中国信息安全认证中心

CHINA INFORMATION SECURITY
CERTIFICATION CENTER

www.isccc.gov.cn

ISO/IEC27001附录A

新旧版标准差异分析和重点解读

程瑜琦

2014年9月24日

附录A

- 附录A是规范性附录。
- 附录A提供参考控制目标和控制措施。
- 附录A中的控制目标和控制措施源自ISO/IEC27002:2013的第5章到第18章
- ISO/IEC27002是信息安全控制措施实用规则，在ISO/IEC27002中有附录A每一个控制措施的实施指南，可以帮助我们理解附录A控制措施的要求，并对控制措施的实际应用提供指导。

附录A

A.5 信息安全方针和策略（POLICES）			A.5 安全方针	
A.5.1 信息安全管理指导			A.5.1 信息安全方针	
目标：依据业务要求和相关法律法规为信息安全提供管理指导和支持。			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	信息安全方针和策略	控制措施 信息安全方针和策略应由管理者批准、发布并传达给所有员工和外部相关方。	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	信息安全方针和策略的评审	控制措施 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和策略评审，以确保其持续的适宜性、充分性和有效性。	5.1.1 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。

附录A

A.6 信息安全组织			A.6 信息安全组织	
A.6.1 内部组织			A.6.1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。			目标：在组织内管理信息安全。	
A.6.1.1	信息安全角色和职责	*控制措施* 所有的信息安全职责应予以定义和分配。	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.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.6.1.2	责任分割	*控制措施* 应分割冲突的责任和职责范围，以降低未授权或无意的修改或者不当使用组织资产的机会。	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。

附录A

A.6 信息安全组织			A.6 信息安全组织	
A.6.1 内部组织			A.6.1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。			目标：在组织内管理信息安全。	
A.6.1.3	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.6.1.6 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.6.1.4	与特定相关方的联系	*控制措施* 应保持与特定相关方、其他专业安全论坛和专业协会的适当联系。	A.6.1.7 与特定权益团体的联系	*控制措施* 应保持与特定权益团体、其他安全专家组和专业协会的适当联系。
A.6.1.5	项目管理中的信息安全	*控制措施* 应解决项目管理中的信息安全问题，无论项目类型。		

附录A

A.6 信息安全组织				
A.6.2 移动设备和远程工作			**A.11.7 移动计算和远程工作**	
目标：确保远程工作和移动设备使用的安全。			目标：确保使用可移动计算和远程工作设施时的信息安全。	
A.6.2.1	移动设备策略	*控制措施* 应采用策略和支持性安全措施以管理使用移动设备时带来的风险。	**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，以防范使用可移动计算和通信设施时所造成的风险。
A.6.2.2	远程工作	*控制措施* 应实施策略和支持性安全措施以保护在远程工作地点访问、处理或存储的信息。	**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、操作计划和程序。

附录A

A.7 人力资源安全			A.8 人力资源安全	
A.7.1 任用前			A.8.1任用 之前	
目标：确保员工和承包方理解其职责，并适合其角色。			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.7.1.1	审查	*控制措施* 对所有任用候选者的背景验证核查应按照相关法律法规和道德规范进行，并与业务要求、访问信息的等级（8.2）和察觉的风险相适宜。	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.7.1.2	任用条款及条件	*控制措施* 应在员工和承包商的合同协议中声明他们和组织对信息安全的职责。	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，这些条款和条件要声明他们和组织的信息安全职责。

附录A

A.7 人力资源安全			A.8 人力资源安全	
A.7.2 任用中			A.8.2 任用中	
目标：确保员工和承包方意识到并履行其信息安全职责。			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，以减少人为过失的风险。	
A.7.2.1	管理职责	*控制措施* 管理者应要求所有员工和承包商按照组织已建立的方针策略和规程应用信息安全。	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程序对安全尽心尽力。
A.7.2.2	信息安全意识、教育和培训	*控制措施* 组织所有员工，适当时包括承包商，应接受与其工作职能相关的适宜的意识教育和培训，及组织方针策略及规程的定期更新的信息。	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。

