* [Coupa GovCloud 和 ITAR 遵从性](https://success.coupa.com/Trust/Security_and_Compliance/Compliance_Certifications/Coupa_GovCloud_and_ITAR_Compliance)
* **GovCloud 和 Itar**
* Coupa 致力于与美国联邦、州、地方政府机构、客户和承包商合作，提供该行业急需的储蓄。
* 作为管理一个全面的 ITAR（国际军控交易）合规计划的一部分，遵守 ITAR 法规的公司必须通过限制对美国人的受保护数据的访问和限制这些数据在美国境内的实际位置来控制非预期出口。 Coupa GovCloud 提供了一个物理上位于美国的环境，Coupa人员的访问仅限于美国人，从而允许合格的公司传输、处理和存储受 ITAR 限制的受保护的物品和数据。这种环境已经被一个独立的第三方审计，以验证是否存在适当的控制。
* 可以通过 self serve 链接索取 Coupa Itar 认证报告的副本：[Coupa 遵从性报告请求](https://get.coupa.com/Compliance-Reports_Request-Report.html).
* [Coupa HIPAA 依从性](https://success.coupa.com/Trust/Security_and_Compliance/Compliance_Certifications/Coupa_HIPAA_Compliance)

## HIPAA 依从性

健康保险可携性和责任法案（HIPAA）规定了保护敏感患者数据的标准。任何处理受保护的健康信息（PHI）的公司都必须确保所有所需的物理、网络和过程安全措施都已到位并得到遵循。

这包括**覆盖实体（CE）**，任何在医疗服务方面提供治疗、付款及运作的人士，以及**商业伙伴（BA）**，并在治疗、付款或手术方面提供支持。分包商，或商业伙伴的商业伙伴，也必须遵守。

Coupa 致力于与健康保险公司和护理提供者合作，在不牺牲病人护理结果或病人经验的情况下，提供该领域急需的储蓄。根据 1996 年的健康保险可携性和责任法案（HIPAA），保险公司和提供者必须采取措施保护他们的客户或病人的电子健康保护信息（ePHI）。 Coupa 的医疗云提供了 HIPAA 所需的 ePHI 保护。

虽然 Coupa 不提供任何病人记录管理或病人护理服务，但在员工将 ePHI 输入 Coupa 的情况下，客户将受到保护。 Coupa 建议不要将 ePHI（如医疗记录编号（MRN））作为业务流程或集成设计的一部分。 在某些情况下，ePHI可能是在金融交易的上下文中输入的。例如，在费用描述中提交患者姓名的花的费用报告，附上患者姓名或房间号的收据，或在发票上附上化验报告。 Coupa 保护客户免受暴露于 ePHI 的风险。

根据 HIPAA，允许服务提供者代表其创建、接收、维护或传输 ePHI 的保险公司和提供者必须与这些提供者签订业务关联协议（BAA）。 BAA 将保护 ePHI 的责任扩大到这些供应商。 Coupa 的医疗云允许 Coupa 与客户建立业务关联关系，确保适当地进入 Coupa 进行开销管理的 ePHI 按照 HIPAA 的规定得到保护。 Coupa 根据 HIPAA 制定的标准采取了一系列措施来保护 ePHI，包括行政保障、实物保障和技术保障。

Coupa 与第三方公司完成年度审计。这项年度审计于 10 月进行，包括对行政、物质和技术控制的审查。这项年度认证的副本可从 Coupa 自助网站下载：[合规报告请求](https://get.coupa.com/Compliance-Reports_Request-Report.html).

有关更多详情，请参阅[Coupa 医疗云数据表](https://www.coupa.com/pdf/datasheet/CoupaHealthcareCloud.pdf).

