INTERNATIONAL STANDARD

ISO/IEC 27001:2022

Third edition: 2022-10

==========

Information security, cybersecurity and privacy protection Information security management systems -Requirements

信息安全、网络安全、隐私保护安全管理体系-要求

==========

目录

前言

ISO(国际标准化组织)和 IEC(国际电工委员会)构成了世界标准化特定体系。作为 ISO 或 IEC 成员的国家机构通过各自组织为处理特定技术活动领域而设立的技术委员会参与制定国际标准。ISO 和 IEC 技术委员会在共同关心的领域合作。与 ISO/IEC 联络的其他国际组织、政府或非政府组织也参与了这项工作

本文件及后续的开发与保持过程运用 ISO/IEC 指令第 1 部分，特别注意的是，不同类型的文件需要不同的批准标准。本文件是按照 ISO/IEC 指令第 2 部分的编辑规则起草的(见 www.iso.org/directives or www.iec.ch/members experts/refdocs)。

注意本文件中的某些要素可能涉及到专利权的主题。ISO 和 IEC 不负责识别任何或所有的这些专利权。在文件编制时确定的任何专利权的细节会在专利声明和或在 ISO 专利清单中获取(见 www.iso.org/patents)或 IEC 专利清单(见 https://patents.iec.ch)。

在本文件中使用的任何商品名都是为了方便用户而提供的信息，并不构成背书。

关于标准自愿性质的解释、ISO 特定术语和合格评定的相关表达的含义、以及关于在技术性贸易壁垒(TBT)中遵守世界贸易组织(WTO)原则的信息见 www.iso.org/iso/foreword.html，在 IEC，见 www.iec.ch/understanding-standards.

本文件由 ISO/IECJTC1 技术委员会 SC27，信息安全、网络安全和隐私保护信息技术分委员会编写。

第三版文件经过技术性修订，取消和替代了第二版(ISO/IEC27001:2013)，也包括 ISO/IEC 27001:2013/C 或-1:2014 及 ISO/IEC27001:2013/C 或-2:2015 的一些技术性勘误。

主要修订如下:

文本与管理体系标准的协调结构及 IS0/IEC27002:2022 保持一致。

本文件的任何反馈与问题宜直接与用户的国家标准机构联络。这些成员的完整列表可在 www.iso.org/members.html 或 www.iec.ch/national-committees_查找。

引言

0.1 总则

本文件提供了建立、实施、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略决策。组织信息安全管理体系的建立和实施受组织的需求和目标、信息安全要求、组织使用的过程、规模和结构的影响。所有这些影响因素都会随着时间而发生变化。

信息安全管理体系通过实施风险管理过程来保持信息的保密性、完整性和可用性，并为相关方树立风险得到充分管理的信心。

重要的是，信息安全管理体系是组织过程和整体管理结构的一部分并且融入其中，并且在过程、信息系统和控制的设计中要考虑到信息安全。期望的是，信息安全管理体系的实施程度应与组织的需求相符合。

本文件可被内部或外部各方用于评估组织的能力是否满足自身的信息安全要求。

本文件中所表述要求的顺序不反映各要求的重要性或暗示这些要求予以实现的顺序。条款的编号仅是为了参考。

ISO/IEC 27000 描述了信息管理体系的概要和词汇，引用了信息安全管理体系标准族(包括 ISO/IEC27003，ISO/IEC27004 及 ISO/IEC27005)及相关的术语和定义。

0.2 与其他管理体系标准的兼容性

本文件应用 ISO/IEC 合并导则附录 SL 第 1 部分中定义的高阶结构，相同的条款标题、相同的文本、通用术语和核心定义，因此维护了与其他采用附录 SL 的管理体系标准具有兼容性。

附录 SL 中定义的通用途径对于选择实施单一管理体系来满足两个或以上管理体系标准要求的组织是有用的。

0.3 交流探讨

本文件翻译时，为区别 IS0/IEC27001:2022 与 2013 版本，其中变化的部分用下划线标出。另外为方便与其他管理体系标准间的兼容性理解，个别词汇采用了与 GB/T22080-2016 不同的表示，如:"purpose"采用"宗旨"而非"意图","responsibilities"采用"职责"而非"责任"等。新版国家标准 GB/T22080 正式发布后以其为准。

