ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22080-2016/ISO/IEC 27001:2013

代替 GB/T 22080-2008

信息技术 安全技术

信息安全管理体系

Information technology — Security techniques —

Information security management systems — Requirements

2017-03-01 实施

2016-08-29 发布

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

前言

引　言

0.1 总则

[illegible]

0.2 与其他管理体系标准的兼容性

[illegible]

信息技术 安全技术 信息安全管理体系 要求

1 范围

2 规范性引用文件

3 术语和定义

4 组织环境

4.1 理解组织及其环境

4.2 理解相关方的需求和期望

4.3 确定信息安全管理体系范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

4.4 信息安全管理体系

组织应按照本标准的要求，建立、实现、维护和持续改进信息安全管理体系。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实对信息安全管理体系的

a) 确保信息安全方针和信息安全目标的建立，并与组织战略方向一致；

b) 确保将信息安全管理体系要求整合到组织过程中；

c) 确保可获得资源用于信息安全管理体系；

d) 沟通有效的信息安全管理及符合信息安全管理体系要求的重要性；

e) 确保信息安全管理体系达到预期结果；

f) 指导并支持人员对信息安全管理体系的有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色，证实其领导力应用于职责范围内如何被实现。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

a) 与组织宗旨相适应；

b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c) 包括对满足适用的信息安全相关要求的承诺；

d) 包括对持续改进信息安全管理体系的承诺。

信息安全方针应：

e) 形成文件化信息并可用；

f) 在组织内得到沟通；

g) 适当时，对相关方可用。

5.3 组织的角色，责任和权限

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通。

最高管理层应分配责任和权限，以：

a) 确保信息安全管理体系符合本标准的要求；

b) 向最高管理层报告信息安全管理体系绩效。

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

在规划信息安全管理体系时，组织应考虑到4.1中提及的因素和4.2中提及的要求，并确定需要应对的风险和机会，以

注：[illegible]

6.2 信息安全目标及其实现规划

组织应在相关职能和层次上建立信息安全目标。

信息安全目标应：

a) 与信息安全方针一致；
b) 可测量（如可行）；
c) 考虑适用的信息安全要求以及风险评估和风险处置的结果；
d) 得到沟通；
e) 适当时更新。

组织应保留有关信息安全目标的文件化信息。

在规划如何达到信息安全目标时，组织应确定：

f) 要做什么；
g) 需要什么资源；
h) 由谁负责；
i) 什么时候完成；
j) 如何评价结果。

7 支持

7.1 资源

组织应确定并提供建立、实现、维护和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应：

a) 确定在组织控制下从事会影响组织信息安全绩效的工作人员的必要能力；
b) 确保这些人员在适当的教育、培训或经验的基础上能够胜任其工作；
c) 适用时，采取措施以获取必要的能力，并评价所采取措施的有效性；
d) 保留适当的文件化信息作为能力的证据。

注：[illegible]

7.3 意识

在组织控制下工作的人员应了解：

a) 信息安全方针；
b) 其对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；
c) 不符合信息安全管理体系要求的后果。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部沟通的需求，包括：

a) 沟通什么；
b) 何时沟通；

c) 与谁沟通；

d) 谁来沟通；

e) 影响沟通的过程。

7.5 文件化信息

7.5.1 总则

7.5.2 创建和更新

7.5.3 文件化信息的控制

8 运行

8.1 运行规划和控制

8.2 信息安全风险评估

8.3 信息安全风险处置

组织应实现信息安全风险处置

9 绩效评价

9.1 监视、测量、分析和评价

组织应评价信息安全绩效以及信息安全管理体系的有效性。

9.2 内部审核

组织应按计划的

a) 对发现的不符合采取适当的纠正措施，且与不符合的影响相适应；

b) 评审不符合的原因，并确定是否存在或可能发生类似的不符合；

c) 确定和实施所需的纠正措施；

d) 评审所采取的纠正措施的有效性；

e) 如有必要，更新在策划期间确定的风险和机会；

f) 如有必要，变更信息安全管理体系。

组织应保留文件化信息，作为不符合的性质及后续所采取措施的证据。

组织应保留文件化信息，作为纠正结果的证据。

附　录　A（规范性附录）
参考控制目的和控制

[redacted]

A.5.1.2	信息安全策略评审	*控制* 应按计划的时间间隔或者当有大变化发生时进行信息安全策略评审，以确保其持续的适宜性、充分性和有效性。

[redacted]

