国　际　电　信　联　盟

ITU-T X.1054

(09/2012)

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

信息技术 – 安全技术 – 信息安全治理

ITU-T X.1054 建议书

国际电信联盟

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
报文处理系统	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**
生物测定安全	X.1080–X.1099
安全应用和服务	
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
网页安全	X.1140–X.1149
安全协议	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	
计算网络安全	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	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

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

信息技术 – 安全技术 – 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。

信息安全已成为各组织的一个关键问题。有关信息安全的监管要求不仅日益增多，而且信息安全措施失效还会对组织的声誉造成直接影响。

因此，作为其治理职责的一部分，管理机构必须对信息安全进行日益严格的监督，以确保实现组织的各项目标。

此外，信息安全治理为组织的管理机构、高级管理层和负责落实和运作信息安全管理系统的人员提供了一个强有力的连接纽带。

信息安全治理确保了在整个组织内推动信息安全举措所必备的职责。

与此同时，有效的信息安全治理还可确保管理机构获取业务开展背景下信息安全相关活动的有关报告。从而能够就信息安全问题做出及时中肯的决定，以支持组织的战略目标。

沿革

版本	建议书	批准日期	研究组	
1.0	ITU-T X.1054	2012-09-07	17	

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，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

国际标准
ITU-T 建议书

信息技术 – 安全技术 – 信息安全治理

1 范围

本建议书 | 国际标准规定了有关信息安全治理原则和程序的概念和指导原则，各组织可依据这些概念和指导原则对信息安全管理进行评估、指导和监控。

该建议书 | 国际标准适用于所有类型和规模的组织。

2 规范性参考文献

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引用而构成本建议书 | 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 27000:2009标准，*信息技术 – 安全技术 – 信息安全管理系统 – 概述和词汇*。

3 定义

ISO/IEC 27000 标准中的术语和定义以及下列定义适用于本建议书 | 国际标准：

3.1 高级管理层：在管理机构授权下负责实施相应战略和政策，以实现组织目标的个人或群体。

注1 – 高级管理层是最高管理层的一部分：为划清职责，这项标准对管理机构和高级管理层这两个最高管理层内部的团队进行了区分。

注2 –高级管理层有时亦称最高管理层，可包括首席执行官（CFO）、首席财务官（COO）、首席信息官（CIO）、首席信息安全官（CISO）等类似角色。

3.2 管理机构：最终负责组织绩效的个人或团体。

注 – 在某些管辖区域内，管理机构可以是整个董事会。

3.3 信息安全治理：组织用于指导和监督信息安全活动的原则和程序。

3.4 利益攸关方：能够影响组织活动、被组织活动影响或能够感受到组织活动的影响的任何个人或组织。

注 – 决策制定者亦可成为利益攸关方。

4 概念

4.1 概述

信息安全治理需要确保信息安全目标和战略与业务目标和战略保持一致，并应遵循相应的法律、规定和合约。信息安全治理应在内控系统的支持下，通过风险管理途径进行评估、分析和实施。

管理机构最终需为组织的决策和绩效负责。在信息安全方面，管理机构的关注重点应该是确保组织在实现信息安全方面的行动方式切实高效、令人满意，并能够充分考虑到利益攸关方的预期。不同的利益攸关方拥有不同的价值取向和需求。

4.2 目标

信息安全治理旨在：

- 使信息安全战略与业务战略/目标保持一致（战略一致），
- 为管理机构和利益攸关方创造价值（价值传递），
- 确保有效应对信息风险（问责机制）。

4.3 预期成果

预期通过有效地开展信息安全治理实现的成果包括：

- 管理机构可掌握信息安全状态，
- 就信息风险做出灵活决策，
- 切实高效的信息安全投资，
- 遵循外部要求（法律和规则要求）。

4.4 关系

组织内部亦存在若干其它治理模式，例如信息技术治理模式和组织治理模式。每个治理模式都是组织治理不可或缺的组成部分，体现了与业务目标保持一致的重要性。通常情况下，管理机构制定一个包含信息安全治理在内的综合完整的治理模式将会从中获益匪浅。治理模式的范围有时会出现重叠。例如图 1 就展示了信息安全治理和信息技术治理之间的关系。

