ISO/IEC 27002:2022

信息安全，网络安全与隐私保护

——信息安全控制

ISO/IEC 27002:2022

信息安全，网络安全与隐私保护 ——信息安全控制

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门体系。作为 ISO 或 IEC 成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定领域的技术活动。ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。与 ISO 和 IEC 保持联系的其他政府和非政府国际组织也参与此项工作。

ISO/IEC 指令第 1 部分描述了用于编制本文件的程序以及旨在进一步维护本文件的程序。特别是，应注意不同类型的文件需要不同的审批标准。本文件根据 ISO/IEC 指令第 2 部分的编辑规则起草（参见 http://www.iso.org/directives 或者 www.iec.ch/members_experts/refdocs ）。

请注意，本文件中的某些内容可能是专利权的主题。ISO 和 IEC 不负责识别任何或所有此类专利权。在文档开发过程中确定的任何专利权的详细信息将在引言和/或收到的 ISO 专利声明列表中列出（参见 http://www.iso.org/patents）或收到的 IEC 专利声明列表（参见 patents.iec.ch）。

本文件中使用的任何商品名称都是为了方便用户而提供的信息，并不构成认可。

有关标准的自愿性质的解释、与合格评定相关的 ISO 特定术语和表述的含义，以及有关 ISO 遵守《技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则》的信息，请参见 http://www.iso.org/iso/foreword.html。IEC 的有关信息请参见 www.iec.ch/understanding-standards。

本文件由 ISO/IEC JTC 1 联合技术委员会信息技术分委员会 SC 27 信息安全、网络安全和隐私保护编写。

第三版取消并取代了第二版（ISO/IEC 27002：2013），包含第二版的技术修订 ISO/IEC 27002:2013/Cor.1:2014 和 ISO/IEC 27002:2013/Cor.2:2015。

主要变化如下：

— 修改了标题；

— 改变了文档的结构，使用简单的分类法和相关属性来呈现控制；

— 一些控制被合并，一些被删除，一些新的控制被引入。

完整的对照见附件 B。

关于本文件的任何反馈或问题应提交给使用者所在国家或地区的标准机构。这些机构的完整清单可在以下网址找到： http://www.iso.org/members.html www.iec.ch/national-committees

0 引言

0.1 背景和语境

本文件适用于各种类型和规模的组织。它将用作在基于 ISO/IEC 27001 的信息安全管理体系（ISMS）中确定和实施信息安全风险处理控制的参考。它还可以用作组织确定和实施普遍接受的信息安全控制措施的指导文档。此外，考虑到特定的信息安全风险环境，本文件旨在用于制定行业和组织特定的信息安全管理准则。本文件中未包括的组织或环境特定的控制措施可根据需要通过风险评估来确定。

各种类型和规模的组织（包括公共和私营部门、商业和非营利组织）以多种形式创建、收集、处理、存储、传输和处置信息，包括电子、物理和口头形式（例如对话和演示）。

信息的价值超越了文字、数字和图像：知识、概念、想法和品牌都是信息的无形形式。在一个相互关联的世界中，信息和其他相关资产值得或需要针对各种风险源进行保护，无论这些风险源是自然的、意外的还是蓄意的。

信息安全是通过实施一套适当的控制措施来实现的，包括策略、规则、流程、程序、组织结构以及软件和硬件功能。为了满足其特定的安全和业务目标，组织应在必要时定义、实施、监控、审查和改进这些控制措施。诸如 ISO/IEC 27001 中规定的 ISMS 对组织的信息安全风险采取整体的、协调的观点，以便在一致的管理系统的总体框架内确定和实施一套全面的信息安全控制。

许多信息系统，包括它们的管理和操作，都没有按照 ISO/IEC 27001 和本文件中规定的 ISMS 来设计安全性。仅通过技术措施实现的安全级别是有限的，应该得到适当的管理活动和组织流程的支持。在进行风险处理时，确定哪些控制措施应该到位需要仔细规划并注意细节。