附录A

A.7 人力资源安全			A.8 人力资源安全	
A.7.2 任用中			A.8.2 任用中	
目标：确保员工和承包方意识到并履行其信息安全职责。			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，以减少人为过失的风险。	
A.7.2.3	纪律处理过程	*控制措施* 应建立正式的且被传达的纪律处理过程以对信息安全违规的员工采取措施。	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。

附录A

A.7 人力资源安全			A.8 人力资源安全	
A.7.3 任用的终止和变更			A.8.3 任用的终止或变化	
目标：在任用变更或终止过程中保护组织的利益。			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.7.3.1	任用职责的终止或变更	*控制措施* 应确定任用终止或变更后仍有效的信息安全职责和责任，传达至员工或承包商并执行。	终止职责	*控制措施* 任用终止或任用变更的职责应清晰的定义和分配。

附录A

A.8 资产管理			A.7 资产管理	
A.8.1资产职责			A.7.1对资产负责	
目标：识别组织资产并确定适当的保护职责。			目标：实现和保持对组织资产的适当保护。	
A.8.1.1	资产清单	*控制措施* 应识别与信息和信息处理设施相关的资产，并编制、维护这些资产的清单。	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.8.1.2	资产责任主体	*控制措施* 应确定资产清单中的资产责任主体。	A.7.1.2资产责任人	*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。

附录A

A.8 资产管理			A.7 资产管理	
A.8.1资产职责			A.7.1对资产负责	
目标：识别组织资产并确定适当的保护职责。			目标：实现和保持对组织资产的适当保护。	
A.8.1.3	资产的可接受使用	*控制措施* 应确定信息及与信息和信息处理设施有关的资产的可接受使用规则，形成文件并加以实施。	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使用允许规则应被确定、形成文件并加以实施。
A.8.1.4	资产归还	*控制措施* 所有员工和外部用户在任用、合同或协议终止时，应归还其占用的所有组织资产。	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。

附录A

A.8 资产管理			A.7 资产管理	
A.8.2 信息分级			A.7.2信息分类	
目标：确保信息按照其对组织的重要程度受到适当级别的保护。			目标：确保信息受到适当级别的保护。	
A.8.2.1	信息的分级	*控制措施* 信息应按照法律要求、价值、关键性及其对未授权泄露或修改的敏感性进行分级。	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.8.2.2	信息的标记	*控制措施* 应按照组织采用的信息分级方案，制定并实施一组适当的信息标记规程。	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.8.2.3	资产的处理	*控制措施* 应按照组织采用的信息分级方案，制定并实施资产处理规程。		

附录A

A.8 资产管理				
A.8.3 介质处理			A.10.7 介质处置	
目的：防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。			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.8.3.1	移动介质的管理	*控制措施* 应按照组织采用的分级方案，实施移动介质管理规程。	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程序。
A.8.3.2	介质的处置	*控制措施* 应使用正式的规程安全地处置不再需要的介质。	A.10.7.2介质的处置	*控制措施* 不再需要的介质，应使用正式的程序可靠并安全地处置。
A.8.3.3	物理介质的转移	*控制措施* 包含信息的介质在运送中应受到保护，以防止未授权访问、不当使用或毁坏。	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。

附录A

A.9 访问控制			A.11访问控制	
A.9.1访问控制的业务要求			A.11.1访问控制的业务要求	
目标：限制对信息和信息处理设施的访问。			目标：控制对信息的访问。	
A.9.1.1	访问控制策略	*控制措施* 应基于业务和信息安全要求，建立访问控制策略，形成文件并进行评审。	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.9.1.2	网络和网络服务的访问	*访问控制* 用户应仅能访问已获专门授权使用的网络和网络服务。	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。

附录A

A.9 访问控制			A.11访问控制	
A.9.2用户访问管理			A.11.2用户访问管理	
目标：确保授权用户对系统和服务的访问，并防止未授权的访问。			目标：确保授权用户访问信息系统，并防止未授权的访问。	
A.9.2.1	用户注册和注销	*控制措施* 应实施正式的用户注册及注销过程来分配访问权限。	A.11.2.1 用户注册	*控制措施* 应有正式的用户注册及注销程序，来授权和撤销对所有信息系统及服务的访问。
A.9.2.2	用户访问配置	*控制措施* 应对所有系统和服务的所有类型用户实施正式的用户访问配置过程以分配或撤销访问权限。		
A.9.2.3	特殊访问权限管理	*控制措施* 应限制和控制特殊访问权限的分配和使用。	A.11.2.2 特权管理	*控制措施* 应限制和控制特殊权限的分配及使用。

