Information Security Management Guidance：ISMG-001-2013

ISO27001：2013（DIS）中文版

内容摘要

现行的信息安全管理体系 ISO27001:2005 标准已经使用了 8 年，日前 ISO 组织（国际标准化组织）终于将新版 ISO27001:2013DIS 版（国际标准草案 Draft International Standard）草稿向公众开放并征求意见，同时，计划在 2013 年 10 月 19 日颁布正式版，本文是安言咨询基于新版 ISO27001:2013DIS 版翻译而来。

声明

关于安言咨询

上海安言信息技术有限公司（Aryasec，简称安言咨询），总部在上海，另设北京和深圳分公司，是国内最早且最富特色的信息安全及 IT 咨询服务机构。公司保持中立和客观立场，与包括 ISCCC、BSI、DNV、TUV、BV、HP、IBM、神州数码、启明、华赛等国内外著名机构建立并保持合作关系，协助企业客户实现符合业务发展需要的信息安全及 IT 建设解决方案。

安言咨询基于独创的咨询服务和培训体系，以强大的专家顾问团队为依托，借助成熟的方法论和工具，为客户提供以业务为导向的咨询服务。安言咨询引入 ISO27001、ISO20000、ISO22301、ITIL、CobiT、SDL、SAS70、PCI 等国际权威标准或最佳实践，协助客户建立符合业务需要的 IT 治理体系，同时有效传递专业知识，增强客户分析问题解决问题的能力。

www.aryasec.com

总部地址： 上海市长宁路 855 号亨通国际大厦 8 楼 B 座
邮政编码： 200050
联系电话： 021 62101209/62139481/62139482
电子邮件： service@aryasec.com
微信二维码：

版本信息

文档名称	**ISO27001：2013（DIS）中文版**		
文档管理编号	ISMG-001-2013		
保密级别	公开	文档版本号	1.0
编制	夏子钦	日期	2013 年 6 月 20 日（V0.1）
校对	张威		2013 年 6 月 28 日（V1.0）
分发范围	在安言咨询客户范围内共享		
分发批准人	张威		

目录

前言

现版的信息安全管理体系 ISO27001:2005 标准已经使用了 8 年，日前 ISO 组织（国际标准化组织）终于将新版 ISO27001:2013DIS 版（国际标准草案 Draft International Standard）草稿向公众开放并征求意见。在新版 ISO27001：2013DIS 中采用 ISO 导则 83 做结构性要求，从 8 个章节拓展到 10 个章节，重新构建了 ISO 标准 PDCA 的章节架构，这个结构在已发布的 ISO22301 中已经进行了应用，未来将在 ISO 其他标准改版中会普遍采用（包括 ISO9000、ISO20000 等）。

ISO 组织公布正式版本的颁布时间预计为 2013 年 10 月 19 日。在新版公布后的 18 至 24 个月内是认证转换缓冲期，即原有已取得 ISO27001 证书的企业最迟需要在 2015 年 10 月 19 日前转换到新版标准。

已通过 ISO27001 认证的企业需要在执行新标时提前做一些应对，主要在 3 方面对现行体系进行调整：

- 风险评估工具需升级。随着新标准控制项架构的调整，企业目前使用的风险评估方法将受到一定影响，核心在于信息资产弱点建模及风险处置的控制项选择部分，需要重新构建符合新标准结构的风险评估工具。

- SOA 适用性声明及文件体系的升级。新标准的实施，将对 SOA 适用性声明及企业现有体系文件制度产生较大影响，体系一二级文件将需进行一个较大的内容调整及升级，不过，对三四级文件的影响较小，在三四级文件层面上，仅需根据新标要求进行少量增补即可。

- 内部审核工具的升级。受内部管理制度的调整，内部审核的开展方式及使用工具将不可避免受到影响，也需根据新标要求进行升级。

本翻译版 DIS 标准非正式发布版本，供企业开展内部信息安全管理体系改进时参考之用，如在开展过程中遇到进一步的疑问，也可与我们联系。

0 引言

0.1 总则

本国际标准提供给准备建立、运作、维护、改进信息安全管理体系（ISMS）的组织。采用 ISMS 应是一个组织的战略决策。组织 ISMS 的设计和实施受业务需求和目标、安全需求、应用的过程及组织的规模、结构的影响。上述因素预计会随时间而变化。

