国 际 电 信 联 盟

ITU-T X.1054

(04/2021)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 安全管理

信息安全、网络安全和隐私保护 – 信息安全治理

ITU-T X.1054建议书

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	**X.1050–X.1069**
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账本技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

国际标准ISO/IEC 27014
ITU-T X.1054 建议书

信息安全、网络安全和隐私保护 – 信息安全治理

摘要

ITU-T X.1054建议书 | 国际标准ISO/IEC 27014为信息安全治理提供了指导原则。

信息安全对于组织来说是一个关键问题，随着攻击方法和技术的快速发展以及相应的法规压力的增加，这一问题变得更加突出。

组织信息安全控制的失败会对组织及其相关方产生许多不利影响，包括但不限于破坏信任。

信息安全治理是指使用资源来确保信息安全的有效实施，并保证：

- 将遵循有关信息安全的指令，且
- 管理机构将收到关于信息安全相关活动的可靠且相关的报告。

这有助于管理机构就组织的战略目标做出决定，提供可能影响这些目标的信息安全信息。它还确保信息安全战略符合实体的总体目标。

在组织中工作的管理人员和其他人需要理解：

- 影响他们工作的治理要求，以及
- 如何满足要求他们采取行动的治理要求。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1054	2012-09-07	17	11.1002/1000/11594
2.0	ITU-T X.1054	2021-04-30	17	11.1002/1000/14248

关键词

信息安全、信息安全治理、信息安全管理、信息安全管理系统（ISMS）

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联没有收到实施本建议书可能需要的受专利/软件版权保护的知识产权通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询可通过ITU-T网站获得的适当的ITU-T数据库，网址为：http://www.itu.int/ITU-T/ipr/。

目录

前言

国际电联（ITU）是从事电信领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电联的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。WTSA第1号决议规定了批准建议书须遵循的程序。属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

ISO（国际标准化组织）和IEC（国际电子技术委员会）共同构成了世界范围的标准专用系统。ISO和IEC的成员实体参与国际标准的研究，是通过由各自组织设立的技术委员会来进行特定技术领域的活动。ISO和IEC技术委员会在相互感兴趣的领域合作。其他政府或者非政府性质的国际组织可以通过与ISO和IEC发布联合声明的方式开展合作。在信息安全、网络安全和隐私保护领域，ISO和IEC成立了一个联合工作委员会ISO/IEC-JTC-1。

本建议书|国际标准是根据ISO/IEC指令（ISO/IEC Directives）第二部分的规定起草的。

联合技术委员会的主要任务是准备本建议书|国际标准。被联合技术委员会接受的国际标准草案会在有投票权的国际实体中使用。作为本建议书|国际标准的印刷本则需要至少75%的国际实体投票通过。

需要提前注意的一种可能性是，本建议书|国际标准中的某些元素可能受专利权影响。ITU、ISO或IEC不对标识任何或全部这些专利权负有责任。

ITU-T X.1054建议书 | ISO/IEC 27014由ISO/IEC联合技术委员会1、《信息技术》杂志、SC附属委员会27和《安全技术、网络安全和隐私保护》杂志与ITU-T第17研究组协作编制。本文同时作为ITU-T X.1054建议书发表。

国际标准
ITU-T建议书

信息安全、网络安全和隐私保护 – 信息安全管理

1 范围

本建议书 | 国际标准提供了有关信息安全治理概念、目标和程序的指导原则，各组织可依据这些指导原则对组织内信息安全相关程序进行评估、指导、监控和传达。

本文件的目标受众是：

- 管理机构和最高管理层；
- 根据ISO/IEC27001，负责评估、指导和监控信息安全管理系统（ISMS）的人员；
- 根据ISO/IEC27001，在ISMS范围之外，但在治理范围内负责信息安全管理的人员。

本建议书 | 国际标准适用于所有类型和规模的组织。

本文件中对ISMS的所有参引均适用于基于ISO/IEC27001的ISMS。

本建议书 | 国际标准侧重于附件B中给出的三种类型的ISMS组织。不过，其亦可用于其他类型的组织。

2 规范性参引

下列建议书和国际标准所包含的条款，通过在本建议书中的参引而构成本建议书 | 国际标准的条款。在出版时注明的版本为有效版本。所有的建议书和国际标准均会得到修订，因此根据本建议书 | 国际标准达成协议的各方应查证是否有可能使用下列建议书和标准的最新版本。IEC和ISO的各成员保存着当前有效的国际标准的目录。国际电联电信标准化局保存着当前有效的ITU-T建议书的清单。

