新版信息安全管理体系标准解析

中国信息安全认证中心

CHINA INFORMATION SECURITY
CERTIFICATION CENTER

www.isccc.gov.cn

中国信息安全认证中心江苏分中心　　陈多思

引言

信息安全管理体系标准（ISO27001：2005），自国际标准化组织（ISO）于2005年发布以来，已经使用8年。依据惯例，ISO组织每个5年左右将会对标准进行一次升级，在2013年10月19日，ISO组织正式发布了新版的信息安全管理体系标准（ISO27001：2013）。

本文目的在于为读者详细介绍ISO27001：2013的演变、价值、框架及内容解读，提供一条关于全面了解ISO27001：2013的途径，帮助大家顺利从2005版过渡到2013版。

内容声明

因为ISO组织并未发布关于本次ISO27001：2013版本官方的升级说明，所以下文中对ISO27001：2013版本的解析仅限于个人经验和理解，疏漏之处，欢迎有不同意见的读者来信指正。

作者在研究ISO27001：2013版过程中，与国内外多家著名信息安全咨询公司和咨询专家交流了对新版控制条款的看法和意见。本文的最终成稿还需感谢他们的帮助和支持。

作者邮箱：**chends@isccc.gov.cn**

ISO27001的起源和演变

1995年 英国标准协会(BSI)的BS7799标准《信息安全管理实施细则》

1999年 BSI修订BS7799，将BS7799分为2个部分:BS7799-1、BS7799-2

2000年 ISO根据BS7799-1制定了ISO/IEC17799-1

2005年 ISO根据修订后的BS7799-2制定了ISO27001:2005

2005年 ISO17799：2000升级为ISO27002：2005

2008年 ISO27001正式等同转化为国家标准GB/T 22080:2008

2013年10月 ISO组织正式发布ISO27001：2013版

至今　ISO27001：2013尚未转为为国家标准

改版影响

ISO组织规定，新版发布后18-24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。

国外目前已经不再颁发ISO27001：2005的证书了，但由于中国目前尚未发布与ISO27001：2013对应的国家标准，所以目前国内还是依据与ISO27001：2005对应的GB/T22080：2008来进行认证。对此，中国合格评定国家认可委员会（CNAS）规定：

“自**2014年9月1日至2015年7月31日**，CNAS将结合年度监督或复评的办公室评审，对已认可的ISMS认证机构实施转换评审。如有需要，认证机构也可向CNAS申请专项评审，以完成转换。自2015年8月1日以后，CNAS不再安排针对ISO/IEC 27001:2013转换的现场评审工作。”

新版特点

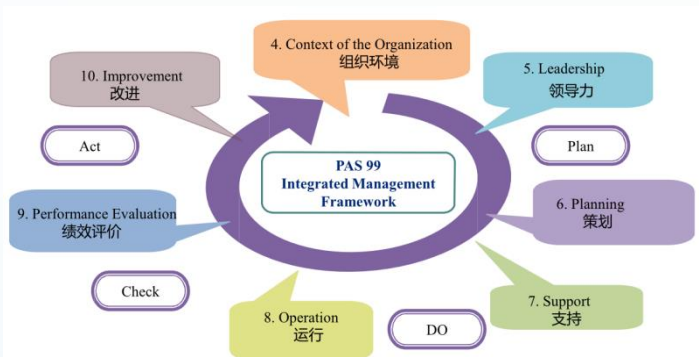
1. 易整合：在新版当中采用ISO导则83做结构性要求，这个结构未来在ISO其他标准改版中会普遍采用。（ ISO 22301已应用）信息安全管理体系更容易与其他管理体系进行融合。
2. 新要求：将旧版11个控制领域拓展到14个，结构更合理，表现更清晰。将旧版133个控制项缩减到113个。对部分控制项进行取消、合并和新增，以反映当前信息安全发展趋势。
3. 清晰明确：对旧版一些表述不清晰、不准确以及重复的部分控制项予以调整。