附录A

A.9 访问控制			A.11访问控制	
A.9.2用户访问管理			A.11.2用户访问管理	
目标：确保授权用户对系统和服务的访问，并防止未授权的访问。			目标：确保授权用户访问信息系统，并防止未授权的访问。	
A.9.2.4	用户的秘密鉴别信息管理	*控制措施* 应通过正式的管理过程控制秘密鉴别信息的分配。	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.9.2.5	用户访问权限的复查	*控制措施* 资产责任主体应定期对用户的访问权限进行复查。	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.9.2.6	访问权限的移除或调整	*控制措施* 所有员工和外部用户对信息和信息处理设施的访问权限在任用、合同或协议终止时，应予以移除，或在变更时予以调整。	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。

附录A

A.9 访问控制			A.11访问控制	
A.9.3 用户职责			A.11.3 用户职责	
目标：使用户承担保护其鉴别信息的责任。			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。	
A.9.3.1	秘密鉴别信息的使用	*控制措施* 应要求用户遵循组织在使用秘密鉴别信息时的惯例。	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。

附录A

A.9 访问控制				
A.9.4系统和应用访问控制				
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	*控制措施* 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.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.9.4.2	安全登录规程	*控制措施* 当访问控制策略要求时，应通过安全登录规程控制对系统和应用的访问。	**A.11.5.1安全登录程序**	*控制措施* 访问操作系统应通过安全登录程序加以控制。
			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。

附录A

A.9 访问控制				
A.9.4系统和应用访问控制				
目的：防止对系统和应用的未授权访问。				
A.9.4.3	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.11.5.3**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.9.4.4	特权实用程序的使用	*控制措施* 对于可能超越系统和应用控制措施的实用程序的使用应予以限制并严格控制。	**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	程序源代码的访问控制	*控制措施* 应限制对程序源代码的访问。	**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。

附录A

A.10 密码			A.12信息系统获取、开发和维护	
A.10.1 密码控制			A.12.3密码控制	
目标： 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。			目标：通过密码方法保护信息的保密性、真实性或完整性。	
A.10.1.1	密码控制的使用策略	*控制措施* 应开发和实施用于保护信息的密码控制使用策略。	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.10.1.2	密钥管理	*控制措施* 应制定和实施贯穿其全生命周期的密钥使用、保护和生存期策略。	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。

附录A

A.11 物理和环境安全			A.9 物理和环境安全	
A.11.1 安全区域			A.9.1安全区域	
目标：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。			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.11.1.1	物理安全边界	*控制措施* 应定义和使用安全边界来保护包含敏感或关键信息和信息处理设施的区域。	A.9.1.1物理安全边界	*控制措施* 应使用安全边界（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.11.1.2	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.9.1.2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.11.1.3	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.9.1.3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。

附录A

A.11 物理和环境安全			A.9 物理和环境安全	
A.11.1 安全区域			A.9.1安全区域	
目标：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。			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.11.1.4	外部和环境威胁的安全防护	*控制措施* 为防止自然灾害、恶意攻击或事件应设计和采取物理保护措施。	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.11.1.5	在安全区域工作	*控制措施* 应设计和应用安全区域工作规程。	A.9.1.5在安全区域工作	*控制措施* 应设计和运用用于安全区域工作的物理保护和指南。
A.11.1.6	交接区	*控制措施* 访问点（例如交接区）和未授权人员可进入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.9.1.6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，要与信息处理设施隔离，以避免未授权访问。

附录A

A.11 物理和环境安全			A.9 物理和环境安全	
A.11.2 设备			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。			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.11.2.1	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。	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。
A.11.2.2	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.9.2.2 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.11.2.3	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、干扰或损坏	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。

附录A

A.11 物理和环境安全			A.9 物理和环境安全	
A.11.2 设备			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。			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.11.2.4	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.9.2.4 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.11.2.5	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.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.11.2.6	组织场所外的设备与资产安全	*控制措施* 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.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。

