



奥邦检验认证集团有限公司企业标准

CTS_ABG 67034-2024

应用程序安全管理体系 要求

Information technology - Security techniques -

Application security management systems-Requirements

2024-06-28 发布

2024-06-28 实施

奥邦检验认证集团有限公司 发布

目录

应用程序安全管理体系 要求	1
1 范围	4
2 规范性引用文件	4
3 术语和定义	4
4 组织环境	4
5 领导作用	5
6 策划	6
7 支持	8
8 运行	9
9 绩效评价	10
10 改进	12

前言

本文件按照 GB/T1.1—2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件规定了应用程序安全管理体系认证的要求，旨在指导企业建立应用程序安全管理体系及相关认证活动，助力企业实现应用程序安全管理。。

本文件由奥邦检验认证集团有限公司技术部提出并起草。

本文件主要起草人：袁海、邵优良。

本文件由奥邦检验认证集团有限公司 2024 年 06 月 28 日批准。

本文件自 2024 年 06 月 28 日起实施。

本文件由奥邦检验认证集团有限公司负责解释。

应用程序安全管理体系 要求

1 范围

本文件规定了在组织范围内建立、实施、维护和持续改进应用程序安全管理体系的要求。本文件还包括针对组织需求量身定制的应用程序安全风险评估和处置要求。本文件中规定的要求是通用的，旨在适用于所有组织，无论其类型、规模或性质如何。

2 规范性引用文件

以下文件在正文中的引用方式使其部分或全部内容构成本文件的要求。对于注明日期的引用文件，仅引用的版本适用。对于未注明日期的引用文件，引用文件的最新版本（包括任何修订）适用。

ISO/IEC 27034:2018 《信息技术-安全技术-应用程序安全》 Information technology - Security techniques - Application security

3 术语和定义

在本文件中，ISO/IEC 27034中给出的术语和定义适用。

4 组织环境

4.1 理解组织及其环境

组织应确定与其目的相关且影响其实现应用程序安全管理体系预期结果的能力的外部 and 内部问题。

4.2 理解相关方的需求和期望

组织应确定：

- a) 与应用程序安全管理体系相关的相关方；
- b) 相关方的相关要求；
- c) 其中哪些要求将通过应用程序安全管理体系解决。

注：相关方的要求可以包括法律法规要求和合同义务。

4.3 确定应用程序安全管理体系的范围

组织应确定应用程序安全管理体系的边界和适用性，以确定其范围。在确定该范围时，组织应考虑：

- a) 4.1中提到的外部和内部问题；
- b) 4.2中提到的要求；
- c) 组织所执行的活动与其他组织所执行活动之间的接口和依赖关系。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1) 通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2) 也可通过客服电话咨询 **025-85307007**。