ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32923—2016/ISO/IEC 27014:2013

信息技术　安全技术　信息安全治理

Information technology—Security techniques—Governance of information security

(ISO/IEC 27014:2013,IDT)

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/IEC 27014:2013《信息技术　安全技术　信息安全治理》。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中电长城网际系统应用有限公司、中国信息安全测评中心、中国电子技术标准化研究院、中国信息安全研究院有限公司。

本标准主要起草人:闵京华、张晓菲、上官晓丽、许玉娜、李斌、罗锋盈、王惠莅、左晓栋、周亚超、刘恒、张兴、李刚、陈洪波、张春明、张劲、刘作康、王琰、王新杰。

引　言

本标准提供关于信息安全治理的指南。

信息安全已成为组织的关键问题。不仅法规要求日益增加，而且组织的信息安全措施失效会直接影响其声誉。

因此，组织治理者越来越需要承担起治理责任中的信息安全监督职责，以确保组织目标的实现。

此外，在组织的治理者、执行管理者和负责实现与运行信息安全管理体系人员之间，信息安全治理提供了强有力的纽带。

信息安全治理为在整个组织内推动信息安全行动倡议提供了必不可少的基础。

再者，信息安全的有效治理确保治理者收到在业务语境下形成的信息安全相关活动的报告，从而能够对信息安全问题作出恰当和及时的决策来支持组织的战略目标。

信息技术　安全技术　信息安全治理

1　范围

本标准就信息安全治理的概念和原则提供指南，通过本标准，组织可以对其范围内的信息安全相关活动进行评价、指导、监视和沟通。

本标准适用于所有类型和规模的组织。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000：2009，IDT)

3　术语和定义

GB/T 29246—2012 界定的以及下列术语和定义适用于本文件。

3.1

执行管理者　executive management

为达成组织意图，承担由组织治理者委派的战略和策略实现责任的个人或一组人。

注 1：执行管理者构成最高管理层的一部分。为明晰角色，本标准在最高管理层内区分两组人员：治理者和执行管理者。

注 2：执行管理者可包括首席执行官/行政总裁(CEO)、政府机构领导、首席财务官/财务总监(CFO)、首席运营官/运营总监(COO)、首席信息官/信息总监(CIO)、首席信息安全官/信息安全总监(CISO)和类似的角色。

3.2

治理者　governing body

对组织的绩效和合规负有责任的个人或一组人。

注：治理者构成最高管理层的一部分。为明晰角色，本标准在最高管理层内区分两组人员：治理者和执行管理者。

3.3

信息安全治理　governance of information security

指导和控制组织信息安全活动的体系。

3.4

利益相关者　stakeholder

对于组织活动能够产生影响、受到影响或感觉受到影响的任何个人或组织。

注：决策者可以是利益相关者。

4　概念

4.1　总则

信息安全治理需要使信息安全目标和战略与业务目标和战略一致，并要求符合法律、法规、规章和

合同。它宜通过风险管理途径被评估、分析和实现，并得到内部控制系统的支持。

治理者最终对组织的决策和绩效负责。在信息安全方面，治理者的关键聚焦点是确保组织的信息安全方法是有效率的、有效果的、可接受的，与业务目标和战略是一致的，并充分考虑到利益相关者的期望。各种利益相关者可能有不同的价值取向和需要。

4.2 目标

信息安全治理目标是：

- 使信息安全目标和战略向业务目标和战略看齐(战略一致)；
- 为治理者和利益相关者带来价值(价值传递)；
- 确保信息风险问题得到充分解决(责任承担)。

4.3 期望成果

有效实现信息安全治理的期望成果包括：

- 信息安全状态对治理者可见；
- 信息风险的决策方法敏捷；
- 信息安全投资高效且有效；
- 符合外部要求(法律、法规、规章或合同)。

4.4 关系

在组织内有一些其他领域的治理模型，诸如信息技术治理和组织治理。每个治理模型都是组织治理的不可分割的组成部分，都强调与业务目标一致的重要性。这通常有益于治理者开发一个整体和集成的组织治理模型视图，信息安全治理是其中的一部分。各治理模型的范围有时会重叠。例如，如图1所示的信息安全治理和信息技术治理之间的关系。