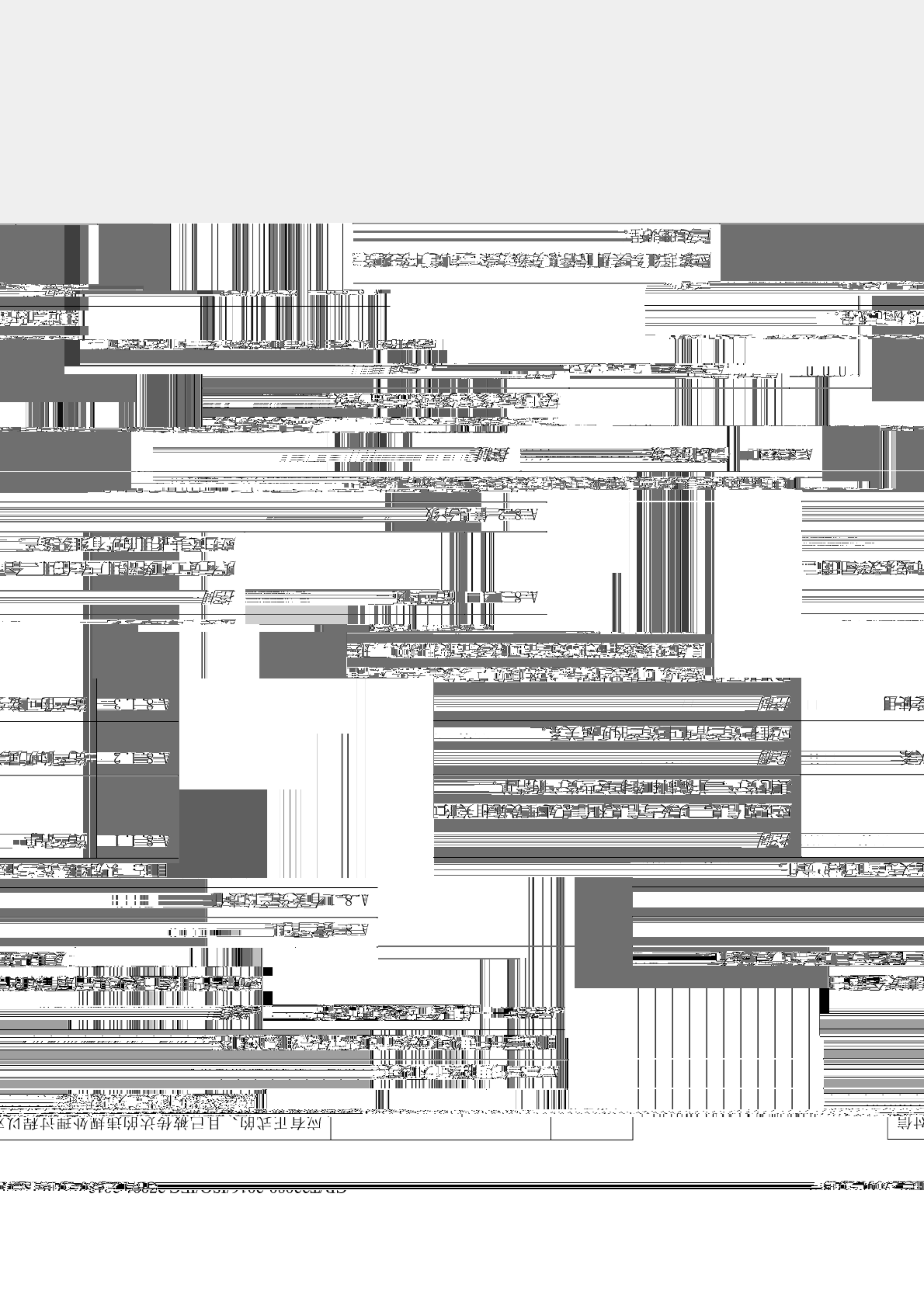
A.6.1.1	信息安全的角色和责任	*控制* 所有的信息安全责任应予以定义和分配。
A.6.1.2	职责分离	*控制*

