ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22080—2008/ISO/IEC 27001:2005

信息技术　安全技术
信息安全管理体系　要求

Information technology—Security techniques—
Information security management systems—Requirements

(ISO/IEC 27001:2005, IDT)

2008-06-19 发布　　2008-11-01 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

本标准等同采用 ISO/IEC 27001:2005《信息技术　安全技术　信息安全管理体系　要求》，仅有编辑性修改。

本标准的附录 A 是规范性附录，附录 B 和附录 C 是资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会归口。

本标准由中国电子技术标准化研究所、上海三零卫士有限公司、北京知识安全工程中心、北京市信息安全测评中心、北京数字认证中心负责起草。

本标准主要起草人：上官晓丽、许玉娜、胡啸、王新杰、赵战生、王连强、曾波、孔一童、刘海峰、汤永利、尚小鹏、闵京华。

引　言

0.1　总则

本标准用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系(Information Security Management System,简称 ISMS)提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组织 ISMS 的设计和实施受其需要和目标、安全要求、所采用的过程以及组织的规模和结构的影响,上述因素及其支持系统会不断发生变化。按照组织的需要实施 ISMS 是本标准所期望的,例如,简单的情况可采用简单的 ISMS 解决方案。

本标准可被内部和外部相关方用于一致性评估。

0.2　过程方法

本标准采用过程方法来建立、实施、运行、监视、评审、保持和改进组织的 ISMS。

为使组织有效运作,需要识别和管理众多相互关联的活动。通过使用资源和管理,将输入转化为输出的活动可视为过程。通常,一个过程的输出直接形成下一个过程的输入。

组织内诸过程的系统的应用,连同这些过程的识别和相互作用及其管理,可称之为“过程方法”。

本标准中提出的用于信息安全管理的过程方法鼓励其用户强调以下方面的重要性:

a)　理解组织的信息安全要求和建立信息安全方针与目标的需要;

b)　从组织整体业务风险的角度,实施和运行控制措施,以管理组织的信息安全风险;

c)　监视和评审 ISMS 的执行情况和有效性;

d)　基于客观测量的持续改进。

本标准采用了“规划(Plan)—实施(Do)—检查(Check)—处置(Act)”(PDCA)模型,该模型可应用于所有的 ISMS 过程。图 1 说明了 ISMS 如何把相关方的信息安全要求和期望作为输入,并通过必要的行动和过程,产生满足这些要求和期望的信息安全结果。图 1 也描述了第 4 章、第 5 章、第 6 章、第 7 章和第 8 章所提出的过程间的联系。

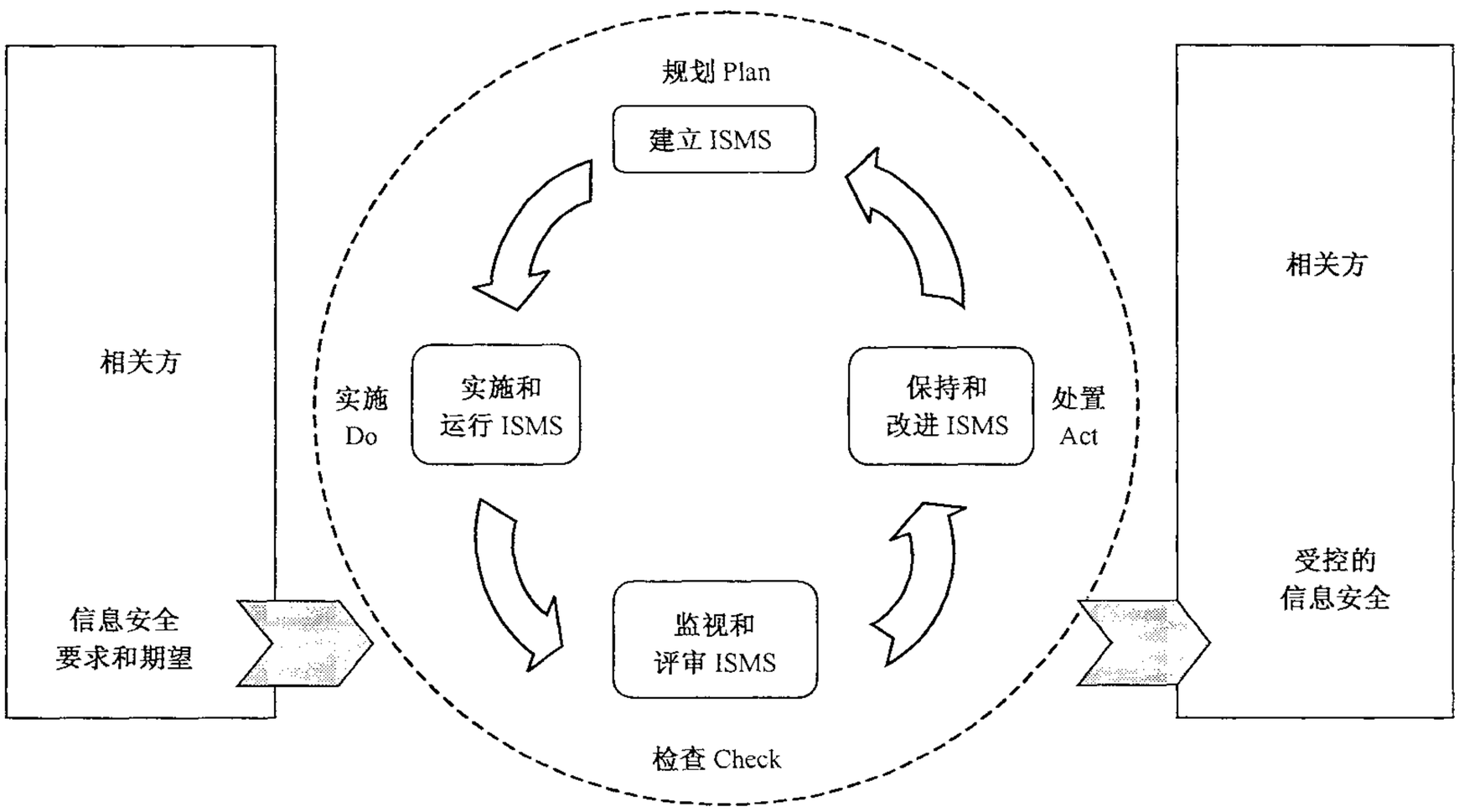

图 1　应用于 ISMS 过程的 PDCA 模型

采用 PDCA 模型还反映了治理信息系统和网络安全的 OECD 指南(2002 版)[1)] 中所设置的原则。本标准为实施 OECD 指南中规定的风险评估、安全设计和实施、安全管理和再评估的原则提供了一个强健的模型。

例 1:某些信息安全违规不至于给组织造成严重的财务损失和/或使组织陷入困境。这可能是一种要求。

例 2:如果发生了严重的事件(可能是组织的电子商务网站被黑客入侵)应有经充分培训的员工按照适当的规程,将事件的影响降至最小。这可能是一种期望。

规划(建立 ISMS)	建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和规程,以提供与组织总方针和总目标相一致的结果。
实施(实施和运行 ISMS)	实施和运行 ISMS 方针、控制措施、过程和规程。
检查(监视和评审 ISMS)	对照 ISMS 方针、目标和实践经验,评估并在适当时测量过程的执行情况,并将结果报告管理者以供评审。
处置(保持和改进 ISMS)	基于 ISMS 内部审核和管理评审的结果或者其他相关信息,采取纠正和预防措施,以持续改进 ISMS。