* [Coupa PCI 云服务](https://success.coupa.com/Trust/Security_and_Compliance/Compliance_Certifications/Coupa_PCI_Cloud_Offering)

## 导论

Coupa 业务支出管理（BSM）平台是作为业界领先的、基于云的解决方案从头开始交付的。对于那些需要完整的信用卡数据安全保障的 BSM 客户，通过支付卡行业数据安全标准（PCI DSS）认证，Coupa 提供了一个完全兼容的 PCI 云环境来支持这些需求。通过实施和维护 PCI DSS，Coupa 符合业界的最佳实践，以维护托管在平台上的客户信用卡信息的机密性。

Coupa 的安全云基础设施已经通过了合格安全评估员（QSA）的认证，获得了 Coupa PCI 认证，并被列入了认证服务提供商的名单。此认证和符合性认证（AOC）是通过 PCI 安全标准的演示实现和操作实现的：

* 建立和维护一个安全的网络
* 保护持卡人数据
* 维护漏洞管理程序
* 实施强有力的访问控制措施
* 定期监测和测试网络
* 维持资讯保安政策

## 关键用例

Coupa 可以存储和维护支付卡信息的情况，包括 Coupa 采购中的支付卡。 Coupa 还可以集成个人和企业信用卡数据提要，以方便在 Coupa 费用范围内自动创建费用项目。在所有情况下，Coupa以一种安全的方式接收、存储和传输信用卡数据，正如 PCI DSS 所规定的那样。

## Coupa 持卡人数据环境

Coupa 持卡人数据环境（CDE）是 Coupa 云基础设施中指定的安全区域，用于接收、存储和传输持卡人数据，以支持上述指定的金融产品工作流。连接到 Coupa CDE 的 Coupa 系统的所有方面都要进行评估，并包括在 PCI 评估中。

通过 PCI DSS，Coupa 已经成功地实现了跨所有 Coupa CDE 网络组件（防火墙、交换机、路由器、接入点、网络设备、安全设备等）的 PCI 需求。服务器（web服务器、应用服务器、数据库服务器、身份验证服务器、邮件服务器、代理服务器、网络时间协议、域名服务器等）。作为资格认证的一部分，包括内部和外部应用程序、虚拟组件和可应用的第三方系统。

Coupa 的 CDE 位于美国和欧盟地区。

## 技术保障

为了保护 PCI 云中的持卡人数据，已经采取了更多的技术保护措施。严格的访问控制已到位，以帮助确保只有适当的缔约方才能访问 Coupa 系统。 Coupa 平台可以在传输和静止时保护数据。

### 过境数据加密

Coupa 对传输中的数据进行加密，以防止其被截获和泄露。 HTTP 数据在通过 web 浏览器、移动应用程序、电子邮件和 API 调用在服务器和最终用户之间传输之前是经过加密的。 CDE 中的服务器之间和存储之间的数据传输也是加密的。文件数据传输使用 SFTP（安全 FTP）和 PGP 文件加密的附加选项。在 PCI 云中使用机会主义 TLS 进行电子邮件通信。作为附加的 PCI 安全措施，TLS 1.0 被禁用。

### 静态数据加密

一般来说，Coupa使用多种策略来对静态数据进行加密。在保存到数据库之前，输入到由 Coupa 指定的特定标识字段的信用卡数据在应用服务器端被加密。文件附件在保存之前是在应用服务器端加密的，在保存之前是在服务器端加密的。 Coupa 移动应用程序被加密以保护静止的数据。

### 强加密

Coupa 使用强大的加密方法来确保信用卡数据不受干扰。

* **加密算法：**Coupa 使用 PGP 加密文件，AES 256 加密应用程序数据。此外，文件也使用 Amazon Web Services（AWS）S3 本地加密进行加密。
* **密钥管理：**Coupa 使用 AWS 密钥管理服务来管理加密密钥。每个 Coupa 客户都被分配了唯一的加密密钥。

## 物理防护

Coupa 使用 AWS 基础设施来提供运行我们的金融应用程序所需的计算、网络和存储服务。 AWS 是一个著名的提供者，它为设备安全、访问控制和应急操作提供了适当的控制。此外，Coupa为自己的设备使用安全条款，包括徽章访问控制、工作站安全、备份和工作站重用。

