国际标准 ISO/IEC 27001

第二版
2013-10-01

中文翻译版
REV4
老李飞刀

信息技术——安全技术——信息安全管理体系——要求

参考号
ISO/IEC 27001:2013（E）

目录

■ 翻译说明

继ISO/IEC 27000系列标准于2005年发布之后，经过漫长的8年，终于等来了ISO27001第二版。相比第一个版本，ISO27001:2013有了很大改进，值得学习和应用。（2013版的具体改进及变化的分析参见老李的《ISO27001:2013 信息安全管理国标新版解读精要》。

写此文时坊间已有标准的数个中文译本，多是出于个别安全公司或咨询公司手笔，但笔者阅读后发现这些译本错漏较多，想到这可能误导广大标准学习的后来者，不利祖国的信息安全建设，老李不禁忧心忡忡。为了便于国内读者的学习和使用正规的标准，笔者2014春节期间翻译了本中文版本。笔者虽实操标准多年，但深知学无止境，追求完美不易。如有错漏，欢迎各位安全界同仁不吝指正。

译者：

老李飞刀，邮箱：46040336@qq.com。老李近期研究方向为新版ISO27000标准族、体系一体化整合、安全管理平台化。有同好者可加本人微信46040336或进群210674629共同探讨。

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

0 介绍

0.1 总则

本国际标准为组织建立、实施、维护和持续改进信息安全管理体系（ISMS）提出相关要求。采用ISMS是组织的一项战略决策。组织ISMS的设计和实施受组织的战略决策、组织需求、目标、安全需求以及工作流程和组织规模等因素的影响。上述因素会随着时间不断发生变化。

信息安全管理体系通过实施风险管理过程来保护组织信息的机密性、完整性和可用性，对风险进行充分的管理并为相关方带去信心。

信息安全管理体系是组织整体管理架构和管理流程的组成部分。组织在进行流程、信息系统、控制措施设计过程中均应考虑信息安全。

本国际标准可以用于内部或外部机构用于对组织的信息安全管理能力进行评估以确认其是否满足组织自身的信息安全需求。

本标准附录中列举的控制措施的先后顺序不代表其重要程度或实施的先后顺序要求。列表编号顺序只做参考用途。

ISO/IEC 27000描述了信息安全管理体系的综述和术语，参考了信息安全管理体系标准族（包括ISO/IEC 27003W, ISO/IEC 27004[3] 和 ISO/IEC 27005[4])的相关名词解释和定义。

0.2 与其他管理体系的兼容性

本国际标准采用了标准化的ISO Annex SL通用架构，采用此架构的好处在于将各标准的要求以统一的架构进行描述。保持了与其他管理体系的兼容性，有利于不同管理体系进行接轨和整合。

1 范围

本国际标准明确了在组织内部建立、实施、维护和持续改进信息安全管理体系的要求。本国际标准还包括了组织进行评估和处置信息安全风险的要求。在本国际标准中规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织宣布符合本国际标准，对于4到10章节的任何条款的删减是不可接受的。

2 规范性引用文件

下面是本标准的规范性引用文件。凡注明日期的引用文件，仅该引用的版本适用。没有注明日期的引用文件，则引用文件的最新版本（包括任何修订后的版本）适用。

ISO/IEC 27000，信息技术-安全技术-信息安全管理体系概述和术语

3 术语与定义

ISO/IEC 27000中的术语与定义适用于本标准。

4 组织环境

4.1 理解组织及其环境

组织应确定与其总体目标相关的内部和外部环境因素，相关因素将影响其实现信息安全管理体系的预期成果。

注： 确定相关因素可参考ISO 31000:2009［5］5.3“环境的建立”。

4.2 理解相关方的需求和期望

组织应确定：

a) 与信息安全管理体系有关的利益相关方；

b) 相关方的信息安全需求。

注 ： 相关方的要求包括法律法规要求和合同规定的义务。

4.2 明确信息安全管理体系的范围

组织应明确信息安全管理体系的边界和适用性，以确定其范围。

确定范围时，组织应考虑：

a）与在4.1章节中有关的内部、外部问题；

b）与在4.2章节中提及的需求；

c）组织自身活动和与其他组织开展活动的接口和依赖关系；

范围的相关内容应形成文档。

4.3 信息安全管理体系

组织应按照本国际标准要求建立、实施、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行动证明其实施了与信息安全管理体系有关的领导工作与承诺：