成功的 ISMS 需要组织中所有人员的支持。它还可能需要其他相关方的参与，如股东或供应商。也可能需要相关领域专家的建议。

一个适当、充分和有效的信息安全管理体系为组织的管理层和其他相关方提供保证，确保他们的信息和其他相关资产得到合理的保护，免受威胁和伤害，从而使组织能够实现既定的业务目标。

0.2 信息安全要求

组织必须确定其信息安全要求。信息安全要求有三个主要来源：

a）考虑到组织的总体业务战略和目标，对组织面临的风险进行评估。这可以通过特定于信息安全的风险评估来促进或支持。这应导致确定必要的控制措施，以确保本组织的剩余风险符合其风险接受标准；

b） 组织及其相关方（贸易伙伴、服务提供商等）必须遵守的法律、法规、规章和合同要求，以及他们的社会文化环境；

c）组织为支持其运营而开发的信息生命周期所有步骤的一系列原则、目标和业务要求。

0.3 控制

控制被定义为改变或保持风险的措施。本文件中的一些控制措施是改变风险的控制措施，而其他控制措施则保持风险。例如，信息安全策略只能保持风险，而遵守信息安全策略可以改变风险。此外，一些控制表现为在不同的风险语境下相同的通用措施。本文件提供了从国际公认的最佳实践中总结出来的组织、人员、物理和技术信息安全控制的通用组合。

0.4 确定控制

确定控制取决于组织在风险评估后做出的决策，并具有明确定义的范围。与已识别风险相关的决策应基于组织采用的风险接受标准、风险处理方案和风险管理方法。控制措施的确定还应考虑到所有相关的国家和国际法律和法规。控制措施的确定还取决于控制措施相互作用以提供深度防御的方式。

组织可以根据需要设计控制或从任何来源识别控制。在指定此类控制措施时，组织应根据实现的业务价值考虑实施和运行控制措施所需的资源和投资。请参见 ISO/IEC 27016，了解有关 ISMS 投资决策的指导，以及这些决策在竞争资源需求背景下的经济后果。

为实施控制措施而部署的资源应该与在没有这些控制的情况下安全事故可能产生的业务影响之间寻求平衡。风险评估的结果应有助于指导和确定适当的管理措施、管理信息安全风险的优先级以及实施防范这些风险所需的控制措施。

本文件中的一些控制措施可视为信息安全管理的指导原则，适用于大多数组织。有关确定控制和其他风险处理选项的更多信息，请参见 ISO/IEC 27005。

0.5 制定组织的个性化指南

该文件可被视为制定组织的个性化指南的起点。并不是本文件中的所有控制和指导都适用于所有组织。还可能需要本文件中未包含的其他控制措施和指南来满足组织的特定需求和已识别的风险。当制定的文件包含额外的指南或控制措施时，包含本文件中条款的交叉引用以供将来参考会很有帮助。

0.6 生命周期考虑因素

信息有一个生命周期，从创建到处置。在整个生命周期中，信息的价值和风险可能会有所不同（例如，未经授权披露或窃取公司的财务账目在发布后并不严重，但完整性仍然至关重要）。因此，在所有阶段，信息安全在某种程度上都很重要。

信息系统和与信息安全相关的其他资产都有生命周期，在这些生命周期内，它们被构思、规定、设计、开发、测试、实施、使用、维护，并最终退役和处置。每个阶段都应该考虑信息安全。新的系统开发项目和对现有系统的改变提供了改善安全控制的机会，同时考虑到本组织的风险和从事故中吸取的教训。

0.7 相关国际标准

本文件提供了许多不同组织中普遍应用的各种信息安全控制的指南，而 ISO/IEC 27000 系列中的其他文档提供了有关信息安全管理整体流程的其他方面的补充建议或要求。

有关 ISMS 和文件系列的一般介绍，请参考 ISO/IEC 27000。ISO/IEC 27000 提供了一个词汇表，定义了 ISO/IEC 27000 文件系列中使用的大多数术语，并描述了该系列每个成员的范围和目标。