国际标准的未来框架

ISCCC

ISO组织对管理体系标准在结构、格式、通用短语和定义方面进行了统一。这将确保今后编制或修订管理体系标准的持续性、整合性和简单化，这也将使标准更易读、易懂。

新的框架重新构建了ISO标准PDCA的章节架构

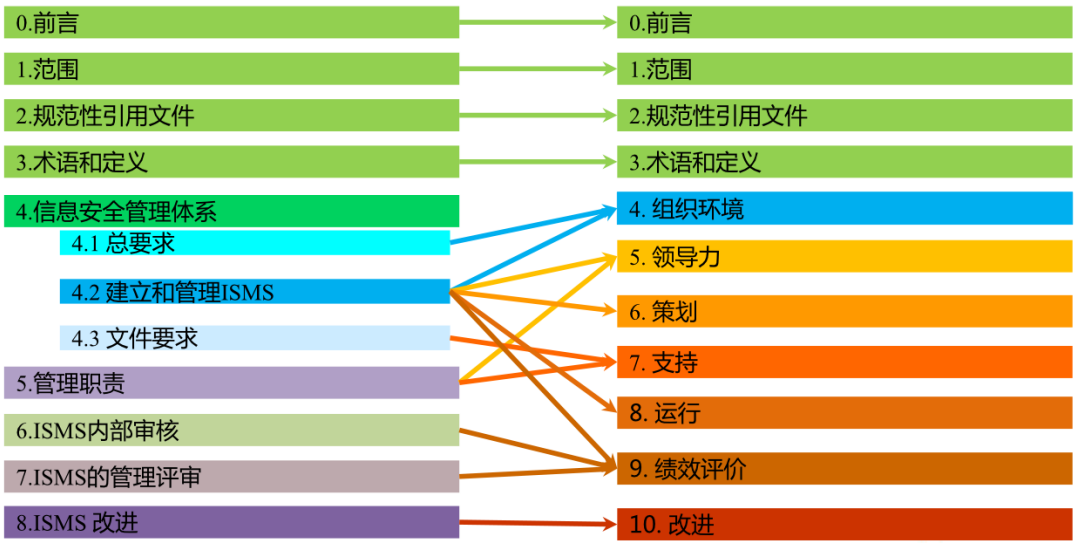


ISO导则83

ISCCC

国际标准的未来框架

新旧版本正文结构变化


0.前言
1.范围
2.规范性引用文件
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
4.3 文件要求
5.管理职责
6.ISMS内部审核
7.ISMS的管理评审
8.ISMS 改进
0.前言
1.范围
2.规范性引用文件
3.术语和定义
4. 组织环境
5. 领导力
6. 策划
7. 支持
8. 运行
9. 绩效评价
10. 改进