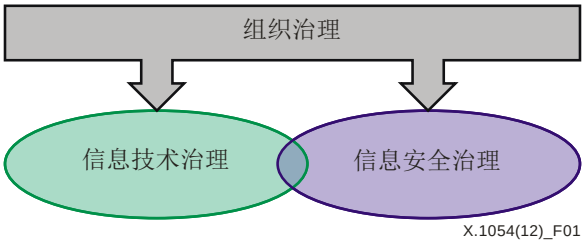

图1 – 信息安全治理与信息技术治理之间的关系

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（EDM）。但信息安全的治理则需要附加的内部“交流”程序。

第 5 节介绍了管理机构在建立信息安全治理方面所必须履行的任务。治理任务亦涉及参考资料所列的 ISO/IEC 27001 标准和其它ISMS系列标准所规定的管理要求。

5 原则和程序

5.1 概述

本节介绍了构成信息安全治理的原则和程序。信息安全治理原则是指治理行动或行为的公认规则，可作为实施治理工作的导则使用。信息安全治理程序则是一系列确保信息安全治理得以实现的任务及其相互关系。同时，信息安全治理程序还体现了信息安全治理与信息安全管理之间的关系。下文子节内容将对这两部分做出一一解释。

5.2 原则

从长期角度而言，实现利益攸关方的需求并为其创造价值是成功的信息安全必须具备的条件。为了实现治理目标，即保持信息安全目标和业务目标的密切一致以及为利益攸关方创造价值，该子节列出了六条以行动为导向的原则。

这些原则为信息安全治理活动的实施提供了良好基础。在阐述每条原则时，仅提到了应该实现的内容，并未指出如何、何时或由谁实施这些原则，原因在于这些内容均取决于实施这些原则的组织的性质。管理机构必须确保这些原则得以采用并任命具有相应责任、义务和职权的人员实施这些原则。

原则1：确立整个组织的安全性

信息安全治理应确保信息安全活动的综合性和整体性。信息安全工作应从整个组织层面着手，其决策过程需同时顾及业务、信息安全以及IT（适当情况下）等各个方面。有关物理安全和逻辑安全的各项活动应予以密切协调。

为了确立整个组织的安全性，应在组织活动的所有环节中建立信息安全责任和问责机制。这往往会超出普遍认为的组织“边界”，例如由外部各方进行信息存储和传输。

原则2：采用基于风险的行动方式

信息安全治理应以基于风险的决策为基础。在确定安全的充分性时，应该以组织的风险偏好为依据，这些风险包括竞争优势的缺乏、合规性和债务风险、运营中断、声誉损害和财务损失。

欲采用组织适合的风险管理，必须与组织整体的风险管理行动方式保持一致并相互结合。应根据组织对失去竞争优势、合规和债务风险、运行中断、名誉损害和财务损失等风险的偏好确定可接受程度的信息安全。实施风险管理方法的相应资源应由管理机构分配。

原则3：确立投资决策方向

信息安全治理应在已经实现的业务成果基础上确立安全投资战略，确保商业要求和安全要求协调一致，从而能够满足利益攸关方的需求。

为了优化安全投资以协助实现组织目标，管理机构应该确保信息安全整合在现有的各项组织工作程序中，包括资本支出和运营支出程序、法律和规则合规程序以及风险报告程序。

原则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，均符合相应的强制性法律法规以及付诸实施的商业或合同要求及其它内外部要求。

为了解决一致性与合规性的问题，管理机构应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。

原则5：营造一个有利于信息安全的环境

信息安全治理应该以人类的行为为基础，包括所有利益攸关方的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，导致业务目标无法实现。因此，在不同利益攸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。

为了营造一种有利于信息安全的文化，管理机构应该要求对所有利益攸关方的行动进行协调，从而为信息安全确立一个一致的方向。这一做法将有助于开展各类安全教育、培训和认识提升计划。

原则6：根据业务成果开展绩效审核

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组织发展这一目标相匹配，提供经过一致认可的信息安全等级。安全绩效应该始终保持在能够符合当前和未来业务要求的水平。

