款项	控制目标	控制项	描述
A.5	**信息安全方针**		
A.5.1	**信息安全方针**		
		A.5.1.1信息安全方针文件	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	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。
A.6	**信息安全组织**		
A.6.1	**内部组织**		
		A.6.1.1 信息安全的管理承诺	管理者应通过清晰的说明、可证实的承诺、明确的信息安全职责分配及确认，来积极支持组织内的安全。
		A.6.1.2 信息安全协调	信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调。
		A.6.1.3信息安全职责的分配	所有的信息安全职责应予以清晰地定义。
		A.6.1.4 信息处理设施的授权过程	应为新的信息处理设施定义和实施一个管理授权过程。
		A.6.1.5 保密性协议	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。
		A.6.1.6 与政府部门的联系	应保持与政府相关部门的适当联系。
		A.6.1.7 与特定利益集团的联系	应保持与特殊利益集团、其他安全专家组和专业协会的适当联系。
		A.6.1.8 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.6.2	**外部伙伴**		
		A.6.2.1与外部各方相关风险的识别	应识别涉及外部各方业务过程中组织的信息和信息处理设施的风险，并在允许访问前实施适当的控制措施。
		A.6.2.2处理与顾客有关的安全问题	应在允许顾客访问组织信息或资产之前处理所有确定的安全要求。

		A.6.2.3处理第三方协议中的安全问题	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需求。
A.7	**资产管理**		
A.7.1	**资产责任**		
		A.7.1.1 资产清单	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.7.1.2 资产责任人	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和人员承担责任。
		A.7.1.3 资产的可接受使用	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.7.2	**信息分类**		
		A.7.2.1 分类指南	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.7.2.2 信息的标记和处理	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	**人力资源安全**		
A.8.1	**聘用之前**		
		A.8.1.1 角色和职责	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
		A.8.1.2 审查	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、被访问的信息的类别和察觉的风险来执行。
		A.8.1.3 任用条款和条件	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，这些条款和条件应声明他们和组织的信息安全职责。
A.8.2	**聘用期间**		
		A.8.2.1 管理职责	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规程对安全尽心尽力。

		A.8.2.2 信息安全意识、教育和培训	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
		A.8.2.3 纪律处理过程	对于安全违规的雇员，应有一个正式的纪律处理过程。
A.8.3	**解聘或变更**		
		A.8.3.1 终止职责	任用终止或任用变更的职责应清晰地定义和分配。
		A.8.3.2 资产的归还	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。
		A.8.3.3 撤销访问权	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。
A.9	**物理和环境安全**		
A.9.1	**安全区域**		
		A.9.1.1 物理安全周边	应使用安全周边（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.9.1.2 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。
		A.9.1.3 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。
		A.9.1.4 外部和环境威胁的安全防护	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.9.1.5 在安全区域工作	应设计和应用用于安全区域工作的物理保护和指南。
		A.9.1.6 公共访问、交接区安全	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.9.2	**设备安全**		
		A.9.2.1 设备安置和保护	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.9.2.2 支持性设施	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.9.2.3 布缆安全	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。
		A.9.2.4 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。
		A.9.2.5 组织场所外的设备安全	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。
		A.9.2.6 设备的安全处置或再利用	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.9.2.7 资产的移动	设备、信息或软件在授权之前不应带出组织场所。
A.10	**通信和操作管理**		
A.10.1	**操作性程序和责任**		
		A.10.1.1 文件化的操作规程	操作规程应形成文件、保持并对所有需求的用户可用。
		A.10.1.2 变更管理	对信息处理设施和系统的变更应加以控制。
		A.10.1.3 责任分割	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
		A.10.1.4 开发、测试和运行设施分离	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。
A.10.2	**第三方服务交付管理**		
		A.10.2.1 服务交付	应确保第三方实施、运行并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	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。
		A.10.2.3 第三方服务的变更管理	应管理服务提供的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑业务系统和涉及过程的关键程度及风险的再评估
A.10.3	**系统规划和验收**		
		A.10.3.1容量管理	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