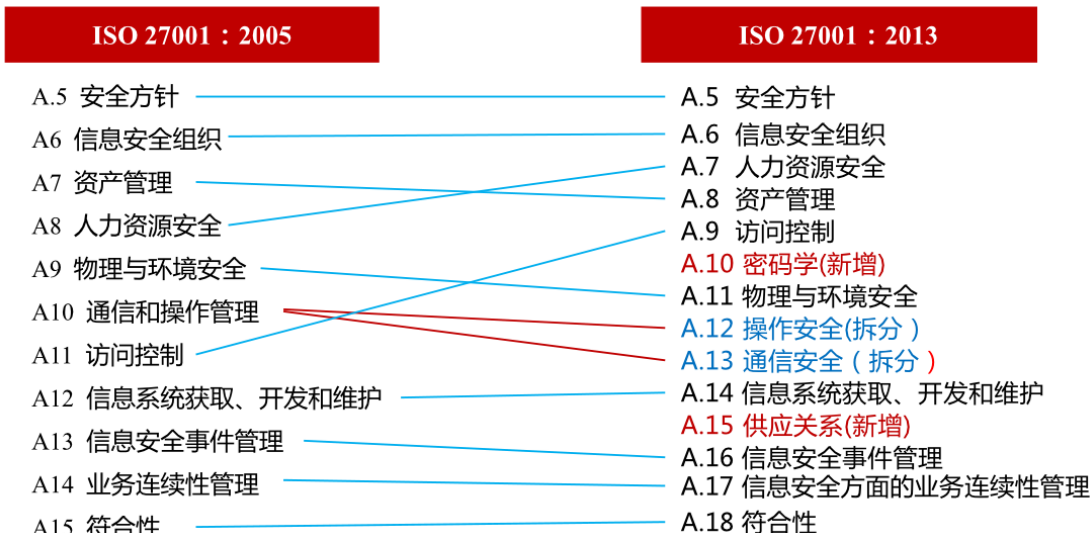
新版标准正文内容

ISCCC

Plan	Do	Check	Act

• 4 组织环境
  • 了解组织背景及现状
  • 理解相关方的需求和期望
  • ISMS的范围
  • ISMS
• 5 领导力
  • 领导作用和承诺
  • 方针
  • 角色、职责和授权
• 6 策划
  • 处理风险和机遇的行动
  • 实现ISMS的目标和实施计划
• 7 支持
  • 资源
  • 能力
  • 意识
  • 沟通
  • 文件化信息
	• 8 运行
	  • 运行计划和控制
	  • 信息安全风险评估
	  • 信息安全风险处置
		• 9 绩效评价
		  • 监视、测量、分析、评价
		  • 内部审核
		  • 管理评审
			• 10 改进
			  • 不符合项与纠正措施
			  • 持续改进

新旧版本附录A部分的变化



为什么要调整2005版的附录A

1. ISO27001：2005控制项逻辑性与充分性等方面存在进一步改进的空间。
2. ISO27001：2005附录A中，存在分散的、重复的、不清晰的控制项。如， A6.1.3信息安全职责分配、A8.1.1角色和职责；
3. ISO27001：2005附录A中，存在过于细化的操作层面的控制项。如，A12.2.1输入数据的验证、A12.2.2内部处理的控制、A12.2.3 消息完整性、A12.3.4输出数据验证

新旧版本附录A控制域变化

1. 从原本的11个控制域调整为14个控制域；
2. 新增了“密码学”、“供应关系”两个控制域；
3. 将原本的控制域“通信及操作管理”拆分为“操作安全”、“通信安全”两个控制域。

注意：除新增和拆分的4个控制域外，其他控制域并非与旧版一一对应。

新旧版本附录A控制项变化

控制项从原来的133项调整为114项，其中的变化分为5大类：

1. 没有变化，只是调整了编号和顺序结构；
2. 变化替代，控制对象或控制范围发生了变化；
3. 完全删除，在新版本中取消了该项控制措施；
4. 合并删除，在新版本中，有其他控制项覆盖了其控制内容；
5. 新增，2005版没有该项控制措施，2013版新增内容

新版本附录A解析 A5

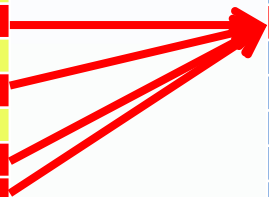
ISO27001：2005	ISO27001:2013
A5 安全方针	A5 安全方针
A6 信息安全组织	A6 信息安全组织
A7 资产管理	A7 人力资源安全
A8 人力资源安全	A8 资产管理
A9 物理和环境安全	A9 访问控制
A10 通信和运作管理	A10 密码学
A11 访问控制	A11 物理环境安全
A12 信息系统的获取开发以及维护	A12 操作安全
A13 信息安全事件管理	A13 通信安全
A14 业务连续性管理	A14 信息系统的获取、开发和维护
A15 符合性	A15 供应商关系
	A16 信息安全事件管理
	A17 信息安全方面的业务连续性管理
	A18 符合性