0.3 与其他管理体系的兼容性

本标准与 GB/T 19001—2000 及 GB/T 24001—2004 相结合,以支持与相关管理标准一致的、整合的实施和运行。因此,一个设计恰当的管理体系可以满足所有这些标准的要求。表 C.1 说明了本标准、GB/T 19001—2000 和 GB/T 24001—2004 的各条款之间的关系。

本标准的设计能够使一个组织将其 ISMS 与其他相关的管理体系要求结合或整合起来。

1) OECD 信息系统和网络安全指南——面向安全文化。巴黎:OECD,2002 年 7 月。www.oecd.org

信息技术　安全技术
信息安全管理体系　要求

重要提示:本出版物不声称包括一个合同所有必要的条款。用户负责对其进行正确的应用。符合标准本身并不获得法律责任的豁免。

1　范围

1.1　总则

本标准适用于所有类型的组织(例如,商业企业、政府机构、非赢利组织)。本标准从组织的整体业务风险的角度,为建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系(ISMS)规定了要求。它规定了为适应不同组织或其部门的需要而定制的安全控制措施的实施要求。

ISMS 的设计应确保选择适当和相宜的安全控制措施,以充分保护信息资产并给予相关方信心。

注 1:本标准中的"业务"一词应广义的解释为关系一个组织生存的核心活动。

注 2:GB/T 22081—2008 提供了设计控制措施时可使用的实施指南。

1.2　应用

本标准规定的要求是通用的,适用于各种类型、规模和特性的组织。组织声称符合本标准时,对于第 4 章、第 5 章、第 6 章、第 7 章和第 8 章的要求不能删减。

为了满足风险接受准则必要的进行的任何控制措施的删减,必须证明是合理的,且需要提供证据证明相关风险已被负责人员接受。除非删减不影响组织满足由风险评估和适用法律法规要求所确定的安全要求的能力和/或责任,否则不能声称符合本标准。

注:如果一个组织已经有一个运转着的业务过程管理体系(例如,与 GB/T 19001—2000 或者 GB/T 24001—2004 相关的),那么在大多数情况下,更可取的是在这个现有的管理体系内满足本标准的要求。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则(ISO/IEC 27002:2005,IDT)

3　术语和定义

下列术语和定义适用于本标准。

3.1

资产　asset

对组织有价值的任何东西。

[ISO/IEC 13335-1:2004]

3.2

可用性　availability

根据授权实体的要求可访问和利用的特性。

[ISO/IEC 13335-1:2004]

3.3

保密性　confidentiality

信息不能被未授权的个人、实体或者过程利用或知悉的特性。

[ISO/IEC 13335-1:2004]

3.4

信息安全 information security

保持信息的保密性、完整性、可用性；另外也可包括例如真实性、可核查性、不可否认性和可靠性等。

[GB/T 22081—2008]

3.5

信息安全事态 information security event

信息安全事态是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。

[GB/Z 20985—2007]

3.6

信息安全事件 information security incident

一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，它们具有损害业务运作和威胁信息安全的极大的可能性。

[GB/Z 20985—2007]

3.7

信息安全管理体系(ISMS) information security management system (ISMS)

基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织整个管理体系的一部分。

注：管理体系包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源。

3.8

完整性 integrity

保护资产的准确和完整的特性。

[ISO/IEC 13335-1:2004]

3.9

残余风险 residual risk

经过风险处置后遗留的风险。

[ISO/IEC Guide 73:2002]

3.10

风险接受 risk acceptance

接受风险的决定。

[ISO/IEC Guide 73:2002]

3.11

风险分析 risk analysis

系统地使用信息来识别风险来源和估计风险。

[ISO/IEC Guide 73:2002]

3.12

风险评估 risk assessment

风险分析和风险评价的整个过程。

[ISO/IEC Guide 73:2002]

3.13

风险评价 risk evaluation

将估计的风险与给定的风险准则加以比较以确定风险严重性的过程。

[ISO/IEC Guide 73:2002]

3.14

风险管理　risk management

指导和控制一个组织相关风险的协调活动。

[ISO/IEC Guide 73:2002]

3.15

风险处置　risk treatment

选择并且执行措施来更改风险的过程。

[ISO/IEC Guide 73:2002]

注：在本标准中，术语“控制措施”被用作“措施”的同义词。

3.16

适用性声明　statement of applicability

描述与组织的信息安全管理体系相关的和适用的控制目标和控制措施的文件。

注：控制目标和控制措施是基于风险评估和风险处置过程的结果和结论、法律法规的要求、合同义务以及组织对于信息安全的业务要求。

4　信息安全管理体系(ISMS)

4.1　总要求

组织应在其整体业务活动中且在所面临风险的环境下建立、实施、运行、监视、评审、保持和改进文件化的 ISMS。在本标准中，所使用的过程基于图 1 所示的 PDCA 模型。

4.2　建立和管理 ISMS

4.2.1　建立 ISMS

组织应做以下方面的工作：

a)　根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的范围和边界，包括对范围任何删减的详细说明和正当性理由(见 1.2)。

