通过ITSM最佳实践实现 Cyber Essentials 合规性

ManageEngine 卓豪
ServiceDesk Plus

什么是Cyber Essentials?

Cyber Essentials 是英国政府支持的网络安全认证计划，由英国国家网络安全中心（NCSC）设计和监督，NCSC 是英国政府的国家技术机构和网络安全的单一联络点。

该认证是一项自我评估计划，用于审查组织的 IT 环境（即用户、网络、软件政策和 IT 资产）如何与五项核心技术控制及其要求保持一致。认证适用于评估范围内的所有 IT 组件，评估范围需要由申请组织和授权认证机构共同定义和商定。

五项技术控制

安全配置

防火墙

恶意软件保护

用户访问控制

安全更新管理

Cyber Essentials 认证有哪两种类型?

Cyber Essentials 认证分为两种：

i) Cyber Essentials

ii) 网络基础知识强化认证

i) Cyber Essentials:

该认证通过回答自我评估问卷来获得，问卷需由贵组织的一名高级董事会成员签署。然后由 IASME（官方网络安全认证交付合作伙伴）授权的合格独立评估员对评估结果进行评分。

ii) Cyber Essentials Plus:

在申请 Cyber Essentials Plus 认证之前，您的组织需要通过经核实的自我评估问卷进行认证。Cyber Essentials Plus 认证包括对贵组织的 IT 系统和网络进行严格的技术审核，以检查其是否符合各项要求。这种审核提供了更多的保证和可证明的合规证据，使您的企业能够更好地赢得客户的信任。

为什么要遵守 Cyber Essentials

在过去的 12 个月中，英国绝大多数大中型企业（准确地说是 79%）都曾遭遇过某种形式的网络事件*，但只有 22% 的英国企业制定了正式的事件响应计划。

这些数字来自英国政府委托进行的《2024 年网络安全漏洞调查》，提醒我们即使是基本的网络安全计划也至关重要的原因。Cyber Essentials 恰恰有助于应对这一挑战。五项技术控制要求代表了网络安全准备工作的基线，可防范一些常见的基于互联网的网络威胁。

以下是遵守 Cyber Essentials 对企业有利的几个原因：

- 通过展示在网络、端点、补丁管理流程等方面实施网络安全控制的证据，让客户放心。
- 您的组织需要符合Cyber-Essentials-compliant 的要求，才能竞标政府合同或获得公共资金，如教育部授予学院和 16 岁后特殊教育机构的资金。
- 它是网络安全标准的低悬果实之一，有助于建立基本的网络卫生实践，并为符合 ISO 27001 等其他标准做好准备。
- 如果贵组织的年营业额低于 2000 万英镑，Cyber Essentials 认证将为贵企业提供网络责任保险。
- 符合 Cyber-Essentials 标准可能会降低网络保险费，因为您的企业可信地展示了网络安全控制措施的证据。

Cyber Essentials + IT服务管理：

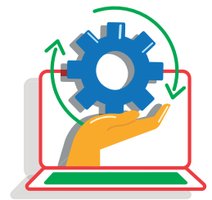
ITSM 如何帮助我遵守 Cyber Essentials?

虽然 Cyber Essentials 为您的网络安全之旅打下了坚实的基础，但有些企业可能会陷入困境，不知道如何或从何处从头开始，而其他已建立网络安全团队的企业则错过了将安全最佳实践集成到 ITSM 流程中的机会。

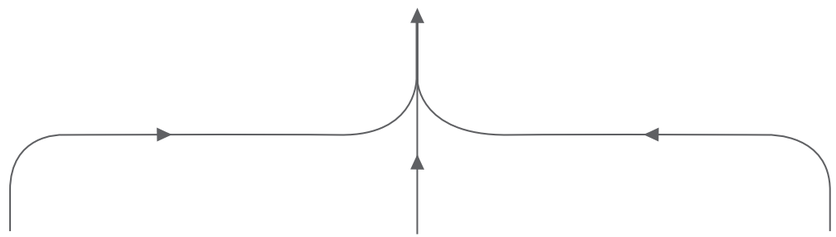
将 ITSM 实践引入网络安全计划至关重要，因为 Cyber Essentials 和 ISO 27001 等认证和法规适用于 IT 管理职能的所有方面，但这些职能往往各自为政。ITSM 与全栈可观察性、身份和访问管理以及统一端点管理等其他 IT 管理功能之间存在着独特的交叉点。