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业务影响评估其绩效，不能仅考虑安全控制的有效性和效率。评估可通过对监控、审计和改善工作的绩效衡量项目开展授权审核的方式予以实施，从而将信息安全绩效与业务绩效挂钩。

5.3 程序

5.3.1 概述

管理机构和高级管理层使用“评估”、“指导”、“监控”和“沟通”程序对信息安全进行治理。除此之外，“保障”程序还可以对信息安全治理情况和已经达到的水平提出独立客观的意见。图2展示了这些程序之间的关系。

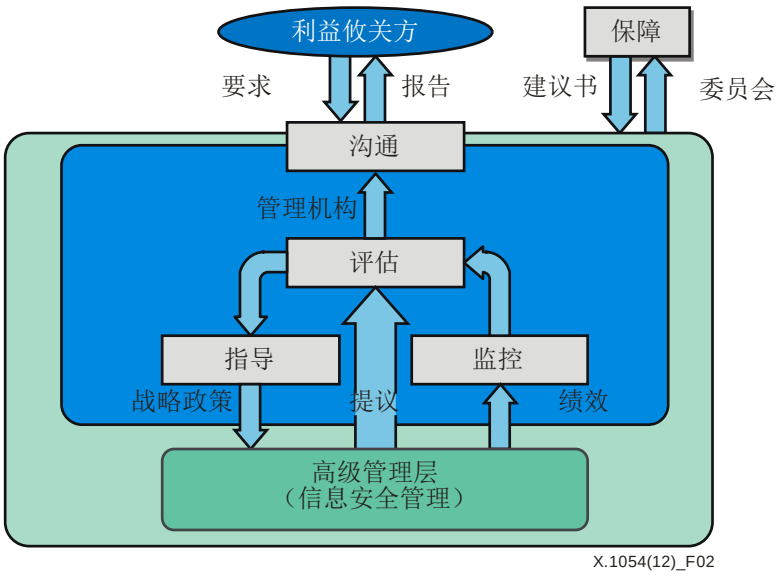

图2 – 在信息安全中采用治理模型

5.3.2 评估

作为治理程序之一，“评估”程序是指在当前程序和计划开展的变革基础上审议安全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，管理机构应该：

- 确保各项业务举措均能顾及信息安全问题，
- 对信息安全绩效成果做出回应，确定各项必要行动的优先顺序并予以实施。

为完成“评估”程序，高级管理层应该：

- 确保信息安全能够充分支持和支撑业务目标，
- 将具有重大影响的新的信息安全项目提交管理机构。

5.3.3 指导

“指导”程序是指管理机构对需要实施的信息安全目标和战略给予指导的治理程序。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：

- 确定组织的风险偏好，
- 批准信息安全战略和政策，
- 分配充足的投资和资源。

为完成“指导”程序，高级管理层应该：

- 制定和实施信息安全战略和政策，
- 将信息安全目标与业务目标协调一致，
- 推动营造积极的信息安全文化。

5.3.4 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：

- 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，
- 考虑到不断变化的业务、法律和监管环境以及这些环境对于信息风险的潜在影响。

为完成“监控”程序，高层管理者应该：

- 从业务角度选择适当的绩效衡量标准，
- 向管理机构提供有关信息安全绩效成果的反馈，包括管理机构过去确定的行动取得的绩效及其对组织的影响，
- 提醒管理机构注意影响信息风险和信息安全的新情况。

5.3.5 沟通

“沟通”是一个双向的治理程序，在该程序中，管理机构和利益攸关方就适合各自具体需求的信息安全交换信息。

开展“沟通”的方法之一是“信息安全状态说明”，使用该方法可向利益攸关方说明信息安全的相关活动和问题，附件A和B提供了这方面的具体范例。

为完成“沟通”程序，管理机构应该：

- 向外部利益攸关方报告说明组织开展的信息安全等级与其业务性质完全匹配，
- 针对所有发现信息安全问题的外部审核，向高级管理层汇报审核结果，并要求采取纠正措施，
- 受理有关监管义务、利益攸关方预期和涉及信息安全的业务需求的信息。