b)　根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 方针。ISMS 方针应：

1)　包括设定目标的框架和建立信息安全工作的总方向和原则；

2)　考虑业务和法律法规的要求，及合同中的安全义务；

3)　在组织的战略性风险管理环境下，建立和保持 ISMS；

4)　建立风险评价的准则(见 4.2.1 c)；

5)　获得管理者批准。

注：就本标准的目的而言，ISMS 方针被认为是信息安全方针的一个扩展集。这些方针可以在一个文件中进行描述。

c)　确定组织的风险评估方法：

1)　识别适合 ISMS、已识别的业务信息安全和法律法规要求的风险评估方法；

2)　制定接受风险的准则，识别可接受的风险级别(见 5.1f))。

选择的风险评估方法应确保风险评估产生可比较的和可再现的结果。

注：风险评估具有不同的方法。在 ISO/IEC TR 13335-3 中描述了风险评估方法的例子。

d)　识别风险：

1)　识别 ISMS 范围内的资产及其责任人[1)]；

2)　识别资产所面临的威胁；

3)　识别可能被威胁利用的脆弱性；

---

1)　术语“责任人”标识了已经获得管理者的批准，负责产生、开发、维护、使用和保证资产的安全的个人或实体。术语“责任人”不是指该人员实际上对资产拥有所有权。

4） 识别丧失保密性、完整性和可用性可能对资产造成的影响。

e） 分析和评价风险：

1） 在考虑丧失资产的保密性、完整性和可用性所造成的后果的情况下，评估安全失效可能造成的对组织的影响；

2） 根据主要的威胁和脆弱性、对资产的影响以及当前所实施的控制措施，评估安全失效发生的现实可能性；

3） 估计风险的级别；

4） 确定风险是否可接受，或者是否需要使用在4.2.1c)2)中所建立的接受风险的准则进行处理。

f） 识别和评价风险处置的可选措施，可能的措施包括：

1） 采用适当的控制措施；

2） 在明显满足组织方针策略和接受风险的准则的条件下，有意识地、客观地接受风险（见4.2.1c)2)）；

3） 避免风险；

4） 将相关业务风险转移到其他方，如：保险，供应商等。

g） 为处理风险选择控制目标和控制措施。

控制目标和控制措施应加以选择和实施，以满足风险评估和风险处置过程中所识别的要求。这种选择应考虑接受风险的准则（见4.2.1c)2)）以及法律法规和合同要求。

从附录A中选择控制目标和控制措施应成为此过程的一部分，该过程适合于满足这些已识别的要求。

附录A所列的控制目标和控制措施并不是所有的控制目标和控制措施，组织也可能需要选择另外的控制目标和控制措施。

注：附录A包含了组织内一般要用到的全面的控制目标和控制措施的列表。本标准用户可将附录A作为选择控制措施的出发点，以确保不会遗漏重要的可选控制措施。

h） 获得管理者对建议的残余风险的批准。

i） 获得管理者对实施和运行ISMS的授权。

j） 准备适用性声明（Statement of Applicability，简称SoA）应从以下几方面准备适用性声明：

1） 4.2.1g)中所选择的控制目标和控制措施，以及选择的理由；

2） 当前实施的控制目标和控制措施（见4.2.1e)2)）；

3） 对附录A中任何控制目标和控制措施的删减，以及删减的合理性说明。

注：适用性声明提供了一份关于风险处置决定的综述。删减的合理性说明提供交叉检查，以证明不会因疏忽而遗漏控制措施。

4.2.2 实施和运行ISMS

组织应：

a） 为管理信息安全风险识别适当的管理措施、资源、职责和优先顺序，即：制定风险处置计划（见第5章）；

b） 实施风险处置计划以达到已识别的控制目标，包括资金安排、角色和职责的分配；

c） 实施4.2.1g)中所选择的控制措施，以满足控制目标；

d） 确定如何测量所选择的控制措施或控制措施集的有效性，并指明如何用这些测量措施来评估控制措施的有效性，以产生可比较的和可再现的结果（见4.2.3c)）；

注：测量控制措施的有效性可使管理者和员工确定控制措施达到既定的控制目标的程度。

e） 实施培训和意识教育计划（见5.2.2）；

f） 管理ISMS的运行；

g) 管理 ISMS 的资源(见 5.2);

h) 实施能够迅速检测安全事态和响应安全事件的规程和其他控制措施(见 4.2.3a))。

4.2.3 监视和评审 ISMS

组织应:

a) 执行监视与评审规程和其他控制措施,以:

1) 迅速检测过程运行结果中的错误;

2) 迅速识别试图的和得逞的安全违规和事件;

3) 使管理者能够确定分配给人员的安全活动或通过信息技术实施的安全活动是否按期望执行;

4) 通过使用指示器,帮助检测安全事态并预防安全事件;

5) 确定解决安全违规的措施是否有效。

b) 在考虑安全审核结果、事件、有效性测量结果、所有相关方的建议和反馈的基础上,进行 ISMS 有效性的定期评审(包括满足 ISMS 方针和目标,以及安全控制措施的评审)。

c) 测量控制措施的有效性以验证安全要求是否被满足。

d) 按照计划的时间间隔进行风险评估的评审,以及对残余风险和已确定的可接受的风险级别进行评审,应考虑以下方面的变化:

1) 组织;

2) 技术;

3) 业务目标和过程;

4) 已识别的威胁;

5) 已实施的控制措施的有效性;

6) 外部事态,如法律法规环境的变更、合同义务的变更和社会环境的变更。

e) 按计划的时间间隔,实施 ISMS 内部审核(见第 6 章)。

注:内部审核,有时称为第一方审核,是用于内部目的,由组织自己或以组织的名义所进行的审核。

f) 定期进行 ISMS 管理评审,以确保 ISMS 范围保持充分,ISMS 过程的改进得到识别(见 7.1)。

g) 考虑监视和评审活动的结果,以更新安全计划。

h) 记录可能影响 ISMS 的有效性或执行情况的措施和事态(见 4.3.3)。

4.2.4 保持和改进 ISMS

组织应经常:

a) 实施已识别的 ISMS 改进。

b) 依照 8.2 和 8.3 采取合适的纠正和预防措施。从其他组织和组织自身的安全经验中吸取教训。

c) 向所有相关方沟通措施和改进情况,其详细程度应与环境相适应,需要时,商定如何进行。

d) 确保改进达到了预期目标。

4.3 文件要求

4.3.1 总则

文件应包括管理决定的记录,以确保所采取的措施符合管理决定和方针策略,还应确保所记录的结果是可重复产生的。

重要的是,能够显示出所选择的控制措施回溯到风险评估和风险处置过程的结果,并进而回溯到 ISMS 方针和目标之间的关系。

ISMS 文件应包括:

a) 形成文件的 ISMS 方针(见 4.2.1b))和目标;

b) ISMS 的范围(见 4.2.1a));

c) 支持 ISMS 的规程和控制措施；
d) 风险评估方法的描述(见 4.2.1c))；
e) 风险评估报告 (见 4.2.1c)到 4.2.1g))；
f) 风险处置计划(见 4.2.2b))；
g) 组织为确保其信息安全过程的有效规划、运行和控制以及描述如何测量控制措施的有效性所需的形成文件的规程(见 4.2.3c))；
h) 本标准所要求的记录(见 4.3.3)；
i) 适用性声明。

注 1：本标准出现“形成文件的规程”之处，即要求建立该规程，形成文件，并加以实施和保持。

注 2：不同组织的 ISMS 文件的详略程度取决于：

——组织的规模和活动的类型；

——安全要求和被管理系统的范围及复杂程度。

注 3：文件和记录可以采用任何形式或类型的介质。

4.3.2 文件控制

ISMS 所要求的文件应予以保护和控制。应编制形成文件的规程，以规定以下方面所需的管理措施：

a) 文件发布前得到批准，以确保文件是适当的；
b) 必要时对文件进行评审、更新并再次批准；
c) 确保文件的更改和现行修订状态得到标识；
d) 确保在使用处可获得适用文件的相关版本；
e) 确保文件保持清晰、易于识别；
f) 确保文件对需要的人员可用，并依照文件适用的类别规程进行传输、贮存和最终销毁；
g) 确保外来文件得到识别；
h) 确保文件的分发得到控制；
i) 防止作废文件的非预期使用；
j) 若因任何目的而保留作废文件时，对这些文件进行适当的标识。

4.3.3 记录控制

应建立记录并加以保持，以提供符合 ISMS 要求和有效运行的证据。应对记录加以保护和控制。ISMS 的记录应考虑相关法律法规要求和合同义务。记录应保持清晰、易于识别和检索。记录的标识、贮存、保护、检索、保存期限和处置所需的控制措施应形成文件并实施。

应保留 4.2 中列出的过程执行记录和所有发生的与 ISMS 有关的重大安全事件的记录。

例如：记录包括访客登记簿、审核报告和已完成的访问授权单。

5 管理职责

5.1 管理承诺

管理者应通过以下活动，对建立、实施、运行、监视、评审、保持和改进 ISMS 的承诺提供证据：

a) 制定 ISMS 方针；
b) 确保 ISMS 目标和计划得以制定；
c) 建立信息安全的角色和职责；
d) 向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性；
e) 提供足够资源，以建立、实施、运行、监视、评审、保持和改进 ISMS (见 5.2.1)；
f) 决定接受风险的准则和风险的可接受级别；
g) 确保 ISMS 内部审核的执行(见第 6 章)；
h) 实施 ISMS 的管理评审(见第 7 章)。