信息安全管理体系通过使用风险管理过程来保护信息的保密性，完整性，可用性，给相关方带来信心并使风险得到充分管理。

重要的是，信息安全管理体系是组织结构过程和整体管理架构的一部分，在设计流程、信息系统、控制措施时都应考虑信息安全。信息安全管理体系应占组织需求的一定比例。

本标准可被用于内部、外部，包括认证机构，评估组织的能力来满足组织自身信息安全要求。

本国际标准中要求的顺序并不能反映他们的重要性或暗示他们实现的顺序。列表中的列举项仅供参考。

ISO/IEC 27000 描述了信息安全管理体系的概述词汇表。主要从 ISMS 标准簇（包括 ISO/IEC 27003, ISO/IEC 27004，ISO/IEC 27005）并定义了相关术语。

0.2 与其他管理体系标准的兼容性

本国际标准适用于高层次的结构，相同的副条款标题，相同的文本，常用词汇和 ISO/ IEC 导则第 1 部分的附件 SL 中定义的核心定义，因此可以采用附件 SL 与其他管理体系标准相兼容。

附件 SL 中定义的这种常见方法，在选择符合两个或两个以上管理系体标准的单一管理系统时是很有用的。

1 适用范围

本国际标准规定了在组织的背景下建立，实施，维护和不断改进信息安全管理体系的要求。本标准还包括信息安全风险评估和根据组织需求定制的信息安全风险处理方法。当一个组织声称其符合此国际标准但没有达到 4 到 10 章规定的要求，是不可接受的。

2 规范性引用

以下引用的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，仅引用的版本适用。 凡是不注日期的引用文件，其最新版本的参考文件（包括所有的修改单）适用。

