云计算系统信息安全评估方案框架

一. 背景

对背景、意义进行简述

1.1. 评估目标

总体目标是，通过风险评估，全面了解云计算系统安全防护情况，查找云计算系统在安全保障方面存在的不足，并提出整改加固建议，为系统上线和运行提供决策依据。

1.2. 评估范围

甲方乙方合同中指定的评估范围。

二. 评估原则

为了确保此次安全评估项目成功实施，我们将遵循以下原则开展工作：

2.1. 保密原则

签署相关的保密协议和非侵害性协议。

2.2. 标准性原则

依据国际、国内及行业标准开展评估，评估过程遵循标准化和规范化原则。

2.3. 可控性原则

- 人员可控性
- 工具可控性
- 服务可控性
- 过程可控性

2.4. 全面性原则

2.5. 重点性原则

从被评估单位的业务期望出发，采用科学的安全风险评估方式对被评估单位提出的承载公开信息的重要业务、承载敏感信息的一般业务或重要业务、关键性业务系统进行重点评估。

2.6. 最小影响原则

三．评估标准

3.1. 信息安全国际、国内标准

3.2. 信息安全法规、政策

3.3. 信息安全行业管理规范

四．风险评估流程

参照 GB/T 20984

五. 资产识别与赋值

5.1. 资产调查

5.1.1. 调查对象

5.1.2. 调查方式

问卷调查

访谈

现场勘查。

5.1.3. 调查内容

调查内容将覆盖被评估系统的安全管理、物理、技术、操作等多方面的内容。

5.2. 资产分类

5.3. 资产赋值

六. 威胁评估

在信息安全风险评估中，威胁评估分为威胁识别和威胁赋值两部分内容。

6.1.1. 威胁分类

6.1.2. 威胁调查

6.1.2.1. 威胁发生频率数据统计

6.1.2.2. 威胁可能性分析

6.1.3. 威胁赋值

七. 安全管理脆弱性评估

安全管理评估以《信息安全技术 云计算服务安全能力要求》、《云计算服务安全指南》为基础，结合国家等级保护安全管理要求和《党政机关信息系统安全评测规范》DB11 T171—2002，评价被评估信息系统是否根据自身安全需求，建立必要的信息系统安全管理制度，对安全管理和执行过程通过安全策略、管理制度、操作规范等文件方式加以固化。安全管理评估主要采取问卷调查、访谈、现场查验等方式进行。管理评估共有495 项。

