【安全管理培训大纲】

第一部分：安全标准培训（2 天）

通过两天的培训，可以使学员深刻的理解与掌握 ISO27000 体系规范、等级保护标准和其他行业的安全管理规范与实施步骤。培训课程采用理论与实施案例相结合、与学员互动的方式，有助于组织团队快速进入实施项目的准备状态，理解 ISO27000 实施过程和如何建立符合标准要求的 ISO27000 体系。

时间	培训大纲	培训内容	学员收益与技能提升
2 小时	ISO27001 标准培训	**ISO27001 标准演进历史** **ISO27001 的 PDCA 方法论** **ISO27001 的安全控制项介绍** ✓ 信息安全方针、策略与目标 ✓ 安全方针 ✓ 信息安全组织 ✓ 人力资源安全 ✓ 资产管理 ✓ 访问控制 ✓ 密码学 ✓ 物理与环境安全 ✓ 操作安全 ✓ 通信安全	使学员了解 ISO27001 标准最新版的 14 个控制领域，以及主要的控制措施建议，包括信息安全涉及的各方面内容，并通过控制措施实施案例，让学员了解不同行业的控制实施特点

		✓ 信息系统获取开发与维护 ✓ 供应关系 ✓ 信息安全事件管理 ✓ 业务连续性管理 ✓ 符合性	
1 小时	**等级保护标准培训**	**GB/T17959 标准介绍** **GB/T18336 标准介绍** **等级保护系列标准介绍**	使学员了解等级保护标准的 10 个控制领域，以及主要的控制措施建议
1 小时	**各类行业安全规范介绍**	**银监会信息科技风险管理指引介绍** **电监会信息安全相关规范介绍**	使学员了解金融行业和电力行业最新的安全行业管理规范
0.5 天	安全管理体系建设—调研方法培训	✓ ISMS 范围制定 ✓ 信息安全组织建立 ✓ 制度审核 ✓ 管理调研 ✓ 技术评估 ✓ 差距分析	使学员掌握 ISMS 范围制定，信息安全组织建立，现有制度审核，安全现状调研的理论基础、方法、实施过程，及相应实施工具，指导学员在组织中开展信息安全调研工作。
	风险评估	✓ 风险评估与管理概述 ✓ 风险评估与管理相关标准 ✓ 风险评估方法与实施	使学员了解信息安全风险评估的理论基础、方法、实施过程，及相应实施工具，指导学员在组织中开展基于信

		✓ 风险评估实施工具 ✓ 利用工具实施风险评估与管理	息资产的风险评估工作。
0.5 天	**体系架构** **体系建设**	✓ ISMS 制度文件体系架构 ✓ ISMS 文件清单梳理 ✓ 信息安全方针文件 ✓ 适用性声明（SOA） ✓ 有效性测量管理 ✓ 内部审核管理 ✓ 管理评审管理 ✓ 纠正预防管理 ✓ 持续改进管理	使学员掌握如何进行 ISMS 文件体系建构设计及文件的编制，掌握信息安全管理体系维护管理过程。
0.5 天	**体系运行** **体系认证**	✓ ISMS 体系运行与优化 ✓ 内部审核 ✓ 管理评审 ✓ 外部认证 ✓ 项目阶段总结与项目汇报	结合案例讲解信息安全体系推进运行的过程，明确 ISMS 体系运行的成功关键因素等，组织内部如何协调，如何进行内部审核与管理评审，如何顺利通过体系认证等。