5.2 资源管理

5.2.1 资源提供

组织应确定并提供所需的资源，以：

a) 建立、实施、运行、监视、评审、保持和改进 ISMS；

b) 确保信息安全规程支持业务要求；

c) 识别和满足法律法规要求、以及合同中的安全义务；

d) 通过正确实施所有的控制措施保持适当的安全；

e) 必要时，进行评审，并适当响应评审的结果；

f) 在需要时，改进 ISMS 的有效性。

5.2.2 培训、意识和能力

组织应通过以下方式，确保所有被赋予 ISMS 职责的人员具有执行所要求任务的能力：

a) 确定从事影响 ISMS 工作的人员所必要的能力；

b) 提供培训或采取其他措施（如聘用有能力的人员）以满足这些需求；

c) 评价所采取的措施的有效性；

d) 保持教育、培训、技能、经历和资格的记录（见 4.3.3）。

组织也应确保所有相关人员意识到他们信息安全活动的相关性和重要性，以及如何为达到 ISMS 目标做出贡献。

6 ISMS 内部审核

组织应按照计划的时间间隔进行 ISMS 内部审核，以确定其 ISMS 的控制目标、控制措施、过程和规程是否：

a) 符合本标准和相关法律法规的要求；

b) 符合已确定的信息安全要求；

c) 得到有效地实施和保持；

d) 按预期执行。

应在考虑拟审核的过程与区域的状况和重要性以及以往审核的结果的情况下，制定审核方案。应确定审核的准则、范围、频次和方法。审核员的选择和审核的实施应确保审核过程的客观性和公正性。审核员不应审核自己的工作。

策划和实施审核、报告结果和保持记录（见 4.3.3）的职责和要求应在形成文件的规程中做出规定。

负责受审区域的管理者应确保及时采取措施，以消除已发现的不符合及其产生的原因。跟踪活动应包括对所采取措施的验证和验证结果的报告（见第 8 章）。

注：GB/T 19011—2003 也可为实施 ISMS 内部审核提供有用的指导。

7 ISMS 的管理评审

7.1 总则

管理者应按计划的时间间隔（至少每年 1 次）评审组织的 ISMS，以确保其持续的适宜性、充分性和有效性。评审应包括评估 ISMS 改进的机会和变更的需要，包括信息安全方针和信息安全目标。评审的结果应清晰地形成文件，记录应加以保持（见 4.3.3）。

7.2 评审输入

管理评审的输入应包括：

a) ISMS 审核和评审的结果；

b) 相关方的反馈；

c) 组织用于改进 ISMS 执行情况和有效性的技术、产品或规程；

d) 预防和纠正措施的状况；

e) 以往风险评估没有充分强调的脆弱点或威胁；
f) 有效性测量的结果；
g) 以往管理评审的跟踪措施；
h) 可能影响 ISMS 的任何变更；
i) 改进的建议。

7.3 评审输出

管理评审的输出应包括与以下方面有关的任何决定和措施：
a) ISMS 有效性的改进。
b) 风险评估和风险处置计划的更新。
c) 必要时修改影响信息安全的规程和控制措施，以响应内部或外部可能影响 ISMS 的事态，包括以下的变更：
1) 业务要求；
2) 安全要求；
3) 影响现有业务要求的业务过程；
4) 法律法规要求；
5) 合同义务；
6) 风险级别和/或接受风险的准则。
d) 资源需求。
e) 控制措施有效性测量方法的改进。

8 ISMS 改进

8.1 持续改进

组织应利用信息安全方针、安全目标、审核结果、监视事态的分析、纠正和预防措施以及管理评审(见第 7 章)，持续改进 ISMS 的有效性。

8.2 纠正措施

组织应采取措施，以消除与 ISMS 要求不符合的原因，以防止再发生。形成文件的纠正措施规程，应规定以下方面的要求：
a) 识别不符合；
b) 确定不符合的原因；
c) 评价确保不符合不再发生的措施需求；
d) 确定和实施所需要的纠正措施；
e) 记录所采取措施的结果(见 4.3.3)；
f) 评审所采取的纠正措施。

8.3 预防措施

组织应确定措施，以消除潜在不符合的原因，防止其发生。预防措施应与潜在问题的影响程度相适应。形成文件的预防措施规程，应规定以下方面的要求：
a) 识别潜在的不符合及其原因；
b) 评价防止不符合发生的措施需求；
c) 确定和实施所需要的预防措施；
d) 记录所采取措施的结果(见 4.3.3)；
e) 评审所采取的预防措施。

组织应识别变化的风险，并识别针对重大变化的风险的预防措施的要求。

预防措施的优先级应根据风险评估的结果确定。

注：预防不符合的措施通常比纠正措施更节约成本。

附 录 A
（规范性附录）
控制目标和控制措施

表 A.1 所列的控制目标和控制措施是直接源自并与 GB/T 22081—2008(ISO/IEC 27002:2005)第 5 章到第 15 章一致。表 A.1 中的清单并不详尽，一个组织可能考虑另外必要的控制目标和控制措施。在这些表中选择控制目标和控制措施是条款 4.2.1 规定的 ISMS 过程的一部分。

GB/T 22081—2008(ISO/IEC 27002:2005)第 5 章至第 15 章提供了最佳实践的实施建议和指南，以支持 A.5 到 A.15 列出的控制措施。

表 A.1 控制目标和控制措施

A.5 安全方针		
A.5.1 信息安全方针 *目标*：依据业务要求和相关法律法规提供管理指导并支持信息安全。		
A.5.1.1	信息安全方针文件	*控制措施* 信息安全方针文件应由管理者批准、发布并传达给所有员工和外部相关方。
A.5.1.2	信息安全方针的评审	*控制措施* 宜按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保它持续的适宜性、充分性和有效性。
A.6 信息安全组织		
A.6.1 内部组织 *目标*：管理组织范围内信息安全。		
A.6.1.1	信息安全的管理承诺	*控制措施* 管理者应通过清晰的说明、可证实的承诺、明确的信息安全职责分配及确认，来积极支持组织内的安全。
A.6.1.2	信息安全协调	*控制措施* 信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调。
A.6.1.3	信息安全职责的分配	*控制措施* 所有的信息安全职责应予以清晰地定义。
A.6.1.4	信息处理设施的授权过程	*控制措施* 应为新的信息处理设施定义和实施一个管理授权过程。
A.6.1.5	保密性协议	*控制措施* 应识别并定期评审反映组织信息保护需要的保密性或不泄露协议的要求。
A.6.1.6	与政府部门的联系	*控制措施* 应保持与政府相关部门的适当联系。
A.6.1.7	与特定利益集团的联系	*控制措施* 应保持与特定利益集团、其他安全专家组和专业协会的适当联系。
A.6.1.8	信息安全的独立评审	*控制措施* 组织管理信息安全的方法及其实施(例如信息安全的控制目标、控制措施、策略、过程和规程)应按计划的时间间隔进行独立评审，当安全实施发生重大变化时，也要进行独立评审。
A.6.2 外部各方 *目标*：保持组织的被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全。		

