信息安全发展至今，人们越来越认识到安全管理在整个信息安全建设过程中的重要性，而作为信息安全管理方面最著名的国际标准——ISO/IEC 27001（即之前所称的 BS7799 标准），则成为可以指导我们现实工作的最好的参照，它也是认证审核的标准。

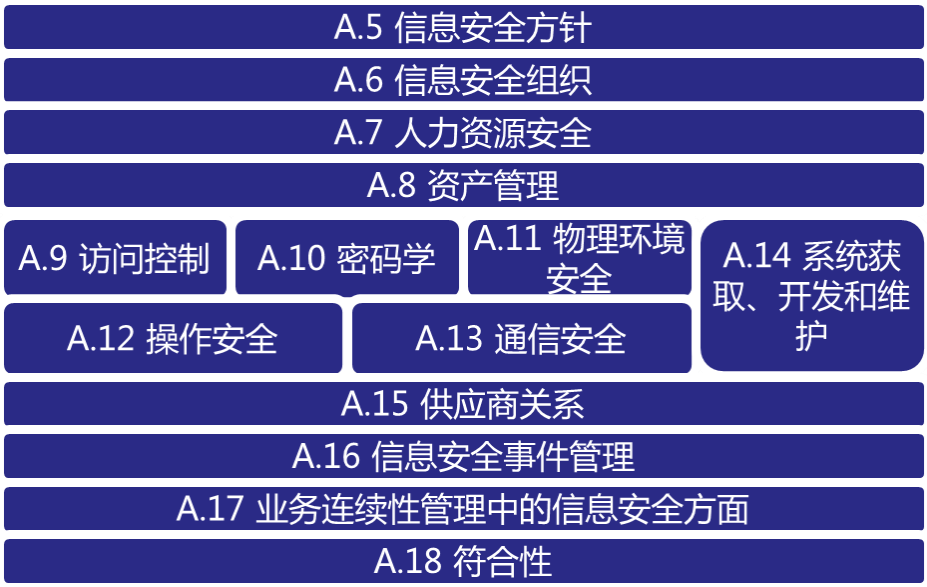
信息安全管理实用规则 ISO/IEC27001 的前身为英国的 BS7799 标准，该标准由英国标准协会（BSI）于 1995 年 2 月提出，并于 1995 年 5 月修订而成的。2000 年，国际标准化组织（ISO）在 BS7799-1 的基础上制定通过了 ISO 17799 标准。BS7799-2 在 2002 年也由 BSI 进行了重新的修订。ISO 组织在 2005 年对 ISO 17799 再次修订，BS7799-2 也于 2005 年被采用为 ISO/IEC 27001:2005。ISO 组织在 2013 年再次进行改版，发布了 ISO/IEC 27001:2013 版.

ISO/IEC 27001 标准，旨在规范、引导信息安全管理体系的发展过程和实施情况。ISO/IEC 27001 标准被外界认为是一个不偏向任何技术、任何企业和产品供应商的价值中立的管理体系。只要实施得当，ISO/IEC 27001 标准将帮助企业检查并确认其信息安全管理手段和实施方案的有效性。从企业外部来看，ISO/IEC 27001 关注信息的可用性、机密性和完整性，至今这仍然是这项标准致力达到的目标。