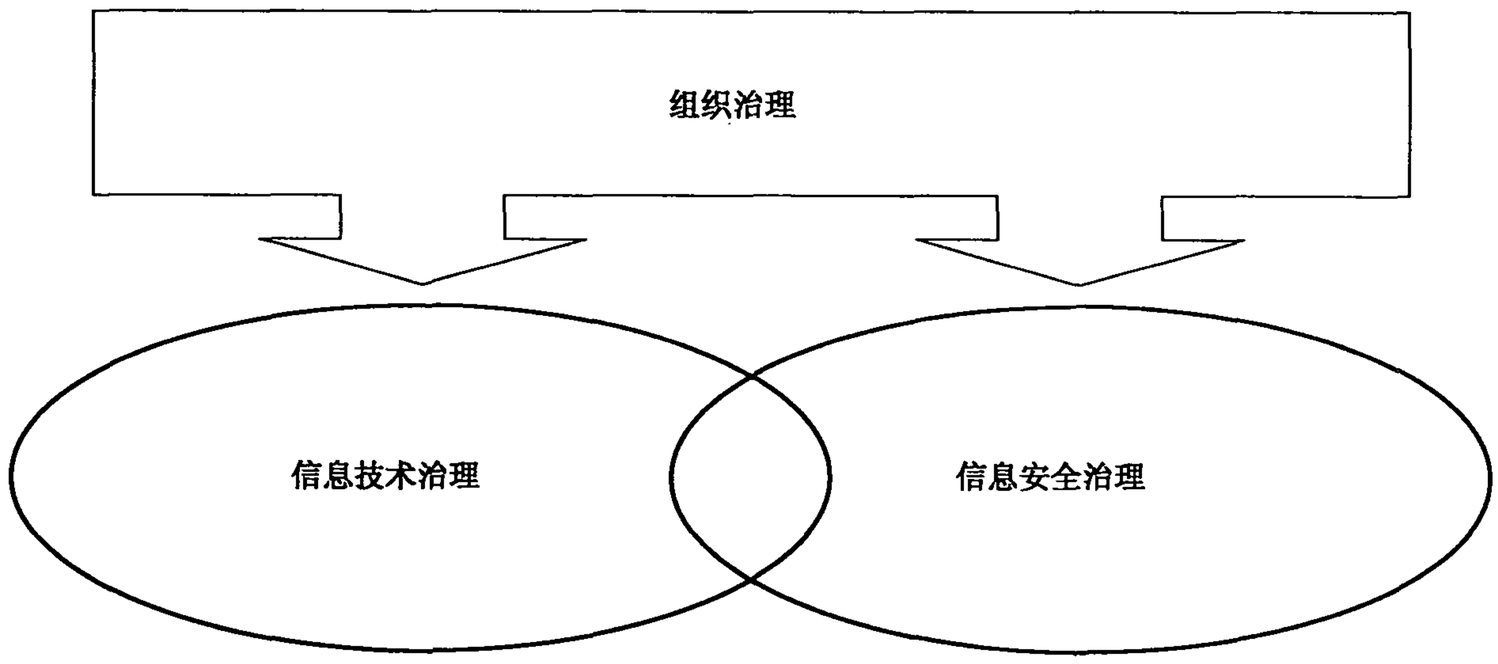

图 1 信息安全治理和信息技术治理之间的关系

信息技术治理的总体范围是针对获取、处理、存储和分发信息的所需资源，而信息安全治理的范围涵盖信息的保密性、完整性和可用性。这两种治理方案都需要由下列治理过程来处理：EDM(评价、指导、监视)。但是信息安全治理需要另外的内部过程“沟通”。

治理者建立信息安全治理所需任务在第5章描述。治理任务还与GB/T 22080以及ISMS族的其他标准(见参考文献)中规定的管理要求相关。

5 原则和过程

5.1 概述

本章描述共同构成信息安全治理的原则和过程。信息安全治理原则是作为治理实现指南的治理行动或行为的公认规则。信息安全治理过程描述推动信息安全治理的一系列任务及其相互关系。它还表示出信息安全治理和管理之间的关系。在随后的条目中解释这两者。

5.2 原则

满足利益相关者的需要，并为他们中的每一位带来价值，从长远来看是信息安全取得成功不可或缺的。为达成使信息安全与业务目标紧密一致的治理目标并为利益相关者带来价值，本条提出 6 项行动原则。

这些原则为信息安全治理过程的实现提供了一个良好基础。每个原则的陈述只提及宜做什么，但不描述如何、何时或由谁实现这些原则，因为这些方面依赖于实现这些原则的组织性质。治理者宜要求应用这些原则，并委派专人且给予责任、问责和权利来落实它们。

原则 1：建立组织范围的信息安全

信息安全治理宜确保信息安全活动是全面的和集成的。宜在组织层面的决策中处理信息安全，其中要考虑到业务、信息安全和所有其他相关方面。宜密切协调涉及物理和逻辑安全的活动。