		A.10.3.2 系统验收	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。
A.10.4	**抵御恶意和移动代码**		
		A.10.4.1 控制恶意代码	应实施恶意代码的检测、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。
		A.10.4.2控制移动代码	当授权使用移动代码时，其配置应确保授权的移动代码按照清晰定义的安全策略运行，应阻止执行未授权的移动代码。
A.10.5	**备份**		
		A.10.5.1 信息备份	应按照已设的备份策略，定期备份和测试信息和软件。
A.10.6	**网络安全管理**		
		A.10.6.1 网络控制	应充分管理和控制网络，以防止威胁的发生，维护使用网络的系统和应用程序的安全，包括传输中的信息。
		A.10.6.2 网络服务安全	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.10.7	**介质处理**		
		A.10.7.1 可移动介质的管理	应有适当的可移动介质的管理规程。
		A.10.7.2 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。
		A.10.7.3 信息处理规程	应建立信息的处理及存储规程，以防止信息的未授权的泄露或不当使用。
		A.10.7.4 系统文件安全	应保护系统文件以防止未授权的访问。
A.10.8	**信息交换**		
		A.10.8.1 信息交换策略和规程	应有正式的交换策略、规程和控制措施，以保护通过使用各种类型通信设施的信息交换。
		A.10.8.2 交换协议	应建立组织与外部方交换信息和软件的协议。
		A.10.8.3 运输中的物理介质	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、不当使用或破坏。
		A.10.8.4 电子消息发送	包含在电子消息发送中的信息应予以适当的保护。

		A.10.8.5 业务信息系统	应建立并实施策略和规程，以保护与业务信息系统互联相关的信息。
A.10.9	**电子商务服务**		
		A.10.9.1 电子商务	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、合同争议以及未授权的泄露和修改。
		A.10.9.2 在线交易	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。
		A.10.9.3 公共可用信息	在公共可用系统中可用信息的完整性应受保护，以防止未授权的修改。
A.10.10	**监视**		
		A.10.10.1 审计记录	应产生记录用户活动、异常情况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.10.10.2 监视系统的使用	应建立信息处理设施的监视使用规程，并经常评审监视活动的结果。
		A.10.10.3 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。
		A.10.10.4 管理员和操作员日志	系统管理员和系统操作员活动应计入日志。
		A.10.10.5 故障日志	故障应被记录、分析，并采取适当的措施。
		A.10.10.6 时钟同步	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。
A.11	**访问控制**		
A.11.1	**访问控制的业务需求**		
		A.11.1.1 访问控制策略	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.11.2	**用户访问管理**		
		A.11.2.1 用户注册	应有正式的用户注册及注销规程，来授权和撤销对所有信息系统及服务的访问。
		A.11.2.2 特殊权限管理	应限制和控制特殊权限的分配及使用。
		A.11.2.3 用户口令管理	应通过正式的管理过程控制口令的分配。
		A.11.2.4 用户访问权的复查	管理者应定期使用正式过程对用户的访问权进行复查。

A.11.3	**用户责任**		
		A.11.3.1 口令使用	应要求用户在选择及使用口令时，遵循良好的安全习惯。
		A.11.3.2 无人值守的用户设备	用户应确保无人值守的用户设备有适当的保护
		A.11.3.3 清空桌面和屏幕策略	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.11.4	**网络访问控制**		
		A.11.4.1使用网络服务的策略	用户应仅能访问已获专门授权使用的服务。
		A.11.4.2 外部链接的用户鉴别	应使用适当的鉴别方法以控制远程用户的访问
		A.11.4.3 网络上的设备标识	应考虑自动设备标识，将其作为鉴别特定位置和设备连接的方法。
		A.11.4.4 远程诊断和配置端口的保护	对于诊断和配置端口的物理和逻辑访问加以控制。
		A.11.4.5 网络隔离	应在网络中隔离信息服务、用户及信息系统。
		A.11.4.6 网络连接控制	对于共享的网络，特别是越过组织边界的网络，用户的联网能力应按照访问控制策略和业务应用要求加以限制（见A.11.1）。
		A.11.4.7 网络路由控制	应在网络中实施路由控制，以确保计算机连接和信息流不违反业务应用的访问控制策略。
A.11.5	**操作系统访问控制**		
		A.11.5.1 安全登录规程	访问操作系统应通过安全登录规程加以控制。
		A.11.5.2 用户标识和鉴别	所有用户应有唯一的、专供其个人使用的标识符（用户ID），应选择一种适当的鉴别技术证实用户所宣称的身份。
		A.11.5.3 口令管理系统	口令管理系统应是交互式的，并应确保优质的口令。
		A.11.5.4 系统实用工具的使用	对于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.11.5.5 会话超时	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	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。
A.11.6	**应用和信息访问控制**		
		A.11.6.1信息访问限制	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	敏感系统应有专用的（隔离的）运算环境。