附录A

A.11 物理和环境安全			A.9 物理和环境安全	
A.11.2 设备			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。			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.11.2.7	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部分应进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全地写覆盖。	A.9.2.6 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检查，以确保在销毁之前，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.11.3.2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.11.2.9	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.11.3.3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。

附录A

A.12 运行安全			A.10通信和操作管理	
A.12.1 运行规程和职责			A.10.1操作程序和职责	
目标：确保正确、安全的操作信息处理设施。			目标：确保正确、安全的操作信息处理设施。	
A.12.1.1	文件化的操作规程	*控制措施* 操作规程应形成文件，并对所需用户可用。	A.10.1.1文件化的操作程序	*控制措施* 操作程序应形成文件、保持并对所有需要的用户可用。
A.12.1.2	变更管理	*控制措施* 应控制影响信息安全的变更，包括组织、业务过程、信息处理设施和系统变更。	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.12.1.3	容量管理	*控制措施* 应对资源的使用进行监视，调整和预测未来的容量需求，以确保所需的系统性能。	A.10.3.1容量管理	*控制措施* 资源的使用应加以监视、调整，并应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、测试和运行环境分离	*控制措施* 开发、测试和运行环境应分离以减少未授权用户访问或改变运行系统的风险。	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。

附录A

A.12 运行安全				
A.12.2恶意代码防范			**A.10.4 防范恶意和移动代码**	
目标：确保信息和信息处理设施防范恶意代码。			目标：保护软件和信息的完整性。	
A.12.2.1	恶意代码的控制	*控制措施* 应实施检测、预防和恢复控制措施以防范恶意代码，并结合适当的用户意识教育。	**A.10.4.1** 控制恶意代码	*控制措施* 应实施恶意代码的监测、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。

附录A

A.12 运行安全				
A.12.3 备份			**A.10.5 备份**	
目标：防止数据丢失			标：保持信息和信息处理设施的完整性和可用性。	
A.12.3.1	信 息备份	*控制措施* 应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。	**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。

附录A

A.12 运行安全				
A.12.4 日志和监视			**A.10.10 监视**	
目的：记录事态并生成证据。			目标：检测未授权的信息处理活动。	
A.12.4.1	事态日志	*控制措施* 应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。	**A.10.10.1** 审计记录	*控制措施* 应产生记录用户活动、异常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.12.4.2	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.10.10.3** 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。

附录A

A.12 运行安全				
A.12.4 日志和监视			**A.10.10 监视**	
目的：记录事态并生成证据。			目标：检测未授权的信息处理活动。	
A.12.4.3	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，并对日志进行保护和定期评审。	**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.12.4.4	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与单一的参考源进行同步。	**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。

附录A

A.12 运行安全				
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	*控制措施* 应实施运行系统软件安装控制规程。	**A.12.4.1**运行软件的控制	*控制措施* 应有程序来控制在运行系统上安装软件。

附录A

A.12 运行安全				
A.12.6 技术脆弱性管理			**A.12.6 技术脆弱性管理**	
目标：防止对技术脆弱性的利用。			目标：降低利用公布的技术脆弱性导致的风险。	
A.12.6.1	技术脆弱性的管理	*控制措施* 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应对相关风险。	**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.12.6.2	软件安装限制	*控制措施* 应建立并实施控制用户安装软件的规则。		

附录A

A.12 运行安全				
A.12.7 信息系统审计的考虑			**A.15.3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。			目标：将信息系统审计过程的有效性最大化，干扰最小化。	
A.12.7.1	信息系统审计的控制	*控制措施* 涉及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，以便最小化业务过程的中断。	**A.15.3.1**信息系统审计控制措施	*控制措施* 涉及对运行系统检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。

附录A

A.13 通信安全					
A.13.1 网络安全管理			A.10.6 网络安全管理		
目标：确保网络及其支持性信息处理设施中的信息得到保护。			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.13.1.1	网络控制	*控制措施* 应管理和控制网络以保护系统和应用中的信息。	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，维护使用网络的应用程序的安全，包括传输中的信息。
A.13.1.2	网络服务的安全	*控制措施* 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.10.6.2 网络服务的安全	*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.13.1.3	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.11.4.5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。