– ISO/IEC 27000：现行，信息技术 – 安全技术 – 信息安全管理系统 – 概述和词汇。

– ISO/IEC 27001：现行，信息技术 – 安全技术 – 信息安全管理系统 – 要求。

3 定义

ISO/IEC 27000和以下标准给出的术语和定义适用于本建议书 | 国际标准：

ISO、IEC和ITU维护的用于标准化的数据库地址如下：

- IEC电子大全见：http://www.electropedia.org/
- ISO在线浏览平台见：http://www.iso.org/obp
- ITU术语和定义见：http://www.itu.int/go/terminology-database

3.1 实体：组织（3.2）和其他机构或各方。

注：一个实体可以是一组公司，或一个公司，或非营利公司，或其他。实体对组织拥有治理权。实体可能与组织相同，例如在较小的公司中。

3.2 组织：运行和管理ISMS的实体（3.1）的一部分。

3.3 治理机构：对实体为绩效和一致性负责的个人或团体。

注：来源：ISO/IEC 27000：2018年，3.24（修改版）–“组织”已被“实体”取代。

3.4 最高管理层：在最高级别领导和控制一个组织（3.2）的人或团体。

注1：来源 ISO/IEC 9001。

注2：最高管理层有权在组织内授权和提供资源。

注3：如果管理系统的范围只包括一个实体的一部分，那么最高管理层是指那些指导和控制该实体那一部分的人。在这种情况下，最高管理层对实体的治理机构负责。

注4：根据组织规模和资源情况，最高管理层可能与治理机构相同。

注5：最高管理层向治理机构报告[来源：ISO/IEC27000：2018年，3.75]。

注6：ISO/IEC 37001 也提供了治理机构和最高管理层的定义。

4 缩写词

就本建议书 | 国际标准而言，下列缩写词适用：

ISMS 信息安全管理系统

IT 信息技术

5 本建议书 | 国际标准的使用和结构

本建议书|国际标准描述了基于ISO/IEC 27001的信息安全治理在ISMS内是如何运作的，以及这些活动如何与在ISMS范围之外运作的其他治理活动相关联。它概述了“评估”、“指导”、“监控”和“沟通”四个主要流程，在这些流程中，可以在组织内部构建ISMS，并提出了将信息安全治理纳入每个流程中的组织治理活动的方法。最后，附件A描述了组织治理、信息技术治理和信息安全治理之间的关系。

根据定义，ISMS涵盖整个组织（见ISO/IEC 27000）。它可以涵盖整个实体，或者实体的一部分。图B.1对此进行了说明。

6 治理和管理标准

6.1 概述

信息安全治理是组织的管理机构，对影响组织信息安全的活动提供总体指导和控制的手段。这种指导和控制侧重于信息安全性不足会对组织实现总体目标的能力产生不利影响的情况。管理机构通常通过以下方式实现其治理目标：

- 通过制定战略和政策提供指导；
- 监控组织的绩效；并
- 评估管理人员制定的提案和计划。

信息安全管理与确保实现管理机构制定的战略和政策中描述的组织目标相关联。这可以包括通过以下方式与管理机构互动：

- 提供建议和计划供管理机构考虑；并
- 向管理机构提供有关组织绩效的信息。

信息安全的有效治理要求管理机构成员和管理人员以一致的方式履行各自的职责。

6.2 ISMS范围内的治理活动

ISO/IEC 27001规定在组织环境中建立、实施、维护和持续改进信息安全管理系统的要求。它还包括针对组织需求的信息安全风险评估和处理要求。

ISO/IEC 27001没有使用术语“治理”一词，但规定的一些要求其实就是治理活动。以下列表提供了这些活动的示例。如前所述，对组织和最高管理层的参引与基于ISO/IEC 27001的ISMS范围相关联。