为建立组织范围的安全，宜横跨组织活动的全部范围建立信息安全的责任制和问责制。这经常超出组织通常被认为的“边界”，例如，被外部方存储或传送的信息。

原则 2：采用基于风险的方法

信息安全治理宜建立在基于风险的决策基础上。决定可接受的安全程度，宜建立在组织对风险承受的基础之上，包括竞争优势的丧失、违规和未尽义务的风险、日常业务中断、声誉受损和经济损失。

就采纳适合组织的信息风险管理，宜与组织的整体风险管理方法一致并集成在其中。信息安全的可接受级别宜基于组织对风险的承受来定义，包括竞争优势的丧失、违规和未尽义务的风险、日常业务中断、声誉受损和经济损失。实现信息风险管理的适当资源宜由治理者来分配。

原则 3：确定投资决策的方向

信息安全治理宜建立基于业务产出的信息安全投资战略，使得业务和信息安全要求之间无论短期还是长期都是相称的，从而满足利益相关者当前和不断变化的需要。

为优化信息安全投资来支持组织目标，治理者宜确保信息安全被集成在资本和运营支出、法律法规符合以及风险报告的现有组织过程中。

原则 4：确保符合内部和外部的要求

信息安全治理宜确保信息安全策略和实践符合相关的强制性法律、法规和规章，以及承诺的业务或合同要求和其他的外部或内部要求。

为解决一致性和合规性问题，治理者宜通过委托独立的安全审核获得对信息安全活动令人满意地达到内部和外部要求的保障。

原则 5：营造安全良好的环境

信息安全治理宜建立在人的行为之上，包括所有利益相关者不断变化的需要，因为人的行为是支撑信息安全适当级别的基本要素之一。如果没有充分的协调，目标、角色、责任和资源可能相互冲突，导致未能达到业务目标。因此，各种利益相关者之间的协调和方向一致非常重要。

为建立良好的信息安全文化，治理者宜要求、促进和支持利益相关者活动的协调，以实现连贯一致的信息安全方向。这将支持开展安全教育、培训和宣传。

原则 6:评审业务产出相关绩效

在约定的信息安全级别下,信息安全治理宜确保保护信息所采用的方法适合支持组织的意图。安全绩效宜被维持在满足当前和未来业务需求所需要的级别上。

为从治理角度评审信息安全绩效,治理者宜评价信息安全在业务影响方面的绩效,而不仅仅是安全控制措施的效率和效果。这可以通过授权执行一个监督、审核和改进的绩效测量程序来做到,从而将信息安全绩效关联到业务绩效。

5.3 过程

5.3.1 概述

治理者执行“评价”“指导”“监督”和“沟通”过程来治理信息安全。另外,“保障”过程提供关于信息安全治理和其所达到级别的独立和客观的意见。图 2 示出了这些过程的关系。

