和记录以及变更管理。其中有些要求对于某一法规相对来说更重要，但在某种程度上而言，它们又是这三种合规标准和许多其他合规标准的普遍要求。

- **保密性。***信息必须保密，以防未授权人员访问。对于 HIPAA 法规，该信息是指 ePHI，即与记录拥有者的帐户有关的信息。对于 SOX 法规，该信息是指各种财务信息记录；对于 PCI 法规是指信用卡信息。将保密信息存储在数据库或文件中时，通过网络传输保密信息时以及将保密信息置于内存中时，应该使用加密措施。*
- **完整性。***记录不应该被未授权的人员或实体修改。所有敏感信息都应该使用完整性/检查机制来限制信息篡改风险。软件需要支持信息未被修改的证据。*
- **可用性。***系统需要能够正确处理错误，能抵御“拒绝服务”攻击。事件日志应该含有足够的信息，以便能将系统的活动修复到故障点，从而快速地解决和纠正错误。*
- **鉴定。***鉴定涉及使信息只能被授权人员使用，并保持对“拒绝服务”攻击的抵抗力。这通常需要使用可靠的数据储存设备、故障转移群集、加密密钥机制和数据恢复功能。为了安全地操作 HIPAA ePHI 等信息，有必要知道使用信息的实体或个人是否合法并有权访问所述信息。*

- **审计和记录。***软件系统必须生成所有必要的日志信息，以便建立明确的审计追踪，以显示用户或实体如何试图访问和使用资源。对于 SOX 法规，这意味着跟踪信息进入或离开公司的关键时刻，例如公司向外部发送的电子邮件、有权访问敏感财务信息的员工离职等。务必定期备份日志，以确保审计信息不会因为系统故障而丢失。日志不得泄露系统试图保护的任何信息。*
- **变更管理。***从审计和运营角度而言，变更管理在合规方面发挥着重要作用，它能确保所有变更满足既定政策和相关法规的规定。变更管理用于确保存储 SOX 信息等监管信息的系统的完整性。SOX 法规涉及变更管理，因为财务记录中的信息可能被篡改，因此需要记下财务记录的访问情况，并保护财务记录。变更管理的一项重要要求是能够记录系统的变更，并且只有授权人员才能访问日志。*

对于 SOX 法规，IT 必须能够存储所有业务记录，包括至少保存 5 年的电子记录和讯息，尤其是财务记录和讯息。记录包括工作文件、备忘录、信件、通信或者创建、发送或接收的与审计或审查有关的其他文档和记录，并且包含与该审计或审查有关的结论、观点、分析或财务信息。

对于 HIPAA 法规，IT 必须提供安全机制来确保任何个人信息的保密性和完整性，并保护所有 ePHI 的保密性。PCI 法规的目标是保护消费者信用卡信息，因为该信息通过各种中介机构从消费者传送到信用卡公司。

SUSE Manager 帮助组织遵守法规要求的 10 种方法

为了满足合规要求中的保密性、完整性、可用性、鉴定、审计和记录以及变更管理要求，需要使用各种系统管理功能，例如安全增补程序管理、日志记录、物理和虚拟资源监视、报告、探测等。所有法规都有严格的安全要求，并将增补程序管理作为重要功能，以确保及时进行安全更新。

SUSE Manager 能以至少 10 种方式帮助各个组织遵守这些法规要求：

1. 安全性是所有法规要求中的一项重要要求。SUSE Manager 使用 OpenSCAP 来审计软件增补程序的状态、自动确认服务器是否拥有最新的安全更新、检查系统安全配置的设置以及检查系统是否有漏洞迹象。用户可以访问 OpenSCAP（**www.open-scap.org/page/Main_Page**）创建的安全日志，其中记录了所有用于审计的活动。SUSE 已与合作伙伴 UPW 开展合作，将 UPW Compliance Guard 解决方案集成到 SUSE Manager 中，以使安全性可测量。组织可使用 UPW Compliance Guard 定期自动运行测试，并创建报告不断跟踪合规情况，以便持续改进 IT 安全性。
2. 增补程序管理（**www.suse.com/promo/automated-patch-management.html**）对于确保受管制的组织拥有最新的安全更新十分重要。如果没有这种保证，组织会陷入无法满足法规安全要求的危险之中。拥有 SUSE Manager 之后，管理员可以检查单个系统或系统组的增补程序的状态，可以直接应用所需的增补程序，或者在维护窗口中安排更新。在生产环境中部署之前，还可以在多个分阶段区域中测试增补程序。借助 SUSE 提供的增补程序元数据，管理员能够评估增补程序的重要性和紧迫性。此外，SUSE Manager 还能根据 MITRE 的“常见漏洞与泄露”（CVE）数据库提供的 ID 来审计系统的软件库存。SUSE Manager 提供了一个 Novell Customer Center 单一访问点来获取更新，以便管理员可以遵守企业的防火墙策略，并自动部署重要的安全增补程序，从而减少漏洞和风险。
3. 保密性是指防止未授权人员访问信息。SUSE Manager 通过鉴定机制、日志记录（即记录谁访问过或试图访问过保密信息）及加密功能来确保信息的保密性。
4. 完整性是指防止记录被未授权人员修改。SOX 法规旨在防止公司中的未授权人员修改财务记录，而 HIPAA 法规则旨