从检测来自可观察性工具的警报并触发事件响应，到通过连接 IAM 解决方案协调入职、角色变更和离职流程，ITSM 平台是网络安全实践的共同点。

多年来，服务管理团队已完善了一系列传统的 ITIL® 实践，如事件管理，以应对中断和服务中断、服务管理和故障。事件管理，以应对故障和服务中断；服务请求管理，以入职、离职员工或提供软件；服务管理，以确保服务质量。服务请求管理，以便入职或离职员工或提供软件，以及 IT 资产管理（ITAM (ITAM) 来核算每项 IT 资产并优化 IT 预算。



信息技术和企业服务管理

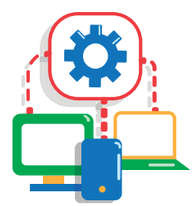


员工旅程或协调

ITAM、补丁合规性和软件配置

重大事件检测和响应

身份和访问管理



统一终端管理

全栈可观测性

他们的目标是不断提高企业 IT 生产率，为员工提供卓越体验。但正是这些做法可以成为您构建网络安全态势的基石，或许还可以在此基础上进行改造，以满足合规授权或要求。这种方法可以解决以下方面的问题：

将 ITAM 重塑为核心安全功能；在其最新更新的 Cyber Essentials v3.1（2023 年 4 月）中，NCSC 增加了一个专门章节，说明为何 ITAM 不应被视为孤立的实践，而应在采购、财务会计、IT 运营和网络安全等组织功能之间进行整合。
建立访问治理工作流程，在满足用户访问控制要求的同时，审查、批准和协调供应任务。
制定网络安全事件响应计划，以应对恶意软件相关事件。

在本指南中，我们将把通过采用 ITSM 最佳实践可以满足的一些 Cyber Essentials 要求映射到 ManageEngine ServiceDesk Plus 的 ITIL 兼容功能中。
对于新手来说，ServiceDesk Plus 是 ManageEngine 推出的人工智能驱动的统一服务管理平台。它将 ITSM 要素、资产管理和 CMDB 与企业服务管理功能相结合，为设计、管理和交付 IT 和业务服务提供了一个全面的平台。

有助于满足网络基本要求的 ITSM 功能

资产管理和 Cyber Essentials

有效的网络安全战略以了解需要保护的内容为前提。而这首先要从 ITAM 开始。

虽然资产管理不是构成Cyber Essentials的五项技术控制之一，但 NCSC 建议企业实施有效的 ITAM 实践，因为跟踪和控制企业日常运营所依赖的 IT 资产有助于满足所有五项Cyber Essentials控制。

以下ITAM最佳实践与ManageEngine ServiceDesk Plus功能的映射源自NCSC关于资产管理的具体指导。

虽然 ITAM 与采购、财务会计和 IT 运营等多个其他业务相关，但我们将仅限于网络安全与 ITAM 的交叉点。因此，这将需要管理可能受到安全事件影响的资产，以及其配置与网络安全结果相关联的资产。

国家计算机安全中心准则	要求	ServiceDesk Plus 起了什么样的作用?
资产管理（不属于技术控制，但被 NCSC 规定为核心安全功能）	资产发现： 使用工具定期或持续扫描环境，查找新的、修改的或移除的资产。	ServiceDesk Plus 功能： - 基于代理和无代理的域和网络扫描 - 远程资产扫描（位于办公场所以外的资产） - 自扫描脚本 - 条形码扫描 - QR 码和 RFID 扫描 - 采购订单应收款 ServiceDesk Plus 使 IT 和网络安全团队能够通过定期的无代理和基于代理的扫描技术发现跨域和网络的资产。 企业还可以通过资产发现代理或远程扫描脚本扫描不属于企业网络的远程资产。 IT 团队还可以安排自动定期资产扫描，以跟踪资产规格或安装软件等变化。 除这些来源外，还可通过条形码、QR 码和 RFID 扫描技术等其他方法发现或扫描 IT 资产。资产还可以通过采购订单添加到资产库存中，并在 ServiceDesk Plus 中进行管理。除发现硬件外，还可扫描和清点这些设备上安装的所有软件。发现的软件可与软件许可证和合同进行映射，帮助识别未授权安装或过度授权的软件。