- ISO/IEC 27001：2013年的分段4.1要求组织确定其目标 – 信息安全的总体目标和具体目的。这些应该与实体的总体目标和目的相关，并为其提供支持。这与本建议书 | 国际标准第7.2段中陈述的治理目标1、3和4相关。
- ISO/IEC 27001：2013年的分段4.2要求组织确定与其ISMS相关的相关方，以及这些相关方对信息安全的要求。这与本建议书 | 国际标准第7.2段中陈述的治理目标4相关。
- ISO/IEC 27001：2013年的分段4.3要求组织定义ISMS的边界和适用性，通过考虑外部问题和内部问题、要求、接口和依赖性来确定其范围。还规定组织应将相关方的要求和期望纳入其信息安全管理系统，以及外部和内部问题（如法律、法规和合同）。这与本建议书 | 国际标准第7.2段中陈述的治理目标1相关。
- ISO/IEC 27001：2013年的第5段规定组织须制定政策、目标，并将信息安全整合到其流程中（可能被认为包括治理流程）。它要求组织提供合适的资源，并传达信息安全管理的重要性。最重要的是，它还指出，本组织须指导和支持人员为ISMS的有效性做出贡献，并应支持其他相关管理角色在其职责范围内发挥作用。ISO/IEC 27001：2013的第5段包含制定策略以及为信息安全管理和报告分配角色的说明。这与本建议书 | 国际标准第7.2段中陈述的治理目标1和3相关。
- ISO/IEC 27001：2013年的第6段考虑组织的风险管理方法的设计，规定组织应识别风险和机会，以确保其ISMS有效。它引入了风险所有者的概念，并将其责任放在组织管理风险和批准风险处理活动的活动中。它还要求组织建立信息安全目标。这与本建议书 | 国际标准第7.2段中陈述的治理目标2相关。
- ISO/IEC 27001：2013年的第7段规定，人员须能够履行其信息安全义务，并提供组织沟通的要求。这与本建议书 | 国际标准第7.2段中陈述的治理目标5有关。
- ISO/IEC 27001：2013年的第8段规定了组织计划、实施和控制其ISMS的责任，包括外包安排。这与本建议书 | 国际标准第7.2段中陈述的治理目标4和6相关。
- ISO/IEC 27001：2013年的第9段要求监控和报告ISMS的所有相关方面、内部审计、最高管理层和管理机构对ISMS运行有效性的审查和决定，包括任何要求的变更。这与本建议书 | 国际标准第7.2段中陈述的治理目标6相关。
- ISO/IEC 27001：2013年的第10段规定了不合规项的识别和处理，持续改进机会的识别要求，以及对这些机会的行动。这与本建议书 | 国际标准第7.2段中陈述的治理目标4相关。

6.3 其他相关标准

ISO/IEC 38500为组织管理机构的成员提供指导原则，指导他们在其组织内有效、高效和以可接受的方式使用信息技术。它还为那些在IT治理方面提供建议、信息或协助管理机构的人提供指导。

6.4 组织内的治理思路

这些思路与第7段中描述的组织治理过程完全一致。列表中的最后两项相当于信息安全环境中的对等治理方面：

- 信息安全目标与业务目标的一致性；
- 根据这些信息安全目标管理信息安全风险；
- 避免信息安全管理中的利益冲突；
- 防止组织的信息技术被用于伤害其他组织。

7 实体治理和信息安全治理

7.1 概述

一个实体内部有许多治理方面，包括信息安全、信息技术、健康与安全、质量和财务。每个治理方面都是实体总体治理目标的一个组成部分，因此应该与实体规程保持一致。治理模型的范围有时会重叠。分段7.2和7.3描述了信息安全治理中涉及的目标和过程，且其适用于任何被治理的领域。

ISMS侧重于信息相关风险的管理。它不直接涉及诸如盈利能力以及资产的获取、使用和变现或其他过程的效率等主题，但它应支持这些主题上的任何组织目标。

7.2 目标

7.2.1 目标 1：建立整个实体综合全面的信息安全

信息安全治理应确保信息安全目标的综合性和整体性。信息安全工作应从整个实体层面着手，其决策过程需同时顾及实体的轻重缓急。有关物理安全和逻辑安全的各项活动应予以密切协调。但这不需要在整个实体内采用唯一一套安全措施或一个信息安全管理系统（ISMS）。