还有一些针对特定行业的标准，这些标准包含针对特定领域的额外控制措施（例如，针对云服务的 ISO/IEC 27017 标准、针对隐私的 ISO/IEC 27701 标准、针对能源的 ISO/IEC 27019 标准、针对电信组织的 ISO/IEC 27011 标准以及针对健康的 ISO 27799 标准）。此类标准包含在参考书目中，其中一些参考了第 5-8 条中的指南和其他信息部分。

信息安全，网络安全与隐私保护 ——信息安全控制

1 范围

本文件提供了一套通用的信息安全控制参考，包括实施指南。旨在供组织用来：

a）在基于 ISO/IEC 27001 的信息安全管理体系（ISMS）的范围内；

b）根据国际公认的最佳实践实施信息安全控制；

c）制定特定于组织的信息安全管理准则。

2 规范性引用文件

本文件中没有规范性引用文件。

3 术语，定义和缩写词

3.1 术语和定义

就本文件而言，以下术语和定义适用。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

— ISO 在线浏览平台：https://www.iso.org/obp

— IEC 电子词典：https://www.electropedia.org/

3.1.1 访问控制 access control

确保基于业务和信息安全要求授权和限制对资产（3.1.2）的物理和逻辑访问的方法。

3.1.2 资产 asset

任何对组织有价值的事物。

条目注释 1：在信息安全环境中，可以区分两种资产：
— 主要资产：
— 信息；
— 业务流程（3.1.27）和活动；
— 所有类型的支持资产（主要资产所依赖的），例如：
— 硬件；
— 软件；
— 网络；
— 工作人员（3.1.20）；
— 站点；
— 组织结构。

3.1.3 攻击 attack

未授权的破坏、更改、禁用、访问资产（3.1.2）的成功或不成功的尝试，或任何试图暴露、窃取或未经授权使用资产（3.1.2）的行为。

3.1.4 鉴别 authentication
保证实体（3.1.11）声称的特征属性是正确的。

3.1.5 真实性 authenticity
一个实体（3.1.11）是它所声称的那样的属性。

3.1.6 监管链 chain of custody
从一个时间点到另一个时间点，材料的可证明的持有、移动、处理和定位

条目注释 1：在 ISO/IEC 27002 环境下，材料包括信息和其他相关资产（3.1.2）。 [资料来源：ISO/IEC 27050-1：2019，3.1，另含修订——添加“条目注释 1”]

3.1.7 机密消息 confidential information
不打算对未经授权的个人、实体（3.1.11）或过程（3.1.27）可用或向其披露的信息。

3.1.8 控制 control
保持和/或改变风险的措施

条目注释 1：控制包括但不限于任何过程（3.1.27）、策略（3.1.24）、设备、实践或其他保持和/或改变风险的条件和/或行动。 条目注释 2：控制可能并不总是产生预期或假定的改变效果。 [资料来源：ISO 31000：2018，3.8]

3.1.9 中断 disruption
一种事故，无论是预期的还是未预期的，都会导致产品和服务的预期交付相对于组织的目标发生计划外的负面偏离。

[资料来源：ISO 22301：2019，3.10]

3.1.10 终端设备 endpoint device
联网的信通技术（ICT）硬件设备。

条目注释 1：端点设备可以指台式计算机、笔记本电脑、智能手机、平板电脑、瘦客户机、打印机或其他专用硬件，包括智能电表和物联网（IoT）设备。

3.1.11 实体 entity
与具有可识别的独特存在的领域的运营目的相关的项目。

条目注释 1：一个实体应有一个物理或逻辑的具象化实例。 例如个人、组织、设备、一组像这样罗列的事物、电信服务的个人订户、SIM 卡、护照、网络接口卡、软件应用、服务或网站等。 [资料来源：国际标准化组织/IEC 24760-1：2019，3.1.1]

3.1.12 信息处理设施 information processing facility
任何信息处理系统、服务或基础设施，或容纳信息的物理位置。

[资料来源：ISO/IEC 27000：2018，3.27，修改——“设施 facilities”替换为“设施 facility”。]