在防止未授权人员修改患者记录。SUSE Manager 的某些功能既可用于管理信息保密性，又可用于管理信息完整性。日志记录特别适合跟踪谁在尝试修改信息，有助于“抓到”不应该修改信息的人。

5. 信息可用性取决于整个系统的安全强度以及系统防止/处理错误、防止/抵御“拒绝服务”攻击、限制系统中断等问题的能力。围绕信息可用性采取的许多措施都涉及监视服务器、网络和其他系统实体（不论是物理的还是虚拟的）的运行状况。SUSE Manager 探测器允许组织监视物理和虚拟服务器、虚拟客户机、网络等的运行状况，防止出现影响可用性的问题。
6. 防止未授权的信息访问或修改只是一方面，通过鉴定功能确保尝试进行访问的实体是授权实体也同样重要。SUSE Manager 基于角色的控制确保管理员拥有合适的权限来访问和/或修改信息。管理员权限可以限制到单个系统或系统组，也可以基于任务进行限制。例如，一名管理员可能有权更改一组系统的更新通道设置，另一名管理员则可能有权实际应用增补程序。
7. 满足多项法规标准要求的一个关键是能够记录各种事件，例如记录谁在尝试访问/修改信息、跟踪信息在组织内的移动位置（内部或远程）等。日志记录可创建审计追踪，以便从 IT 角度了解相关情况，并为外部的法规审计员准备好报告。SUSE Manager 具有这些记录和审计功能以及重要的报告功能，不仅可用于提供审计报告，还能用于创建内部使用的报告来检查 IT 系统的运行状况。
8. 在满足合规要求方面，变更管理是经常被忽视的一个方法。它能记录所发生的变更，例如安装新的服务器、更改/更新硬件/软件（包括安全更新）等。变更管理日志对于监视/检测与违反保密性、完整性及其他法规要求有关的问题十分有用。SUSE Manager 会自动跟踪服务器的变化情况，并保存历史记录，使组织可以轻松地向审计人员提供变更信息。
9. SUSE Manager 监视模块让用户能够监视物理资源的运行状况，例如物理服务器和内存以及虚拟服务器的内存、磁盘空间和 CPU 利用率，从而主动确保服务的持续可用性。监视功能得益于使用探测器和通知。组织可以创建自定义探测器，使用内置的 SUSE Linux Enterprise Server 探测器，甚至使用第三方探测器来监视物理和虚拟服务器的运行状况。当服务器即将超过利用率阈值时，或者在潜在的系统故障实际出现之前，SUSE Manager 通知功能将通过电子邮件或寻呼机提醒系统管理员。管理员可以方便地从一个控制台监视服务器运行状况，通过单页面更新和图形报告洞悉服务器性能。监视系统的运行状况和快速的响应能力增强了系统可用性，满足了这一项合规要求。
10. SUSE Manager API 可以创建自定义脚本来管理任务或者与第三方应用程序和管理工具协同工作。

摘要

SOX、HIPAA 和 PCI 等合规标准使许多组织在满足法规要求方面的负担日益加重。所有合规标准都包含大量的安全要求，例如保密性、完整性、可用性、鉴定、审计和记录以及变更管理要求。

如今，许多组织合规负责人都在寻求 IT 的帮助，因为显然需要借助技术来实现合规和降低成本。SUSE Manager 是少数几个能够提供必要功能来满足合规要求的系统管理工具之一。它采用的技术包括增补程序管理、鉴定、资源监视、日志记录、报告生成、变更管理审计等，可以满足上述的所有法规要求。SUSE Manager 通过一个管理界面即可做到所有这一切。

此外，SUSE Manager 是唯一能同时管理 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux 系统的 Linux 系统管理解决方案。

请联系当地的 Solutions Provider
解决方案提供商或致电 SUSE

澳大利亚
1-800-668-355

中国大陆
400-120-3101

中国台湾
886-2-23760000

中国香港特别行政区
800-906-194

印度
91-80-4002-2300

日本
0800-100-5575

马来西亚
60-3-7722-6100

新西兰
0800-441-671

新加坡
65-6395-6888

韩国
82-11-3131-464

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

www.suse.com