企业管理信息系统风险评估项目实施方案

一 目的

企业信息管理系统使企业常用的信息系统，它为企业内部管理信息，数据，人员，文档提供了一个信息化的平台 。对于企业信息管理系统，其安全需求主要表现为系统的机密性，完整性，而可用性安全需求会比较低，因此风险评估主要是围绕系统的机密性和可用性展开，风险评估的目的是通过分析系统面临的影响系统机密性，可用性的安全风险，并选用相应的安全措施降低风险。

二参考依据

本次风险评估依据的标准和政策是基于我国的《信息安全评估指南》

三项目范围

本次评估对象只有一个信息系统，我们的评估范围从系统所依赖的计算机以及网络设备，传输设备，移动存储设备，保障电子设备，安全保障设备等其他电子设备，还有信息系统所设计的系统软件，系统软件，应用软件，信息数据以及文档，网络服务，人员管理等方面进行评估。

四项目成果

1 节能型公司企业信息管理系统风险评估报告
2 企业管理信息系统风险评估项目实施方案
3 企业信息管理系统风险评估展示 PPT

五 项目组织

（1）xx 负责资产识别与评估
（2）xx 负责威胁识别与评估，脆弱点识别与评估
（3）xx 负责风险分析与评估
（4）xx 负责安全措施的选取工作

六项目实施

1 准备阶段
(1) 成立风险评估项目组，明确组织领导及协调人员，确定项目组织结构及相关各方职责；
(2) 收集被评估单位及信息系统相关资料文档；
(3) 确定项目实施具体范围、工作要求及工作安排；
2 实施阶段
2.1 资产识别

对被评估信息系统的关键资产进行识别，并合理分类；在资产识别过程中，需要详细识别核心资产的安全属性，重点识别出资产在遭受泄密、中断、损害等破坏时所遭受的影响，为资产影响分析及综合风险分析提供参考数据

工作方式：资产识别会议，相关资料的审查确认,主要由 xx 负责

2.2 威胁识别

通过威胁调查、取样等手段识别被评估信息系统的关键资产所面临的威胁源，及其威胁所常采用的威胁方法，对资产所产生的影响，并为后续威胁分析及综合风险分析提供参考数

据。

工作方式：人工问询，威胁识别会议，主要由 xx 负责

2.3 脆弱性识别

（1） 基础环境脆弱性识别

与信息系统有关的办公室，线路，硬件设备，计算机等

工作方式：现场调查

（2） 安全管理脆弱性识别

与信息系统有关的策略，组织架构，企业人员，安全控制等

工作方式：查资料，组内讨论

（3） 技术脆弱性识别

与信息系统有关的，在我们评估工作范围内的网络设备，操作系统等

工作方式：实地调查，组内讨论

主要由 xx 负责

3 分析阶段

3.1 资产分析

主要由 xx 完成

3.2 威胁分析

主要由 xx 完成

3.3 脆弱性分析

主要由 xx 完成

3.4 综合风险分析

主要由 xx 完成

3.5 安全措施有效性分析

主要由 xx 完成

4 汇报验收阶段

对项目依照考核要求进行验收，提交相关评估材料和整改方案。