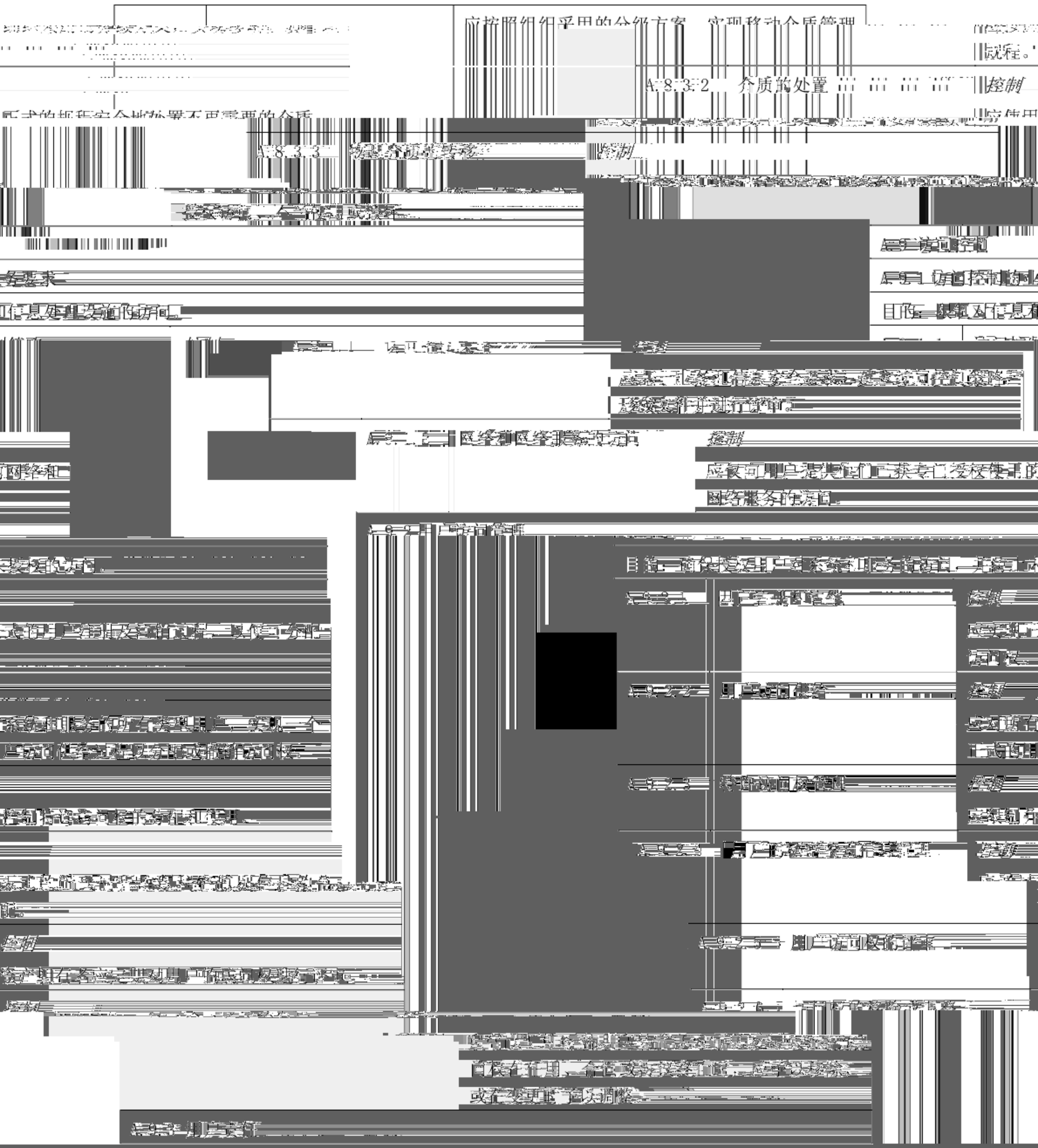
[redacted]

A.6.1.4	与特定相关方的联系	*控制*

A.6.2.1	移动设备策略	*控制*
A.6.2.2	远程工作	*控制*

A.7.2.1	管理责任	*控制*
A.7.2.2	信息安全意识、教育和培训	*控制*
A.7.2.3		





目的：让用户承担保护其鉴别信息的责任。		
A.9.3.1	秘密鉴别信息的使用	*控制* 应要求用户遵循组织在使用秘密鉴别信息时的规则。

目的：防止对系统和应用的未授权访问。		
A.9.4.1	信息访问限制	*控制* 应按照访问控制策略限制对信息和应用系统功能的访问。
A.9.4.2	安全登录规程	*控制* 当访问控制策略要求时，应通过安全登录规程来控制对系统和应用的访问。
A.9.4.3	口令管理系统	*控制* 口令管理系统应是交互式的，并应确保优质的口令。
A.9.4.4	特权实用程序的使用	*控制*
A.9.4.5	程序源代码的访问控制	*控制*