3 术语和定义

ISO / IEC 27000 的术语和定义适用于本文档。

4 组织的背景

4.1 了解组织现状及背景

组织应明确与信息安全管理体系目的及影响其能力有关的内外部问题，以达到信息安全管理体系的预期效果。

注：确定这些问题是指建立 ISO 31000 第 5.3.1 考虑外部和内部环境的组织。

4.2 理解相关方的需求和期望

组织应确定：

a) 信息安全管理体系的相关方；

b) 这些相关方信息安全相关要求。

注：有关各方的要求可能包括法律、监管规定和合同义务。

4.3 确定 ISMS 的范围

组织应确定信息安全管理体系的边界和适用性，以确定其范围。

在确定此范围时，组织应考虑：

a) 4.1 提及的外部和内部的问题；

b) 4.2 提及的要求；

c) 接口和执行组织之间活动的依赖关系，以及其他组织的相关活动。

范围应可成为文档化信息。

4.4 ISMS

组织应按照本国际标准的要求建立，实施，保持和持续改进信息安全管理体系。

5 领导力

5.1 领导力和承诺

最高管理者应表现出对信息安全管理体系的领导力和承诺：

a) 确保信息安全策略和信息安全目标的制定，并与组织的战略方向兼容；

b) 确保信息安全管理体系的要求整合到组织的过程中；

c) 确保信息安全管理体系所需要的资源；

d) 传达有效的信息安全管理的重要性，并符合信息安全管理体系的要求；

e) 确保信息安全管理体系达到其预期的效果；

f) 指导和支持员工对信息安全管理体系作出有效的贡献；

g) 促进持续改进；

h) 支持其他相关管理角色来展示自己的领导力，因为它适用于他们的职责范围。

5.2 方针

最高管理者应建立一个信息安全方针：

a) 与组织的宗旨相适应；

b) 包括信息安全目标（见 6.2），或为信息安全目标提供框架；

c) 包括满足与信息安全相关要求的承诺；

d) 包括信息安全管理体系持续改进的承诺。

信息安全的方针应：

e) 可成为文档化信息；

f) 在组织内沟通；

g) 视情况提供给相关方。

5.3 角色，责任和承诺

最高管理者应确保与信息安全相关角色的职责和权限的分配和沟通。

最高管理者应指定责任和权限：

a) 确保信息安全管理体系符合本国际标准的要求；

b) 将 ISMS 的绩效报告给最高管理者。

注：最高管理层可以授权他人负责 ISMS 的绩效报告。

6 计划

6.1 处理风险和机遇的行动

6.1.1 总则

当规划组织的信息安全管理体系时，应当考虑 4.1 提到的问题和 4.2 中所提到的要求，并确定需要解决的风险和机遇：

a) 确保信息安全管理体系可实现预期的结果；

b) 防止或减少不良影响；

c) 实现持续改进。

组织应策划：

d) 解决这些风险和机遇的措施；

e) 如何

1) 整合和实施这些措施，并纳入其信息安全管理体系过程中；

2) 评估这些措施的有效性。

6.1.2 信息安全风险评估

组织应确定信息安全风险评估过程：

a) 建立和维护信息安全风险的标准，包括风险接受准则；

b) 决定执行的信息安全风险评估的标准；

c) 确保重复使用信息安全风险评估过程能产生一致的，有效的和可比较的结果。

组织应：

d) 识别信息安全的风险。

1) 应用信息安全风险评估过程，以识别 ISMS 范围内的信息保密性，完整性和可用性的损失风险。

2） 识别风险的所有者。

e） 分析信息安全风险。

1） 评估 6.1.1e）1）实现后潜在的后果。

2） 评估 6.1.1e）1）实现的可能性。

3） 确定风险等级。

f） 评估信息安全风险。

1） 用 6.1.2a）建立的风险标准比较风险分析结果，并建立优先级。

组织应保留的信息安全风险评估过程中的文档化信息。

6.1.3 信息安全风险处置

组织应采用信息安全风险处置过程：

a） 选择适当的信息安全风险处理方法，考虑风险评估的结果；

b） 确定所有实施的信息安全风险处置措施是必要的；

注：组织可以设计所需的控制项，或从任何来源中识别它们。

c） 比较 6.1.3 b)中与附件 A 中的控制项，并确认已省略没有必要的控制项；

注 1：附件 A 中包含控制目标和控制项的完整列表。本国际标准的用户应注意附件 A，以确保没有重要的控制项被忽略

注 2：控制目标是隐含在所选择的控制项中。附件 A 所列的控制目标和控制项并不详尽，可能还需要额外的控制目标和控制项。

d） 制作一个包含必要的控制项（见 6.1.3），B)和 C））和包含理由的适用性声明，无论实施与否，并应包含删减附件 A 中控制项的理由；

e） 制定信息安全风险处置计划；

f） 风险处置方案和残余风险应得到风险负责人的批准。

组织应保留信息安全风险的处理过程中的文档化信息。

注意：信息安全风险评估和处置过程与国际标准 ISO 31000 规定的原则和通用的准则相一致。

6.2 可实现的信息安全目标和计划

组织应建立相关职能和层次的信息安全目标。

信息安全目标应：

a） 与信息安全方针一致；

b） 是可衡量的（如果可行）；

c） 考虑到适用的信息安全要求，以及风险评估和处置结果；

d） 是可沟通的；

e） 能适时更新。

组织应保留信息安全目标相关的文档化信息。

当计划如何实现信息安全目标时，组织应确定：

f） 做什么；

g） 需要哪些资源；

h） 谁负责；

i） 何时完成；

j） 如何评估结果。

7 支持

7.1 资源

组织应确定并提供信息安全管理体系的建立，实施，维护和持续改进所需的资源。

7.2 能力

组织应：

a） 确定员工在 ISMS 管控下工作的必备能力，这会影响到组织的信息安全绩效；

b） 确保这些人在适当的教育，培训或取得经验后是能胜任的；

c） 在适当情况下，采取行动以获得必要的能力，并评估所采取行动的有效性；