新版本附录A解析 A5

A5 安全方针		1	来源
A5.1 信息安全管理方针			
目标：依据业务要求以及相关的法律法规提供管理指导并支持信息安全。			
A5.1.1	信息安全方针文件	信息安全方针文件应该由管理者批准、发布并传递给所有员工和外部相关方。	A5.1.1
A5.1.2	信息安全方针的评审	应按计划的时间间隔或者当重大变化发生时进行信息安全方针评审，以确保它持续适宜性、充分性和有效性。	A5.1.2

新版本附录A解析 A6

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性



ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A6

A6 信息安全组织		7	来源
A6.1 内部组织			
目标：建立一个管理框架，以启动和控制组织内信息安全的实施和运行。			
A6.1.1	信息安全的角色和职责	所有信息安全职责应被定义及分配。	A6.1.3 A8.1.1
A6.1.2	责任分割	冲突的职责和权限应被分开，以减少对组织资产未经授权或无意的修改与误用。	A10.1.3
A6.1.3	与监管机构的联系	应与监管机构保持适当的联系。	A6.1.6
A6.1.4	与特殊利益团体的联系	与特定礼仪团队、其他专业安全论坛或行业协会应保持适当联系。	A6.1.7
A6.1.5	项目管理中的信息安全	信息安全应融入所受项目管理中，不论项目类型。	新增
A6.2 移动设备和远程办公			
目标：确保远程办公和使用移动设备的安全性。			
A6.2.1	移动设备策略	应使用配套策略和安全措施来防范因使用移动设备带来的风险。	A11.7.1
A6.2.2	远程办公	应使用配套策略和安全措施来保护在远程对信息的访问、处理和存储。	A11.7.2

新版本附录A解析 A7

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A7

A7 人力资源安全		6	来源
A7.1 任用之前			
目标：确保雇佣和承包方人员理解其职责、考虑对其承担的角色是适合的。			
A7.1.1	审查	对所有任用的候选者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需求、被访问信息的类别和察觉的风险来执行。	A8.1.2
A7.1.2	任用的条款及条件	员工和承包方人员应同意并签署任用合同中关于表明他们和组织的信息安全职责的条款和条件。	A8.1.3
A7.2 任用中			
目标：确保员工和承包方人员用户知悉并履行信息安全职责。			
A7.2.1	管理职责	管理者应该要求员工和承包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。	A8.2.1
A7.2.2	信息安全意识、教育和培训	组织的所有员工，适当时，包括承包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程序的定期更新培训。	A8.2.2
A7.2.3	纪律处理过程	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。	A8.2.3
A7.3 任用的终止或变化			
目标：保证组织利益是雇佣终止和变更的一部分。			
A7.3.1	任用终止或变化的责任	应该界定任用终止或变更后依然有信息安全责任和义务的员工或承包方人员，并进行沟通和执行。	A8.3.1

新版本附录A解析 A8

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

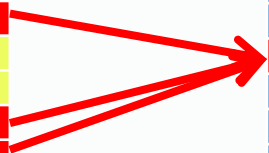
ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A8

A8 资产管理		10	来源
A8.1 对资产负责			
目标：实现和保持对组织资产的适当保护			
A8.1.1	资产清单	应识别与信息和信息处理设施相关的资产，并编制和维护资产清单。	A7.1.1
A8.1.2	资产责任人	应为资产清单内的资产指定责任人。	A7.1.2
A8.1.3	资产的合理使用	与信息处理设施有关的信息和资产合理使用规则应被确定、形成文件并加以实施。	A7.1.3
A8.1.4	资产的归还	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。	A8.3.2
A8.2 信息分类			
目标：确保信息得到与其重要性程度相适应的保护。			
A8.2.1	信息的分类	信息应依照法律要求、对组织的价值，关键性和敏感性进行分类。	A7.2.1
A8.2.2	信息的标记	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程序。	A7.2.2
A8.2.3	资产的处理	应按照组织所采纳的信息分类机制，建立和实施一组合适的处理规程。	A7.2.2
A8.3 介质处理			
目标：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。			
A8.3.1	可移动介质的管理	根据组织采用的分类机制来执行可移动介质管理流程。	A10.7.1
A8.3.2	介质的处置	不再需要的介质，应使用正式的规程可靠并安全地处置。	A10.7.2
A8.3.3	运输中的物理介质	包含信息的介质在传输过程中，应加以保护，防止未经授权的访问，滥用或损坏。	A10.8.3

