



供应链安全管理体系 认证实施规则

版 本： A/1

编 写： 质量技术部

审 核： 于书梅

批 准： 于贤达

生效日期： 2025年9月1日

荣南认证中心有限公司



目 录

1 适用范围	1
2 认证实施模式	1
3 认证申请的基本条件	1
4 认证申请	2
5 审核	3
6 获得认证后的监督	13
7 再认证	14
8 认证证书和认证标志	15
9 认证的暂停（恢复）、撤销和注销	17
10 认证标准更改	21
11 认证记录的管理	21
12 受理组织的申诉、投诉	22
13 费用	22
14 其他	22



1 适用范围

本认证方案适用于荣南认证中心有限公司（简称：RNCC）实施的供应链安全管理体系认证，满足国家相关认证制度规定，为认证服务提供规范，必要时，在认证合同中补充相关的技术要求。

本认证方案在认证双方签订合同时予以确认和采用。

2 认证实施模式

本认证方案规定，首先对被认证方的供应链安全管理体系进行初次审核，经过评定，作出是否批准认证的决定；在通过认证之后，在认证证书的有效期内对获证客户的供应链安全管理体系进行监督，按期进行监督审核，确认其能否保持认证资格，并在第三年认证到期前进行再认证审核。

3 认证申请的基本条件

申请认证的组织按照 ISO 28000-2022 标准的要求，建立供应链安全管理体系，并实施了覆盖所有程序的内部审核和管理评审。管理体系运行时间为 3 个月以上。

在组织提出认证申请时，应特别关注以下事项：

- 1) 申请组织应提供其法人营业执照或证明其法律地位的文件；
- 2) 申请组织在一年内，未发生供应链安全重大事故、重大投诉事件（如媒体曝光等）以及违反国家相关法律法规，虚报、瞒报获证所需信息的情况
- 3) 申请组织应提供其对适用的法律法规符合性的评价情况，以证明组织已建立、实施并保持了用于识别其活动、产品或服务的适用的法律法规和其它应遵守的要求的程序，且已将这些要求运用于组织的供应链安全管理体系中；

目 录

- 1、ISO28000-2022（中文版）：安全和复原力-安全管理系统-要求
1-28页
- 2、ISO28000-2022（英文版）：Security and resilience-
Security management systems-Requirements 29-56页

安全和复原力 - 安全管理系统 - 要求





受版权保护的文件

© ISO 2022

保留所有权利。除非另有规定，或在实施过程中需要，未经事先书面许可，不得以任何形式或任何手段，包括电子或机械，复制或利用本出版物的任何部分，或在互联网或内部网上发布。可以通过以下地址向国际标准化组织或请求者所在国家的国际标准化组织的成员机构申请许可。

ISO版权局

CP 401 - Ch. de Blandonnet 8

CH-1214 Vernier, Geneva 电

话: +41 22 749 01 11

电子邮件: copyright@iso.org

网站: www.iso.org

发表于瑞士

内容

前言简介

- 1 范围**
- 2 规范性参考资料**
- 3 术语和定义**
- 4 组织的背景**
 - 4.1 了解组织和其背景
 - 4.2 了解有关各方的需求和期望
 - 4.2.1 一般
 - 4.2.2 法律、监管和其他要求
 - 4.2.3 原则
 - 4.3 确定安全管理系统的范围
 - 4.4 安全管理制度
- 5 领导人**
 - 5.1 领导和承诺
 - 5.2 安全政策
 - 5.2.1 建立安全政策
 - 5.2.2 安全政策要求
 - 5.3 角色、责任和权力
- 6 规划**
 - 6.1 应对风险和机遇的行动
 - 6.1.1 一般
 - 6.1.2 确定与安全有关的风险并确定机会
 - 6.1.3 应对与安全有关的风险和利用机会
 - 6.2 安全目标和实现这些目标的规划
 - 6.2.1 确立安全目标
 - 6.2.2 确定安全目标
 - 6.3 变化的规划
- 7 支持**
 - 7.1 资源
 - 7.2 能力
 - 7.3 认识
 - 7.4 沟通
 - 7.5 记录的信息
 - 7.5.1 一般
 - 7.5.2 创建和更新文件化的信息
 - 7.5.3 对文件资料的控制
- 8 运作**
 - 8.1 业务规划和控制
 - 8.2 确定过程和活动
 - 8.3 风险评估和治疗
 - 8.4 控制措施
 - 8.5 安全战略、程序、过程和处理
 - 8.5.1 确定和选择战略和治疗方法
 - 8.5.2 所需资源
 - 8.5.3 实施治疗
 - 8.6 安全计划
 - 8.6.1 一般
 - 8.6.2 响应结构
 - 8.6.3 警告和沟通
 - 8.6.4 安全计划的内容

ISO 28000:2022(e)

8.6.5 恢复

9 业绩评估

9.1 监测、测量、分析和评价

9.2 内部审计

9.2.1 一般

9.2.2 内部审计方案

9.3 管理审查

9.3.1 一般

9.3.2 管理审查投入

9.3.3 管理审查结果

10 改进

10.1 持续改进

10.2 不合格品和纠正措施

书目

前言

ISO（国际标准化组织）是一个由国家标准机构（ISO成员机构）组成的全球联合会。制定国际标准的工作通常是通过ISO技术委员会进行的。每个对某一主题感兴趣的成员机构都有权在该技术委员会中任职。与国际标准化组织联络的国际组织、政府和非政府组织也参与这项工作。国际标准化组织与国际电工委员会（IEC）在所有电工标准化问题上紧密合作。

用于制定本文件的程序和打算进一步维护本文件的程序在ISO/IEC指令第1部分中有描述。特别要注意的是，不同类型的ISO文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.org/directives）。

请注意，本文件中的某些内容可能是专利权的对象。ISO不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的细节将在引言中和/或在ISO收到的专利声明列表中（见www.iso.org/patents）。

本文件中使用的任何商品名称是为方便用户而提供的信息，不构成对其的认可。

关于标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达方式的含义，以及关于ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，见www.iso.org/iso/foreword.html。

本文件由ISO/TC 292技术委员会（*安全和复原力*）编写。

第二版取消并取代了第一版（ISO 28000:2007），第一版在技术上进行了修订，但保留了现有的要求，为使用前一版的组织提供连续性。主要变化如下。

- 在[第4条中](#)加入了关于原则的建议，以便与ISO 31000更好地协调。
- 在[第8条中](#)增加了建议，以便与ISO 22301更好地保持一致，促进整合，包括。
 - 安全战略、程序、过程和处理。
 - 安全计划。

对本文件的任何反馈或问题应直接向用户的国家标准机构提出。这些机构的完整名单可在www.iso.org/members.html。

如您需获取上述认证规则全文及对应认证依据的全文，可通过以下方式联系 RNCC 获取。

联系电话：0871-63517098

邮箱：rnccyn@163.com