d） 保留适当的文档化信息作为证据。

注：适用的行动可能包括，例如：提供培训，指导，或重新分配现有雇员、主管人员的聘用或承包。

7.3 意识

为组织工作的人员应了解：

a） 信息安全方针；

b） 他们对信息安全管理体系有效性的贡献，包括提高信息安全绩效的收益；

c） 不符合信息安全管理体系要求所带来的影响，。

7.4 沟通

组织应确定信息安全管理体系中内部和外部相关的沟通需求：

a） 沟通什么；

b） 何时沟通；

c） 和谁沟通；

d） 谁应该沟通；

e） 怎样的沟通过程是有效的。

7.5 文档化信息

7.5.1 总则

组织的信息安全管理体系应包括：

a） 本国际标准所需要的文档化信息；

b） 记录信息安全管理体系有效性必要的文档化信息。

注意：不同组织的信息安全管理体系文档化信息的多少与详略程度取决于：

1） 组织的规模、活动的类型，过程，产品和服务；

2） 过程及其相互作用的复杂性；

3） 人员的能力。

7.5.2 创建和更新

当创建和更新文档化信息时，组织应确保适当的：

a） 识别和描述（如标题，日期，作者，或参考号码）；

b） 格式（如语言，软件版本，图形）和媒体（如纸张，电子）；

c） 适当和足够的审查和批准。

7.5.3 文档化信息的控制

信息安全管理体系与本国际标准要求的文档化信息应被管理，以确保：

a） 当文档化信息被需要时是可用且适用的；

b） 得到充分的保护（例如保密性丧失，使用不当，完整性丧失）。

对于文档化信息的控制，组织应制定以下活动（如适用）：

c） 分配，访问，检索和使用；

d） 存储和保存，包括易读性的保存；

e） 变更管理（例如版本控制）；

f） 保留和处置。

组织信息安全管理体系的规划和运作必要的外来文档化信息，应被适当识别和管理。

注：访问表示有权查看文档化信息，或获得授权以查看和更改文档化信息等。

8 运行

8.1 运行计划及控制

组织应策划，实施和控制过程需求以满足信息安全要求，并实施在 6.1 中确定措施。组织还应当实施计划，以实现信息安全在 6.2 中确定的目标。

组织应保存相关的文档化信息，以保证过程已按照计划实施。

组织应控制计划变更，同时审计非计划变更，并采取适当措施以减轻任何不良影响。

组织应确保外包过程是被确定和受控。

8.2 信息安全风险评估

组织应在技术时间间隔或发生重大变化时执行信息安全风险评估，将 6.1.2 中建立的标准纳入考虑范围。

组织应保留信息安全风险评估结果的相关文档化信息。

8.3 信息安全风险处置

组织应实施信息安全风险处置计划。

组织应保留信息安全风险处置结果的文档化信息。

9 绩效评价

9.1 监控，度量，分析和评价

组织应评估信息安全绩效和信息安全管理体系的有效性。

组织应确定：

a） 需要进行监视和测量，包括信息安全过程和控制要求；

b） 监测，测量，分析和评估（如适用）的方法，以确保结果有效；

注：选择被认为是有效的方法应该可以产生可比性和可再现的结果。

c） 监视和测量时间；

d） 谁应监视和测量；

e） 何时对监视和测量的结果进行分析和评估；

f） 谁应分析和评估这些结果。

组织应保留适当的监视和测量结果的文档化信息作为证据。

9.2 内部审核

组织应在计划的时间间隔进行内部审核，根据提供的信息判断是否安全管理体系：

a） 符合

1） 组织自身信息安全管理体系的要求；

2） 本国际标准的要求；

b） 有效实施和保持。

组织应：

c） 计划，建立，实施并保持审核方案，其中包括频率，方法，职责，计划要求和报告。 审核程序应考虑相关过程和以往审核结果的重要性；

d） 定义每次审核的章程和范围；

e） 选择审核员和审核组长以确保审核过程的客观性和公正；

f） 确保审核结果报告提交相关管理层；

g） 保留审核程序和审核结果相关的文档化信息作为证据。

9.3 管理评审

最高管理者应在计划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性，充分性和有效性。

管理评审应考虑：

a） 以往管理评审行动措施的状态；

b） 与信息安全管理体系相关的内外部问题的变化；

c） 反馈信息安全绩效和趋势，包括：

1） 不符合与纠正措施；

2） 监控和测量结果；

3） 审核结果；

4） 信息安全目标的实现；

d） 相关方的反馈；

e） 风险评估的结果和风险处置的状态；

f） 持续改改进的机会。

管理评审的输出应包括持续改进的机会和任何信息安全管理体系需要变更的相关决定。

组织应保留管理评审结果的文档化信息作为证据。

10 改进

10.1 不符合及纠正措施

出现不符合时，组织应：

a） 对不符合作出反应，如适用：

1） 采取行动控制和纠正；

2） 处理结果；

b） 评估采取措施的必要性，以消除不符合的原因，使不复发或不在其他地方发生，通过：

1） 审查不符合；

2） 确定不符合的原因；

3） 确定是否存在类似的不符合和发生的可能；

c） 实施所需的任何措施；

d） 审查已采取纠正措施的有效性；

e） 如果有必要的话，改进信息安全管理体系。

纠正措施应对不符合产生适当的影响。

组织应保留以下文档化信息作为证据：

f） 不符合的性质和后续措施；

g） 任何纠正措施的结果。

10.2 持续改进

组织应不断提高信息安全管理体系的适宜性，充分性和有效性。

附录 **A**

（规范性附录）

参考控制目标和控制项

表 A.1 所列的控制目标和控制项，直接与 ISO / IEC DIS 27002 第 5 至 18 所对应。表中的控制目标和控制项并不详尽，如有必要,组织可以考虑增加额外的控制目标和控制项。作为信息安全管理体系过程中的一部分,表中的控制目标和控制措施，应在实施 6.1.3 节中被选择。