a) 确保建立与组织战略目标一致的信息安全方针和信息安全目标；

b) 确保信息安全管理体系要求集成到组织的管理流程；

c) 确保提供信息安全管理体系需要的各项资源；

d) 传达信息安全管理的重要性及信息安全管理体系要求；

e) 确保信息安全管理体系实现其预期目标；

f) 指导和支持信息安全团队；

g) 促使持续改进；

h) 支持其他相关的管理者在其职责范围内履行管理职责。

5.2 方针

最高管理层应建立的信息安全方针：

a）应适合组织的目标；

b）应包括信息安全目标（见6.2）或者提供建立信息安全目标的框架；

c）应包括承诺满足信息安全的相关要求；

d）应包括承诺持续改进信息安全管理体系。

信息安全管理方针应：

e）形成文档；

f）在组织内部充分沟通；

g）需要时对外部相关方可用。

5.3 组织角色、职责和权力

最高管理层应确保信息安全管理角色和权力得到分配和沟通。

最高管理层应对以下职责和权力进行分派：

a) 确保组织建立的信息安全管理体系符合本国际标准要求；

b) 向高层汇报信息安全管理体系的执行情况。

注： 最高管理层也应被赋予相应的职责和权力，向组织内部汇报信息安全管理体系的执行情况。

6 计划

6.1 处置风险和机遇

6.1.1总则

当进行信息安全管理体系规划时，组织应参考4.1中的问题和4.2中的需求，来决定需要被处置的风险和机遇：

a) 确保信息安全管理体系可以实现其预期目标；

b) 避免或减少不良影响；

c) 实现持续改进。

组织应规划：

d) 处置风险和机遇的行动；

e) 如何

1) 将实施行动整合到信息安全管理体系流程中；

2) 评价行动的有效性。

6.1.2信息安全风险评估

组织应定义和实施信息安全风险评估流程，从而：

a) 建立和维护信息安全风险标准，包括：

1) 风险接受标准；

2) 实施信息安全风险评估的标准；

b) 确保信息安全风险评估活动产生一致性，产生有效的和可比较的结果；

c) 识别信息安全风险：

1) 在信息安全管理体系范围内，通过信息安全风险评估流程，识别由于信息的机密性、完整性和可用性的丧失带来的风险；

2) 识别风险的属主；

d) 分析信息安全风险：

1) 评估在6.1.2 c）1）中识别的风险产生的潜在后果；

2) 评估在6.1.2 c）1）中识别的风险转化为事件的可能性；

3) 确定风险的等级；

e) 评价信息安全风险：

1) 将风险分析结果与在6.1.2 a）中所定义的风险标准进行比较；

2) 根据风险等级确定风险处置的优先级。

组织应保留有关信息安全风险评估的过程文档。

6.1.3 信息安全风险处置

组织应定义和实施信息安全风险处置过程：

a) 依据风险评估的结论，选择适当的信息安全风险处置方式；

b) 确定信息安全风险处置选用的各项控制措施；

注： 组织可以根据标准要求来设计控制措施，也可以从其他来源中识别。

c) 比较6.1.3 b）中的和附录A的控制措施，确保必要的控制措施未被遗漏；

注1： 附录A包括了全面的控制对象和控制措施的列表，使用本标准的用户可以直接使用附录A的内容，并确保必要的控制措施未被忽略。

注2：控制目标隐含在选择的控制措施中。附录A中的控制对象和控制措施并非详尽的列表，必要时可选用额外的控制目标和控制措施。

d) 制定包含必需控制措施和原因（见6.1.3 b）和c））的适用性声明（SOA），包括说明对附录A中的控制措施删减的理由；

e) 制定信息安全风险处置计划；

f) 风险处置计划和残余风险接受应得到风险属主的审批。

组织应保留信息安全风险处置的过程文档。

注：本标准中的信息安全风险评估和处置流程与ISO 31000[5]中的原则和通用指南保持一致。

6.2 信息安全目标的计划和实现

组织应建立不同职能及层级的信息安全目标。

信息安全目标应：

a) 与信息安全方针一致；

b) 可度量（如果可行）；

c) 考虑适用的信息安全要求, 以及风险评估和风险处置结果；

d) 得到传达；

e) 及时更新。

组织应将信息安全目标以文档化形式保留。

在规划如何实现信息安全目标时，组织应明确：

f) 要做什么；

g) 需要什么资源；

h) 谁来负责；

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、实施、维持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) 确定员工为完成其本职工作所所需的安全技能；