为了确保整个实体的信息安全，应在实体活动的所有环节中建立信息安全责任和问责机制。这可能会超出普遍认为的实体“边界”，例如，包含由外部各方存储和传输的信息。

7.2.2 目标2：采用基于风险的方式做出决策

信息安全治理应以合规义务为基础并基于各实体具体的风险决策。在确定安全的充分性时，除满足相关规定要求外，应以实体的风险偏好为依据，这些风险包括竞争优势的缺乏、合规性和债务风险、运行中断、声誉损害和财务损失。

信息安全风险管理应在整个实体范围内保持一致，并考虑违规和不遵从的负面财务、运行和声誉影响。此外，信息安全风险管理应与实体的整体风险管理方法相结合，这样就不会孤立地进行，也不会造成混乱，例如，与实体的方法对照或在实体的风险登记册中捕捉战略信息风险。

作为安全治理流程的一部分，应分配适当的资源来实施信息风险管理。

7.2.3 目标3：确立获取方向

开展新活动时，应充分评估信息安全风险的影响，包括但不限于任何投资、采购、合并、新技术的采用、外包安排和与外部供应商的合同。

为优化信息安全获取方式以支持实体目标，管理机构应确保信息安全与现有实体流程相集成，包括项目管理、采购、财务支出、法律和法规合规性以及战略风险管理。

ISMS最高管理层应根据实体目标制定信息安全战略，确保实体要求和组织信息安全要求之间的协调，从而满足相关方当前和不断变化的需求。

7.2.4 目标4：确保符合内部及外部要求

信息安全治理应该确保信息安全政策与做法均符合相关方的要求。这可能包括法律和法规，以及合同要求及内部承诺。

为了解决一致性与合规性的问题，最高管理层可通过委托开展独立的安全审计的方式确保信息安全活动能够令人满意地达到各项内部及外部要求。

7.2.5 目标5：培育有利于信息安全的文化

信息安全治理应该以实体文化为基础，包括所有相关方当前以及不断变化的需求。如果未能予以适当协调，各种目标、职责、责任和资源便有可能相互冲突，导致目标无法实现。因此，在不同相关方之间开展相互协调和确立一致的行动方向具有极其重要的意义。

为了培育有利于信息安全的文化，最高管理层应该要求、促进并支持对相关方的活动进行协调，从而为信息安全确立一个一致的方向。这一做法有助于提供安全教育、培训和认识提升计划。信息安全责任应整合到员工和其他方的角色中，且后者应通过承担这些责任来确保每个ISMS的成功。

7.2.6 目标 6：确保安全绩效满足实体当前和未来的要求

信息安全治理应该确保为保护信息而采取的行动方式与支持实体发展这一目标相匹配，提供经过一致认可的信息安全等级。安全绩效应该得到监督并始终保持在能够符合当前和未来要求的水平。