## 行政保障措施

Coupa 已经实施了业务政策和程序来控制对所有安全系统的访问。 Coupa 的安全和合规副总裁负责制定和实施这些政策和程序。只有在完成信用和犯罪背景调查后，美国人才可以使用 Coupa 系统。终止程序确保访问被适当地终止。安全事故响应和违反通知程序确保任何事故都按法律要求向监督机构、客户和监管机构进行适当的报告。应急计划确保在发生灾难时数据的可获得性。

## PCI 遵从性报告

一份最新的报告PCI 依从性认证可从[符合性报告请求门户](https://get.coupa.com/Compliance-Reports_Request-Report.html).

* [Coupa II 型 SOC 1 符合性报告](https://success.coupa.com/Trust/Security_and_Compliance/Compliance_Certifications/Coupa_Type_II_SOC_1_Compliance_Report)

# Coupa II 型 SOC 1 符合性报告

1. 最后更新

2019 年 12 月 11 日

1. [另存为 PDF](https://success.coupa.com/@api/deki/pages/3405/pdf/Coupa%2bType%2bII%2bSOC%2b1%2bCompliance%2bReport.pdf?stylesheet=default)

### Coupa 每年完成一次 II 类 SOC1 审计。

#### SOC1 报告：它是什么 ？

与用户实体的财务报告的内部控制相关的服务组织的控制报告：SOC1活动在 SSAE 18 下执行，报告服务组织的控制。 SOC1 报告是由服务审计员进行的审查活动，报告在一个向用户实体提供服务的组织的控制，当这些控制可能与用户实体的财务报告的内部控制相关时。

SOC1 报告有两种类型：

* **第 1 型**— —一份关于管理部门对服务组织系统的描述和设计控制的适宜性的报告，以便在指定日期实现描述中包含的相关控制目标。
* **2 型**— —一份关于管理当局对服务组织系统的描述，以及控制的设计和操作有效性是否适当的报告，以实现在指定期间内包括在描述中的相关控制目标。

SOC1 审计每两年进行一次，我们的报告期是 11 月 1 日圣特到 4 月 30 日经纬仪5 月 1 日圣特到 10 月 31 日圣特.在报告期间之后，外聘审计员进行审计，并在每个报告期间之后的 6 月和 12 月印发报告。

桥梁（差距）的信件，以确定任何变化/差距，因为最后一次审计是每月发出的，在每个月初。

如果您希望获得当前 Coupa Type II SOC 1 报告或 SOC Gap 信件的副本，可以从[符合性报告请求门户](https://get.coupa.com/Compliance-Reports_Request-Report.html).

* [Coupa II 型 SOC 2 符合性报告](https://success.coupa.com/Trust/Security_and_Compliance/Compliance_Certifications/Coupa_Type_II_SOC_2_Compliance_Report)

### Coupa 在 2015 年成功完成了其首款用于安全和保密的 II 型 SOC2 审计。

#### SOC2 报告：它是什么 ？

与安全、可用性、处理完整性、机密性和隐私相关的服务组织的控制报告：许多实体将任务或整个功能外包给服务组织，这些服务组织为用户实体操作、收集、处理、传输、存储、组织、维护和处理信息。 SOC2 协议在信托服务原则、标准和说明中使用预定义的标准，以及 at101 部分 “认证协议”（AICPA，专业标准，卷）中的要求和指导。 1）. SOC2 报告类似于 SOC1 报告。可以发布类型 1 或类型 2 的报告，该报告提供了对服务组织系统的描述。

对于类型 2 的报告，它还包括对服务审计人员执行的测试和这些测试的结果的描述。 SOC2 报告专门针对以下五个关键系统属性中的一个或多个：

* 安全 — —系统不受未经授权的访问（包括物理访问和逻辑访问）的保护。
* 保密 — —被指定为机密的信息受到承诺或同意的保护。
* 没有测试隐私、可用性和流程完整性。
* 隐私 — —个人信息的收集、使用、保留、披露和处理符合实体隐私声明中的承诺，也符合美国会计师公会（AICPA）和加拿大特许会计师协会（Canadian Institute of Chartered Accountants）发布的《普遍接受的隐私原则》（GAPP）中的标准。
* 可用性 — —系统可按承诺或约定进行操作和使用。
* 处理完整性 - 系统处理是完整的，准确的，及时的和授权的。