b）确保员工具备完成工作所需的教育、培训和经验；

c）采取合适的措施确保员工具备相应的技能并对技能进行考核；

d）保留适当的文档信息作为证据。

注：适当的措施可能包括，例如：提供培训、指导或重新分派现有员工，或雇用具备相关技能的人士。

7.3 意识

组织的员工应了解：

a）信息安全方针；

b）个人对于实现信息安全管理的重要性，提高组织信息安全绩效获得的收益；

c）不符合信息安全管理体系要求所造成的影响。

7.4 传达

组织应明确与信息安全管理体系相关的内、外部沟通需求，包括：

a）传达什么；

b）何时传达；

c）传达给谁；

d）谁来传达；

e）哪种沟通过程有效。

7.5 文档要求

7.5.1 综述

组织的信息安全管理体系应包括：

a）符合本国际标准的文件；

b）组织所明确的，表明信息安全管理体系有效性的必要的记录文档。

注：不同组织的信息安全管理体系的文档的复杂程度根据以下情况有所不同：

1）组织的规模、活动类型、过程、产品和服务；

2）过程的复杂程度及其相互作用。

3）人员能力

7.5.2 创建和更新

组织应明确何时创建和更新文档信息是适合的：

a）识别和描述（例如：标题、日期、作者和版本号）；

b）格式（例如：语言、软件版本和图形）与介质（例如：纸质、电子）；

c）适宜性和充分性经过评审。

7.5.3 文档控制

信息安全管理体系和本国际标准要求的存档信息应予以控制以确保：

a）在需要的时间和场合可用；

b）文档得到充分保护（例如：防止泄密、不当使用或丧失完整性）。

为做好文件控制，组织应明确以下文档控制活动的恰当执行：

c）分发、访问、收回和使用；

d）得到良好存储和保管，确保清晰易读；

e）变更控制（例如：版本控制）；

f）归档和处置。

明确组织进行信息安全管理体系规划和运行所必需的外部文档，并进行适当的标识和控制。

注：访问意味着允许查看文档信息，或经许可和授权对文档进行查看和修改。

8 实施

8.1 运行计划和控制

组织应计划、实施和控制相关过程以满足信息安全要求所需的过程。包括实施在6.1中决定采取的行动，按计划实现在6.2中所明确的信息安全目标。

组织应保留必要的过程文档信息，以表明相关过程已按照计划执行。

组织应控制计划更改，并审核计划变更的影响，如有必要采取措施减少不利影响。

组织应确保外包过程受控。

8.2 信息安全风险评估

组织应按照计划，或者在重大改变提出或发生时进行信息安全风险评估，并考虑6.1.2a）制

订的标准。

组织应将信息安全风险评估的结果作为文档信息保留。

8.3 信息安全风险处置

组织应执行风险处置计划。

组织应将信息安全风险处置的结果作为文档信息保留。

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管理体系的绩效。

组织应明确：

a) 包括信息安全过程和控制措施在内，应监控和测量什么；

b) 适用的监视、测量、分析和评价方法，以确保结果有效；

注：选用的方法应能产生可比较的和可重现的结果。

c) 何时实施监视和测量；

d) 谁负责监视和测量；

e) 何时分析和评价监视和测量的结果；

f) 谁应分析和评价这些结果。

组织应保留适当的文档信息作为监视和测量已开展的证据。

9.2 内部审核

组织应定期进行内部审核以表明信息安全管理体系是否：

a) 符合

1) 满足组织自身的信息安全管理要求；

2) 本国际标准的要求；

b) 有效的执行和保持。

组织应：