若从治理角度审核信息安全绩效，管理机构应根据信息安全的实体水平影响评估其绩效，不能仅考虑安全控制的有效性和效率。

在每个ISMS中，应要求ISMS的最高管理层实施衡量项目，以监控、审计和确定改善机遇。管理机构应将信息安全绩效与组织和实体的绩效结合起来。

7.3 程序

7.3.1 概要

实体内的管理机构实施“评估”、“指导”、“监控”和“沟通”程序。图1展示了这些程序之间的关系。

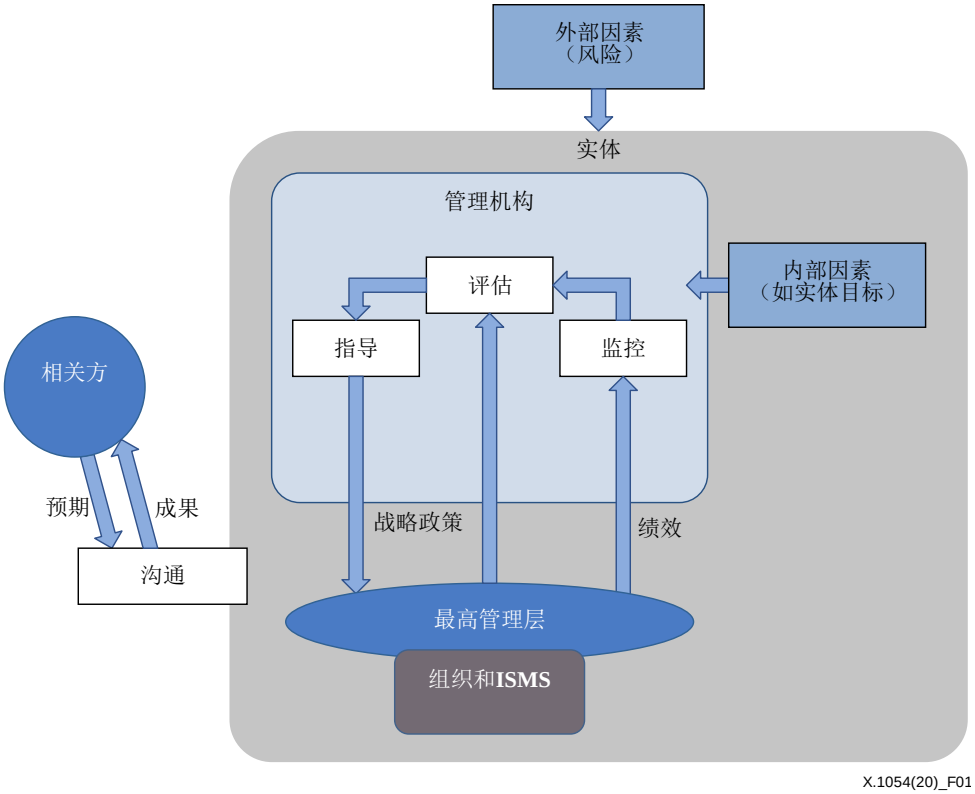


图1 – 采用一个ISMS的实体的治理模式

注1 – “组织”的定义[见本文件第3.2分段]意味着最高管理层一直参与组织的运作。

注2 – 一个实体可以包含一个以上的ISMS，并且适用治理的实体的某些部分可能不属于ISMS。见第8分段和附件B。

7.3.2 评估

作为治理程序，“评估”程序是指在当前程序和计划开展的变革基础上审议目标在当前以及未来的实现情况，并确定需要做出哪些调整以优化未来的战略目标完成情况。

为完成“评估”程序，

– 实体的管理机构应该：
  - 确保各项举措均能顾及相关的风险和机遇；
  - 通过在每个ISMS的背景下指定所需目标并确定其优先级（包括考虑ISMS范围之外的要求），对信息安全和ISMS衡量和报告做出响应；以及

– 每个ISMS的最高管理层应：
  - 确保信息安全能够充分支持和支撑实体的目标；
  - 将具有重大影响的新的信息安全项目提交管理机构批准。

7.3.3 指导

“指导”作为治理程序指管理机构对实体目标和战略给予指导。指导内容可包括资源等级的变更、资源分配、活动优先顺序排列、政策批准、重大风险受理和风险管理计划。

为完成“指导”程序，

– 管理机构应该：

- 确定实体的整体战略方向和目标；
- 确定实体的风险偏好；
- 批准信息安全战略；以及

– 每个ISMS的最高管理层应：

- 划拨充足的投资和资源；
- 将组织信息安全目标与实体目标协调一致；
- 划清信息安全职责；
- 制定信息安全政策。

注 – 风险偏好指一个组织愿意接受或保持的风险数量和类型。[8]

7.3.4 监控

“监控”是指可令管理机构对战略目标实现情况予以评估的治理程序。

为完成“监控”程序，

– 管理机构应该：

- 接收关于每个ISMS运行有效性的报告；
- 在实体的轻重缓急内予以评估；
- 将工作重点传达给每个ISMS的最高管理层；以及

– 每个ISMS的最高管理层应：

- 评估信息安全管理活动的有效性：
- 确保遵循各项内部和外部要求；
- 考虑到不断变化的实体、法律和监管环境以及对于信息风险的任何潜在影响；
- 从组织角度选择适当的绩效衡量标准并要求及时做出报告；
- 向管理机构提供有关信息安全绩效成果的反馈；
- 提醒管理机构注意影响信息风险和信息安全的新情况。