新版本附录A解析 A9

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性



ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A9

A9 访问控制		14	来源
A9.1 访问控制的业务要求			
目标：控制对信息和信息处理设施的访问			
A9.1.1	访问控制策略	应建立访问控制策略，形成文件化，并基于业务和访问的安全要求进行评审。	A11.1.1
A9.1.2	访问网络和网络服务	用户应仅能访问已获专门授权使用的网络和网络服务。	A11.4.1
A9.2 用户访问管理			
目标：确保授权用户访问系统和服务，并防止未授权的访问。			
A9.2.1	用户注册和注销	应当有一个正式的用户注册和注销程序，适当地批准和撤回对所有信息系统和服务的访问。	A11.2.1 A11.5.2
A9.2.2	用户访问权限的提供	应有正式的用户权限控制规程来授权或撤销对所有信息系统及服务的访问。	新增
A9.2.3	特殊权限管理	应限制和控制特殊权限的分配和使用。	A11.2.2
A9.2.4	用户保密认证信息的管理	应使用正式的管理规程来控制保密认证信息的分配。	A11.2.3
A9.2.5	用户访问权的复查	资产所有者应当定期审查用户的访问权限。	A11.2.4
A9.2.6	移除或调整访问权限	所有工作人员和外部人员用户，当合同或协议终止后，应删除或调整其信息和信息处理设施的访问权限。	A8.3.3

新版本附录A解析 A9

A9.3 用户责任			
目标：确保用户对身份认证信息的保护责任。			
A9.3.1	保密认证信息的使用	应要求用户按照组织规定来使用保密认证信息。	A11.3.1
A9.4 系统和应用程序的访问控制			
目标：防止对系统和应用的未经授权使用。			
A9.4.1	信息访问限制	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。	A11.6.1
A9.4.2	安全登录规程	如访问控制策略需要，应通过安全登录程序控制对系统和应用的访问。	A11.5.1 A11.5.5 A11.5.6
A9.4.3	口令管理系统	口令管理系统应是互交式的，并确保口令质量。	A11.5.3
A9.4.4	特权实用程序的使用	对可能超越系统和应用程序控制措施的实用程序的使用应加以限制并严格控制。	A11.5.4
A9.4.5	程序源代码的访问控制	对程序源代码的访问应被限制。	A12.4.3

新版本附录A解析 A10

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A10

A10 密码学		2	来源
A10.1 密码控制			
目标：使用密码适当有效的保护信息的保密性、真实性“和/或”完整性。			
A10.1.1	密码使用控制策略	应开发和实施信息保护密码控制策略。	A12.3.1
A10.1.2	密钥管理	应开发和实施密钥的使用、保护的策略并贯穿其整个生命周期。	A12.3.2

新版本附录A解析 A11

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A11

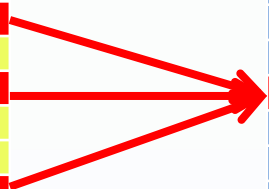
A11 物理环境安全		15	来源
A11.1 安全区域			
目标：防止对组织场所和信息的未授权物理访问、损坏和干扰。			
A11.1.1	物理安全边界	应该使用安全边界来保护包含敏感信息、关键信息和信息处理设施的区域。	A9.1.1
A11.1.2	物理入口控制	安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。	A9.1.2
A11.1.3	办公室、房间和设施的安全保护	应为办公室、房间和设施设计并采取物理安全措施。	A9.1.3
A11.1.4	外部和环境威胁的安全防护	应设计并采取物理安全措施来防范自然灾害、恶意攻击或意外事故。	A9.1.4
A11.1.5	在安全区域工作	应设计和应用用于安全区域工作的规程。	A9.1.5
A11.1.6	交付和交接区	类似于交付和交接区这样非授权可以进入的场所应加以控制，如果可能，应与信息处理设施隔离，以避免未授权访问。	A9.1.6