c) 规划、建立、执行和保持审核程序，包括频率、方法、责任、计划要求和报告。审核程

序应考虑组织所关注的重要过程和之前的审核结果；

d）定义审核准则和审核范围；

e）选择审核员并进行审核，确保审核过程的客观和公正；

f）确保审核结果报告给相关管理层；

g）组织应保留内部审核的过程文档作为证据。

9.3 管理评审

最高管理层应定期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。

管理评审应关注：

a）以往管理评审后所采取措施的状态；

b）内、外部信息安全管理体系相关环境的变化；

c）安全控制措施执行的反馈情况，包括如下趋势：

1）不符合情况和改正措施

2）监控和测量的结果；

3）审核结果；

4）信息安全目标实现情况；

d）相关方的反馈；

e）风险评估的结果和风险处置计划的状态；

f）持续改进的时机。

管理评审的输出应包括持续改进的时机和安全管理体系所需变更的决定。

组织应保留文档信息作为管理评审结果的证据。

10 改进

10.1 不符合项和纠正措施

当不符合情况项时，组织应：

a）对不符合情况采取措施，如：

1）采取措施，以控制和改正它；

2）处置影响；

b）明确必要的控制措施，以消除不符合情况产生的原因，确保它不会再发生或在其他地方

发生，通过：

1）评审不符合项；

2）明确不符合项产生的原因；

3）明确是否存在或可能发生类似的不符合项；

c）采取必要的措施；

d）评审已采取的改正措施的有效性；

e）必要时改进信息安全管理体系。

纠正措施应与所发生的不符合的影响程度相适应。

组织应保留以下文档信息作为证据：

f）不符合情况的性质和所采取的后续行动；

g）纠正措施的结果。

10.2 持续改进

组织应不断完善信息安全管理体系的适宜性、充分性和有效性。

附录 A

（引用）

参考控制目标和控制措施

表A.1列出的控制目标和控制措施直接引用了BS ISO/IEC 27002:2013[1] 中章节5至18的内容，这些选择控制目标和控制措施也可以被用于本文的6.1.3章节。

表A.1－控制目标和控制措施

A.5 信息安全方针		
A.5.1 信息安全管理指向		
目标：提供符合有关法律法规和业务需求的信息安全管理指引和支持。		
A.5.1.1	信息安全策略	应定义信息安全方针，信息安全方针文件应经过管理层批准，并向所有员工和相关方发布和传达。
A.5.1.2	信息安全策略的评审	应定期或在发生重大的变化时评审方针文件，确保方针的持续性、稳定性、充分性和有效性。
A.6 信息安全组织		
A.6.1 内部组织		
目标：应在组织内建立信息安全管理架构以启动和控制信息安全的实施。		
A.6.1.1	信息安全的角色和职责	应全面定义和分配信息安全职责。
A.6.1.2	职责分离	有冲突的职责和责任范围应加以分离，以减少对组织资产未经授权访问、无意修改或误用的机会。
A.6.1.3	与政府部门的联系	应与相关的政府部门保持适当联系。
A.6.1.4	与特定利益团体的联系	与特定利益团体、其他安全论坛或专业协会应保持适当联系。
A.6.1.5	项目管理中的信息安全	实施任何项目时应考虑信息安全相关要求。
A.6.2 移动设备和远程办公		
目标：应确保远程办公和使用移动设备的安全性。		
A.6.2.1	移动设备策略	应采取安全策略和配套的安全措施管控使用移动设备带来的风险。
A.6.2.2	远程办公	应实施安全策略和配套的安全措施以保障远程办公时信息的访问、处理和存储的安全。