国家计算机安全中心准则	要求	ServiceDesk Plus 起了什么样的作用?
资产管理（不属于技术控制，但被 NCSC 规定为核心安全功能）	权威信息源： 维护一份公认能反映实际环境的资产记录。考虑对资产信息进行标准化和整合，以避免重复并提高其可访问性。	ServiceDesk Plus 功能： - 根据产品类型分类的单一资产库存 - 资产组 - 资产核对 - 资产审计 - 自动定期资产扫描 ServiceDesk Plus 中的资产清单是 IT 和网络安全团队的单一信息来源。所有资产，无论是 IT 资产还是非 IT 资产，都可以分配给特定的用户或部门，并清楚地了解资产的状态，如是否在库、维修中或已报废。通过自动定期扫描，资产库存信息保持最新。 可根据操作系统、供应商、域或地点等特定参数对资产进行上下文分组。此外，ServiceDesk Plus 还提供内置的资产审计功能，可帮助验证资产的物理位置和所有权，从而帮助锁定丢失的资产或偏离原始所有权的资产。
	准确的信息来源： 应定期收集资产信息，确保其保持最新，并记录置信度分数或最后看到的时间戳，以反映信息的陈旧程度或不确定性。	ServiceDesk Plus 功能： - 计划资产扫描 - 跟踪最后登录的用户 ServiceDesk Plus 中的计划资产扫描有助于确保每天、每周或每月定期更新资产清单中的资产信息。

国家计算机安全中心准则	要求	ServiceDesk Plus 起了什么样的作用?
资产管理（不属于技术控制，但被 NCSC 规定为核心安全功能）	资产信息的可用性： 确保资产信息可供访问，以支持企业中的相关用例。CMDB 可能是资产管理解决方案的重要组成部分。	ServiceDesk Plus 的功能： - 与其他 ITSM 实践的上下文集成 - 具有可视化依赖关系映射的本地 CMDB ServiceDesk Plus 中的 ITAM 与事件管理、服务请求管理、问题管理和变更管理等其他 ITSM 实践紧密集成。这种上下文一致性有助于跟踪针对特定资产（如工作站或服务器）报告的安全事件，加快事件响应速度。 ServiceDesk Plus 还提供开箱即用的本地 CMDB，有助于将关键业务 IT 资产指定为配置项（CI）。CI 之间的依赖关系可以映射并可视化为业务视图，这有助于事件响应团队找出网络安全事件的根本原因和影响。
	自动化：在可行的情况下，使用自动化机制更新资产记录。自动机制来更新资产记录。理想情况下，工具应根据环境变化记录资产信息，而不是在发生变化后才检测。	ServiceDesk Plus 功能： - 无代码自动化的可视化 ITAM 工作流 ServiceDesk Plus 提供端到端的可视化工作流，有助于实现资产生命周期（从采购分配到报废）的自动化。这些工作流将在特定接触点触发通知、现场更新，甚至是低代码自定义自动化，从而建立管理和问责制。

国家计算机安全中心准则	要求	ServiceDesk Plus 起了什么样的作用?
资产管理（不属于技术控制，但被 NCSC 规定为核心安全功能）	完整性： 确保资产管理流程记录所有资产。这应包括物理、虚拟和云资源。	ServiceDesk Plus 功能： - 资产库存 - 资产扫描和对账 - 资产审计 - 资产工作流程和生命周期 ServiceDesk Plus 中的定期资产扫描可确保资产库存与最新数据保持一致。此外，IT 团队还可以将库存中的资产与采购订单进行核对。 IT 资产经理可以将资产处理流程转化为嵌入了自动化功能的可视化工作流。他们还可以通过 ServiceDesk Plus 进行资产审计，核实资产的当前位置和所有者。任何偏差都会突出显示，IT 团队可以采取适当措施。
	变更检测： 确保记录资产信息的变更，并使用多种数据源识别不一致之处。	ServiceDesk Plus 功能：计划资产扫描、资产审计、自定义触发器 定期资产扫描可确保资产库存保持最新。资产属性的任何变化都可记录在 ServiceDesk Plus 的报表中，以便进行快速审查。可配置自定义触发器，以便在编辑资产或 CI 时通知特定的利益相关者。 IT 和网络安全团队还可以运行资产审计，捕捉指定位置或所有者与实际位置或所有者之间的差异。这些资产会被标记，IT 团队可以启动调查，以确定这些偏差是否令人担忧。

