**第六章 信息安全管理基础**

**1．什么是信息安全管理，为什么要实行信息安全管理？**

**2．信息安全管理应遵循的原则有哪些？**

**3．简要介绍信息安全管理模型的内容？**

**4．BS7799准则的主要内容是什么？**

**5．信息安全管理体系的过程包含哪些内容？**

**6．简要概述PDCA的过程内容？**

**7．如何确定ISMS的安全方针？**

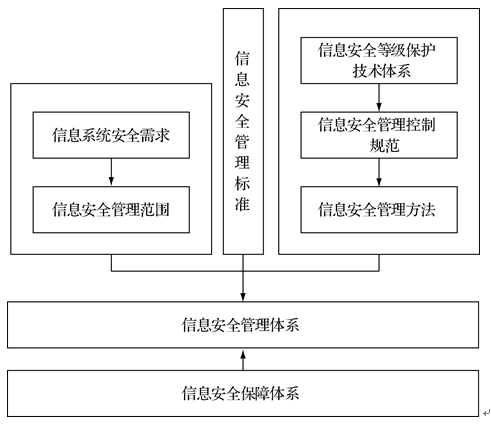
**8．如何修正ISMS内容中的不符合项？**

**9．如何进行ISMS的内部审核与管理评审？**

**10．为什么要进行信息安全管理体系的认证？**

1.（1）信息系统的规范化管理是建立在自身管理规范化的基础上，依照自身的运维流程对系统进行建设和管理，解决内部管理中的权限分发与权限集中的问题，要求对整个系统的流程形成制度化、流程化、标准化、表单化以及数据化。（2）信息管理的目的是让参与信息安全的所有人员都能够按照确定的要求去行动。对开发者的管理是为了开发出符合安全要求的系统或产品；对测试与评估者的管理是为了对开发的系统和产品严格把关；对运行管理者的管理是为了确保运行管理者对系统或产品的运行进行正确控制；对使用者的管理是为了让使用者按规定合理使用系统或产品；对监督检查者的管理是为了让执法者严格执法。不同安全等级的信息安全对管理有不同的要求。为了达到高级别的安全要求，需要更加严格的管理。

2. 信息安全管理应遵循如下统一的安全管理原则。①规范化原则：各阶段都应遵循安全规范要求，根据组织安全需求，制定安全策略；②系统化原则：根据安全工程的要求，对系统各阶段，包括以后的升级、换代和功能扩展进行全面统一的考虑；③综合保障原则：人员、资金、技术等多方面综合保障；④以人为本原则：技术是关键，管理是核心，提高管理人员的技术素养和道德水平；⑤预防原则：安全管理以预防为主，并要有一定的超前意识；⑥风险评估原则：根据实践对系统定期进行风险评估以改进系统的安全状况；⑦动态原则：根据环境的改变和技术的进步，提高系统的保护能力；⑧成本效益原则：根据资源价值和风险评估结果，采取适当的保护措施。此外，在信息安全管理的具体实施过程中还应道循以下原则：分权制衡原则、最小特权原则、职权分离原则、普遍参与原则、审计独立原则等。

3. 

信息系统安全需求是构建安全信息系统的基础。系统安全需求分析是指针对安全的指标，对信息系统中可能存在的风险及潜在威胁进行评估和分析，并以此为依据对信息及信息系统进行安全分类，从而利用不同的安全技术制定保护措施来应对风险。

信息安全管理范围是由信息系统安全需求决定的信息安全控制点，对这些控制点实施适当的控制措施就可以确保组织相应环节的信息安全，从而保证整个组织的整体信息安全水平。

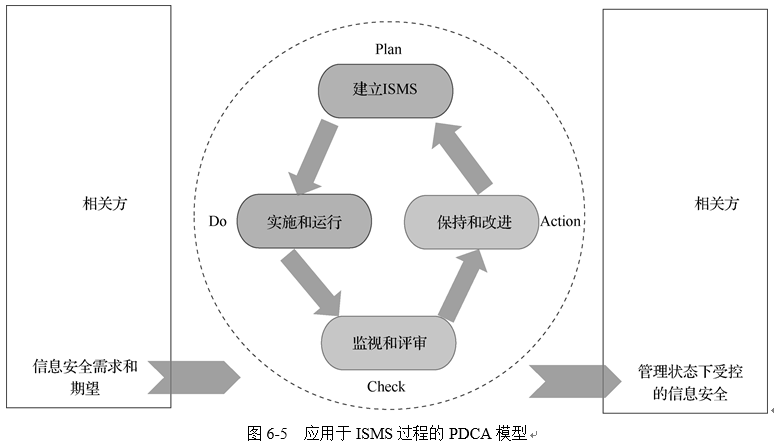
信息安全等级保护技术体系为信息安全管理提供了相应的理论依据，是对信息安全管理活动或结果规定的共同的和重复使用的具有指导性的规则、导则或特性文件。