Coupa II 型 SOC2 审计每年进行一次，报告期为 11 月 1 日至 10 月 31 日。报告期间结束后，外聘审计员进行审计，并编制 12 月印发的报告。

现有的 Coupa II 型 SOC 2 报告和其他 Coupa 遵从性报告可从[符合性报告请求门户](https://get.coupa.com/Compliance-Reports_Request-Report.html).

* [ISO 27001 认证](https://success.coupa.com/Trust/Security_and_Compliance/Compliance_Certifications/ISO_27001_Certification)

# ISO 27001 认证

1. 最后更新

2019 年 12 月 14 日

1. [另存为 PDF](https://success.coupa.com/@api/deki/pages/9487/pdf/ISO%2b27001%2bCertification.pdf?stylesheet=default)

## Coupa ISO 27001 认证

ISO 27001 是全球公认的建立和认证信息安全管理体系（ISS）的标准。该标准规定了在组织整体业务风险范围内建立、实施、操作、监视、审查、维护和改进文件化 ISM 的要求。它提出了一种基于风险的方法，其重点是适当和适当的安全控制，以保护信息资产并使有关方面有信心。

认证由[舍尔曼](https://www.schellmanco.com/)美国 ANAB 和 UKAS 认证机构。

Schellman 认证的 Coupa 符合所有 ISO/IEC 27001:2013 认证要求 — —来自[国际标准化组织](https://en.wikipedia.org/wiki/International_Organization_for_Standardization)（iso）及[国际电工技术委员会](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission).ISO 27001 是全球公认的信息安全管理体系（ISS）的建立、维护和认证标准。有关 Coupa 的 ISO 27001 ISS 认证的详情，可在[谢尔曼证书目录](https://cert.schellmanco.com/?certhash=0tBxnmDDskBk)或者您可以从 Coupa 自助服务链接中获取副本：[合规报告请求](https://get.coupa.com/Compliance-Reports_Request-Report.html).

“Coupa致力于通过第三方审计和认证（如 SSAE 16 和 ISO 27001）为我们的安全控制和实践提供独立的保证，” Coupa 安全和合规副总裁 Phil Cox 说。 “获得 ISO 27001 认证是一个巨大的成就，因为我们继续向我们的客户提供我们的安全控制和实践遵循国际公认的安全标准的信心。”

ISO 27001 标准规定了在组织整体业务风险范围内建立、实施、操作、监视、审查、维护和改进文件化 ISM 的要求。它提出了一种基于风险的方法，其重点是适当和适当的安全控制，以保护信息资产并使有关方面有信心。  
  
Schellman & Company, LLC（Schellman）是一家领先的认证和合规服务提供商。 Schellman 是世界上唯一一家注册会计师事务所、全球授权的 PCI 安全评估员、ISO认证机构、HITRUST CSF 评估员和 FedRAMP 3 PAO 的公司。谢尔曼的专业人员以丰富的实践经验著称，他们为客户提供优质的服务，并以坚定的独立性来平衡。 Schellman 方法建立了成功的、长期的关系，并允许其客户通过一个第三方评估员实现多个遵从性目标。

Coupa 诞生于云端，它提供了一个现代化的消费管理平台，通过统一员工所有消费方式的流程，加快了业务的发展。这些过程包括旅行和费用管理，采购，发票和相关的来源到结算领域。通过使用 Coupa Open business Network，该平台已经连接了 200 多万个供应商，并为致力于控制支出的企业提供了一个强大的解决方案。

Coupa ISO 27001监视报告和注册证明书可从[符合性报告请求门户](https://get.coupa.com/Compliance-Reports_Request-Report.html).