2005/9-12建立ISMS（信息安全管理体系）计划

	主要项目内容	重要	9月				10月				11月				12月				编号 负责人	具体内容
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
1	确定信息安全管理体系的方针、目标和范围	✦		⇨																
1.1	制定信息安全方针																			
1.2	制定信息安全目标																			
1.3	确定信息安全管理体系的范围																			
2	对管理层进行信息安全管理体系基本知识培训			⇨																
2.1	对BS7799安全筹划指导委员会成员宣传培训（2H）																			编制相应的宣传培训资料
a	管理会议或更高级会议宣传																			
2.2	对BS7799推行干事标准理解培训（2H）																			编制相应的宣传培训资料
3	信息安全体系内部审核员培训																			
4	建立信息安全管理组织机构			⇨																
4.1	信息安全管理组织机构图																			
a	任命一名信息安全管理者代表（MR）																			
b	安全筹划指导委员会																			
c	建立安全风险管理小组																			
d	建立详细的安全风险管理承担人员/缓解风险责任人																			
4.2	职责权限描述																			
a	明确信息资产和与每个系统相关安全进程的负责人																			
b	确定负责信息资产和安全进程的管理人员																			
c	明确规定授权级别并进行备案																			
5	信息资产分类	✦		⇨	⇨															
5.1	信息资产责任/目录																			
5.2	信息资产分类																			
a	制定信息分类原则																			
b	信息资产分类																			
c	信息资产标识																			
6	风险评估	✦			⇨	⇨														
6.1	组织风险信息																			
a	确定组织资产和方案																			
b	确定威胁																			
c	确定漏洞																			
d	评估资产暴露程度																			
e	评估威胁的可能性																			
f	确定现有控制措施和利用可能性																			
6.2	确定汇总级安全风险优先级																			
a	确定影响等级																			
b	评估汇总总级可能性																			
c	完成汇总级风险列表																			
6.3	进行详细级风险优先级确定																			

2005/9-12建立ISMS（信息安全管理体系）计划

	主要项目内容	重要	9月				10月				11月				12月				编号 负责人	具体内容
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
a	确定影响和暴露程度																			
b	确定当前控制措施																			
c	确定影响可能性																			
d	确定详细风险级别																			
6.4	量化风险																			
a	为组织指定各个资产类别的货币值																			
b	为各个风险输入资产价值																			
c	制定单一预期损失																			
d	确定年发生率（ARO）																			
e	确定年预期损失（ALE）																			
7	实施决策支持				⇨	⇨														
7.1	定义功能要求																			
7.2	选择控制解决方案																			
a	集体讨论方法																			
b	分类控制																			
b.1	组织性控制措施																			
b.2	操作性控制措施																			
b.3	技术性控制措施																			
7.3	根据要求审查解决方案																			
7.4	评估各项控制措施降低风险的程度																			
7.5	评估各个解决方案的成本																			
a	购买成本																			
b	实施成本																			
c	持续成本																			
d	通信成本																			
e	IT员工的培训成本																			
f	用户的培训成本																			
g	生产力和方便性成本																			
h	审核和验证有效性的成本																			
7.6	选择风险缓解策略																			
8	制定信息安全方针手册					⇨														
9	制定各类控制程序					⇨														
10	制定适用性声明 （SOA）					⇨														
11	制定商业可持续性发展计划 （BCP）					⇨		⇨												
12	审批文件、发布实施							⇨												
13	文件到现场实施的转换							⇨	⇨	⇨										
14	(实施控制）体系运行									⇨	⇨	⇨	⇨	⇨	⇨	⇨	⇨	⇨		
15	(评定计划有效性）内部审核																⇨			