信息安全管理控制规范是为了改善具体信息安全问题而设置的技术管理手段，并运用信息安全管理相关的方法来选择和实施控制规范，为信息安全管理体系服务。

4.BS7799内容主要由两大部分组成：BS7799-1：2000（《信息安全管理实施细则》）以及BS7799-2：2002（《信息安全管理体系规范》）。BS7799-1作为国际信息安全指导标准ISO／IECl7799基础的指导性文件，主要让负责开发的人员作为参考文档使用，从而在他们的机构内部实施和维护信息安全。这一部分包括十大管理要项，36个执行目标，127种控制方法。它涵盖了信息系统日常安全管理和控制方面的内容，提供了一个可持续提高的信息安全管理环境。BS7799-2作为信息安全管理体系ISMS（Information Security Management System）的规范，详细说明了建立、实施和维护信息安全管理体系的要求，规定了建立、实施信息安全管理体系的文档。BS7799完整覆盖了当前信息安全中的所有内容，提供了信息安全的统一的规范和要求。但是它没有详细说明信息安全管理是如何实施的，需要科学的流程和方法来指导实施。信息安全管理系统的规范，详细说明了建立、实施和维护信息安全管理系统（ISMS）的要求，指出实施组织需遵循某一风险评估来鉴定最适宜的控制对象，并对自己的需求采取适当的控制措施。

5.信息安全管理体系过程主要分为6个部分：准备、建立、实施和运行、监视和评审、保持和改进、认证。

6.信息安全管理体系的PDCA循环具有以下内容。①计划（Plan）——根据风险评估结果、法律法规要求、组织业务运作自身需要来确定控制目标与控制措施。②实施（Do）——实施所选的安全控制措施。③检查（Check）——依据策略、程序、标准和法律法规，对安全措施的实施情况进行符合性检查。④改进（Action）——根据ISMS审核、管理评审的结果及其他相关信息，采取纠正和预防措施，实现ISMS的持续改进。



7.制定信息安全方针应该参考以下原则。①包括制定目标框架和建立信息安全工作的总方向和原则；②考虑业务和法律法规的需求以及合同中包含的安全义务；③建立保持ISMS在风险管理环境下；④建立风险评价的准则和评估架构；⑤得到管理层的许可。

8.①执行监视、评审规程和其他控制措施，以达到如下目的：迅速检测过程运行结果中的错误；迅速识别已经或将要出现的安全违规及事故；使管理者能够确定分配给人员的安全活动或通过信息技术实施的安全活动是否如期执行；通过使用指示器等，帮助检测安全事件并预防安全事故；确定解决安全违规的措施是否有效等。②在考虑安全审核结果、事件、有效性测量结果、所有相关方的建议和反馈的基础上，定期评审ISMS的有效性，包括满足ISMS方针和目标，以及安全控制措施的评审。③测量控制措施的有效性以验证安全要求是否被满足。④定期进行风险评估的评审，对残余风险和已确定的可接受的风险级别进行评审，并且要考虑各方面的变化，如：组织情况、技术情况、业务目标和过程、已识别的威胁、已实施的控制措施的有效性、法律法规环境的变更、合同义务的变更和社会环境的变更等。⑤定期进行ISMS内部审核和管理评审。

9.（1）ISMS内部审核：①建立内部ISMS审核程序文件；②做好充分的内审准备；③执行内审；④报告审核结果；⑤讨论审核发现；⑥报告审核结果；⑦跟踪审核发现。（2）ISMS管理评审：管理层必须按计划的时间间隔（至少一年一次）评审ISMS，以确保其能持续保持合适性、充分性和有效性。评审必须包括评估ISMS的改进机会和变更需要，包括信息安全策略和信息安全目标。评审结果必须清楚地记入文件，并做好维护工作。

10.认证，是一种信用保证形式，是第三方所从事的活动，是一个组织证明其信息安全水平和能力符合国际标准要求的有效手段，它将帮助组织节约信息安全成本，增强客户、合作伙伴等相关方的信心，提高组织的公众形象和竞争力。具体来说，ISMS认证可以给组织带来如下收益：使组织获得最佳的信息安全运行方式；保证组织业务的安全；降低组织业务风险、避免组织损失；保持组织核心竞争优势；提升组织在业务活动中的信誉；增强组织竞争力；满足客户要求；保证组织业务的可持续发展；使组织符合法律法规的要求。