ISO / IEC DIS 27002 第 5 至 18 条规定实施最佳实践的建议和指导，支持 A.5 到 A.18（A.0 以 A.4 指定的控制中未使用 - 控制项参考指导部分与 ISO / IEC DIS 27002）。

A.5 安全方针		
A.5.1 信息安全管理方向 目的：为信息安全提供管理指导和支持并确保信息安全符合业务需求和相关法律、法规		
A.5.1.1	信息安全方针	*控制* 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* 应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 目的：建立一个管理框架，启动和控制组织内实施信息安全		
A.6.1.1	信息安全的角色和职责	*控制* 所有信息安全职责应被定义及分配
A.6.1.2	与监管机构的联系	*控制* 应与监管机构保持适当的接触
A.6.1.3	与特殊利益团体的联系	*控制* 与特定利益团队、其他专业安全论坛或行业协会应保持适当联系

A.6.1.4	项目管理中的信息安全	*控制* 信息安全应融入项目管理中，与项目类型无关
A.6.1.5	职责分离	*控制* 冲突的职责和权限应被分开，减少对资产未经授权或无意的修改与误用
A.6.2 移动设备和远程办公 目的：确保远程办公和移动设备使用的安全性		
A.6.2.1	移动设备策略	*控制* 应使用配套策略和安全措施来防止移动设备带来的风险
A.6.2.2	远程办公	*控制* 应使用配套策略和安全措施来保护信息访问，处理或远程存储
A.7 人力资源安全		
A.7.1 任用之前 目的：确保组织内人员理解其职责、考虑其承担的角色是适合的。		
A.7.1.1	筛选	*控制* 根据相关法律、法规、道德规范，对员工、合同人员及第三方人员的应聘人员进行背景调查，调查应符合业务需求、访问信息的类别及已知风险
A.7.1.2	任用的条款及条件	*控制* 作为合同义务的一部分，员工应同意并签订就业合同的条款和条件，应当载明其对组织信息安全的职责
A.7.2 任用中 目的：确保员工和外部方用户意识到并履行信息安全职责		
A.7.2.1	管理职责	*控制* 管理层应要求员工、合同方和第三方用户应用符合组织建立的安全策略和程序的安全
A.7.2.2	信息安全意识，教育和培训	*控制* 组织内所有员工、相关合同人员及第三方人员应接受适当的意识培训，并定期更新与他们工作相关的组织策略及程序
A.7.2.3	纪律处理过程	*控制*

		对于安全违规的雇员，应有一个正式与可沟通的纪律处理过程
A.7.3 任用的终止或变化 目的：保证组织利益是雇佣终止和变更的一部分		
A.7.3.1	任用终止或变化的责任	*控制* 任用终止或变更后依然有信息安全责任和义务的人，应该被界定和传达给雇员或给外部方执行。
A.8 资产管理		
A.8.1 对资产负责 目的：实现和保持对组织资产的适当保护		
A.8.1.1	资产清单	*控制* 应确定与信息和信息处理设施相关的资产，编制并维护资产清单
A.8.1.2	资产责任人	*控制* 库存的资产应有责任人
A.8.1.3	资产的允许使用	*控制* 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.8.2 信息分类 目的：依照信息重要性分级，确保信息受到分级保护		
A.8.2.1	信息的分类	*控制* 信息应依照其对组织的价值，法律要求，敏感性和关键性分类
A.8.2.2	信息的标记	*控制* 根据组织采用的信息分类方案，应制定并实施一套信息标记流程
A.8.2.3	资产的处理	*控制* 根据组织采用的信息分类方法，应制定并实施一套资产处理流程
A.8.2.4	资产的归还	*控制* 所有员工、外部方用户在合同终止或协议终止后应归还组织的资产
A.8.3 介质处理 目的：为了防止存储在介质上的信息被未经授权的披露，修改，删除或破坏		