表 A.1（续）

A.6.2.1	与外部各方相关风险的识别	*控制措施* 应识别涉及外部各方业务过程中组织的信息和信息处理设施的风险，并在允许访问前实施适当的控制措施。
A.6.2.2	处理与顾客有关的安全问题	*控制措施* 应在允许顾客访问组织信息或资产之前处理所有确定的安全要求。
A.6.2.3	处理第三方协议中的安全问题	*控制措施* 涉及访问、处理或管理组织的信息或信息处理设施以及与之通信的第三方协议，或在信息处理设施中增加产品或服务的第三方协议，应涵盖所有相关的安全要求。
A.7 资产管理		
A.7.1 对资产负责 *目标*：实现和保持对组织资产的适当保护。		
A.7.1.1	资产清单	*控制措施* 应清晰的识别所有资产，编制并维护所有重要资产的清单。
A.7.1.2	资产责任人[1)]	*控制措施* 与信息处理设施有关的所有信息和资产应由组织的指定部门或人员承担责任。
A.7.1.3	资产的可接受使用	*控制措施* 与信息处理设施有关的信息和资产可接受使用规则应被确定、形成文件并加以实施。
A.7.2 信息分类 *目标*：确保信息受到适当级别的保护。		
A.7.2.1	分类指南	*控制措施* 信息应按照它对组织的价值、法律要求、敏感性和关键性予以分类。
A.7.2.2	信息的标记和处理	*控制措施* 应按照组织所采纳的分类机制建立和实施一组合适的信息标记和处理规程。
A.8 人力资源安全		
A.8.1 任用[2)]之前 *目标*：确保雇员、承包方人员和第三方人员理解其职责、考虑对其承担的角色是适合的，以降低设施被窃、欺诈和误用的风险。		
A.8.1.1	角色和职责	*控制措施* 雇员、承包方人员和第三方人员的安全角色和职责应按照组织的信息安全方针定义并形成文件。
A.8.1.2	审查	*控制措施* 关于所有任用的候选者、承包方人员和第三方人员的背景验证核查应按照相关法律法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。
A.8.1.3	任用条款和条件	*控制措施* 作为他们合同义务的一部分，雇员、承包方人员和第三方人员应同意并签署他们的任用合同的条款和条件，这些条款和条件应声明他们和组织的信息安全职责。

1) 解释：术语“责任人”是被认可，具有控制生产、开发、保持、使用和资产安全的个人或实体。术语“责任人”不指实际上对资产具有财产权的人。

2) 解释：这里的“任用”意指以下不同的情形：人员任用（暂时的或长期的）、工作角色的指定、工作角色的变化、合同的分配及所有这些安排的终止。

表 A.1（续）

A.8.2 任用中 *目标*：确保所有的雇员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务、并准备好在其正常工作过程中支持组织的安全方针，以减少人为出错的风险。		
A.8.2.1	管理职责	*控制措施* 管理者应要求雇员、承包方人员和第三方人员按照组织已建立的方针策略和规程对安全尽心尽力。
A.8.2.2	信息安全意识、教育和培训	*控制措施* 组织的所有雇员，适当时，包括承包方人员和第三方人员，应受到与其工作职能相关的适当的意识培训和组织方针策略及规程的定期更新培训。
A.8.2.3	纪律处理过程	*控制措施* 对于安全违规的雇员，应有一个正式的纪律处理过程。
A.8.3 任用的终止或变化 *目标*：确保雇员、承包方人员和第三方人员以一个规范的方式退出一个组织或改变其任用关系。		
A.8.3.1	终止职责	*控制措施* 任用终止或任用变更的职责应清晰地定义和分配。
A.8.3.2	资产的归还	*控制措施* 所有的雇员、承包方人员和第三方人员在终止任用、合同或协议时，应归还他们使用的所有组织资产。
A.8.3.3	撤销访问权	*控制措施* 所有雇员、承包方人员和第三方人员对信息和信息处理设施的访问权应在任用、合同或协议终止时删除，或在变化时调整。
A.9 物理和环境安全		
A.9.1 安全区域 *目标*：防止对组织场所和信息的未授权物理访问、损坏和干扰。		
A.9.1.1	物理安全周边	*控制措施* 应使用安全周边（诸如墙、卡控制的入口或有人管理的接待台等屏障）来保护包含信息和信息处理设施的区域。
A.9.1.2	物理入口控制	*控制措施* 安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。
A.9.1.3	办公室、房间和设施的安全保护	*控制措施* 应为办公室、房间和设施设计并采取物理安全措施。
A.9.1.4	外部和环境威胁的安全防护	*控制措施* 为防止火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为灾难引起的破坏，应设计和采取物理保护措施。
A.9.1.5	在安全区域工作	*控制措施* 应设计和应用用于安全区域工作的物理保护和指南。
A.9.1.6	公共访问、交接区安全	*控制措施* 访问点（例如交接区）和未授权人员可进入办公场所的其他点应加以控制，如果可能，应与信息处理设施隔离，以避免未授权访问。
A.9.2 设备安全 *目标*：防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。		
A.9.2.1	设备安置和保护	*控制措施* 应安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。

表 A.1（续）

A.9.2.2	支持性设施	*控制措施* 应保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。
A.9.2.3	布缆安全	*控制措施* 应保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏。
A.9.2.4	设备维护	*控制措施* 设备应予以正确地维护，以确保其持续的可用性和完整性。
A.9.2.5	组织场所外的设备安全	*控制措施* 应对组织场所的设备采取安全措施，要考虑工作在组织场所以外的不同风险。
A.9.2.6	设备的安全处置或再利用	*控制措施* 包含储存介质的设备的所有项目应进行核查，以确保在处置之前，任何敏感信息和注册软件已被删除或安全地写覆盖。
A.9.2.7	资产的移动	*控制措施* 设备、信息或软件在授权之前不应带出组织场所。
A.10 通信和操作管理		
A.10.1 操作规程和职责 *目标*：确保正确、安全的操作信息处理设施。		
A.10.1.1	文件化的操作规程	*控制措施* 操作规程应形成文件、保持并对所有需要的用户可用。
A.10.1.2	变更管理	*控制措施* 对信息处理设施和系统的变更应加以控制。
A.10.1.3	责任分割	*控制措施* 各类责任及职责范围应加以分割，以降低未授权或无意识的修改或者不当使用组织资产的机会。
A.10.1.4	开发、测试和运行设施分离	*控制措施* 开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。
A.10.2 第三方服务交付管理 *目标*：实施和保持符合第三方服务交付协议的信息安全和服务交付的适当水准。		
A.10.2.1	服务交付	*控制措施* 应确保第三方实施、运行和保持包含在第三方服务交付协议中的安全控制措施、服务定义和交付水准。
A.10.2.2	第三方服务的监视和评审	*控制措施* 应定期监视和评审由第三方提供的服务、报告和记录，审核也应定期执行。
A.10.2.3	第三方服务的变更管理	*控制措施* 应管理服务提供的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务系统和涉及过程的关键程度及风险的再评估。
A.10.3 系统规划和验收 *目标*：将系统失效的风险降至最小。		
A.10.3.1	容量管理	*控制措施* 资源的使用应加以监视、调整，并作出对于未来容量要求的预测，以确保拥有所需的系统性能。
A.10.3.2	系统验收	*控制措施* 应建立对新信息系统、升级及新版本的验收准则，并且在开发中和验收前对系统进行适当的测试。

