**步步高2016年信息安全风险改善项目**

**立项报告**

项目编号:

撰写人: 肖红开

撰写日期: 2016-08-30

最后更改日期： 2016-09-19

文控编号:

版本号:  1.3

1. **项目背景**

公司运营过程中各业务系统数据访问的管控存在不足，往年常有发生公司商业机密信息、业务运营信息泄露事件，导致公司出现过不同程度的经济损失。随着集团业务发展的不断延伸，公司业务依赖信息系统越来越多，对业务数据的安全性要求也越来越高。因此，为提升公司信息系统安全管理，先行推动公司重要性等级较高业务系统中已知风险项的改善。

**二、业务现状**

通过2016年信息资产安全评估项目，共识别出安全风险68个。其中不可接受风险44个，可接受但需要控制的风险12个，可接受暂时无需采取安全措施的风险11个。

对于不可接受风险以及需要控制的风险，需要采取相应的风险管理措施降低风险。

**三、项目可解决的关键问题**

|  |  |  |
| --- | --- | --- |
| **序号** | **系统现状** | **解决方案（及可规避的风险）** |
| 1 | EBS、Retek备份数据不能有效还原 | 采用Active Data Guard存储方案，解决大数据系统数据还原问题，可保护数据完整性，防止数据丢失。 |
| 2 | 中心机房缺失自动灭火系统 | 部署自动灭火装置，可有效保障机房消防安全。 |
| 3 | 核心网络架构安全性不足，不能有效发现、拦截内部网络攻击 | 公司内网核心网络区域的关键业务节点部署防火墙，启用安全策略，可有效拦截内、外网的攻击，或入侵。 |
| 4 | 重要性等级较高的应用系统、数据库系统密码策略存在不足 | 增强应用系统、数据库密码安全策略，可有效提高密码爆破/猜解的可能。 |
| 5 | 离职人员账号及权限未及时清理 | 通过线上离职流程，或业务系统与PS系统集成，实现离职员工的系统账号权限及时清理 |
| 6 | 测试环境存有生产环境数据 | 对测试环境关键数据进行脱敏处理，避免生产业务信息的泄露。 |
| 7 | 系统用户密码以明文存储 | 规范用户口令密文存储机制，避免应系统口令泄露，而被他人利用的可能性。（如POS系统） |
| 8 | 系统用户的权限分配未标准化 | 规范用户权限分配准则，避免不相容职责的分配，可防止因用户权限过大导致数据泄密或产生舞弊行为。 |
| 9 | 资金相关的系统，未定期数据归档 | 制定数据归档方案，定期对系统数据归档处理，可有效提高系统处理能力并避免数据存储占用。 |
| 10 | 系统上线测试与评审不足 | 规范信息系统上线评审流程，可避免因系统功能不完善、存在安全漏洞，造成数据丢失、泄露等风险。 |

**四、项目回报**

针对 2016年Q2信息安全风险评估出的44个不可接受风险点的改善，将有效提升公司重要业务系统（包括资金相关系统）数据的完整性、可用性和保密性，从而有效保障了业务系统运行的稳定性，以及数据存储的安全性。

**五、项目范围**

执行的改善项共有14个大类，包括有：集团网络架构、机房消防系统、EBS系统、RETEK系统、Siebel系统、POS系统、长益系统（百货）、金力系统（家电）、餐饮卡系统、NC资金系统、PS系统、SSOA系统、海波龙系统、B2B系统（订货平台、销售系统）。

**六、项目内容与目标**

**项目内容：**推动2016年Q2风险评估项目已识别安全风险的改善。

**项目目标：**本次信息安全改善项，主要围绕2016年度内必须完成项进行（项目的总体完成目标为2016年12月31日前），各IT系统安全风险项对应责任人，依据各自提交的改善计划推进整改。

**七、项目团队**

以快消品事业群信息部主导，应用组与技术支持组执行系统改善的实施服务，开发组协助完成功能建设工作，PMO&信息安全组负责协调与跟进，项目团队成员如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目角色** | **项目成员** | **项目参与度**  **（人天）** |
| 1 | 项目总监 | 彭雄 | 5 |
| 2 | 项目经理/技术经理 | 王刚华/刘琳娜 | 25 |
| 3 | 应用组 | 陈宇、罗平、任重昊、余学明、文艳、张志林、邓宗勇、朱彩霞、侯智雄、胡赛徽、丁旺、佘水平、贺丽君 | 130 |
| 4 | 系统管理组 | 王晖（组长）、李海玲、陈文杰、马雄、杨迪、郭迪 | 40 |
| 5 | 开发组 | 祝坤、王应超、其他开发人员 | 20 |
| 7 | PMO&信息安全组 | 蒲振、黎建、肖红开 | 15 |

**八、项目周期、预算与激励**

**周期：其体计划如下：（附：项目关键节点计划表）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **实施阶段** | **计划开始时间** | **计划完成时间** |
| 1 | 项目启动 | 2016年9月19日 | 2016年9月23日 |
| 2 | 方案梳理 | 2016年9月26日 | 2016年10月20日 |
| 3 | 方案实施 | 2016年10月21日 | 2016年11月30日 |
| 4 | 切换运行 | 2016年11月20日 | 2016年12月20日 |
| 5 | 项目验收 | 2016年12月25日 | 2016年12月31日 |

**激励：**本项目为集团级项目，共需投入人力27人，预计总投入时间为235天，设立激励奖金2.35万。

**附件：**《步步高2016年信息安全风险改善项目行动计划》

《步步高2016年信息安全风险改善项目激励预算》

信息安全与综合管理部

2016年09月19日

主题词： 2016信息安全风险改善项目 立项报告

送：集团信息部 公司领导