

关于信息安全管理体系认证标准转换工作告客户书

尊敬的客户：

感谢贵组织对上海波西认证有限公司（以下简称 **POSI**）的信任和支持，选择我们为贵司提供管理体系认证服务。

国际标准化组织（ISO）于 2022 年 10 月发布了 **ISO/IEC 27001:2022**《信息安全 网络安全和隐私保护 信息安全管理体系 要求》，该标准代替了 **ISO/IEC 27001:2013**，标准要求发生了变化。

根据 **IAF MD26** 文件规定，转换期为标准发布之日起三年，即从 2022 年 10 月至 2025 年 10 月 31 日。所有依据 **ISO/IEC 27001:2013** 标准颁发的证书如未能在转换期内完成转换，将于 2025 年 10 月 31 日失效。

为了确保获证客户做好依据 **ISO/IEC 27001:2022** 标准认证转换工作，POSI 作出如下安排：

一、认证申请

1. 即日起至 2024 年 4 月 29 日，POSI 依然可以依据 **ISO/IEC 27001:2013** 标准（以下简称“旧版标准”）受理认证申请、实施审核并在认证决定通过后颁发认证证书，证书有效截止日期为 2025 年 10 月 31 日；

2. 自 2024 年 4 月 30 日起，POSI 不再受理依据“旧版标准”提出的认证申请，将全部依据 **ISO/IEC 27001:2022**（以下简称“新版标准”）实施初次认证审核和再认证审核。

二、认证证书的转换方式和审核时间

依据 **IAF MD26** 文件要求，获证客户可以选择结合再认证、监督审核或专项审核方

式进行转换：

1. 结合再认证审核进行转换的，转换审核需至少增加 **0.5** 个人日；
2. 结合监督审核或单独进行专项审核进行转换的，转换时间需至少增加 **1.0** 个人日。

依据客户的特定情况（例如客户所在行业的风险级别、过程的复杂程度等），审核时间可能还会增加。

三、证书的有效期

1. **2023 年 3 月 31 日**后所有依据旧版标准颁发的初次/再认证证书的有效截止日期统一为 **2025 年 10 月 31 日**；

2. 对于在 **2022 年 11 月 1 日**至 **2023 年 3 月 31 日**期间颁发的有效期超过 **2025 年 10 月 31 日**的依据旧版标准颁发的认证证书，**POSI** 将为客户免费更换证书，更换后的认证证书有效期统一为 **2025 年 10 月 31 日**。

- 如获证组织选择监督审核或专项审核方式完成新版标准转换后，新颁发的认证证书有效截止日期与原颁发的认证证书有效截止日期保持一致；
- 如原证书的截止日期受转换期的限制少于 **3** 年的，当组织完成新版标准转换后，证书的有效截止日期重新恢复原有证书的剩余周期，即会还原为 **3** 年周期。如：
原证书的有效期为 **2023 年 2 月 1 日**至 **2025 年 10 月 31 日**，成功完成转换后，证书的有效截止日期为 **2026 年 1 月 31 日**；
- 如获证组织选择再认证审核转换，新认证证书的生效日期为重新颁发之日，有效截止日期为原证书截止日期后 **3** 年。

四、客户转换工作准备建议

1. 对新旧标准进行差异化对比，并结合在组织内部应用情况进行分析，确定相应

的措施;

2. 应针对体系范围内相关人员进行全面有效的培训, 并完成内审员的转版培训;
3. 应按照新版标准更新现有信息安全管理体系, 修订和完善相关管理文件, 并予以实施, 确保新版标准的所有要求在组织内得到实施, 并保存相应的记录;
4. 至少应针对新版标准开展的体系运行情况完成一次内部审核和管理评审;
5. 应尽早与我司联系, 商榷新版标准转换审核的安排。

五、客户沟通的方式

POSI 认为最好的转换审核时机是在最早一次审核时进行, 因此, 我们相关的业务经理会联系您了解关于贵组织新版标准的转换情况及具体申请转换的审核时间, 以便 **POSI** 进行适当的转换审核安排。

相关内容请密切关注我司官方网站 <http://www.posicert.com>

POSI 的工作人员随时为您提供相关转换的任何疑问的解答。

联系电话: 021-6858 3896

E-mail: info@posicert.com