表 A.1（续）

A.10.4 防范恶意和移动代码 *目标*：保护软件和信息的完整性。		
A.10.4.1	控制恶意代码	*控制措施* 应实施恶意代码的检测、预防和恢复的控制措施，以及适当的提高用户安全意识的规程。
A.10.4.2	控制移动代码	*控制措施* 当授权使用移动代码时，其配置应确保授权的移动代码按照清晰定义的安全策略运行，应阻止执行未授权的移动代码。
A.10.5 备份 *目标*：保持信息和信息处理设施的完整性及可用性。		
A.10.5.1	信息备份	*控制措施* 应按照已设的备份策略，定期备份和测试信息和软件。
A.10.6 网络安全管理 *目标*：确保网络中信息的安全性并保护支持性的基础设施。		
A.10.6.1	网络控制	*控制措施* 应充分管理和控制网络，以防止威胁的发生，维护使用网络的系统和应用程序的安全，包括传输中的信息。
A.10.6.2	网络服务安全	*控制措施* 安全特性、服务级别以及所有网络服务的管理要求应予以确定并包括在所有网络服务协议中，无论这些服务是由内部提供的还是外包的。
A.10.7 介质处置 *目标*：防止资产遭受未授权泄露、修改、移动或销毁以及业务活动的中断。		
A.10.7.1	可移动介质的管理	*控制措施* 应有适当的可移动介质的管理规程。
A.10.7.2	介质的处置	*控制措施* 不再需要的介质，应使用正式的规程可靠并安全地处置。
A.10.7.3	信息处理规程	*控制措施* 应建立信息的处理及存储规程，以防止信息的未授权的泄漏或不当使用。
A.10.7.4	系统文件安全	*控制措施* 应保护系统文件以防止未授权的访问。
A.10.8 信息的交换 *目标*：保持组织内以及与组织外信息和软件交换的安全。		
A.10.8.1	信息交换策略和规程	*控制措施* 应有正式的交换策略、规程和控制措施，以保护通过使用各种类型通信设施的信息交换。
A.10.8.2	交换协议	*控制措施* 应建立组织与外部方交换信息和软件的协议。
A.10.8.3	运输中的物理介质	*控制措施* 包含信息的介质在组织的物理边界以外运送时，应防止未授权的访问、不当使用或毁坏。
A.10.8.4	电子消息发送	*控制措施* 包含在电子消息发送中的信息应给予适当的保护。
A.10.8.5	业务信息系统	*控制措施* 应建立并实施策略和规程，以保护与业务信息系统互联相关的信息。

表 A.1（续）

A.10.9 电子商务服务 *目标*：确保电子商务服务的安全及其安全使用。		
A.10.9.1	电子商务	*控制措施* 包含在使用公共网络的电子商务中的信息应受保护，以防止欺诈活动、合同争议以及未授权的泄露和修改。
A.10.9.2	在线交易	*控制措施* 在线交易中的信息应受保护，以防止不完全传输、错误路由、未授权的消息篡改、未授权的泄露、未授权的消息复制或重放。
A.10.9.3	公共可用信息	*控制措施* 在公共可用系统中可用信息的完整性应受保护，以防止未授权的修改。
A.10.10 监视 *目标*：检测未经授权的信息处理活动。		
A.10.10.1	审计记录	*控制措施* 应产生记录用户活动、异常情况和信息安全事态的审计日志，并要保持一个已设的周期以支持将来的调查和访问控制监视。
A.10.10.2	监视系统的使用	*控制措施* 应建立信息处理设施的监视使用规程，并经常评审监视活动的结果。
A.10.10.3	日志信息的保护	*控制措施* 记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。
A.10.10.4	管理员和操作员日志	*控制措施* 系统管理员和系统操作员活动应记入日志。
A.10.10.5	故障日志	*控制措施* 故障应被记录、分析，并采取适当的措施。
A.10.10.6	时钟同步	*控制措施* 一个组织或安全域内的所有相关信息处理设施的时钟应使用已设的精确时间源进行同步。
A.11 访问控制		
A.11.1 访问控制的业务要求 *目标*：控制对信息的访问。		
A.11.1.1	访问控制策略	*控制措施* 访问控制策略应建立、形成文件，并基于业务和访问的安全要求进行评审。
A.11.2 用户访问管理 *目标*：确保授权用户访问信息系统，并防止未授权的访问。		
A.11.2.1	用户注册	*控制措施* 应有正式的用户注册及注销规程，来授权和撤销对所有信息系统及服务的访问。
A.11.2.2	特殊权限管理	*控制措施* 应限制和控制特殊权限的分配及使用。
A.11.2.3	用户口令管理	*控制措施* 应通过正式的管理过程控制口令的分配。
A.11.2.4	用户访问权的复查	*控制措施* 管理者应定期使用正式过程对用户的访问权进行复查。
A.11.3 用户职责 *目标*：防止未授权用户对信息和信息处理设施的访问、损害或窃取。		

表 A.1（续）

A.11.3.1	口令使用	*控制措施* 应要求用户在选择及使用口令时，遵循良好的安全习惯。
A.11.3.2	无人值守的用户设备	*控制措施* 用户应确保无人值守的用户设备有适当的保护。
A.11.3.3	清空桌面和屏幕策略	*控制措施* 应采取清空桌面上文件、可移动存储介质的策略和清空信息处理设施屏幕的策略。
A.11.4 网络访问控制 *目标*：防止对网络服务的未授权访问。		
A.11.4.1	使用网络服务的策略	*控制措施* 用户应仅能访问已获专门授权使用的服务。
A.11.4.2	外部连接的用户鉴别	*控制措施* 应使用适当的鉴别方法以控制远程用户的访问。
A.11.4.3	网络上的设备标识	*控制措施* 应考虑自动设备标识，将其作为鉴别特定位置和设备连接的方法。
A.11.4.4	远程诊断和配置端口的保护	*控制措施* 对于诊断和配置端口的物理和逻辑访问应加以控制。
A.11.4.5	网络隔离	*控制措施* 应在网络中隔离信息服务、用户及信息系统。
A.11.4.6	网络连接控制	*控制措施* 对于共享的网络，特别是越过组织边界的网络，用户的联网能力应按照访问控制策略和业务应用要求加以限制（见 A.11.1）。
A.11.4.7	网络路由控制	*控制措施* 应在网络中实施路由控制，以确保计算机连接和信息流不违反业务应用的访问控制策略。
A.11.5 操作系统访问控制 *目标*：防止对操作系统的未授权访问。		
A.11.5.1	安全登录规程	*控制措施* 访问操作系统应通过安全登录规程加以控制。
A.11.5.2	用户标识和鉴别	*控制措施* 所有用户应有唯一的、专供其个人使用的标识符（用户 ID），应选择一种适当的鉴别技术证实用户所宣称的身份。
A.11.5.3	口令管理系统	*控制措施* 口令管理系统应是交互式的，并应确保优质的口令。
A.11.5.4	系统实用工具的使用	*控制措施* 对于可能超越系统和应用程序控制措施的实用工具的使用应加以限制并严格控制。
A.11.5.5	会话超时	*控制措施* 不活动会话应在一个设定的休止期后关闭。
A.11.5.6	联机时间的限定	*控制措施* 应使用联机时间的限制，为高风险应用程序提供额外的安全。
A.11.6 应用和信息访问控制 *目标*：防止对应用系统中信息的未授权访问。		