3.1.13 信息安全的违背 information security breach
危及信息安全，导致传输、存储或以其他方式处理的受保护信息遭到意外破坏、丢失、篡改、泄露或访问。

3.1.14 信息安全事件 information security event
表明可能发生信息安全的破坏（3.1.13）或控制失败（3.1.8）的事件

[资料来源：ISO/IEC 27035-1：2016，3.3，修改——“信息安全的违背 breach of information security”替换为“信息安全的违背 information security breach”]

3.1.15 信息安全事故 information security incident
一个或多个相关且已确定的信息安全事件（3.1.14）,可能会损害组织的资产（3.1.2）或干扰其运营

[资料来源：ISO/IEC 27035-1：2016，3.4]

3.1.16 信息安全事故管理 information security incident management
采用一贯的、有效的方法处理信息安全事故（3.1.15）

[资料来源：ISO/IEC 27035-1：2016，3.5]

3.1.17 信息系统 information system
一组应用程序、服务、信息技术资产（3.1.2）或其他信息处理部件。

[资料来源：国际标准化组织/IEC 27000：2018，3.35]

3.1.18 利益相关方 interested party/stakeholder
能够影响决策或活动、被决策或活动影响或认为自己受决策或活动影响的个人或组织。

[资料来源：国际标准化组织/IEC 27000：2018，3.37]

3.1.19 不可否认性 non-repudiation
证明声称的事件或行动及其发起实体发生的能力（3.1.11）

3.1.20 工作人员 personnel
在组织的指导下工作的人员

条目注释 1：工作人员的概念包括组织的成员，如理事机构、最高管理层、雇员、临时工作人员、承包商和志愿者。

3.1.21 个人可识别信息 personally identifiable information/PII

（a）可用于在信息和与信息相关的自然人之间建立联系的任何信息，或（b）直接或间接与自然人相关联的任何信息。

条目注释 1：定义中的“自然人”是指 PII 主体（3.1.22）。要确定 PII 主体是否可识别，应考虑持有数据的隐私利益相关方或任何其他方可以合理使用的所有方法，以建立 PII 集和自然人之间的联系。 [资料来源：ISO/IEC 29100：2011/Amd.1：2018，2.9]

3.1.22 PII 主体 PII principal
与 PII 个人可识别信息（3.1.21）相关的自然人。

条目注释 1：根据司法管辖区和特定的数据保护和隐私立法，也可以使用同义词“数据主体”代替术语“PII 主体”。 [资料来源：国际标准化组织/IEC 29100：2011，2.11]

3.1.23 PII 处理者 PII processor
代表 PII 控制者并根据其指示处理 PII 个人可识别信息（3.1.21）的隐私利益相关方。

[资料来源：国际标准化组织/IEC 29100：2011，2.12]

3.1.24 策略 policy
由最高管理者正式表达的组织的意图和方向

[资料来源：ISO/IEC 27000：2018，3.53]

3.1.25 隐私影响评估 privacy impact assessment
识别、分析、评估、咨询、沟通和规划处理 PII 个人可识别信息（3.1.21）的潜在隐私影响的整体流程（3.1.27），在组织更广泛的风险管理框架内制定

[资料来源：ISO/IEC 29134：2017，3.7，修改——删除条目注释 1。]

3.1.26 程序 procedure
开展活动或过程（3.1.27）的特定方式。

[资料来源：ISO 30000：2009，3.12]

3.1.27 过程 process
使用或转换输入以交付结果的一组相互关联或相互作用的活动

[资料来源：ISO 9000：2015，3.4.1，修改——删除条目注释]。

3.1.28 记录 record
组织或个人在履行法律义务或业务交易中，被作为证据、同时也作为资产创建、接收和维护的信息（3.1.2）

条目注释 1：此处的法律义务包括所有法律、法规、监管和合同要求。 [资料来源：ISO 15489-1：2016，3.14，修改——添加“条目注释 1”。]

3.1.29 恢复点目标 recovery point objective/RPO
发生中断（3.1.9）后数据将要恢复到的时间点。

[资料来源：ISO/IEC 27031：2011，3.12，修改——“必须 must”替换为“将要 are to be”。]