为了从治理的角度审查信息安全的性能，最高管理层应该根据信息安全在组织和实体层面的影响来评估信息安全的性能，而不仅仅是安全控制的有效性和效率。这可以通过实施绩效衡量计划来实现，以监控、审核和识别改进机会，将信息安全绩效与组织和实体的绩效联系起来。

7.3.5 沟通

“沟通”是一个双向的治理程序，在该程序中，管理机构和相关方就适合各自具体需求的信息开展交换。

开展“沟通”的一个方法是“信息安全状态说明”，向相关方说明信息安全的相关活动和问题，

沟通的原因之一是允许实体对股东等相关方负责。这一点越来越重要，组织现在提供关于其信息安全管理实施和维护信息，以及其在管理风险方面的有效性。同样，在发生信息安全事故的情况下，各实体应向其相关方解释影响、原因以及为应对事故重复发生风险对控制措施的修改，并酌情单独向公众做出解释。

沟通可以通过多种方法进行。它也可以有各种各样的内容以及不同的受众。任何沟通均应考虑到受众以及受众应该理解的信息。然后，这两个因素应该用来确定沟通的内容，以及向预期受众传递信息的渠道。附件C提供了一个范例。

为完成“沟通”程序，

– 管理机构应该：
  - 向外部相关方做出报告，说明实体开展的信息安全等级与其活动性质和工作重点完全匹配；
  - 确定监管义务并明确轻重缓急、相关方预期和涉及信息安全的实体要求信息；
  - 就需要其注意的事项和决策向ISMS最高管理层献计献策；
  - 为支持信息安全优先事项，就详细目标向相关方做出指示；
  - 推广积极的信息安全文化；
  - 在ISMS范围内向工作人员及他人提供培训并沟通其各自的职责。

8 管理机构有关ISMS的责任

8.1 组织和ISMS

管理机构应要求设计一个或多个ISMS来支持实体的目标。每个ISMS的目标可以与所属实体的目标相同，也可能不同，这取决于整个实体的规模、范围和结构，但它们应该保持一致。信息安全治理和信息技术治理之间的可能关系在附件A中做了说明。

管理机构还应要求每个ISMS的设计符合整体实体政策和流程，包括风险管理。一个ISMS采用与管理机构相同的风险评估程序可能是合适的，以便能够清楚地传达风险信息。如果管理机构使用的风险评估程序不符合ISO/IEC 27001的要求，那么，如果该组织希望实现合规，其ISMS应使用与该实体不同的风险评估方法，并商定一种与管理机构相一致的方式向管理机构传达风险相关信息。或者，管理机构可以选择改变实体现有的风险评估流程，以符合ISO/IEC 27001的要求。

管理机构可以授权使用ISMS来管理与知识产权损失、声誉损害以及与信息保密性、完整性或可用性损害相关的财务损失相关的战略风险。

ISMS可以向管理机构提供以下方面的管理信息：

- 实体的风险；
- ISMS的有效性。

管理机构应：

- 批准每个ISMS的创建；
- 定义每个ISMS和认证的范围（这些范围可能各不相同）；
- 向每个ISMS提供指导，包括目标、要求、角色和资源；
- 就可接受的剩余风险水平或适当的风险处理做出决定；
- 向每个ISMS提供沟通渠道，并授权其使用这些渠道向该ISMS范围内的相关方和所有人员传达适当的信息。

8.2 情形（见附件B）

8.2.1 A类：ISMS组织为整个实体

如果现有的唯一管理系统符合ISO/IEC 27001，它可以用来提供风险信息，从而使组织实现对信息风险的治理。然而，支持信息技术治理、财务治理、运行治理和其他治理活动仍存在不同的流程。

如果ISMS组织适用于整个实体：

- 第7.3段中描述的治理流程没有变化；
- 除了信息安全治理，最高管理层还将承担多项治理责任，例如公司治理。

组织的信息安全目标与实体的总体目标的一致性应该是直接了当的，因为最高管理层同时负责两者的制定。如果一个职责同时负责信息安全的治理和管理，则应提供适当的建议，以确保政策制定和政策执行的责任充分分离。

8.2.2 B类：ISMS组织构成更大实体的一部分

一些ISMS组织是一个更大实体的一部分。由于治理活动通常适用于整个法律实体、公司、慈善机构、公共机构或其他实体，在这种情况下，该实体的治理将超出ISMS的范围。一个组织在其边界内可以有多个ISMS。因此，一个管理机构可以管理多个ISMS。本文的大部分内容都考虑到了这种方法。