A.8.3.1	可移动介质的管理	*控制* 根据组织采用的分类方法来执行可移动介质管理流程
A.8.3.2	介质的处置	*控制* 不再需要的介质，应使用正式的规程可靠并安全地处置
A.8.3.3	物理介质传输	*控制* 在传输过程中，包含信息的介质应加以保护，防止未经授权的访问，滥用或损坏
A.9 访问控制		
A.9.1 访问控制的业务要求 目的：限制访问信息和信息处理设施		
A.9.1.1	访问控制策略	*控制* 应建立一个访问控制策略，并基于业务和访问的安全要求进行评审
A.9.1.2	网络服务的使用政策	*控制* 只提供用户已授权的网络访问与网络服务
A.9.2 用户访问管理 目的：确保授权用户访问系统和服务，并防止未授权的访问		
A.9.2.1	用户注册和注销	*控制* 应为所有系统和服务中所有用户类型的授权和撤销建立一套注册与注销的流程
A.9.2.2	特权管理	*控制* 应限制和控制特殊权限的分配及使用
A.9.2.3	用户秘密认证信息的管理	*控制* 应使用正式的管理流程来控制秘密认证信息的分配
A.9.2.4	用户访问权的复查	*控制* 资产所有者应当定期审查用户的访问权限
A.9.2.5	移除或调整访问权限	*控制* 当合同或协议终止后，应删除或调整所有工作人员和外部人员用户信息和信息处理设施的访问权限
A.9.3 用户职责		

目的：让用户明确身份认证信息的保护负责		
A.9.3.1	秘密认证信息的使用	*控制* 应要求用户按照组织安全实践来使用秘密认证信息
A.9.4 系统和应用程序的访问控制 目的：防止对系统和应用的未授权使用		
A.9.4.1	信息访问限制	*控制* 应依据访问控制策略来限制对信息和应用系统功能的访问
A.9.4.2	安全登录程序	*控制* 如果访问控制策略需要，应通过安全登录程序控制对操作系统的访问
A.9.4.3	口令管理系统	*控制* 口令管理系统应采用交互式口令并确保口令质量
A.9.4.4	特权实用程序的使用	*控制* 对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.9.4.5	程序源码的访问控制	*控制* 对程序源代码的访问应被限制
A.10 密码学		
A.10.1 密码控制 目的：使用密码适当有效的保护信息的机密性、真实性和完整性		
A.10.1.1	密码使用控制政策	*控制* 应制定和实施信息保护密码控制策略
A.10.1.2	密钥管理	*控制* 应制定和实施密钥的使用，保护，使用期策略并贯穿其整个生命周期
A.11 物理和环境安全		
A.11.1 安全区域 目的：阻止对组织场所和信息的未授权屋里访问、损坏和干扰		
A.11.1.1	物理安全边界	*控制* 应设置安全边界来保护包含敏感信息，危险信息和信息处理设施的安

		全
A.11.1.2	物理入口控制	*控制* 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.11.1.3	办公室，房间和设施的安全保护	*控制* 应为办公室、房间和设施设计并采取物理安全措施
A.11.1.4	外部和环境威胁的安全防护	*控制* 应设计并采取物理安全措施来防范自然灾害，恶意攻击或事故
A.11.1.5	在安全区域工作	*控制* 应设计和应用用于安全区域工作的物理保护措施和指南
A.11.1.6	交付和交接区	*控制* 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.11.2 设备 目的：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.11.2.1	设备安置和保护	*控制* 应妥善安置及保护设备，以减少来自环境的威胁与危害以及未经授权的访问
A.11.2.2	支持性设备	*控制* 应保护设备使其免于支持性设施的失效而引起的电源故障和其他中断
A.11.2.3	布缆安全	*控制* 应保护传输数据或支持信息服务的电力及通讯电缆，免遭拦截或破坏
A.11.2.4	设备维护	*控制* 设备应予以正确地保护，以确保其持续的可用性的完整性
A.11.2.5	资产的移动	*控制* 设备、信息或软件在授权之前不应带出组织
A.11.2.6	场外设备和资产安全	*控制* 应对组织场所外的资产采取安全措施，要考虑工作在组织场所外的不同风险

A.11.2.7	设备的安全处置或再利用	*控制* 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.11.2.8	无人值守的用户设备	*控制* 用户应确保无人值守的用户设备有适当的保护
A.11.2.9	清除桌面和清屏策略	*控制* 应采取清空桌面上的文件、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.12 操作安全		
A.12.1 操作程序和职责 目的：确保正确、安全的操作信息处理设施		
A.12.1.1	文件化的操作程序	*控制* 操作过程应形成文件，并提供给所有需要的用户
A.12.1.2	变更管理	*控制* 对组织，业务流程，信息处理设施和系统的变更应加以控制
A.12.1.3	容量管理	*控制* 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.12.1.4	开发，测试和运行环境的分离	*控制* 开发及测试环境应与运营环境分离。减少未授权访问和对操作系统变更的风险
A.12.2 恶意软件防护 目的：确保信息和信息处理设施不受恶意软件侵害		
A.12.2.1	控制恶意软件	*控制* 应实现结合适当的用户体验，使用检测、预防和恢复控制的手段来防范恶意软件
A.12.3 备份 目的：防止数据丢失		
A.12.3.1	信息备份	*控制* 根据既定的备份策略备份信息，软件和系统映象，并定期测试