A.11.7	**移动计算和通信**		
		A.11.7.1 移动计算和通信	应有正式策略并且采用适当的安全措施，以防范使用移动计算和通信设施时所造成的风险。
		A.11.7.2 远程工作	应为远程工作活动开发和实施策略、操作计划和规程。
A.12	**信息系统获取、开发与维护**		
A.12.1	**信息系统的安全需求**		
		A.12.1.1 安全要求分析和说明	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。
A.12.2	**应用程序中正确的处理**		
		A.12.2.1 输入数据确认	应对输入应用系统的数据加以确认，以确保数据是正确且恰当的。
		A.12.2.2 内部处理的控制	确认核查应整合到应用中，以检测由于处理的差错或故意的行为造成的信息的任何讹误。
		A.12.2.3 消息完整性	应用中的确保真实性和保护消息完整性的要求应得到识别，适当的控制措施也应得到识别和实施。
		A.12.2.4 输出数据确认	从应用系统输出的数据应加以确认，以确保对所存储信息的处理是正确的且适于环境的。
A.12.3	**密码控制**		
		A.12.3.1 使用密码控制的策略	应开发和实施使用密码控制措施来保护信息的策略。
		A.12.3.2 密钥管理	应有密钥管理以支持组织使用密码技术。
A.12.4	**系统文件的安全**		
		A.12.4.1运行软件的控制	应有规程来控制在运行系统上安装软件。
		A.12.4.2 系统测试数据的保护	测试数据应认真地加以选择、保护和控制。
		A.12.4.3 对程序源代码的访问控制	应限制访问程序源代码。
A.12.5	**开发和支持过程的安全**		
		A.12.5.1 变更控制规程	应使用正式的变更控制规程来控制变更的实施
		A.12.5.2 操作系统变更后应用的技术评审	当操作系统发生变更时，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.12.5.3 软件包变更的限制	应对软件包的修改进行劝阻，只限于必须的变更，且对所有的变更加以严格控制。

		A.12.5.4 信息泄露	应防止信息泄露的额可能性。
		A.12.5.5 外包软件开发	组织应管理和监视外包软件的开发。
A.12.6	**技术漏洞管理**		
		A.12.6.1技术脆弱性的控制	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的风险。
A.13	**信息安全事件管理**		
A.13.1	**报告信息安全事件和缺陷**		
		A.13.1.1 报告信息安全事态	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.13.1.2 报告安全弱点	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。
A.13.2	**管理信息安全事件和改进**		
		A.13.2.1 职责和规程	应建立管理职责和规程，以确保快速、有效和有序地响应信息安全事件。
		A.13.2.2 对信息安全事件的总结	应有一套机制量化和监视信息安全事件的类型、数量和代价。
		A.13.2.3 证据的收集	当一个信息安全事件涉及到诉讼（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，以使其符合相关管辖区域对证据的要求。
A.14	**业务连续性管理**		
A.14.1	**业务连续性管理的信息安全方面**		
		A.14.1.1 在业务连续性管理过程中包含信息安全	应为贯穿于组织的业务连续性开发和保持一个管理过程，以解决组织的而业务连续性所需的信息安全要求。
		A.14.1.2 业务连续性和风险评估	应识别能引起业务过程中断的事态，连同这种中断发生的概率和影响，以及它们对信息安全所造成的后果。
		A.14.1.3 制定和实施包含信息安全的连续性计划	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。

		A.14.1.4 业务连续性计划框架	应保持一个唯一的业务连续性计划框架，以确保所有计划是一致的，能够协调地解决信息安全要求，并为测试和维护确定优先级。
		A.14.1.5 测试、维护和再评估业务连续性计划	业务连续性计划应定期测试和更新，以确保其及时性和有效性。
A.15	**符合性**		
A.15.1	**符合法律要求**		
		A.15.1.1 可用法律的识别	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.15.1.2 知识产权（IPR）	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.15.1.3 保护组织的记录	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.15.1.4 数据保护和个人信息的隐私	应依照相关的法律、法规和合同条款的要求，确保数据保护和隐私。
		A.15.1.5 防止滥用信息处理设施	应禁止用户使用信息处理设施用于未授权的目的。
		A.15.1.6 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。
A.15.2	**符合安全策略和标准**		
		A.15.2.1 符合安全策略和标准	管理人员应确保在其职责范围内的所有安全规程被正确地执行，以确保符合安全策略及标准
		A.15.2.2 技术符合性核查	信息系统应被定期核查是否符合安全实施标准
A.15.3	**信息系统审计的考虑**		
		A.15.3.1 信息系统审计控制措施	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.15.3.2 信息系统审计工具的保护	对于信息系统审计工具的访问应加以保护，以防止任何可能的滥用或损害。