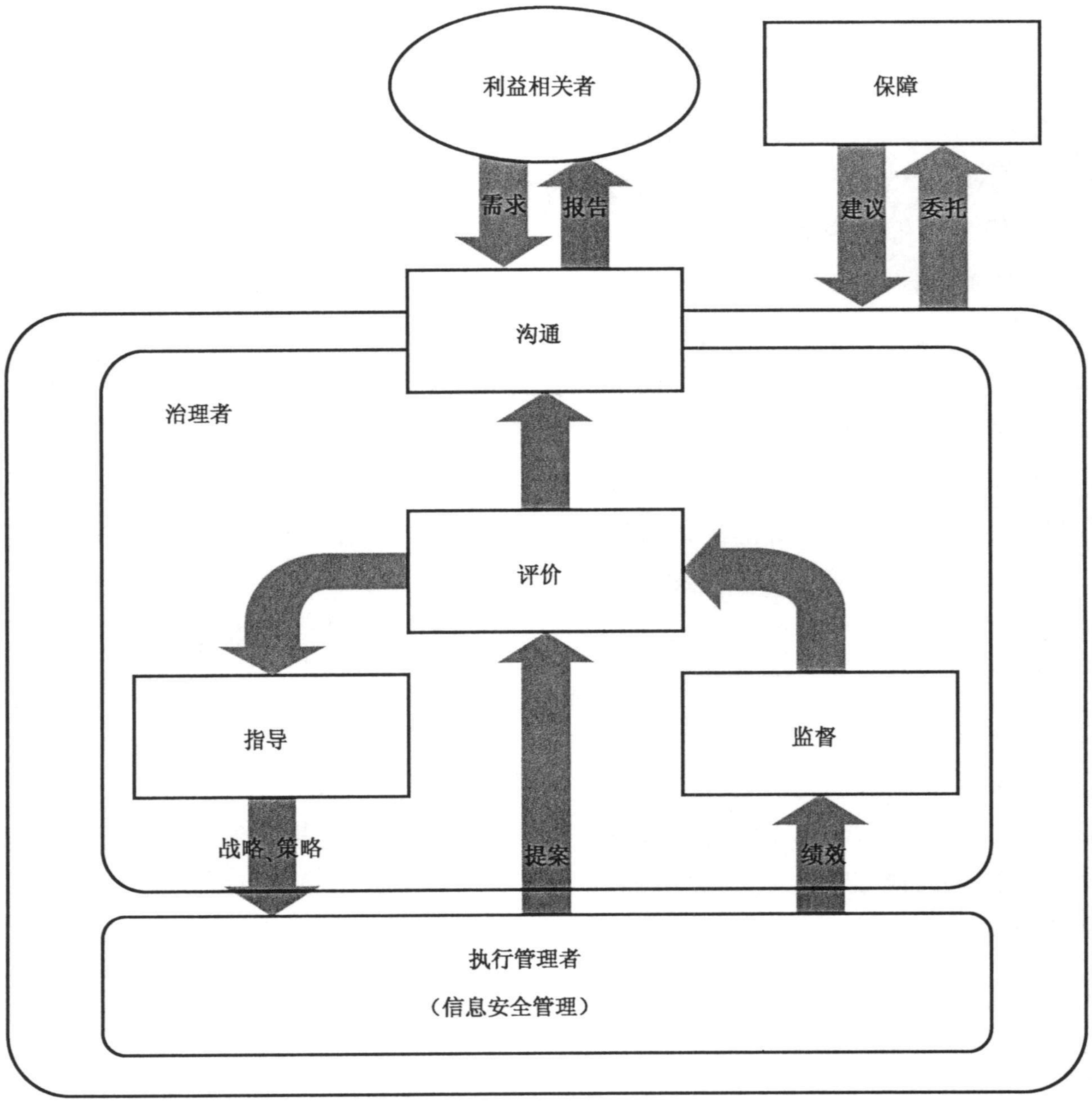

图 2 信息安全治理模型的实现

5.3.2 评价

“评价”这一治理过程是基于当前的过程和计划的变更,考虑到当前和预期要达到的安全目标,确定最能有效达成未来战略目标所需要的任何调整。

为执行“评价”过程,治理者宜:

- 确保业务新计划考虑到了信息安全问题;

- 响应信息安全绩效结果，优化并启动所需要的行动。

为推动“评价”过程，执行管理者宜：

- 确保信息安全充分支持和维持业务目标；
- 向治理者提交有显著影响的新的信息安全项目。

5.3.3 指导

治理者通过“指导”这一治理过程为需要实现的信息安全目标和战略指明方向，可包括资源配置级别的变更、资源的分配、活动的优先级，以及策略、重大风险接受和风险管理计划的批准。

为执行“指导”过程，治理者宜：

- 确定组织对风险的承受；
- 批准信息安全战略和策略；
- 分配足够的投资和资源。

为推动“指导”过程，执行管理者宜：

- 制定和实现信息安全战略和策略；
- 使信息安全目标与业务目标一致；
- 促进良好的信息安全文化。

5.3.4 监督

“监督”这一治理过程使治理者能够评估战略目标的实现。

为执行“监督”过程，治理者宜：

- 评估信息安全管理活动的效果；
- 确保符合内部和外部的要求；
- 考虑不断变化的业务、法律、法规和规章环境及其对信息风险的潜在影响。

为推动“监督”过程，执行管理者宜：

- 从业务角度选择适当的绩效测度；
- 向治理者反馈信息安全绩效结果，包括之前由治理者所确定的行动的绩效及其对组织的影响；
- 向治理者预警影响信息风险和信息安全的新的发展状况。

5.3.5 沟通

治理者和利益相关者通过“沟通”这一双向的治理过程交换适合他们特定需要的关于信息安全的信息。

“沟通”的方法之一是向利益相关者提供解释信息安全活动和问题的信息安全状态，附录 A 和附录 B 给出了例子。

为执行“沟通”过程，治理者宜：

- 向外部利益相关者报告组织在实行与其业务性质相称的信息安全级别；
- 通知执行管理者任何发现信息安全问题并要求采取纠正措施的外部评审结果；
- 识别信息安全相关的监管义务、利益相关者期望和业务需要。