为完成“沟通”程序，高级管理层应该：

- 就需要其注意的事项向管理机构提供建议，并在可能的情况下做出相关决定，
- 针对为支持管理机构的指令和决定而需采取的具体行动向内部利益攸关方做出指示。

5.3.6 保障

“保障”程序是指管理机构委托开展独立客观的审计、审核或认证的治理程序。该程序可以确认和证实相应的目标和行为，这些目标和行为均与为了达到期望的信息安全等级而开展的治理活动和营业行为相关。

为完成“保障”程序，管理机构应该：

- 就管理机构在达到信息安全预期等级方面的责任履行情况委托开展独立客观的评价。

为完成“保障”程序，高级管理层应该：

- 为管理机构委托开展的审计、审核或认证提供支持。

附件 A

信息安全状态说明范例

（本附件不属于本建议书 | 国际标准的组成部分。）

组织可编制一份信息安全状态说明，将其作为一项沟通工具，向客户和利益攸关方披露信息安全情况。

信息安全状态说明的格式和内容应由组织自行选择决定。附件A介绍了一个利用信息安全审计声明公布满意度情况的范例。

表 A – 信息安全状态说明

在**mmm**至**nnn**这段时期内，针对组织运营程序和系统开展的基于**xyz**标准（例如 27000 系列，COBIT）的信息安全控制工作和程序在高级管理控制工作的补充下，通过充分有效的实施，为实现保密性、完整性和可用性等相关既定信息安全控制目标提供了合理保障。管理层对此表示满意。管理层特向外部信息安全审计机构**ABC**提供一份声明书对此予以说明。 ABC受董事会委派，负责审查管理层就信息安全控制工作做出的声明。审查工作依照既定标准开展，包括通过抽样测试评估信息安全控制工作和程序的设计及执行的有效性。为此，**ABC**向管理层发表了一份意见声明 – 测试结果显示，除个别例外情况，根据已经确立的**xyz**管理标准（例如 27000 系列，CobiT），具体方面的控制工作均切实有效。 完整的管理层声明书以及明确了信息安全控制例外情况的外部审计报告已经过审计委员会讨论，并已提交所有董事。同时可应利益攸关方的要求提供相关副本。

注 – “nnn”、“mmm”、“xyz”和“ABC”均属占位符。实际声明中应以具体的日期和名称替代。

附件B

详细信息安全状态范例

（本附件不属于本建议书 | 国际标准的组成部分。）

本附件介绍了一份披露具体信息安全内容的信息安全状态说明范例。此类状态说明对于期望通过重视安全性提高其声誉的组织（例如ICT企业）尤其有用。组织处理安全风险的做法的透明程度和适当的信息披露对于提高组织可信度也非常有效。通过开展上述行动，可以在利益攸关方之间共享普遍认识。

表 B – 信息安全状态详细说明

引言

- **范围**（战略、政策、标准），**界限**（地域/组织单位），**涵盖期限**（月/季度/半年/年）

整体状态

- **满意/未达满意程度/不满意**

更新情况（在适当且相关的情况下）

- 在实现信息安全战略方面的进展
  基本完成/进行中/计划中
- 信息安全管理系统的变化
  ISMS政策修订、实施ISMS的组织结构（包括责任分配）
- 认证进展
  ISMS（再）认证、经认证的信息安全审计
- 预算编制/职工安置/培训
  财务状况、人员充足性、信息安全资质
- 其它信息安全活动
  业务连续性管理参与、认识识提升活动、内部/外部审计协助

重要问题（如有）

- 信息安全审核结果
  建议、管理层的响应、行动计划、目标日期
- 主要内部/外部审计报告方面的进展
  建议、管理层的响应、行动计划、目标日期
- 信息安全事件
  预计影响、行动计划、目标日期
- （不）合规性
  预计影响、行动计划、目标日期

必要决定（如有）

- 附加资源
  确保信息安全能够支持业务活动

参考资料

[1] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[2] ISO/IEC 27001:2005, *Information technology – Security techniques – Requirements of information security management systems*.

[3] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[4] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management.*

[5] ISO/IEC 38500:2008, *Corporate Governance of Information technology*.

[6] ITGI, *Information Security Governance framework: 2009.*

[7] ISF, *Standard of Good Practice for Information Security: 2011*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
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	传输系统和媒质、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、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、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
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、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2013年，日内瓦