A.7 人力资源安全		
A.7.1 任用前		
目标：确保员工、合同方人员适合他们所承担的角色并理解他们的安全责任。		
A.7.1.1	审查	根据相关法律、法规、道德规范，对所有应聘人员进行背景调查，调查应符合业务需求、所访问的信息类别及已知风险。
A.7.1.2	任用条款和条件	与员工和承包方的合同协议应当规定他们对组织的信息安全责任。
A.7.2 任用中		
目标：确保员工和合同方了解并履行他们的信息安全责任。		
A.7.2.1	管理职责	管理层应要求员工、合同方符合组织建立的信息安全策略和程序。
A.7.2.2	信息安全意识、教育与培训	组织内所有员工、相关合同人员及合同方人员应接受适当的安全意识培训，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	应建立并传达正式的惩戒程序，据此对违反安全策略的员工进行惩戒。
A.7.3 任用终止和变更		
目标：在任用变更或中止过程保护组织利益		
A.7.3.1	任用终止或变更的责任	应定义信息安全责任和义务在任用终止或变更后仍然有效，并向员工和合同方传达并执行。
A.8 资产管理		
A.8.1 资产的责任		
目标：识别组织资产并确定适当的保护责任。		
A.8.1.1	资产清单	应识别信息和信息处理设施的相关资产并制定和维护资产清单。
A.8.1.2	资产责任人	资产清单中应指定资产责任人。
A.8.1.3	资产的合理使用	应明确信息和信息处理设施相关资产的合理使用准则，形成文件并实施。
A.8.1.4	资产的归还	在劳动合同或协议终止后，所有员工和外部方人员应退还所有他们持有的组织资产。
A.8.2 信息分类		
目标：确保信息资产是按照其对组织的重要性受到适当级别的保护。		
A.8.2.1	信息分类	应根据法规、价值、重要性和敏感性对信息进行分类，保护信息免受未授权泄露或篡改。

A.8.2.2	信息标识	应制定和实施合适的信息标识程序,并与组织的信息分类方案相匹配。
A.8.2.3	资产处理	应根据组织采用的资产分类方法制定和实施资产处理程序
A.8.3 介质处理		
目标：防止存储在介质上的信息被非授权泄露、修改、删除或破坏。		
A.8.3.1	可移动介质管理	应实施移动介质的管理程序，并与组织的分类方案相匹配。
A.8.3.2	介质处置	当介质不再需要时，应按照正式程序进行可靠的、安全的处置。
A.8.3.3	物理介质传输	含有信息的介质应加以保护，防止未经授权的访问、滥用或在运输过程中的损坏。
A.9 访问控制		
A.9.1 访问控制的业务需求		
目标：限制对信息和信息处理设施的访问。		
A.9.1.1	访问控制策略	应建立文件化的访问控制策略，并根据业务和安全要求对策略进行评审。
A.9.1.2	对网络和网络服务的访问	应只允许用户访问被明确授权使用的网络和网络服务。
A.9.2 用户访问管理		
目标：确保已授权用户的访问，预防对系统和服务的非授权访问。		
A.9.2.1	用户注册和注销	应实施正式的用户注册和注销程序来分配访问权限。
A.9.2.2	用户访问权限提供	应有正式的用户访问分配程序，以分配和撤销对于所有信息系统及服务的访问。
A.9.2.3	特权管理	应限制及控制特权的分配及使用。
A.9.2.4	用户认证信息的安全管理	用户鉴别信息的权限分配应通过一个正式的管理过程进行安全控制。
A.9.2.5	用户访问权限的评审	资产所有者应定期审查用户访问权限。
A.9.2.6	撤销或调整访问权限	在跟所有员工和承包商人员的就业合同或协议终止和调整后，应相应得删除或调整其信息和信息处理设施的访问权限。
A.9.3 用户责任		
目标：确保用户对认证信息的保护负责。		
A.9.3.1	认证信息的使用	应要求用户遵循组织的规则使用其认证信息。

