网络安全弹性法案符合性认证

您是否已为新的欧盟网络恢复能力法案（CRA）做好准备？评估您遵守 CRA 基本网络安全要求的程度，提高产品和公司流程的网络弹性成熟度。Applus+网络恢复能力认证可帮助您评估产品是否符合 CRA（网络恢复能力法案）的基本要求，适用于 '默认 '或 '未分类 '类别。

CRA 法规预计将于2024年下半年正式生效，制造商将有36个月的时间来执行这项要求，但制造商对事件和漏洞的报告义务将只有21个月的有效期限。CRA对在欧洲销售数字产品的众多企业都有影响，但严格程度各不相同。请阅读我们的出版物，深入了解CRA的基本要求和受影响的产品。

受新法规影响的所有供应商都需有所应对，因为合规性将影响产品开发的核心，以评估公司的网络弹性成熟度。Applus+ Laboratories开发了一项新的符合性认证，主要针对非关键产品的供应商，这些产品将符合 CRA 定义的 '默认 '或 '未分类 '标准。预计约 90% 的受影响产品属于这些分类。尽管产品供应商可以选择自我评估，但遵守 CRA 的要求将是一项法律义务，包括提供所需的所有凭据（对违规公司可能会处以罚款）。

网络恢复能力的评估方法

Applus+ Laboratories已开发了一套内部方法，并在欧洲信息和通信技术产品网络安全评估方法 (FITCEM) EN 17640:2022 中得到确定。

FITCEM EN 17640:2022是一个通用框架，用于开发基于一组预定义任务的评估方法。它由 CEN CENELEC 制定，旨在将现有的国家方法标准化，如LINCE（西班牙）、CSPN（法国）或 BSZ（德国），Applus+ Laboratories的专家作为共同编辑参与其中。我们的内部方法是 FITCEM 的实例化，是根据 CRA 的未来需求量身定制的。我们不同技术领域的专家可根据产品类型分析具体需求。

根据FITCEM的规定，服务包括的评估任务

- **完整性检查:** 一项完整性的检查，审查 Applus+ Laboratories是否收到所要求的所有凭据。
- **安全功能审查:** 对制造商进行的强制性风险分析评估进行审查，以确保安全功能定义明确并涵盖制造商确定的风险。
- **开发文档:** 分析制造商提供的流程和文档，验证是否符合 CRA 有关产品和漏洞处理的要求。
- **漏洞审查:** 根据已公开的产品及其组件或已知漏洞进行漏洞分析审查

网络恢复能力符合性认证所需凭据

制造商应提供技术档案/技术文件（见 CRA 附件 II 和附件 V）中包含的以下凭据：

- **产品描述**，包括产品标识和安全功能、手册、用户指南等。
- **设计** (功能规格、加密算法、模块、组件.....) 、开发和生产过程以及漏洞处理和补丁管理过程的**说明**。
- 根据《计算机设备安全条例》第 10 条的规定，对设计、开发、生产、交付和维护具有数字元素的产品所面临的**网络安全风险进行评估**。风险评估程序和最新风险分析。
- 全部或部分应用的统**一标准、通用规格和网络安全计划** （如有）的清单。如果未采用这些协调标准、通用规格或网络安全认证计划，则说明为满足基本要求而采用的解决方案。
- 为验证产品和漏洞处理过程是否符合 CRA-Annex I 第 1 和第 2 部分中规定的适用基本要求而进行的**测试报告**。
- **欧盟符合性声明副本**（可选，本次评估不需要）。
- 如适用，提供CRA第3条第36点定义的**软件物料清单**

您将得到什么?

评估结果是一份 CoC（符合性认证证书），其中列出了产品和漏洞处理要求中已达到的要求。CoC 将附有使用 Applus+网络恢复能力标志的权利。

为什么选择APPLUS+网络恢复能力符合性认证?

Applus+ Laboratories是您构建网络弹性数字未来的合作伙伴。我们是通用标准认证的三大网络安全实验室之一。我们是一流的安全评估厂家，为不同的垂直行业提供 20 多种网络安全方案，从支付到物联网，再到汽车或密码学国防应用。

领先于即将出台的网络安全法规

无论您的产品被归类为默认、I 级还是 II 级，Applus+网络恢复能原力符合性认证服务都能为您提供帮助：

- 展现贵司对网络恢复能力的承诺
- 向您的客户和合作伙伴保证，您的产品领先于新出台的要求
- 确保您处于监管合规的最前沿

联系我们，了解更多有关Applus+网络恢复能力认证如何提升您的网络安全态势并在当今数字世界中提供竞争优势的信息。