国家计算机安全中心准则	要求	ServiceDesk Plus 起了什么样的作用?
资产管理（不属于技术控制，但被 NCSC 规定为核心安全功能）	保密性： 考虑所收集资产数据的敏感性。应用适当的保护措施和访问限制，同时确保支持相关用例。	ServiceDesk Plus 功能： - 基于角色的访问权限 - ITAM 模块的细粒度访问权限 可以在 ServiceDesk Plus 中定义角色和权限，确保只有经过授权的 IT 人员才能访问资产库存数据。可对这些权限进行调整，以确保对资产子集的细粒度访问，例如，由位置、产品类型、可借出资产或任何自定义字段定义的子集。
	资产分类： 考虑定义和使用类别对资产进行分类。这应与风险管理方法保持一致。	ServiceDesk Plus 功能： - 资产清单 - 基于产品类型的资产分类 - 资产组 发现并添加到 ServiceDesk Plus 中的每项资产都会大致分为 IT 资产和非 IT 资产，然后再分为各种产品类型。IT 团队还可以定义自定义产品类型，并将其分配给扫描的资产，从而与组织量身定制的风险管理策略保持一致。

Cyber Essentials技术控制和 ITSM 功能有助于遵守这些控制和功能

Cyber Essentials 控制	要求	ServiceDesk Plus 起了什么样的作用?
控制 2: **安全配置**	适用于 服务器、台式电脑、笔记本电脑、平板电脑、手机、IaaS、PaaS 和 SaaS	目标：确保正确配置计算机和网络设备 - 减少漏洞。 - 仅提供履行其职责所需的服务。
	贵组织必须主动管理计算机和网络设备。您必须定期：删除或禁用不必要的软件（包括应用程序、系统实用程序和网络服务）。	ServiceDesk Plus 功能： - 软件扫描 - 将特定软件标记为禁用软件 - 通知规则 - 与 ManageEngine Endpoint Central 集成 可以使用 ServiceDesk Plus 扫描和清点计算机上安装的所有软件。不必要或有害的软件可标记为禁止软件。只要检测到违禁软件，就可以通知特定技术人员，并向运行违禁软件的终端用户发送警告通知。 此外，通过将 ServiceDesk Plus 与 ManageEngine Endpoint Central 集成，IT 和安全团队还可以卸载违禁软件并采取补救措施。

Cyber Essentials 控制	要求	ServiceDesk Plus 起了什么样的作用?
控制 3: **安全更新管理**	要求 适用于：服务器、台式电脑、笔记本电脑、平板电脑、手机、防火墙、路由器、IaaS、PaaS、SaaS	目标：确保设备和软件不会受到已有修复程序的已知安全问题的影响。
	您必须确保范围内的所有软件都是最新的。 范围内设备上的所有软件必须 - 获得许可并得到支持。 - 更新，包括应用 在更新发布后 14 天*内更新，包括应用更新生效所需的任何手动配置变更。	ServiceDesk Plus 功能： - 软件资产库存 - 软件许可证管理 - 软件许可证合规性仪表板 ServiceDesk Plus 可帮助 IT 资产管理人员发现、盘点和管理安装在员工设备上的软件。在 ServiceDesk Plus 中添加和管理的软件许可证可映射到软件安装。它通过聚焦未授权的安装，帮助跟踪软件许可证合规情况。 ServiceDesk Plus 还会主动通知指定的技术人员许可证到期。ServiceDesk Plus 与 ManageEngine Patch Manager Plus 和 Endpoint Central 集成，可从 IT 资产库存中跟踪和管理每个端点的补丁程序。

Cyber Essentials 控制	要求	ServiceDesk Plus 起了什么样的作用?
控制 4: **用户访问控制**	适用于：服务器、台式电脑、笔记本电脑、平板电脑、手机、IaaS、PaaS、SaaS	目标：确保用户账户 - 只分配给获得授权的个人。 - 只允许用户访问其履行职责所需的应用程序、计算机和网络。
	您的组织必须 - 建立创建和批准用户账户的流程。 - 在不再需要用户账户时删除或禁用用户账户（例如，当用户离开组织或在规定的账户闲置期后）。 - 不再需要特殊访问权限时（例如，当员工更换角色时），删除或禁用该权限。	ServiceDesk Plus 功能： - 服务请求管理工作流程 - 服务请求模板 - 单触式工作流程自动化 - 自定义模块 从访问请求到员工入职和离职请求，企业都可以在 ServiceDesk Plus 中创建和实施独特的工作流，从而实现通知、审批、访问和账户供应及取消供应等的自动化。 动态表单（ServiceDesk Plus 中称为模板）使组织能够捕获特定的访问要求，并请求适当的主管和利益相关者批准。通过在 ServiceDesk Plus 中设置定制的用户访问管理实践，可以使用自定义模块对每个入职、离职和员工变更请求进行审计。