A.9.4 系统和应用访问控制		
目标：防止对系统和应用的未授权访问。		
A.9.4.1	信息访问限制	应基于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	安全登录程序	在需要进行访问控制时，应通过安全的登录程序，控制对系统和应用的访问。
A.9.4.3	密码管理系统	应使用交互式口令管理系统，确保口令质量。
A.9.4.4	特权程序的使用	对于可以超越系统和应用控制的工具程序应严格限制和控制使用。
A.9.4.5	对程序源码的访问控制	对程序源代码的访问应进行限制。
A.10 加密技术		
A.10.1 加密控制		
目标：确保适当和有效地使用加密技术来保护信息的机密性、真实性/完整性。		
A.10.1.1	使用加密控制的策略	应开发和实施加密控制措施的策略以保护信息。
A.10.1.2	密钥管理	应开发和实施一个贯穿密钥全生命周期的策略，对加密密钥的使用、保护和有效周期进行管理。
A.11 物理和环境安全		
A.11.1 安全区域		
目标：防止对组织信息和信息处理设施的未经授权物理访问、破坏和干扰。		
A.11.1.1	物理安全边界	应定义安全边界，用来保护包含敏感或关键信息和信息处理设施的区域。
A.11.1.2	物理进入控制	安全区域应有适当的进入控制保护，以确保只有授权人员可以进入。
A.11.1.3	办公室、房间及设施的安全	应设计和实施保护办公室、房间及设施的安全措施。
A.11.1.4	防范外部和环境威胁	应设计和应用物理保护措施以应对自然灾害、恶意攻击或意外。
A.11.1.5	在安全区域工作	应设计和应用在安全区域工作的程序。
A.11.1.6	送货和装卸区	访问区域如装卸区域，及其他未经授权人员可能进入的地点应加以控制，如果可能的话，信息处理设施应隔离以防止未授权的访问。
A.11.2 设备安全		
目标：防止资产的遗失、损坏、偷窃等导致的组织业务中断。		

A.11.2.1	设备安置及保护	应妥善安置及保护设备，以减少来自环境的威胁与危害，并减少未授权访问的机会。
A.11.2.2	支持设施	应保护设备免于电力中断及其它因支持设施失效导致的中断。
A.11.2.3	线缆安全	应保护传输数据或支持信息服务的电力及通讯电缆，免遭中断或破坏。
A.11.2.4	设备维护	应正确维护设备，以确保其持续的可用性及完整性。
A.11.2.5	资产转移	未经授权，不得将设备、信息及软件带离。
A.11.2.6	场外设备和资产安全	应对场外资产进行安全防护，考虑在组织边界之外工作的不同风险。
A.11.2.7	设备报废或重用	含有存储介质的所有设备在报废或重用前，应进行检查，确保任何敏感数据和授权软件被删除或被安全重写。
A.11.2.8	无人值守的设备	用户应确保无人值守的设备有适当的保护。
A.11.2.9	桌面清空及清屏策略	应采用清除桌面纸质和可移动存储介质的策略，以及清除信息处理设施屏幕的策略。
A.12 操作安全		
A.12.1 操作程序及职责		
目标：确保信息处理设施正确和安全的操作。		
A.12.1.1	文件化操作程序	操作程序应编制成文，并确保所有需要的用户可以获得。
A.12.1.2	变更管理	对组织、业务流程、信息处理设施和信息系统安全性有影响的变更应加以控制。
A.12.1.3	容量管理	应监控、调整资源的使用，并对未来容量的需求做预测以确保所需的系统性能。
A.12.1.4	开发、测试与运行环境的分离	应分离开发、测试和运行环境，以降低未授权访问或对运行环境变更的风险。
A.12.2 防范恶意软件		
目标：确保对信息和信息处理设施的保护，防止恶意软件。		
A.12.2.1	控制恶意软件	应实施检测、预防和恢复性控制以应对恶意软件，结合适当的用户意识教育。
A.12.3 备份		
目标：防止数据丢失		
A.12.3.1	数据备份	应按既定的备份策略备份信息，软件及系统镜像，并定期测试。
A.12.4 日志记录和监控		