附录A

A.13 通信安全				
A.13.2 信息传输			**A.10.8 信息的交换**	
目标： 保持在组织内及与外部实体间传输信息的安全。			目标：保持组织内信息和软件交换及与外部组织信息和软件交换的安全。	
A.13.2.1	信息传输策略和规程	*控制措施* 应有正式的传输策略、规程和控制措施，以保护通过使用各种类型通信设施进行的信息传输。	**A.10.8.1** 信息交换策略和程序	*控制措施* 应有正式的交换策略、程序和控制措施，以保护通过使用各种类型通信设施的信息交换。
A.13.2.2	信息传输协议	*控制措施* 协议应解决组织与外部方业务信息的安全传输。	**A.10.8.2** 交换协议	*控制措施* 应建立组织与外部团体交换信息和软件的协议。

附录A

A.13 通信安全				
A.13.2 信息传输			**A.10.8 信息的交换**	
目标： 保持在组织内及与外部实体间传输信息的安全。			目标：保持组织内信息和软件交换及与外部组织信息和软件交换的安全。	
A.13.2.3	电子消息发送	*控制措施* 应适当保护包含在电子消息发送中的信息。	**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.13.2.4	保密或不泄露协议	*控制措施* 应识别、定期评审和文件化反映组织信息保护需要的保密性或不泄露协议的要求。	**A.6.1.5** 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。

附录A

A.14 系统获取、开发和维护				
A.14.1信息系统的安全要求			**A.12.1信息系统的安全要求**	
目标： 确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求			目标：确保安全是信息系统的一个有机组成部分。	
A.14.1.1	信息安全要求分析和说明	*控制措施* 新建信息系统或增强现有信息系统的要求中应包括信息安全相关要求。	**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.14.1.2	公共网络上应用服务的安全保护	*控制措施* 应保护在公共网络上的应用服务中的信息以防止欺诈行为、合同纠纷以及未经授权的泄露和修改。	**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、合同争议和未授权的泄露和修改。

附录A

A.14 系统获取、开发和维护				
A.14.1信息系统的安全要求			**A.12.1信息系统的安全要求**	
目标： 确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求			目标：确保安全是信息系统的一个有机组成部分。	
A.14.1.3	应用服务事务的保护	*控制措施* 应保护应用服务事务中的信息，以防止不完整的传输、错误路由、未授权的消息变更、未授权的泄露、未授权的消息复制或重放。	**A.10.9.2** 在线交易	*控制措施* 包含在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。

附录A

A.14 系统获取、开发和维护				
A.14.2开发和支持过程中的安全			**A.12.5开发和支持过程中的安全**	
目标：确保信息安全在信息系统开发生命周期中得到设计和实施。			目标：维护应用系统软件和信息的安全。	
A.14.2.1	安全的开发策略	*控制措施* 针对组织内的开发，应建立软件和系统开发规则并应用。		
A.14.2.2	系统变更控制规程	*控制措施* 应使用正式的变更控制规程来控制开发生命周期内的系统变更。	**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控制变更的实施。
A.14.2.3	运行平台变更后对应用的技术评审	*控制措施* 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。	**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后，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。

附录A

A.14 系统获取、开发和维护				
A.14.2开发和支持过程中的安全			**A.12.5开发和支持过程中的安全**	
目标：确保信息安全在信息系统开发生命周期中得到设计和实施。			目标：维护应用系统软件和信息的安全。	
A.14.2.4	软件包变更的限制	*控制措施* 应不鼓励对软件包进行修改，仅限于必要的变更，且对所有变更加以严格控制	**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，限制必要的变更，且对所有的变更加以严格控制。
A.14.2.5	安全的系统工程原则	*控制措施* 应建立、文件化和维护安全的系统工程原则，并应用到任何信息系统实施工作中		
A.14.2.6	安全的开发环境	*控制措施* 组织应针对覆盖系统开发生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。		