新版本附录A解析 A11

A11.2 设备			
目标：防止资产丢失、损坏、失窃或危害资产安全以及组织活动的中断。			
A11.2.1	设备安置和保护	应妥善安全及保护设备，以减少来自环境的威胁与危害以及未经授权的访问。	A9.2.1
A11.2.2	支持性设施	应保护设备使其免于支持性设施的失败而引起的电源故障和其他中断。	A9.2.2
A11.2.3	布缆安全	应当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。	A9.2.3
A11.2.4	设备维护	设备应予以正确地维护，以确保其持续的可用性和完整性。	A9.2.4
A11.2.5	资产的移动	设备、信息或软件在获得授权之前不应带出组织场所。	A9.2.7
A11.2.6	场所外设备和资产安全	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。	A9.2.5
A11.2.7	设备的安全处置或再利用	包含存储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。	A9.2.6
A11.2.8	无人值守的用户设备	用户应确保无人值守的用户设备得到适当的保护。	A11.3.2
A11.2.9	清楚桌面和清屏策略	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。	A11.3.3

新版本附录A解析 A12

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性



ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A12

A12 操作安全		14	来源
A12.1 操作程序和职责			
目标：确保正确、安全地操作信息处理设施。			
A12.1.1	文件化的操作程序	操作规程应形成文件，并提供给所有需要的用户。	A10.1.1
A12.1.2	变更管理	对影响信息的组织、业务流程、信息处理设施和系统的变更应加以控制。	A10.1.2
A12.1.3	容量管理	资源的使用应加以监视、调整，并做出对于未来容量要求的预测，以确保拥有所需的系统性能。	A10.3.1
A12.1.4	开发、测试和运行环境的分离	开发及测试环境应与运营环境分离，减少未授权访问和改变运行系统的风险。	A10.1.4
A12.2 恶意软件防护			
目标：确保信息和信息处理设施不受恶意软件侵害。			
A12.2.1	控制恶意软件	应实施恶意代码的监测、预防和恢复的控制措施，并与适当的提高用户安全意识相结合。	A10.4.1
A12.3 备份			
目标：防止数据丢失。			
A12.3.1	信息备份	根据既定的备份策略备份信息、软件和系统镜像，并定期测试。	A10.5.1

新版本附录A解析 A12

A12.4 记录和监控			
目标：记录事件并生成证据。			
A12.4.1	事件日志	应产生记录用户活动、异常情况、故障和信息安全事件的日志，并定期审核。	A10.10.1 A10.10.2 A10.10.5
A12.4.2	日志信息的保护	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。	A10.10.3
A12.4.3	管理员和操作员日志	系统管理员和系统操作员的活动应记入日志，对其保护，并定期评审。	A10.10.4
A12.4.4	时钟同步	一个组织或安全区域内的所有相关信息处理设施的时钟应使用已设的单一参考时间源进行同步。	A10.10.6
A12.5 运行软件的控制			
目标：保证运行系统的完整性。			
A12.5.1	运行系统软件的安装	应实施控制在运行系统上安装软件的规程。	A12.4.1
A12.6 技术漏洞管理			
目标：防止利用技术脆弱性。			
A12.6.1	技术漏洞管理	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。	A12.6.1
A12.6.2	限制软件安装	应建立和实施控制用户安装软件的规则。	新增
A12.7 信息系统审计考虑			
目标：将业务系统审计过程的影响最小化。			
A12.7.1	信息系统审计控制	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。	A15.3.1

新版本附录A解析 A13

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

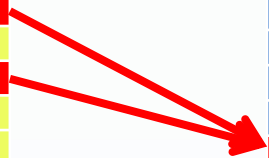
ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A13