为推动“沟通”过程，执行管理者宜：

- 向治理者建议任何需要其注意，还可能需要决策的事项；
- 在采取支持治理者指示和决定的具体行动上指导有关的利益相关方。

5.3.6 保障

治理者通过“保障”这一治理过程以委托方式开展独立和客观的审核、评审或认证，以此识别和确认

与治理活动开展和操作运行相关的目标和行动，以便获得信息安全的期望水平。

为执行“保障”过程，治理者宜：

- 通过委托获得对其履行信息安全期望水平责任的独立和客观的意见。

为推动“保障”过程，执行管理者宜：

- 支持由治理者委托的审核、评审或认证。

附 录 A
（资料性附录）
信息安全状态示例

组织可以生成一个信息安全状态，并将其作为信息安全的沟通工具披露给利益相关者。

组织宜选择和决定信息安全状态的格式和内容。附录 A 是利用信息安全审核陈述来声明满意的例子（见表 A.1）。

表 A.1 信息安全状态

管理者对信息安全控制措施和规程在 **mmm** 至 **nnn** 期间的足够有效运行是满意的，这些控制措施和规程是基于 **xyz**（例如，ISMS 系列标准、CobiT）中的准则，与高层管理控制措施辅助下的组织运营规程和系统有关，为实现已确定的关系到保密性、完整性和可用性的信息安全控制目标提供了合理保障。管理者已为作为外部信息安全审核员的 **ABC** 提供了这种效果的一份声明书。 **ABC** 由董事会任命来审查管理者对信息安全控制措施的断言。他们的审查依据已建立的标准，包括通过抽样测试评价信息安全控制措施和规程的设计和运行效果。在这方面，**ABC** 向管理者出具他们测试结果表明的意见，即除特定例外，基于 **xyz**（例如，ISMS 系列标准、CobiT）中准则的控制措施在重大方面是有效的。 已经与审核委员会讨论了与信息安全控制措施有关的管理者的完整断言书和带有任何已识别例外的外部审核报告，并提供给了所有董事会成员。副本可应要求提供给利益相关者。

注：“nnn”“mmm”“xyz”“ABC”为占位符。具体日期和名字宜出现在实际陈述中。

附 录 B
（资料性附录）
详细的信息安全状态示例

本附录是披露详细内容的一个信息安全状态例子(见表 B.1)。它对于希望通过强调安全提高声誉的组织尤为有用,例如,ICT 业务。组织对安全风险和适当披露之方法的透明性也有效增加信任。通过这些活动可以在利益相关者中分享共同的意识。

表 B.1 详细的信息安全状态

介绍

- **范围(战略、策略、标准)、边界(地理/组织单元)、覆盖时期(月/季/半年/年)**

整体状态

- **满意/尚未满意/不满意**

更新(适当和相关时)

- **实现信息安全战略的进展**

  完成/处理中/计划的要素
- **信息安全管理体系中的变更**

  ISMS 策略修订、实现 ISMS(包括责任分配)的组织结构
- **认证的进展**

  ISMS(再)认证、得到认证的信息安全审核
- **预算/人员配备/培训**

  财务状况、人员充足性、信息安全资格
- **其他信息安全活动**

  业务持续性管理加入、宣传活动、内部/外部审核协助

显著问题(如果有)

- **信息安全评审结果**

  建议、管理者响应、行动计划、目标日期
- **有关主要内部/外部审核报告的进展**

  建议、管理者响应、行动计划、目标日期
- **信息安全事件**

  估计的影响、行动计划、目标日期
- **(不)符合相关法律和法规**

  估计的影响、行动计划、目标日期

所需决策(如果有)

- **附加资源**

  使信息安全能够支持业务新计划

参 考 文 献

[1] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求

[2] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

[3] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理

[4] ISO/IEC 38500:2008 Corporate Governance of Information technology—A standard for corporate governance of information technology

[5] ITU-T Recommendation X.1051 (2008) | ISO/IEC 27011:2008 Information technology—Security techniques—Information security management guidelines for telecommunications organisations based on ISO/IEC 27002

[6] ITGI, Information Security Governance framework:2009

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

中华人民共和国
国家标准
信息技术　安全技术　信息安全治理
GB/T 32923—2016/ISO/IEC 27014:2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 20 千字
2016年10月第一版　2016年10月第一次印刷
*
书号:155066·1-55031　定价　18.00 元

GB/T 32923-2016