A.12.4 记录和监控 目的：记录事件并生成证据		
A.12.4.1	事件日志	*控制* 应产生记录用户活动、异常情况、错误和信息安全事件的事件日志，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.12.4.2	日志信息的保护	*控制* 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.12.4.3	管理员和操作员日志	*控制* 系统管理员和系统操作员的活动应当记录日志，并对其保护和定期检讨
A.12.4.4	时钟同步	*控制* 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的时间源进行同步
A.12.5 操作软件的控制 目的：保证操作系统的完整性		
A.12.5.1	操作系统软件的安装	*控制* 应建立流程对操作系统软件安装进行控制
A.12.6 技术漏洞管理 目的：防止利用公布的技术脆弱性导致的风险		
A.12.6.1	技术漏洞的管理	*控制* 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风险
A.12.6.2	限制软件安装	*控制* 应建立规则来控制用户安装软件
A.12.7 信息系统审计考虑 目的：将业务系统审计过程的影响最小化		
A.12.7.1	信息系统审计控制	*控制* 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.13 通信安全		

A.13.1 网络安全管理 目的：确保网络中信息的安全性并保护支持性的信息处理设施		
A.13.1.1	网络控制	*控制* 应管理和控制网络以保护系统和应用程序中的信息
A.13.1.2	网络服务的安全	*控制* 所有网络服务的安全机制，服务水平和管理要求，应予以明确并列入网络服务协议中，无论这些服务是否由公司内部提供还是外包
A.13.1.3	网络隔离	*控制* 应在网络中隔离信息服务、用户及系统信息
A.13.2 信息传输 目的：维护组织与任何外部实体的信息传输安全		
A.13.2.1	信息传输的策略和程序	*控制* 应建立正式的传输策略，流程和控制措施，以保证所有类型的通信设施间的信息传输安全
A.13.2.2	信息传输协议	*控制* 应建立组织与外部方传输商业信息的安全传输协议
A.13.2.3	电子消息	*控制* 涉及电子消息的信息应适当保护
A.13.2.4	保密或不泄露协议	*控制* 应确定组织信息保护需要的保密性或不泄露协议的要求，定期审查并记录
A.14 系统获取，开发和维护		
A.14.1 信息系统的安全要求 目的：确保安全是信息系统生命周期中的一个组成部分，包括对向公共网络提供服务的设备的特殊要求		
A.14.1.1	安全需求分析和规范	*控制* 应建立对信息安全控制的要求，包括财务报表和新的信息系统或现有信息系统增强的技术要求，同时考虑所有相关的标准，如生命周期或应用程序在公共网络上是否可用
A.14.1.2	保护公共网络上的	*控制*

	应用服务	公网上应用服务中传输的信息应被保护，以免遭受欺诈、合同纠纷，未经授权的披露和修改
A.14.1.3	保护应用服务交易	*控制* 应用服务传输中所涉及到的信息应加以保护，以防止未经授权的消息改变，不完整的传输，路由错误，未授权披露，未经授权的消息复制或重放
A.14.2 开发和支持过程中的安全 目的：确保在整个信息系统生命周期中的信息安全设计与实施		
A.14.2.1	安全开发策略	*控制* 应制定及应用关于软件和系统的开发规则
A.14.2.2	变更控制程序	*控制* 应使用正式的变更控制规程来控制变更的实施
A.14.2.3	操作平台变更后对应用的技术评估	*控制* 当操作平台发生变更时，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.14.2.4	软件包变更的限制	*控制* 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控制
A.14.2.5	系统开发程序	*控制* 应建立安全系统开发流程，记录，维护并应用到任何信息系统开发工作
A.14.2.6	安全的开发环境	*控制* 组织应建立并适当保护开发环境安全，并集成涵盖整个系统开发周期的工作
A.14.2.7	外包开发	*控制* 组织应监管和监督外包的系统开发工作
A.14.2.8	系统安全性测试	*控制* 在开发的过程中，必须测试功能的安全性
A.14.2.9	系统验收测试	*控制* 在建立新系统，升级系统和更新版本时，必须建立验收测试程序和相关标准