附录A

A.14 系统获取、开发和维护				
A.14.2开发和支持过程中的安全			A.12.5开发和支持过程中的安全	
目标：确保信息安全在信息系统开发生命周期中得到设计和实施。			目标：维护应用系统软件和信息的安全。	
A.14.2.7	外包开发	*控制措施* 组织应督导和监视外包系统开发活动	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.14.2.8	系统安全测试	*控制措施* 应在开发过程中进行安全功能测试。		
A.14.2.9	系统验收测试	*控制措施* 应建立对新的信息系统、升级及新版本的验收测试方案和相关准则。	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。

附录A

A.14 系统获取、开发和维护				
A.14.3 测试数据			**A.12.4系统文件的安全**	
目标：确保用于测试的数据得到保护。			目标：确保系统文件的安全	
A.14.3.1	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。	**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。

附录A

A.15 供应商关系				
A.15.1 供应商关系中的信息安全				
目标：确保供应商可访问的组织资产受到保护。				
A.15.1.1	供应商关系的信息安全策略	*控制措施* 为降低供应商访问组织资产的相关风险，应与供应商就信息安全要求达成一致，并形成文件		
A.15.1.2	在供应商协议中解决安全	*控制措施* 应与每个可能访问、处理、存储、传递组织信息或为组织信息提供IT基础设施组件的供应商建立所有相关的信息安全要求，并达成一致。	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。

附录A

A.15 供应商关系				
A.15.1 供应商关系中的信息安全				
目标：确保供应商可访问的组织资产受到保护。				
A.15.1.3	信息与通信技术供应链	*控制措施* 供应商协议应包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。		

附录A

A.15 供应商关系				
A.15.2 供应商服务交付管理			**A.10.2 第三方服务交付管理**	
目标：保持与供应商协议一致的信息安全和服务交付的商定级别。			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.15.2.1	供应商服务的监视和评审	*控制措施* 组织应定期监视、评审和审核供应商服务交付。	**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。

附录A

A.15 供应商关系				
A.15.2 供应商服务交付管理			**A.10.2 第三方服务交付管理**	
目标：保持与供应商协议一致的信息安全和服务交付的商定级别。			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.15.2.2	供应商服务的变更管理	*控制措施* 应管理供应商所提供服务的变更，包括保持和改进现有的信息安全策略、规程和控制措施，管理应考虑变更涉及到的业务信息、系统和过程的关键程度及风险的再评估。	**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方针策略、规程和控制措施，要考虑业务系统和涉及过程的关键程度及风险的再评估。

附录A

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			**A.13.1报告信息安全事件和弱点**	
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，包括对安全事态和弱点的沟通。			目标：确保与信息系统有关的信息安全事件和弱点能够以某种方式传达，以便及时采取纠正措施。	
A.16.1.1	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.13.2.1** 职责和程序	*控制措施* 应建立管理职责和程序，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	*控制措施* 应通过适当的管理渠道尽快地报告信息安全事态。	**A.13.1.1** 报告信息安全事态	*控制措施* 信息安全事态应该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	*控制措施* 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任何观察到的或可疑的系统或服务中的信息安全弱点。	**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。

附录A

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： 确保采用一致和有效的方法对信息安全事件进行管理，包括对安全事态和弱点的沟通。				
A.16.1.4	信息安全事态的评估和决策	*控制措施* 应评估信息安全事态并决定其是否属于信息安全事件。		
A.16.1.5	信息安全事件的响应	*控制措施* 应按照文件化的规程响应信息安全事件。		

附录A

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： 确保采用一致和有效的方法对信息安全事件进行管理，包括对安全事态和弱点的沟通。				
A.16.1.6	从信息安全事件中学习	*控制措施* 应利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。	**A.13.2.2** 对信息安全事故的总结	*控制措施* 应有一套机制量化和监视信息安全事故的类型、数量和代价。
A.16.1.7	证据的收集	*控制措施* 组织应确定和应用规程来识别、收集、获取和保存可用作证据的信息。	**A.13.2.3** 证据的收集	*控制措施* 当一个信息安全事故涉及到诉讼（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，以使其符合相关诉讼管辖区域对证据的要求。