目标：记录事件和生成的证据		
A.12.4.1	事件日志	应产生记录用户活动、意外和信息安全事件的日志，保留日志并定期评审。
A.12.4.2	日志信息保护	应保护日志设施和日志信息免受篡改和未授权访问。
A.12.4.3	管理员和操作者日志	应记录系统管理员和系统操作者的活动，进行日志保护及定期评审。
A.12.4.4	时钟同步	组织内或安全域内的所有相关联的信息处理系统的时钟应按照统一的参考时间源保持同步。
A.12.5 运营中软件控制		
目标：确保运营中系统的完整性。		
A.12.5.1	运营系统的软件安装	应建立程序对运营中的系统的软件安装进行控制。
A.12.6 技术漏洞管理		
目标：防止技术漏洞被利用。		
A.12.6.1	管理技术漏洞	应及时获得组织所使用的信息系统的技术漏洞的信息，对漏洞进行评估，并采取适当的措施去解决相关风险。
A.12.6.2	限制软件安装	应建立和实施用户软件安装规则。
A.12.7 信息系统审计的考虑因素		
目标：最小化审计活动对系统运营影响。		
A.12.7.1	信息系统审核控制	应谨慎策划对系统运行验证所涉及的审核要求和活动并获得许可，以最小化中断业务过程。
A.13 通信安全		
A.13.1 网络安全管理		
目标：确保网络及信息处理设施中信息的安全。		
A.13.1.1	网络控制	应对网络进行管理和控制，以保护系统和应用程序的信息。
A.13.1.2	网络服务安全	应识别所有网络服务的安全机制、服务等级和管理要求，并包括在网络服务协议中，无论这种服务是由内部提供的还是外包的。
A.13.1.3	网络隔离	应在网络中按组隔离信息服务、用户和信息系统。
A.13.2 信息传输		
目标：应确保信息在组织内部或与外部组织之间传输的安全。		

A.13.2.1	信息传输策略和程序	应建立正式的传输策略、程序和控制，以保护通过通讯设施传输的所有类型信息的安全。
A.13.2.2	信息传输协议	建立组织和外部各方之间的业务信息的安全传输协议。
A.13.2.3	电子消息	应适当保护电子消息的信息。
A.13.2.4	保密或不披露协议	应制定并定期评审组织的信息安全保密协议或不披露协议，该协议应反映织对信息保护的要求。
A.14 系统的获取、开发及维护		
A.14.1 信息系统安全需求		
目标：确保信息安全成为信息系统整个生命周期的组成部分，包括通过公共网络提供服务的信息系统的要求。		
A.14.1.1	信息安全需求分析和规范	新建信息系统或增强现有信息系统的需求中应包括信息安全相关的要求。
A.14.1.2	公共网络应用服务的安全	应保护流经公共网络的应用服务信息，以防止欺诈、合同争议、未授权的泄漏和修改。
A.14.1.3	保护在线交易	应保护应用服务传输中的信息，以防止不完整的传输、路由错误、未授权的消息修改、未经授权的泄漏、未授权的信息复制和重放。
A.14.2 开发和支持过程的安全		
目标：确保信息系统开发生命周期中设计和实施信息安全。		
A.14.2.1	开发的安全策略	应建立组织内部的软件和系统开发准则。
A.14.2.2	系统变更控制程序	应通过正式的变更控制程序，控制在开发生命周期中的系统变更。
A.14.2.3	操作平台变更后的技术评审	当操作平台发生变更后，应评审并测试关键业务系统，以确保变更不会对组织的运营或安全产生负面影响。
A.14.2.4	软件包变更限制	不鼓励对软件包进行变更，对必要的更改需严格控制。
A.14.2.5	安全系统工程原则	应建立、文件化、维护和应用安全系统工程原则，并应用于任何信息系统工程。
A.14.2.6	开发环境安全	在整个系统开发生命周期的系统开发和集成工作中，应建立并妥善保障开发环境的安全。
A.14.2.7	外包开发	组织应监督和监控系统外包开发的活动。
A.14.2.8	系统安全测试	在开发过程中，应进行安全性的测试。
A.14.2.9	系统验收测试	应建立新信息系统、系统升级及新版本的验收测试程序和相关准则。
A.14.3 测试数据		
目标：确保测试数据安全。		