表 A.1（续）

A.11.6.1	信息访问限制	*控制措施* 用户和支持人员对信息和应用系统功能的访问应依照已确定的访问控制策略加以限制。
A.11.6.2	敏感系统隔离	*控制措施* 敏感系统应有专用的(隔离的)运算环境。
A.11.7 移动计算和远程工作 *目标*：确保使用移动计算和远程工作设施时的信息安全。		
A.11.7.1	移动计算和通信	*控制措施* 应有正式策略并且采用适当的安全措施，以防范使用移动计算和通信设施时所造成的风险。
A.11.7.2	远程工作	*控制措施* 应为远程工作活动开发和实施策略、操作计划和规程。
A.12 信息系统获取、开发和维护		
A.12.1 信息系统的安全要求 *目标*：确保安全是信息系统的一个有机组成部分。		
A.12.1.1	安全要求分析和说明	*控制措施* 在新的信息系统或增强已有信息系统的业务要求陈述中，应规定对安全控制措施的要求。
A.12.2 应用中的正确处理 *目标*：防止应用系统中的信息的差错、遗失、未授权的修改或误用。		
A.12.2.1	输入数据确认	*控制措施* 应对输入应用系统的数据加以确认，以确保数据是正确且恰当的。
A.12.2.2	内部处理的控制	*控制措施* 确认核查应整合到应用中，以检测由于处理的差错或故意的行为造成的信息的任何讹误。
A.12.2.3	消息完整性	*控制措施* 应用中的确保真实性和保护消息完整性的要求应得到识别，适当的控制措施也应得到识别并实施。
A.12.2.4	输出数据确认	*控制措施* 从应用系统输出的数据应加以确认，以确保对所存储信息的处理是正确的且适于环境的。
A.12.3 密码控制 *目标*：通过密码方法保护信息的保密性、真实性或完整性。		
A.12.3.1	使用密码控制的策略	*控制措施* 应开发和实施使用密码控制措施来保护信息的策略。
A.12.3.2	密钥管理	*控制措施* 应有密钥管理以支持组织使用密码技术。
A.12.4 系统文件的安全 *目标*：确保系统文件的安全。		
A.12.4.1	运行软件的控制	*控制措施* 应有规程来控制在运行系统上安装软件。
A.12.4.2	系统测试数据的保护	*控制措施* 测试数据应认真地加以选择、保护和控制。

表 A.1（续）

A.12.4.3	对程序源代码的访问控制	*控制措施* 应限制访问程序源代码。
A.12.5 开发和支持过程中的安全 *目标*：维护应用系统软件和信息的安全。		
A.12.5.1	变更控制规程	*控制措施* 应使用正式的变更控制规程来控制变更的实施。
A.12.5.2	操作系统变更后应用的技术评审	*控制措施* 当操作系统发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。
A.12.5.3	软件包变更的限制	*控制措施* 应对软件包的修改进行劝阻，只限于必要的变更，且对所有的变更加以严格控制。
A.12.5.4	信息泄露	*控制措施* 应防止信息泄露的可能性。
A.12.5.5	外包软件开发	*控制措施* 组织应管理和监视外包软件的开发。
A.12.6 技术脆弱性管理 *目标*：降低利用公布的技术脆弱性导致的风险。		
A.12.6.1	技术脆弱性的控制	*控制措施* 应及时得到现用信息系统技术脆弱性的信息，评价组织对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。
A.13 信息安全事件管理		
A.13.1 报告信息安全事态和弱点 *目标*：确保与信息系统有关的信息安全事态和弱点能够以某种方式传达，以便及时采取纠正措施。		
A.13.1.1	报告信息安全事态	*控制措施* 信息安全事态应尽可能快地通过适当的管理渠道进行报告。
A.13.1.2	报告安全弱点	*控制措施* 应要求信息系统和服务的所有雇员、承包方人员和第三方人员记录并报告他们观察到的或怀疑的任何系统或服务的安全弱点。
A.13.2 信息安全事件和改进的管理 *目标*：确保采用一致和有效的方法对信息安全事件进行管理。		
A.13.2.1	职责和规程	*控制措施* 应建立管理职责和规程，以确保快速、有效和有序地响应信息安全事件。
A.13.2.2	对信息安全事件的总结	*控制措施* 应有一套机制量化和监视信息安全事件的类型、数量和代价。
A.13.2.3	证据的收集	*控制措施* 当一个信息安全事件涉及到诉讼(民事的或刑事的)，需要进一步对个人或组织进行起诉时，应收集、保留和呈递证据，以使其符合相关管辖区域对证据的要求。
A.14 业务连续性管理		
A.14.1 业务连续性管理的信息安全方面 *目标*：防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保它们的及时恢复。		
A.14.1.1	在业务连续性管理过程中包含信息安全	*控制措施* 应为贯穿于组织的业务连续性开发和保持一个管理过程，以解决组织的业务连续性所需的信息安全要求。

表 A.1（续）

A.14.1.2	业务连续性和风险评估	*控制措施* 应识别能引起业务过程中断的事态，连同这种中断发生的概率和影响，以及它们对信息安全所造成的后果。
A.14.1.3	制定和实施包含信息安全的连续性计划	*控制措施* 应制定和实施计划来保持或恢复运行，以在关键业务过程中断或失败后能够在要求的水平和时间内确保信息的可用性。
A.14.1.4	业务连续性计划框架	*控制措施* 应保持一个唯一的业务连续性计划框架，以确保所有计划是一致的，能够协调地解决信息安全要求，并为测试和维护确定优先级。
A.14.1.5	测试、维护和再评估业务连续性计划	*控制措施* 业务连续性计划应定期测试和更新，以确保其及时性和有效性。
A.15 符合性		
A.15.1 符合法律要求 *目标*：避免违反任何法律、法令、法规或合同义务以及任何安全要求。		
A.15.1.1	可用法律的识别	*控制措施* 对每一个信息系统和组织而言，所有相关的法令、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义，形成文件并保持更新。
A.15.1.2	知识产权(IPR)	*控制措施* 应实施适当的规程，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求。
A.15.1.3	保护组织的记录	*控制措施* 应防止重要的记录遗失、毁坏和伪造，以满足法令、法规、合同和业务的要求。
A.15.1.4	数据保护和个人信息的隐私	*控制措施* 应依照相关的法律、法规和合同条款的要求，确保数据保护和隐私。
A.15.1.5	防止滥用信息处理设施	*控制措施* 应禁止用户使用信息处理设施用于未授权的目的。
A.15.1.6	密码控制措施的规则	*控制措施* 使用密码控制措施应遵从相关的协议、法律和法规。
A.15.2 符合安全策略和标准以及技术符合性 *目标*：确保系统符合组织的安全策略及标准。		
A.15.2.1	符合安全策略和标准	*控制措施* 管理人员应确保在其职责范围内的所有安全规程被正确地执行，以确保符合安全策略及标准。
A.15.2.2	技术符合性核查	*控制措施* 信息系统应被定期核查是否符合安全实施标准。
A.15.3 信息系统审计考虑 *目标*：将信息系统审计过程的有效性最大化，干扰最小化。		
A.15.3.1	信息系统审计控制措施	*控制措施* 涉及对运行系统核查的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化造成业务过程中断的风险。
A.15.3.2	信息系统审计工具的保护	*控制措施* 对于信息系统审计工具的访问应加以保护，以防止任何可能的滥用或损害。