A13 通信安全		7	来源
A13.1 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信息处理设施。			
A13.1.1	网络控制	应管理和控制网络，以保护系统和应用程序中的信息。	A10.6.1
A13.1.2	网络服务安全	所有网络服务的安全机制、服务级别和管理要求，应予以确定并包含在网络服务协议中，无论这些服务是否由公司内部提供还是外包。	A10.6.2
A13.1.3	网络隔离	应在网络隔离信息服务、用户及系统信息。	A11.4.5
A13.2 信息传输			
目标：维护组织与任务外部实体的信息传输安全。			
A13.2.1	信息传输的策略和程序	应建立正式的传输策略、规程和控制措施，以保证所有类型的通信设施间的信息传输安全。	A10.8.1
A13.2.2	信息传输协议	应建立组织与外部方传输业务信息安全传输的协议。	A10.8.2
A13.2.3	电子消息	涉及电子消息的信息应适当保护。	A10.8.4
A13.2.4	保密或不泄露协议	应确定组织信息保护需要的保密性或不泄露协议的要求，定期评审并形成文档。	A6.1.5

新版本附录A解析 A14

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性



ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A14

A14 信息系统的获取、开发和维护		13	来源
A14.1 信息系统的安全要求			
目标：确保安全是信息系统生命周期中的组成部分。包括对通过公共网络提供服务的信息系统要求。			
A14.1.1	安全需求分析和说明	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。	A12.1.1
A14.1.2	保护公共网络上的应用服务	在公共网络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。	A10.9.1 A10.9.3
A14.1.3	保护应用服务交易	应用服务交易中所涉及到的信息应加以保护，以防止不完整的传输、路由错误、未经授权的信息改变、未经授权的披露和未经授权的消息复制或重播。	A10.9.2
A14.2 开发和支持过程中的安全			
目标：确保在整个信息系统开发生命周期中设计与实施信息安全。			
A14.2.1	安全开发策略	应制定及应用关于软件和系统的开发规则。	新增
A14.2.2	系统变更控制程序	应使用正式的变更控制程序来控制开发生命周期中对系统的变更。	A12.5.1
A14.2.3	运行平台变更后的技术评估	当运行平台发生变更时，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。	A12.5.2
A14.2.4	软件包变更的限制	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。	A12.5.3
A14.2.5	安全系统设计原则	应建立、维护文件化的安全系统工程的设计原则，并应用到任何信息系统开发工作中。	新增
A14.2.6	安全的开发环境	组织应建立并适当保护开发环境的安全，并涵盖整个系信托开发周期。	新增
A14.2.7	外包软件开发	组织应监管和监视外包的系统开发活动。	A12.5.5
A14.2.8	系统安全性测试	在开发的过程中，必须测试安全功能。	新增
A14.2.9	系统验收测试	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准则。	A10.3.2
A14.3 测试数据			
目标：确保测试数据的安全。			
A14.3.1	测试数据的保护	测试数据应被仔细筛选、保护和控制。	A12.4.2

新版本附录A解析 A15

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A15

A15 供应商关系		5	来源
A15.1 供应商关系中的信息安全			
目标：确保供应商访问的组织资产的安全。			
A15.1.1	供应商关系的信息安全策略	对于减少供应商访问组织资产风险的信息安全要求应得到供应商的认可并形成文件。	新增
A15.1.2	供应商协议中的安全	应建立与信息安全相关的要求并获得供应商的认可。包括可能处理、存储及交换组织信息，或提供IT基础设施部件的供应商。	A6.2.3
A15.1.3	信息和通信技术供应链	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。	新增
A15.2 供应商服务交付管理			
目标：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。			
A15.2.1	监视和审查供应商服务	组织应定期监视，评审和审计供应商提供的服务。	A10.2.2
A15.2.2	供应商服务变更管理	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、程序和控制措施，应考虑所涉及业务信息、系统、流程的关键性以及风险的重新评估。	A10.2.3