3.1.30 恢复时间目标 recovery time objective/RTO
发生中断（3.1.9）后，服务和/或产品以及支持系统、应用程序或功能恢复到最低水平所历经的时长。

[资料来源：ISO/IEC 27031：2011，3.13，修改——“必须 must”替换为“将要 are to be”。]

3.1.31 可靠性 reliability
与预期行为和结果一致的特性。

3.1.32 规则 rule
被接受的原则或指示，说明组织要求做什么、允许什么或不允许什么。

条目注释 1：规则可以在专题策略（3.1.35）和其他类型的文件中正式表述。

3.1.33 敏感信息 sensitive information
由于对个人、组织、国家安全或公共安全的潜在不利影响，需要防止其不可用、未经授权的访问、修改或公开披露的信息。

3.1.34 威胁 threat
可能对系统或组织造成损害的意外事故的潜在原因

[来源：ISO/IEC 27000：2018，3.74]

3.1.35 专题策略
由适当层级的管理者正式表达的，关于特定对象或主题的意图和方向。

条目注释 1：专题策略可以正式表达规则（3.1.32）或组织标准。 条目注释 2：一些组织对这些专题策略使用其他术语。条目注释 3：本文档中提及的专题策略与信息安全相关。关于访问控制的专题策略示例（3.1.1），关于桌面清晰和屏幕清晰的专题策略。

3.1.36 用户 user
有权访问组织信息系统（3.1.17）的相关方（3.1.18）。

比如工作人员（3.1.20）、客户、供应商。

3.1.37 用户终端设备 user endpoint device
用户用来访问信息处理服务的终端设备（3.1.10）。

条目注释 1：用户终端设备可以指台式计算机、膝上型计算机、智能电话、平板电脑、瘦客户机等。

3.1.38 脆弱性 vulnerability
可能被一个或多个威胁（3.1.34）利用的资产（3.1.2）或控制（3.1.8）的弱点

[资料来源：国际标准化组织/IEC 27000：2018，3.77]

3.2 缩写词
ABAC

attribute-based access control

基于属性的访问控制

ACL

access control list

访问控制列表

BIA

business impact analysis

业务影响分析

BYOD

bring your own device

自带设备办公

CAPTCHA

completely automated public Turing test to tell computers and humans apart

全自动公共图灵测试，区分计算机和人类

CPU

central processing unit

中央处理单元

DAC

discretionary access control

自主访问控制

DNS

domain name system

域名系统

GPS

global positioning system

全球定位系统

IAM

identity and access management

身份与访问管理

ICT

information and communication technology

信息与通讯技术

ID

Identifier

标识符

IDE

integrated development environment

集成开发环境

IDS

intrusion detection system

入侵检测系统

IoT

internet of things

物联网

IP

internet protocol

互联网协议

IPS

intrusion prevention system

入侵防御系统

IT

information technology

信息技术

ISMS

information security management system

信息安全管理体系

MAC

mandatory access control

强制访问控制

NTP

network time protocol

网络时间协议

PIA

privacy impact assessment

隐私影响分析

PII

personally identifiable information

个人可识别信息

PIN

personal identification number

个人识别码

PKI

public key infrastructure

公钥基础设施

PTP

precision time protocol

精密时钟协议

RBAC

role-based access control

基于角色的访问控制

RPO

recovery point objective

恢复点目标

RTO

recovery time objective

恢复时间目标

SAST

static application security testing

静态应用程序安全测试

SD

secure digital

安全数字

SDN

software-defined networking

软件定义网络

SD-WAN

software-defined wide area networking

软件定义广域网

SIEM

security information and event management

安全信息与事件管理

SMS

short message service

短消息服务

SQL

structured query language

结构化查询语言

SSO

single sign on

单点登录

SWID

software identification

软件识别

UEBA

user and entity behaviour analytics

用户和实体行为分析

UPS

uninterruptible power supply

不间断电源

URL

uniform resource locator

统一资源定位符

USB

universal serial bus

通用串行总线

VM

virtual machine

虚拟机

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。