本文件由逯伟防组织翻译，仅限于相关人员学习交流，非商用，欢迎探讨。反馈可发邮件 1wf000@126.com 或微信公众号"新版 ISO 管理体系标准解读"(luweifang9001)。

信息安全网络安全隐私保护信息安全管理体系要求

1 范围

本文件规定了在组织环境下建立、实施、维护和持续改进信息安全管理体系的要求。本文件还包括了根据组织需求所剪裁的信息安全风险评估和处置的要求。本文件规定的要求是通用的，适用于各种类型、规格或性质的组织。当组织声称符合本文件时，不能排除第 4 章到第 10 章中所规定的任何要求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件;不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000 信息技术安全技术信息安全管理体系概述和词汇

3 术语和定义

ISO/IEC 27000 界定的术语和定义适用于本文件。

ISO 和 IEC 保持的用于标准化术语数据库地址如下:

—— ISO 在线浏览平台:https:// www.iso .org/ obp

--IEC 电子化平台:https://www.electropedia.org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关的,且影响其实现信息安全管理体系预期结果的能力相关的外部和内部因素。

注:对这些因素的确定，参见 ISO 31000:2018，5.4.1 中建立外部和内部环境的内容。

4.2 理解相关方的需求和期望

组织应确定:

a)与信息安全管理体系有关的相关方;

b)这些相关方的相关要求;

c)需要通过信息安全管理体系应对的要求。

注:相关方的要求可包括法律法规要求和合同义务。

4.3 确定信息安全管理体系范围

组织应确定信息安全管理体系的边界和适用性以建立其范围。

当确定范围时，组织应考虑:

a)4.1 中提到的外部和内部因素;

b)4.2 中提到的要求

c)组织实施活动之间及与其他组织间实施活动的接口和依赖关系。

范围应形成文件化信息并可获得。

4.4 信息安全管理体系

组织应根据本文件的要求，建立、实施、维护和持续改进信息安全管理体系，包括所需过程及其相互作用。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动证实其对信息安全管理体系的领导作用和承诺:

a)确保建立信息安全方针和信息安全目标，并与组织的战略方向相一致;

b)确保将信息安全管理体系的要求融合入组织的过程中;

c)确保信息安全管理体系所需的资源可获得;

d)沟通有效的信息安全管理以及符合信息安全管理体系要求的重要性;

e)确保信息安全管理体系达成其预期结果;

f)指导并支持相关人员为信息安全管理体系的有效性做出贡献;

g)促进持续改进;并

h)支持其他相关管理角色在其职责范围内发挥领导作用。

注:本文件使用的"业务"一词可广义地理解为涉及组织存在目的的核心活动。

5.2 方针

最高管理者应建立信息安全方针，该方针应:

a)与组织的宗旨相适宜;

b)包括信息安全目标(见 6.2)或为设定信息安全目标提供框架;

c)包括对满足适用的信息安全相关要求的承诺;

d)包括对信息安全管理体系持续改进的承诺。

信息安全方针应:

e)形成文件化信息并可获取;

f)在组织内得到沟通;

g)适当时，可被相关方获取。

5.3 组织角色、职责和权限

最高管理者应确保与信息安全相关的角色、职责和权限在组织内得到分配和沟通。

最高管理者应分配职责和权限，以:

a)确保信息安全管理体系符合本文件的要求;

b)向最高管理者报告信息安全管理体系的绩效。

注:最高管理者也可分配在组织内报告信息安全管理体系绩效的职责和权限。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

当策划信息安全管理体系时，组织应考虑 4.1 中提到的因素和 4.2 中提到的要求，并确定需要应对的风险和机遇，以:

a)确保信息安全管理体系能够实现其预期结果;

b)预防或减少不良影响;

实现持续改进。

组织应策划:

d)应对这些风险和机遇的措施，并

e)如何:

1)将这些措施融合到信息安全管理体系过程中，并予以实现;

2) 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应确定和实施信息安全风险评估过程，以:

a)建立并维护信息安全风险准则，包括:

1)风险可接受准则;