- **什么是信息安全管理**

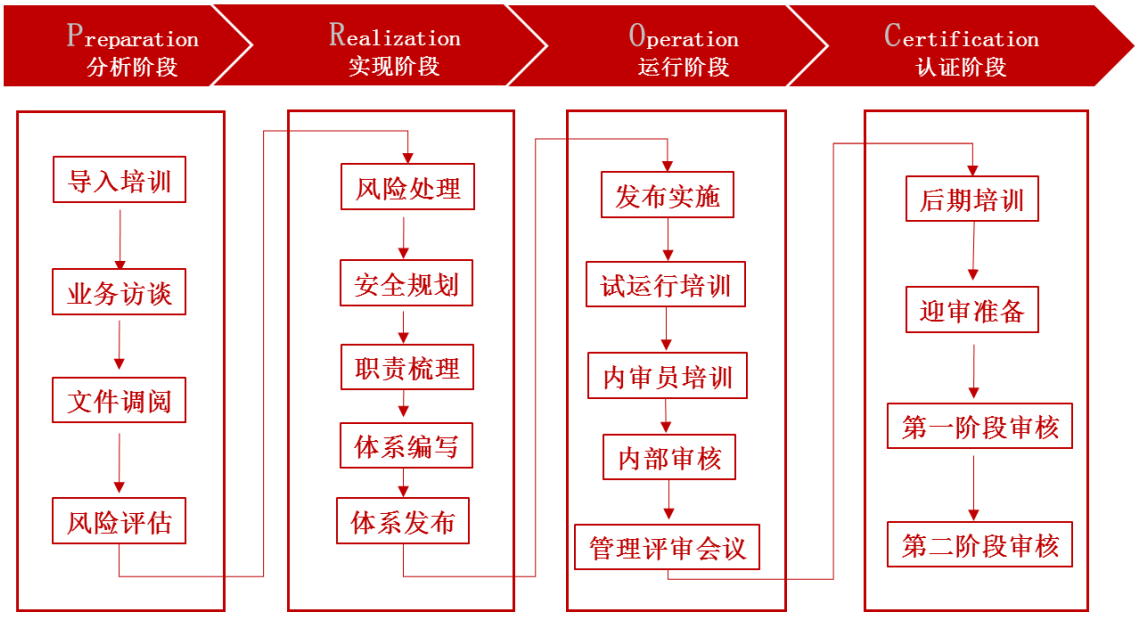
ISO/IEC 27001 标准，为建立、实施、运行、监视、评审、保持和改进信息安全管理体系提出了模型，其中详细说明了建立、实施和维护信息安全管理系统的要求，指出实施机构应该遵循的风险评估标准。作为一套管理标准，ISO/IEC 27001 指导相关人员怎样去应用 ISO/IEC 27001，其最终目的，还在于建立适合企业需要的信息安全管理系统。

ISO/IEC 27001 标准，定义了 14 个安全域和 114 个安全控制措施项。如下：



ISO/IEC 27001 标准要求的建立 ISO/IEC 27001 框架的过程：制定信息安全策略，确定体系范围，明确管理职责，通过风险评估确定控制目标和控制方式。体系一旦建立，组织应该实施、维护和持续改进 ISO/IEC 27001，保持体系的有效性。

- **如何实施基于 ISO27001 标准的信息服务管理体系**



ISO27001 管理体系咨询方法论

——分析阶段

通过前期的项目准备，使企业领导能充分的支持与授权相应人员进行信息安全的建设，并且通过安全意识的培训，使企业项目人员逐步了解信息安全管理相关的知识并树立

信息安全管理的理念

安言咨询将于企业主要人员一起，对企业业务目标进行分析。同时客观准确地评估信息安全管理现状、进行差距分析、评价安全管理成熟度，为后续风险评估和建立管理体系打下基础。

风险评估工作是风险管理的基础，同时也是建立企业信息安全管理体系的重要工作，风险评估工作主要是安言咨询对企业信息安全现状从技术与管理方面进行评估，同时与ISO27001 的标准及结合各类内外部监管要求进行差距对比，并确定企业今后风险评估方法。

——实现阶段

ISO/IEC 27001 把 信息安全管控的工作内容划分为 14 个安全控制域。这就要求项目组在项目实施阶段将 ISO/IEC 27001 的组织架构进行优化从而更有效、合理分配人员职责。人员职责分配是项目和后续运行成功的基础。因此安言咨询首先协助建立合理的项目组织及职责分配，这是成功的基础和组织保证。

安言咨询咨询配合企业根据国际信息安全管理标准 ISO27001 标准，在体系范围内建立完整的信息安全管理体系，达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式。主要是制定风险处置计划、ISMS 一、二级文件体系修订设计、体系文件编制辅导、内审与管理评审工作的指导。

——运行阶段

为了确保体系试运行的效果，安言咨询采取“先培训、后指导再推”工作思路使相关人员全面参与到体系的试运行过程中，同时建立畅通反馈渠道不断收集意见和建议，然后根据这些意对体系进行优化调整使有效运落实。

——认证阶段

安言咨询为企业培训迎审技巧及注意事项，然后由安言咨询项目经理和咨询顾问，和客户方项目组配合第三方认证机构进行第一阶段的认证审核，咨询机构协助通过并整改不符合项。完成后安排第三方认证机构的第二阶段注册审核，全面协助企业通过现场认证。

- **实施基于 ISO27001 标准的信息安全管理体系的必要性**

ISO27001 不仅是目前国际上最权威的信息安全管理体系标准，更重要的是它为企业的信息安全管理体系实施和落地提供了非常优秀的管理控制方法和风险评估理念。因此，企业需要在不断满足和更新相关安全技术产品的同时，不断反思和持续改进内部的安全管理科学性、有效性和适宜性，同时掌握正确的信息安全风险评估技能保持风险的可控和稳定。