附 录 B
（资料性附录）
OECD 原则和本标准

在 OECD 信息系统和网络安全指南中给出的原则适用于治理信息系统和网络安全的所有方针和操作层。本标准提供信息安全管理体系框架，通过使用 PDCA 模型以及第 4 章、第 5 章、第 6 章和第 8 章所述的过程，来实现的某些 OECD 原则，如表 B.1 所示。

表 B.1 OECD 原则和 PDCA 模型

OECD 原则	相应的 ISMS 过程和 PDCA 模型
意识 参与者应知悉信息系统和网络的安全需求，并知悉在提高信息安全方面，他们能够做些什么。	本活动是实施(Do)阶段的一部分(见 4.2.2 和 5.2.2)。
责任 所有参与者对信息系统和网络的安全都有责任。	本活动是实施(Do)阶段的一部分(见 4.2.2 和 5.1)。
响应 参与者对安全事故应以及时的和合作的方式进行预防、检测和响应。	这是检查(Check)阶段的监视活动(见 4.2.3 和第 6 章到 7.3)和处置(Act)阶段的响应活动(见 4.2.4 和 8.1 到8.3)的一部分。这也涵盖于规划(Plan)和检查(Check)阶段中的某些方面。
风险评估 参与者应进行风险评估。	本活动是规划(Plan)阶段的一部分(见 4.2.1)，而风险再评估是检查(Check)阶段的一部分(见 4.2.3 和第 6 章到 7.3)。
安全设计与实施 参与者应把安全作为信息系统和网络的基本要素。	一旦风险评估完成，就要为风险的处理选择控制措施作为规划(Plan)阶段的一部分(见 4.2.1)。然后，在实施(Do)阶段(见 4.2.2 和 5.2)包含这些控制措施的实施和运行使用。
安全管理 参与者应采用综合的方法进行安全管理。	风险的管理是一种包括预防、检测与响应事故、日常维护、评审和审核的过程。所有这些方面包含于规划(Plan)、实施(Do)、检查(Check)和处置(Act)阶段。
再评估 参与者应评审和再次评估信息系统和网络的安全，并适当改进安全策略、实践、措施和程序。	信息安全的再评估是检查(Check)阶段的一部分(见 4.2.3和第 6 章到 7.3)。这里，应经常进行评审以检查信息安全管理体系的有效性。改进安全是处置(Act)阶段的一部分(见 4.2.4 和 8.1 到 8.3)。

附 录 C
（资料性附录）
GB/T 19001—2000，GB/T 24001—2004 和本标准之间的对照

表 C.1 显示了 GB/T 19001—2000、GB/T 24001—2004 和本标准之间的对应关系。

表 C.1 GB/T 19001—2000、GB/T 24001—2004 和本标准之间的对应关系

本标准	GB/T 19001—2000	GB/T 24001—2004
0 引言 0.1 总则 0.2 过程方法 0.3 与其他管理体系的兼容性	0 引言 0.1 总则 0.2 过程方法 0.3 与 GB/T 19004 的关系 0.4 与其他管理体系的相容性	引言
1 范围 1.1 总则 1.2 应用	1 范围 1.1 总则 1.2 应用	1 范围
2 规范性引用文件	2 引用标准	2 规范性引用文件
3 术语和定义	3 术语和定义	3 术语和定义
4 信息安全管理体系 4.1 总要求 4.2 建立和管理 ISMS 4.2.1 建立 ISMS 4.2.2 实施和运行 ISMS 4.2.3 监视和评审 ISMS 4.2.4 保持和改进 ISMS 4.3 文件要求 4.3.1 总则 4.3.2 文件控制 4.3.3 记录控制	4 质量管理体系 4.1 总要求 8.2.3 过程的监视和测量 8.2.4 产品的监视和测量 4.2 文件要求 4.2.1 总则 4.2.2 质量手册 4.2.3 文件控制 4.2.4 记录控制	4 EMS 要求 4.1 总要求 4.4 实施和运行 4.5.1 监视和测量 4.5.2 合规性评价 4.4.5 文件控制 4.5.4 记录控制
5 管理职责 5.1 管理承诺	5 管理职责 5.1 管理承诺 5.2 以顾客为关注焦点 5.3 质量方针 5.4 策划 5.5 职责、权限和沟通	 4.2 环境方针 4.3 策划
5.2 资源管理 5.2.1 资源提供 5.2.2 培训、意识和能力	6 资源管理 6.1 资源提供 6.2 人力资源 6.2.2 能力、意识和培训 6.3 基础设施 6.4 工作环境	 4.4.2 能力、培训和意识
6 ISMS 内部审核	8.2.2 内部审核	4.5.5 内部审核

表 C.1（续）

本标准	GB/T 19001—2000	GB/T 24001—2004
7 ISMS 的管理评审 7.1 总则 7.2 评审输入 7.3 评审输出	5.6 管理评审 5.6.1 总则 5.6.2 评审输入 5.6.3 评审输出	4.6 管理评审
8 ISMS 改进 8.1 持续改进 8.2 纠正措施 8.3 预防措施	8 测量、分析和改进 8.5.1 持续改进 8.5.2 纠正措施 8.5.3 预防措施	 4.5.3 不合格，纠正和预防措施
附录 A 控制目标和控制措施 附录 B OECD 原则和本标准 附录 C GB/T 19001—2000、GB/T 24001—2004 和本标准之间的对照	附录 A GB/T 19001—2000 与 GB/T 24001—1996 之间的对照	附录 A 本标准使用指南 附录 B GB/T 24001 和 GB/T 19001 之间的联系

参 考 文 献

标准出版物

[1] GB/T 19001—2000 质量管理体系 要求

[2] GB /T 19011—2003 质量和(或)环境管理体系审核指南

[3] GB/T 24001—2004 环境管理体系要求及使用指南

[4] GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理

[5] ISO/IEC 指南 62:1996 从事质量体系的评估和认证/注册的机构的通用要求

[6] ISO/IEC 指南 73:2002 风险管理 术语 标准使用指南

[7] ISO/IEC 13335-1:2004 信息技术 安全技术 信息和通信技术安全管理 第 1 部分:管理和规划 ICT 安全的概念和模型

[8] ISO/IEC TR 13335-3:1998 信息技术 IT 安全管理指南 第 3 部分:IT 安全管理技术

[9] ISO/IEC TR 13335-4:2000 信息技术 IT 安全管理指南 第 4 部分:防护措施的选择

其他出版物

[1] OECD. OECD 信息系统和网络安全指南——面向安全的文化. 巴黎:OECD,2002 年 7 月. www. oecd. org

[2] NIST SP 800-30 信息技术系统的风险管理指南.

[3] Deming W. E. Out of the crisis,剑桥,Mass:MIT,高级工程研究中心,1986.