第7.3段中描述的四个治理过程仍然相关。但是，根据ISMS组织和所属实体之间的关系，以下情况之一可能适用：

- 每个ISMS组织作为所属实体的一个独立部分运作，因此有自己的业务目标。在这种情况下，ISMS组织的信息安全目标应该与其自身的业务目标保持一致。
- 每个ISMS组织负责实现其所属实体的一个或多个业务目标。在这种情况下，ISMS组织的信息安全目标应该与其所属实体的业务目标保持一致。

每个ISMS组织都代表所属实体负责管理信息安全风险的一个方面，在这种情况下，ISMS组织的信息安全目标应由所属实体规定，这将确保与所属实体的业务目标保持一致。

每个ISMS组织的最高管理层和所属实体的管理机构之间也将存在关系。最高管理团队和管理机构可以是相同的，可以有一些共同的人员，也可以没有共同之处。应使用图B.1确定哪些个人应被分配承担管理机构成员和相关方的责任。

8.2.3 C类：ISMS组织包括若干实体的多个部分

在这种情况下，ISMS组织像往常一样由最高管理层管理和控制，但是跨越许多实体。这可以在这样的情况下看到：一个较大的实体管理一组实体，这些实体共享一个共同的信息安全环境和对其部分活动的要求，例如，个人数据的收集、处理、存储和用于提供服务的方式。多个管理机构也可以共享一个ISMS；例如，一个组织可以提供可供许多客户使用的作为服务的ISMS。

如果ISMS组织包括若干实体的多个部分：

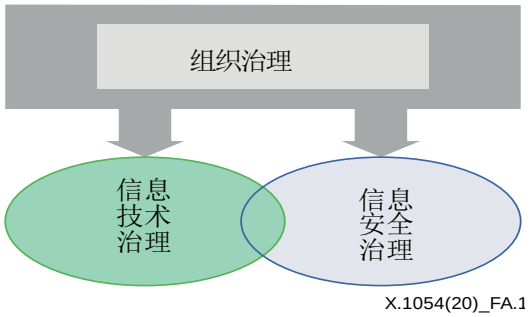
- 第7.3段中描述的治理流程没有变化。
- ISMS组织的信息安全目标应与将成员实体联系在一起的共同业务目标保持一致。

附件A

治理关系

（此附件不构成本建议书 | 国际标准不可分割的组成部分）

图A.1展示了信息安全治理和信息技术治理之间的关系。



图A.1 – 信息安全治理与信息技术治理之间的关系

信息技术治理的总体范围以获取、处理、存储和传播信息的资源为重心，而信息安全治理则强调信息的保密性、完整性和可用性。两种治理方案均需要采取以下治理步骤：评估、指导、监控和沟通。

附件B

ISMS组织类型

（此附件不构成本建议书 | 国际标准不可分割的组成部分）

管理ISMS的组织和应用ISMS的实体之间有三种关系。这些关系还影响到ISMS最高管理层的成员和该实体的管理机构。下面的列表和图B.1说明了这些类型的关系。

A类：实体和ISMS组织相同：

- 管理机构与ISMS的最高管理层相同。

B类：该实体包含ISMS组织（该实体内可能有一个以上的ISMS在运行）。

- 管理机构可以与每个ISMS共享一些成员，但成员不尽相同。

C类：一个ISMS由多个实体共享：

- 如果实体在ISMS有直接利益，每个实体的管理机构都可以成为ISMS最高管理层的成员。
- 如果ISMS是由第三方提供的服务，ISMS最高管理层的成员不太可能包括共享ISMS的实体的管理机构成员。