A.14.3.1	测试数据的保护	应谨慎选择测试数据，并加以保护和控制。
A.15 供应商关系		
A.15.1 供应商关系的信息安全		
目标：确保组织被供应商访问的信息的安全。		
A.15.1.1	供应商关系的信息安全策略	为降低供应商使用组织的资产相关的风险，应与供应商签署安全要求的文件协议。
A.15.1.2	在供应商协议中强调安全	与每个供应商签订的协议中应覆盖所有相关的安全要求。如可能涉及对组织的 IT 基础设施组件、信息的访问、处理、存储、沟通。
A.15.1.3	信息和通信技术的供应链	供应商协议应包括信息、通信技术服务和产品供应链的相关信息安全风险。
A.15.2 供应商服务交付管理		
目标：保持符合供应商协议的信息安全和服务交付水平。		
A.15.2.1	供应商服务的监督和评审	组织应定期监、评审和审核供应商的服务交付。
A.15.2.2	供应商服务的变更管理	应管理供应商服务的变更，包括保持和改进现有信息安全策略、程序和控制措施，考虑对业务信息、系统、过程的关键性和风险的再评估。
A.16 信息安全事件管理		
A.16.1 信息安全事件的管理和改进		
目标：确保一致和有效的方法管理信息安全事件，包括对安全事件和弱点的沟通。		
A.16.1.1	职责和规程	应建立管理职责和规程，以确保快速、有效和有序的响应信息安全事件。
A.16.1.2	报告信息安全事态	应通过适当的管理途径尽快报告信息安全事态。
A.16.1.3	报告信息安全弱点	应要求使用组织信息系统和服务的员工和承包商注意并报告系统或服务中任何已发现或疑似的信息安全弱点。
A.16.1.4	评估和确定信息安全事态	应评估信息安全事态，以决定其是否被认定为信息安全事件。
A.16.1.5	信息安全事件响应	应按照文件化程序响应信息安全事故。
A.16.1.6	从信息安全事件中学习	分析和解决信息安全事件获得的知识应用来减少未来事件的可能性或影响。
A.16.1.7	证据收集	组织应定义和应用程序，识别、收集、采集和保存可以作为证据的信息。
A.17 业务连续性管理中的信息安全		
A.17.1 信息安全的连续性		

目标：信息安全连续性应嵌入到组织的业务连续性管理体系。		
A.17.1.1	规划信息安全的连续性	组织应确定其需求，以保证在不利情况下信息安全和安全管理的连续性，如在危机或灾难时。
A.17.1.2	实施信息安全的连续性	组织应建立、文件化、实施和维护规程和控制，以确保处理不利的情况过程中所需的信息安全连续性水平。
A.17.1.3	验证、评审和评价信息安全的连续性	组织应定期验证已建立并实施的信息安全连续性控制，以确保其有效并可在灾害情况下奏效。
A.17.2 冗余		
目标：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	信息处理设施应具备足够的冗余以满足可用性要求。
A.18 符合性		
A.18.1 符合法律和合同要求		
目标：避免违反有关信息安全的法律、法规、规章或合同要求以及任何安全要求。		
A.18.1.1	识别适用的法律法规和合同要求	应清楚的识别所有相关法律、法规与合同的要求及组织满足要求的方法并形成文件，并针对组织及每个信息系统进行更新。
A.18.1.2	知识产权	应实施适当的程序，以确保对知识产权软件产品的使用符合相关的法律、法规和合同要求。
A.18.1.3	保护记录	应按照法律法规、合同和业务要求，保护记录免受损坏、破坏、未授权访问和未授权发布，或伪造篡改。
A.18.1.4	个人信息和隐私的保护	个人身份信息和隐私的保护应满足相关法律法规的要求。
A.18.1.5	加密控制法规	加密控制的使用应遵循相关的协议、法律法规。
A.18.2 信息安全评审		
目标：确保依照组织的策略和程序实施信息安全。		
A.18.2.1	信息安全的独立评审	应定期或发生重大变化时，对组织的信息安全管理方法及其实施情况（如，信息安全控制目标、控制措施、策略、过程和程序）进行独立评审。
A.18.2.2	符合安全策略和标准	管理层应定期评审管辖范围内的信息处理过程符合安全策略、标准及其他安全要求。
A.18.2.3	技术符合性评审	应定期评审信息系统与组织的信息安全策略、标准的符合程度。

参考书目

[1] ISO/IEC 27002:2013, Information technology _ Security Techniques _ Code of practice for information security controls
[2] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance
[3] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement
[4] ISO/IEC 27005, Information technology—Security techniques—Information security risk management
[5] ISO 31000:2009, Risk management — Principles and guidelines
[6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement - Procedures specific to ISO, 2012
[7] ISO/IEC 27001-2013 信息安全管理国标新版解读精要(By 老李飞刀)