附录A

A.17业务连续性管理的信息安全方面”			A.14业务连续性管理	
A.17.1 信息安全的连续性			A.14.1业务连续性管理的信息安全方面	
目标：应将信息安全连续性纳入组织业务连续性管理之中。			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.17.1.1	规划信息安全连续性	*控制措施* 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.14.1.1业务连续性管理过程中包含的信息安全	*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。
A.17.1.2	实施信息安全连续性	*控制措施* 组织应建立、文件化、实施并维持过程、规程和控制措施，以确保在不利情况下信息安全连续性达到要求的级别。	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。

附录A

A.17业务连续性管理的信息安全方面”				
A.17.1 信息安全的连续性				
目标：应将信息安全连续性纳入组织业务连续性管理之中。				
A.17.1.3	验证、评审和评价信息安全连续性	*控制措施* 组织应定期验证已建立和实施的信息安全连续性控制措施，以确保这些措施在不利情况下是正当和有效的。		

附录A

A.17业务连续性管理的信息安全方面”				
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	*控制措施* 信息处理设施应具有足够的冗余以满足可用性要求。		

附录A

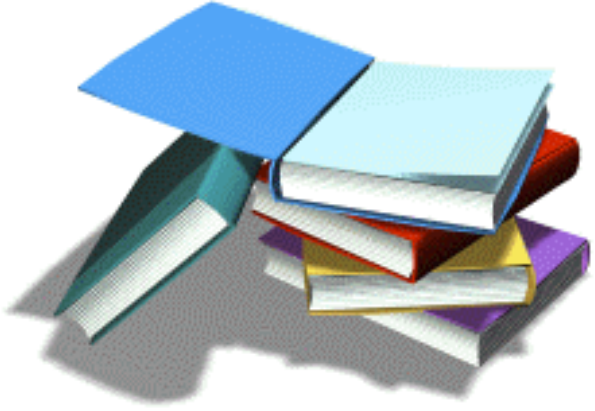
A.18 符合性			A.15符合性	
A.18.1 符合法律和合同要求			A.15.1符合法律要求	
目标：避免违反与信息安全有关的法律、法规、规章或合同义务以及任何安全要求。			目标：避免违反任何法律、法令、法规或合同义务，以及任何安全要求。	
A.18.1.1	可用的法律和合同要求的识别	*控制措施* 对每一个信息系统和组织而言，所有相关的法律、法规、规章和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。	A.15.1.1可用法律的识别	*控制措施* 对每一个信息系统和组织而言，所有相关的法令、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。
A.18.1.2	知识产权	*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.15.1.2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。

附录A

A.18 符合性			A.15符合性	
A.18.1 符合法律和合同要求			A.15.1符合法律要求	
目标：避免违反与信息安全有关的法律、法规、规章或合同义务以及任何安全要求。			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.18.1.3	记录的保护	*控制措施* 应根据法律、法规、规章、合同和业务要求，对记录进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。	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.18.1.4	个人身份信息的隐私和保护	*控制措施* 应依照相关的法律、法规和合同条款的要求，确保个人身份信息的隐私和保护。	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，确保护数据保护和隐私。
A.18.1.5	密码控制规则	*控制措施* 密码控制措施的使用应遵从所有相关的协议、法律和法规。	A.15.1.6密码控制措施的规则	*控制措施* 使用密码控制应遵从相关的协议、法律和法规。

附录A

A.18 符合性			A.15符合性	
A.18.2 信息安全评审			A.15.2符合安全策略和标准和技术符合性	
目标：确保依据组织方针策略、规程实施和运行信息安全。			目标：确保系统符合组织的安全策略及标准。	
A.18.2.1	信息安全的独立评审	*控制措施* 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施（如信息安全的控制目标、控制措施、方针策略、过程和规程）进行独立评审。	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.18.2.2	符合安全策略和标准	*控制措施* 管理者应定期评审其职责范围内的信息处理、规程与适当的安全方针策略、标准和任何安全要求的符合性。	A.15.2.1 符合安全策略和标准	*控制措施* 管理者应确保在其职责范围内的所有安全程序被正确地执行，以确保符合安全策略及标准。
A.18.2.3	技术符合性评审	*控制措施* 应定期评审信息系统与组织的信息安全方针策略和标准的符合性。	A.12.5.2 技术符合性检查	*控制措施* 信息系统应被定期核查是否符合安全实施标准。



Q&A ?