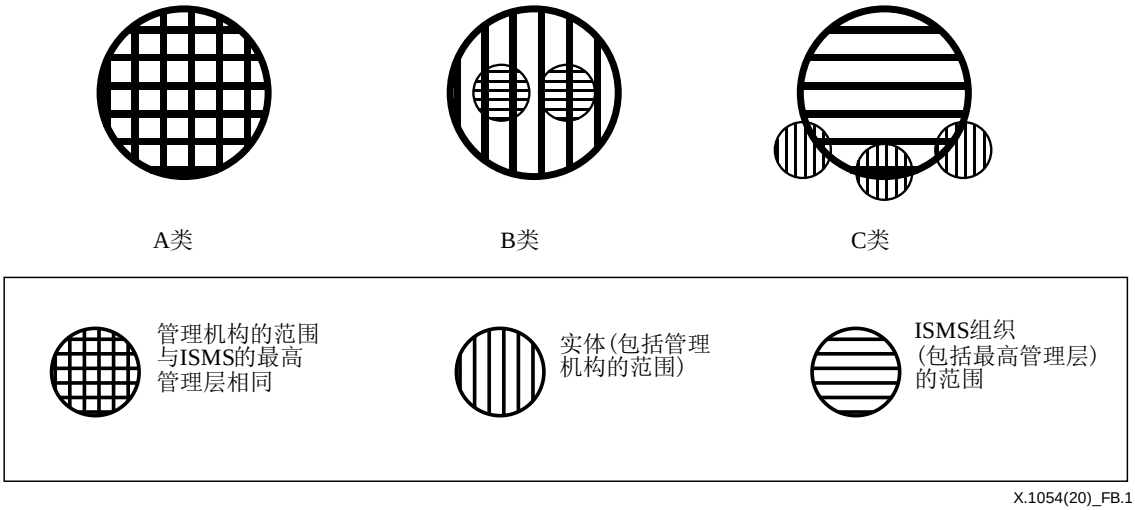


图 B.1 – 实体与ISMS之间可能的关系

附件C

沟通实例

（此附件不构成本建议书 | 国际标准不可分割的组成部分）

一个沟通的例子就是股票市场，由于法律或行业规则，公司必须披露信息安全风险。另一个例子是环境、社会和治理（ESG）报告，作为组织从环境、社会和经济角度向相关方解释/通报其努力的一种手段。一些ESG报告描述了隐私数据保护、信息安全活动和危机管理以防止发生安全事故的方法。

沟通设计活动还应考虑到因受众误解或推断附加内容产生的非预期效果，以及传播到预期受众以外的其他人所产生的非预期效果。

参考文献

[1] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[2] ISF, Standard of Good Practice for Information Security: 2018.

[3] ISO 37001:2016, *Anti-bribery management systems – Requirements with guidance for use*.

[4] ISO/IEC 9001:2015, *Quality management systems – Requirements*.

[5] ISO/IEC 27000:2018, *Information security, cybersecurity and privacy protection – Overview and vocabulary*.

[6] ISO/IEC 27002:2013, *Information security, cybersecurity and privacy protection – Code of practice for information security controls*.

[7] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization*.

[8] ISO Guide 73:2009

[9] IT Governance Institute (ITGI), *Information Security Governance: Guidance for Information Security Managers: 2008*.

[10] ITGI, *Information Security Governance Guidance for Boards of Directors and Executive Management*, 2nd Edition: 2006.

[11] ITGI, *COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance*, 2nd Edition: 2007.

[12] Ohki E., Harada Y., Kawaguchi S., Shiozaki T., Kgaua T., *Information Security Governance framework, Proceedings of the first ACM workshop on Information security governance*, pp. 1-6, 2009.

ITU-T 建议书系列

A 系列	ITU-T 工作的组织
D 系列	资费及结算原则和国际电信/ICT 的经济和政策问题
E 系列	综合网络运行、电话业务、业务运行和人为因素
F 系列	非话电信业务
G 系列	传输系统和媒介、数字系统和网络
H 系列	视听及多媒体系统
I 系列	综合业务数字网
J 系列	有线网络和电视、声音节目及其他多媒体信号的传输
K 系列	干扰的防护
L 系列	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M 系列	电信管理，包括 TMN 和网络维护
N 系列	维护：国际声音节目和电视传输电路
O 系列	测量设备的技术规范
P 系列	电话传输质量、电话设施及本地线路网络
Q 系列	交换和信令，以及相关联的测量和测试
R 系列	电报传输
S 系列	电报业务终端设备
T 系列	远程信息处理业务的终端设备
U 系列	电报交换
V 系列	电话网上的数据通信
X 系列	**数据网、开放系统通信和安全性**
Y 系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z 系列	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