A.10 密码		
A.10.1 密码控制		
目的：确保适当和有效地使用密码技术以保护信息的保密性、真实性和（或）完整性。		
A.10.1.1	密码控制使用规则	*控制*
A.10.1.2	密钥管理	*控制*

A.11 物理和环境安全		
A.11.1 安全区域		
目的：防止对组织信息和信息处理设施的未授权物理访问、损坏和干扰。		
A.11.1.1	物理安全边界	*控制*

安全区域应由适合的入口控制所保护，以确保只

允许访问

目标	防止对组织信息和信息处理设施的未经授权的物理访问，以及设施的丢失、损坏、盗窃或危害。

A.11.1.1 物理安全边界

控制

应定义并使用边界（例如墙、卡控入口、有人值守的接待处）来保护包含信息和信息处理设施的区域。

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，以确保只允许经过授权的人员访问。

A.11.1.3 办公室、房间和设施的安全

控制

为办公室、房间和设施设计并应用物理安全措施。

A.11.1.4 外部和环境威胁的安全防护

控制

应设计并应用物理保护措施，以防自然灾害、恶意攻击或意外事故。

A.11.1.5 在安全区域工作

控制

应设计和应用安全区域工作规程。

A.11.1.6 交接区

控制

访问点（例如交接区）和未授权人员可进入的其

A.11.2 设备

目的：防止资产的丢失、损坏、失窃或危害，防止

A.11.2.1 设备安置和保护

控制

A.11.2.2 支持性设施

控制

A.11.2.3 布缆安全

控制

		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活动应记入日志，并对日志进行保护和定期评审。
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系统的时钟应与单一基准时间源保持同步。
A.12.5 运行软件控制		
目标：确保运行系统的完整性。		
A.12.5.1	运行系统的软件安装	*控制* 应实现运行系统软件安装控制规程。
A.12.6 技术脆弱性管理		
目标：防止对技术脆弱性的利用。		
A.12.6.1	技术脆弱性的管理	*控制* 应及时获取在用的信息系统的技术脆弱性信息，评价组织对这些脆弱性的暴露状况，并采取适当的措施来处理相关的风险。
A.12.6.2	软件安装限制	*控制* 应建立并实现控制用户安装软件的规则。
A.12.7 信息系统审计考虑		
目标：使审计活动对运行系统的影响最小化。		
A.12.7.1	信息系统审计控制	*控制* 涉及对运行系统验证的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化对业务过程的中断。
A.13 通信安全		
A.13.1 网络安全管理		
目标：确保网络中的信息及其支持性的信息处理设施得到保护。		
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、服务级别和管理要求应予以确定并包括在网络服务协议中，无论这些服务是由内部提供的还是外包的。
A.13.1.3	网络中的隔离	*控制* 应在网络中隔离信息服务、用户及信息系统。

A.13.2 信息传输

A.13.2.1 信息传输策略和规程

控制

应有正式的传输策略、规程和控制，以保护通过使用各种类型通信设施进行的信息传输。

A.13.2.2 信息传输协议

控制

的商定级别。

A.15.2 供应商服务交付管理

目的：维护与供应商协议一致的信息安全和服务交付

A.17.1.1	规划信息安全连续性	*控制* 组织应确定在不利情况（如危机或灾难）下，对信息安全及信息安全管理连续性的要求。
A.17.1.2	实现信息安全连续性	*控制*

		法规。
A.18.2 信息安全评审		
目的：确保依据组织策略和规程来实现和运行信息安全。		
A.18.2.1 信息安全的独立评审	*控制*	应按计划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实现（安全的控制目标、控制、方针、过程和规程）进行独立评审。
A.18.2.2 符合安全策略和标准	*控制*	管理者应定期评审信息处理和程序符合适用的安全策略、标准和任何其他的安全要求。
A.18.2.3 技术符合性评审	*控制*	应定期评审信息系统与组织的信息安全策略和标准的符合性。

参 考 文 献

[1] ISO/IEC 27002:2013, 信息技术 安全技术 信息安全控制实用规则

[2] ISO/IEC 27003:2010, 信息技术 安全技术 信息安全管理体系实施指南

[3] ISO/IEC 27004:2009, 信息技术 安全技术 信息安全管理 测量

[4] ISO/IEC 27005:2011, 信息技术 安全技术 信息安全风险管理

[5] ISO/IEC 导则, 第1部分: ISO补充规定 ISO单体机构工作导则, 2012