新版本附录A解析 A16

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A16

A16 信息安全事件管理		7	来源
A16.1 信息安全事件和改进的管理			
目标：确保一致和有效的方法来管理信息安全事件，包括安全事件和弱点的报告。			
A16.1.1	职责和程序	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。	A13.2.1
A16.1.2	报告信息安全事件	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。	A13.1.1
A16.1.3	报告信息安全弱点	应要求信息系统和服务的所有员工、承包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。	A13.1.2
A16.1.4	信息安全事件的评估和决策	应对信息安全事件进行评估，以确定是否应归类为信息安全事件。	新增
A16.1.5	信息安全事件的响应	信息安全事件应依照文件化的程序进行响应。	新增
A16.1.6	从信息安全事件中学习	从分析和解决信息安全事件中获取知识，减少未来事件发生的可能性或影响。	A13.2.2
A16.1.7	收集证据	组织应制定并应用规程，以识别、收集、获取和保存可作为证据的信息。	A13.2.3

新版本附录A解析 A17

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A17

A17 信息安全方面的业务连续性管理		4	来源
A17.1 信息安全连续性			
目标：信息安全的连续性应融入组织的业务连续性管理。			
A17.1.1	规划信息安全连续性	组织应确定其在不利情形时信息安全和信息安全管理的连续性要求，如危机或灾难时。	A14.1.2
A17.1.2	实施信息安全连续性	组织应建立、实施、维护文件化的流程、程序、控制措施，以保证在不利情形时所要求的信息安全连续性级别。	新增
A17.1.3	验证、检查和评估信息安全连续性	组织应每隔一段时间检查其建立和实施的信息安全连续性控制措施，以确保他们在不利情形时是有效的。	A14.1.5
A17.2 冗余			
目标：确保信息处理实施的可用性。			
A17.2.1	信息处理设施的可用性	信息处理设施应当实现充分的冗余，以满足可用性要求。	新增

新版本附录A解析 A18

ISO27001：2005
A5 安全方针
A6 信息安全组织
A7 资产管理
A8 人力资源安全
A9 物理和环境安全
A10 通信和运作管理
A11 访问控制
A12 信息系统的获取开发以及维护
A13 信息安全事件管理
A14 业务连续性管理
A15 符合性

ISO27001:2013
A5 安全方针
A6 信息安全组织
A7 人力资源安全
A8 资产管理
A9 访问控制
A10 密码学
A11 物理环境安全
A12 操作安全
A13 通信安全
A14 信息系统的获取、开发和维护
A15 供应商关系
A16 信息安全事件管理
A17 信息安全方面的业务连续性管理
A18 符合性

新版本附录A解析 A18

A18 符合性		8	来源
A18.1 符合法律和合同的要求			
目标：避免违反相关信息安全的法律、法令、法规或信息安全相关的合同义务的任务安全要求。			
A18.1.1	识别适用的法律和合同要求	对每一个信息系统和组织而言，法令、法规及合同内容所规定的所有相关要求，以及满足这些要求的组织方法，应加以明白地界定、文件化并保持更新	A15.1.1
A18.1.2	知识产权	应实行适当的程序，以确保在使用具有知识产权的产品和专有软件产品时，能符合法律法规和合同条款的要求	A15.1.2
A18.1.3	记录的保护	应根据法律、规章、合同和业务的要求，保护重要记录防止其丢失、损坏和篡改	A15.1.3
A18.1.4	隐私和个人信息的保护	应该确保数据保护和隐私符合相应的法律法规要求，使用时也应该满足合同条款的要求	A15.1.4
A18.1.5	密码控制措施的规则	使用密码控制措施应遵从相关的协议、法律和法规。	A15.1.6
A18.2 信息安全评审			
目标：确保信息安全设施依照组织的策略和程序运行和实施。			
A18.2.1	信息安全的独立评审	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，也应进行独立评审。	A6.1.8
A18.2.2	符合安全政策和标准	管理者应定期评审其职责范围内的信息处理流程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。	A15.2.1
A18.2.3	技术符合性评审	应定期评审信息系统是否符合组织信息安全策略和标准。	A15.2.2

结束语

ISCCC

真诚合作、共谋发展