A.14.3 测试数据 目的：确保测试数据的安全		
A.14.3.1	测试数据的保护	*控制* 测试数据应被仔细筛选，保护和控制
A.15 供应关系		
A.15.1 供应关系的安全 目的：确保供应商访问的组织信息的安全		
A.15.1.1	供应关系的信息安全策略	*控制* 对于减小与供应商相关的信息安全风险或信息处理设施的信息安全要求应被记录
A. 15.1.2	供应商协议中的安全	*控制* 应建立与信息安全相关的要求并获得供应商的认可，包括处理，存储，沟通或提供组织 IT 基础设施的信息
A.15.1.3	ICT 供应链	*控制* 与供应商的协议应包括解决信息、通信技术服务、产品供应链相关信息安全风险的要求
A.15.2 供应商服务交付管理 目的：维持与供应商协议中商定的信息安全要求和服务交付水平		
A.15.2.1	监测和审查供应商服务	*控制* 组织应定期监测，审查和审核供应商的服务
A.15.2.2	供应商服务变更管理	*控制* 应管理供应商提供服务的变更,包括维护、改进现有的信息安全策略、程序和控制，应将商业信息的关键性，系统、流程和风险的重新评估考虑在内
A.16 信息安全事件管理		
A.16.1 信息安全事件管理和持续改进 目的：确保一致和有效的方法来管理信息安全事件，包括通信安全事件和弱点的报告		
A.16.1.1	职责和程序	*控制* 应建立管理职责和程序，以确保快速、有效和有序地响应信息安全事件

A.16.1.2	报告信息安全事态	*控制* 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.16.1.3	报告信息安全弱点	*控制* 应要求信息系统和服务的所有员工、外部方人员记录并报告他们观察到的或可以的任何系统或服务的安全弱点
A.16.1.4	信息安全事件的评估和决策	*控制* 信息安全事件应当被评估与决策，如果他们被归类为信息安全事件
A.16.1.5	信息安全事故的响应	*控制* 信息安全事件应依照程序文件响应
A.16.1.6	回顾信息安全事故	*控制* 从分析和解决信息安全事故中获取知识，减少未来事故的可能性或影响
A.16.1.7	收集证据	*控制* 组织应制定和应用程序，用于鉴定，收集，获得和保存那些可作为证据的信息
A.17 信息安全方面的业务连续性管理		
A.17.1 信息安全连续性 目的：信息安全的连续性应嵌入组织的业务连续性管理（BCM），以确保任何时间都能保护信息并对不良事件进行预测		
A.17.1.1	规划信息安全连续性	*控制* 组织应确定其在不利情况下的信息安全和信息安全管理连续性要求，如危机或灾难
A.17.1.2	实现信息安全的连续性	*控制* 组织应建立，记录，实施，维护流程、程序、控制项，以保证在不利情况下要求的信息安全连续性的等级
A.17.1.3	验证，评审和评估信息安全的连续性	*控制* 组织应每隔一段时间核实其建立和实施的信息安全连续性控制，以确保他们在不利情况下是有效和生效的。
A.17.2 冗余 目的：确保信息处理设施的可用性		

A.17.2.1	信息处理设施的可用性	*控制* 信息处理设施应当实现冗余，以满足可用性需求
A.18 符合性		
A.18.1 信息安全审查 目的：确保信息安全设施依照组织的策略和程序运行和实施		
A.18.1.1	信息安全的独立审查	*控制* 组织管理信息安全的方法及实施（例如信息安全的控制目标、控制措施、策略、过程和规程）应按照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.18.1.2	符合安全政策和标准	*控制* 管理者应定期审查其职责范围内的信息处理和规程被正确的执行，以确保符合安全策略、标准和其他安全要求
A.18.1.3	技术符合性检查	*控制* 信息系统应被定期检查是否符合组织信息安全策略和标准
A.18.2 符合法律和合同的要求 目的：避免违反相关信息安全的法律，法规，规章，合同义务以及任何安全要求		
A.18.2.1	识别使用的法律和合同的要求	*控制* 对每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取的方法，应加以明确地定义，形成文件并保持更新
A.18.2.2	知识产权（IPR）	*控制* 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、法规和合同要求
A.18.2.3	文档化信息的保护	*控制* 按照法律，法规，合同和业务需求保护文档化信息，以免遭受损失，破坏，篡改，未经授权的访问和擅自发布
A.18.2.4	隐私和个人信息的保护	*控制* 应依照相关的法律、法规和合同条款的要求，确保隐私和个人信息的保护
A.18.2.5	密码控制措施的监管	*控制* 使用密码控制措施应遵从相关的协议、法律和法规