Cyber Essentials 控制	要求	ServiceDesk Plus 起了什么样的作用?
控制 5: **恶意软件保护**	适用于：服务器、台式电脑、笔记本电脑、平板电脑、手机、IaaS、PaaS、SaaS	目标：限制已知恶意软件和不受信任软件的执行，防止其造成破坏或访问数据。
	如果使用反恶意软件保护设备，则必须将其配置为 - 根据供应商建议进行更新。 - 防止恶意软件运行。 - 防止执行恶意代码。 - 防止通过互联网连接恶意网站。	ServiceDesk Plus 功能： - 事件管理 - 问题管理 - CMDB - 内置人工智能 Zia，用于工单预测、对话和事故后审查 - 与 ManageEngine 的 UEM 解决方案 Endpoint Central 集成 虽然 ITSM 平台通常不用于恶意软件保护，但其 CMDB 和事件管理功能可通过主动响应威胁检测和警报来预防恶意软件感染。 来自 UEM 和 EDR 应用程序（如 Endpoint Central）的电子邮件警报和通知可自动记录为 ServiceDesk Plus 中的事件单。这些事件会通过 ManageEngine 的本机人工智能助手 Zia 智能路由到正确的技术人员和事件响应团队 (IRT)。然后，IRT 可以遵循预定义的事件响应流程，与利益相关者合作，整理证据并解决根本原因。 ServiceDesk Plus 中的 CMDB 使 IRT 能够了解错综复杂的 CI 依赖关系、衡量安全事件的影响、计划补救措施并找出根本原因。

在全球范围内，数据泄露的平均成本在 2024 年将达到约 378 万英镑（约合 488 万美元）*，达到历史最高水平。面对这一统计数字和业务各方面的数字化，企业及其领导层应该立即行动起来，采取基本的网络安全措施，如 Cyber Essentials 中概述的措施。然而，要达到基本的安全态势似乎遥不可及，尤其是当企业的 IT 管理职能高度孤立时。ITSM 最佳实践和 ServiceDesk Plus 等平台可帮助企业弥合这一差距，并利用现有流程和工具，以最小的学习成本实现更好的安全态势。

关于 ServiceDesk Plus

ServiceDesk Plus 是 Zoho 公司企业 IT 管理部门 ManageEngine 推出的人工智能驱动的统一服务管理解决方案。它将 ITSM 要素、资产管理和 CMDB 与企业服务管理功能相结合，为设计、管理和交付 IT 与业务服务提供了一个全面的平台。

ServiceDesk Plus 采用专有的人工智能技术和公共 LLM 集成，为员工、技术人员和流程所有者带来无与伦比的效率和体验。

以下是一些全球领先企业信赖 ServiceDesk Plus 的五个原因

- 用于 IT 和企业服务管理的高价值 AI 功能不是付费的附加组件，而是包含在您的订购中。
- 功能强大的现代 ITIL 工作流程可协调端到端的企业和 IT 服务。
- 从服务器、网络和交换机到工作站和外围设备，它是您记录整个数字基础设施的单一系统。
- 平台功能支持 ServiceDesk Plus 实现工作场所服务交付的数字化和优化。
- ServiceDesk Plus 可与所有 ManageEngine 应用程序和其他第三方业务应用程序原生集成。

关于ManageEngine

ManageEngine是Zoho公司的一个部门，为全球企业和托管服务提供商提供全面的内部部署和云原生IT和安全运营管理解决方案。成熟企业和新兴企业都依赖 ManageEngine 的实时 IT 管理工具来确保其 IT 基础设施（包括网络、服务器、应用程序、端点等）的最佳性能。ManageEngine在全球拥有18个数据中心、20个办事处和200多个渠道合作伙伴，帮助企业将业务与IT紧密结合。欲了解更多信息，请访问公司网站，关注公司博客，并在 LinkedIn、Facebook、Instagram 和 X（原 Twitter）上与我们联系。

ManageEngine 卓豪
ServiceDesk Plus

免责声明：

ManageEngine并不声称使用ServiceDesk Plus或其他产品的实体将符合Cyber-Essentials标准。使用 ServiceDesk Plus 可帮助客户实现 Cyber Essentials 中列出的特定控制和要求，其认证取决于认证机构可能规定的多种因素。与其他适当的解决方案、流程、人员、控制和政策相结合，ManageEngine ServiceDesk Plus 可帮助组织符合 Cyber Essentials 准则。

本资料仅供参考之用，不应被视为有关Cyber Essentials合规性的法律建议。ManageEngine 对本资料中的信息不作任何明示、暗示或法定保证。请联系您的法律顾问，了解 Cyber Essentials 对您的组织有何影响，以及您需要采取哪些措施来遵守 Cyber Essentials。