7.1.1. 政策、策略与计划

7.1.1.1. 信息安全方针和政策

7.1.1.2. 安全管理策略与制度

7.1.1.3. 云安全计划

7.1.1.4. 安全责任

（1）云服务商与用户安全责任划分标准

（2）云服务商安全责任内容

7.1.2. 安全集中管理体系

7.1.2.1. 安全管理中心

7.1.2.2. 运维管理中心

7.1.2.3. 安全审计中心

7.1.3. 安全组织与人员

7.1.3.1. 安全组织

7.1.3.2. 安全规章制度

7.1.3.3. 岗位风险与职责

7.1.3.4. 关键岗位人员管理

7.1.3.5. 人员筛选

7.1.3.6. 人员离职

7.1.3.7. 人员调动

7.1.3.8. 访问协议

7.1.3.9. 第三方人员安全

7.1.3.10. 人员处罚

7.1.3.11. 安全培训

7.1.3.12. 安全保密

7.1.4. 资产管理

7.1.4.1. 信息资产分类与标识

7.1.4.2. 资产登记

7.1.4.3. 资产定性赋值

7.1.5. 系统开发与供应链

7.1.5.1. 资源分配

7.1.5.2. 系统生命周期

7.1.5.3. 采购过程

7.1.5.4. 系统文档

7.1.5.5. 安全工程原则

7.1.5.6. 关键性分析

7.1.5.7. 外部信息系统服务

7.1.5.8. 开发商安全体系架构

7.1.5.9. 开发过程、标准和工具

7.1.5.10. 开发商配置管理

7.1.5.11. 开发商提供的培训

7.1.5.12. 防篡改

7.1.5.13. 组件真实性

7.1.5.14. 不被支持的系统组件

7.1.5.15. 供应链保护

7.1.5.16. 安全系统的设计和采购

7.1.5.17. 工程项目的控制和验收

7.1.5.18. 开发文件的控制和保护

7.1.6. 配置管理

7.1.6.1. 配置管理计划

7.1.6.2. 基线配置

7.1.6.3. 变更控制

7.1.6.4. 设置配置项的参数

7.1.6.5. 最小功能原则

7.1.6.6. 信息系统组件清单

7.1.7. 运行维护管理

7.1.7.1. 设备使用管理

7.1.7.2. 病毒防护

7.1.7.3. 密码和密钥管理

7.1.7.4. 运行状况监控

7.1.7.5. 用户管理

7.1.7.6. 受控维护

7.1.7.7. 维护工具

7.1.7.8. 远程维护

7.1.7.9. 维护人员

7.1.7.10. 及时维护

7.1.7.11. 缺陷修复

7.1.7.12. 安全功能验证

7.1.7.13. 软件、固件、信息完整性

7.1.8. 系统部置和迁移

7.1.8.1. 部署方案

7.1.8.2. 投入运行

7.1.8.3. 系统迁移

7.1.9. 应急响应与灾备

7.1.9.1. 事件处理计划

7.1.9.2. 事件处理

7.1.9.3. 安全事件报告

7.1.9.4. 事件响应支持

7.1.9.5. 安全警报

7.1.9.6. 错误处理

7.1.9.7. 应急响应计划

7.1.9.8. 应急培训

7.1.9.9. 应急演练

7.1.9.10. 信息系统备份

7.1.9.11. 支撑客户的业务连续性计划

7.1.9.12. 电信服务

7.1.10. 风险评估与持续监控

7.1.10.1. 风险评估

7.1.10.2. 脆弱性扫描

7.1.10.3. 持续监控

7.1.10.4. 信息系统监测

7.1.10.5. 垃圾信息监测

7.1.11. 审计

7.1.11.1. 可审计事件

7.1.11.2. 审计记录内容

7.1.11.3. 审计记录存储容量

7.1.11.4. 审计过程失败时的响应

7.1.11.5. 审计的审查、分析、报告

7.1.11.6. 审计处理和报告生成

7.1.11.7. 时间戳

7.1.11.8. 审计信息保护

7.1.11.9. 不可否认性

7.1.11.10. 审计记录留存

7.1.12. 其他管理要求

7.1.12.1. 知识产权要求

7.1.12.2. 保护证据纪录

7.1.12.3. 法律管辖要求

八. 技术脆弱性评估

8.1.1. 物理与环境安全

8.1.1.1. 物理设施与设备选址

8.1.1.2. 物理和环境规划

8.1.1.3. 物理环境访问授权

8.1.1.4. 物理环境访问控制

8.1.1.5. 通信能力防护

8.1.1.6. 输出设备访问控制

8.1.1.7. 物理访问监控

8.1.1.8. 访客访问记录

8.1.1.9. 电力设备和电缆安全保障

8.1.1.10. 应急照明能力

8.1.1.11. 消防能力

8.1.1.12. 温湿度控制能力

8.1.1.13. 防水能力

8.1.1.14. 设备运送和移除

8.1.2. 通信安全

8.1.2.1. 边界保护

8.1.2.2. 传输保密性和完整性

8.1.2.3. 网络中断

8.1.2.4. 可信路径

8.1.2.5. 会话认证

8.1.2.6. 通信完整性

8.1.3. 访问控制

8.1.3.1. 用户标识与鉴别

8.1.3.2. 设备标识与鉴别

8.1.3.3. 标识符管理

8.1.3.4. 鉴别凭证管理

8.1.3.5. 鉴别凭证反馈

8.1.3.6. 密码模块鉴别

8.1.3.7. 访问控制的实施

8.1.3.8. 信息流控制

8.1.3.9. 存储加密

8.1.3.10. 最小特权

8.1.3.11. 未成功的登录尝试

8.1.3.12. 系统使用通知

8.1.3.13. 前次访问通知

8.1.3.14. 并发会话控制

8.1.3.15. 会话锁定

8.1.3.16. 安全属性

8.1.3.17. 远程访问

8.1.3.18. 无线访问

8.1.3.19. 外部信息系统的使用

8.1.3.20. 信息共享

8.1.3.21. 可供公众访问的内容

8.1.3.22. 数据挖掘保护

8.1.3.23. 介质访问和使用

8.1.4. 主机和虚拟化安全

8.1.4.1. 主机服务器安全

8.1.4.2. 操作系统安全

8.1.4.3. 协同计算设备

8.1.4.4. 移动代码

8.1.4.5. 移动设备的物理连接

8.1.4.6. 恶意代码防护

8.1.4.7. 内存防护

8.1.4.8. 系统虚拟化安全性

8.1.4.9. 网络虚拟化安全性

8.1.5. 应用安全

8.1.5.1. 应用系统安全

8.1.5.2. WEB、应用接口及用户端安全

8.1.5.3. 源代码安全

8.1.6. 数据安全

8.1.6.1. 数据库安全

8.1.6.2. 数据保护

8.1.6.3. 数据隔离

8.1.6.4. 数据备份和恢复

九. 已有安全措施确认

十. 风险分析

10.1. 风险分析原理及内容

风险分析的原理

风险分析内容

风险值计算方法

10.2. 风险结果判定

10.3. 风险处置建议

十一. 评估计划

11.1. 项目组织结构

11.1.1. 甲方项目组结构

11.1.2. 乙方项目组结构

11.1.3. 人员名单及联系方式

11.2. 项目进度安排

11.3. 乙方配合事项

11.4. 评估风险控制

11.4.1. 评估风险监控

11.4.2. 评估风险的应对措施

11.4.3. 评估风险应急预案

11.5. 项目过程文档

注：此云计算系统风险评估方案框架是在原《云计算系统风险评估方案》基础上经过大幅度缩减而形成的。如果您觉得对您的工作有帮助，并且强列需要云计算系统风险评估方案》模版，请通过QQ：1044314296 联系本人。