2)实施信息安全风险评估准则。

b)确保重复的信息安全风险评估产生一致、有效和可比较的结果。

c)识别信息安全风险;

1)实施信息安全风险评估过程以识别与信息安全管理体系范围内与信息的保密性、完整性和可用性损失有关的风险;

2)识别风险所有者;

d)分析信息安全风险;

1)评估 6.1.2c)1 中所识别的风险发生后，可能导致的潜在后果;

2)评估 6.1.2c)1 中所识别的风险实际发生的可能性;

3)确定风险级别。

e)评价信息安全风险:

1)将风险分析的结果与 6.1.2a)中建立的风险准则进行比较;

2)为风险处置排序已分析风险的优先级

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.3 信息安全风险处置

组织应确定并实施信息安全风险处置过程，以:

a)在风险评估结果的基础上，选择适当的信息安全风险处置选项;

b)确定实现已选的信息安全风险处置选项所必需的所有控制;

注 1:当需要时，组织可设计控制，或识别来自任何来源的控制。

c)将 6.1.3b)确定的控制与附录 A 的控制进行比较，并验证没有忽略必要的控制;

注 2:附录 A 包括了可能的信息安全控制清单，本文件的用户可在附录 A 的指导下，确保所必需的信息安全控制措施没有被忽视。

注 3:附录 A 的信息安全控制清单并不是详尽的，如需要，可以附加信息安全控制。

d)制定一个适用性声明，包括:

-一必要的控制[见 6.1.3b)和 c)];

-一包含这些控制的正当理由;

-一是否实施了所必需的控制;

-一排除附录 A 控制的正常理由。

2)评价这些措施的有效性。

e)制定正式的信息安全风险处置计划;

f)获得风险所有者对信息安全风险处置计划以及对信息安全残余风险接受的批准。

组织应保留有关信息安全风险处置过程的文件化信息。

注 4:本文件中的信息安全风险评估与处置过程与 ISO31000 中给出的原则和通用指南相匹配。

6.2 信息安全目标及其实现的策划

组织应在相关的职能和层级上建立信息安全目标。

信息安全目标应:

a)与信息安全方针相一致;

b)可测量(如可行);

c)应考虑适用的信息安全要求，以及信息评估和信息处置的结果;

d) 得到监视

e)得到沟通;

f)适当时更新;

g)作为文件化信息可获取。

组织应保留信息安全目标的文件化信息。

在策划如何实现信息安全目标时，组织应确定:

h) 要做什么:

i)需要什么资源;

j)由谁负责;

k)什么时候完成;

l)如何评价结果。

6.3 变更策划

当组织确定需要变更信息安全管理体系时，变更应按计划的方式实施。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应:

a) 确定在组织控制下从事会影响信息安全绩效的工作人员所需的能力;

b)确保上述人员在适当的教育、培训、经验方面能够胜任;

e) 适用时，采取措施以获得必要的能力，并评价所采取措施的有效性;

d)保留适当的文件化信息作为能力的证据。

注:适用的措施可包括，如针对现有雇员提供培训、指导或重新分配;雇佣或签约有能力的人员。

7.3 意识

组织控制下的工作人员应意识到:

a) 信息安全方针

b)其对信息安全管理体系有效性的贡献，包括改进信息安全绩效的益处;

c)不符合信息安全管理体系要求带来的影响。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部沟通的需求，包括:

a) 沟通什么:

b)何时沟通;

c)与谁沟通;

d)怎么沟通。

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系应包括:

a)本文件要求的文件化信息;

组织的信息安全管理体系有效性所必需的文件化信息。

注:信息安全管理体系文件化信息的详略程度因组织而异，取决于:

1)组织的规模及其活动、过程、产品和服务的类型;

2)过程及其相互作用的复杂程度;

3) 人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的:

a)标识和说明(如标准、日期、作者或索引编号);

b)形式(如语言、软件版本、图表)和载体(如纸质的、电子的);

c)评审和批准，以保持其适宜性和充分性。

7.5.3 文件化信息的控制

信息安全管理体系及本文件所要求的文件化信息应得到控制，以确保:

a)在需要的场合和时机，均可获得并适用;