

**傲基电子商务股份有限公司**

**信息系统一般控制**

**管理建议书**

**2015年01月01日- 2017年12月31日**

**目录**

[一、程序变更管理缺陷 - 2 -](#_Toc502310166)

[1 程序变更管理流程 - 2 -](#_Toc502310167)

[2 服务器操作系统/数据库维护管理机制 - 4 -](#_Toc502310168)

[3 变更管理监控机制 - 5 -](#_Toc502310169)

[二、逻辑访问管理缺陷 - 6 -](#_Toc502310170)

[4 系统安全设置 - 6 -](#_Toc502310171)

[5 系统用户权限管理 - 8 -](#_Toc502310172)

[6 逻辑访问监控流程 - 10 -](#_Toc502310173)

[三、数据备份缺陷 - 11 -](#_Toc502310174)

[7 备份恢复性测试及计划任务管理 - 11 -](#_Toc502310175)

# 一、程序变更管理缺陷

## 1 程序变更管理流程

**金蝶EAS系统，E登系统，佰易系统**

**观察所得**

* 在审计过程中，我们发现公司对于程序开发和采购、程序变更、参数/配置变更以及紧急变更制定了规章制度，但《软件开发流程管理制度》和《项目版本发布流程》对于流程中涉及的需求授权、用户部门测试确认、上线前审批环节（审批依据，审批人职位，节点设置等）没有做出具体规定。因此在日常执行过程中存在流程不规范的情况，同时缺乏完整的变更记录进行归档保存。

**存在的风险**

规范完整的程序变更流程能有效的确保程序变更满足业务需求，详细完整的《程序变更申请表》可以控制在授权、测试、审批过程中不同岗位的人员各司其职，建立有效的授权审批制度，同时可以方便在变更实施后对变更项目进行跟进监督。

* 如果缺乏变更中最初授权的控制，则容易造成变更需求不符合业务规定；
* 如果缺乏测试报告及测试人员签字的控制，则容易造成上线后功能不可用或不符合预期，以及测试责任缺失，无法准确的判断变更情况；
* 如果缺乏最终审批的控制，则容易造成上线过程对业务造成影响。另外由于变更涉及系统功能；
* 如果缺乏最终的审批也容易导致在未来使用过程中存在权责纠纷。

**我们的建议**

以下建议需同时建立以下流程制度并严格执行：

1. 变更管理流程（包含程序开发和采购、程序变更、配置/参数变更、紧急变更，维护）：
   * 程序变更的需求申请；
   * 业务部门负责人审阅需求并授权签字；
   * 软件服务提供商分析需求并签字确认；
   * 开发完成后上线前业务部门进行用户测试（UAT），并出具测试报告并签字；
   * 双方协商出具上线计划并取得业务部门审批；
   * 变更执行并签字
   * 业务部门验收并出具报告，

应保留各环节的正式书面记录，也可考虑通过建立OA系统进行变更流程的管理。

**管理层回复**

针对以上问题，IT运维部门需要制定变更管理流程并推进落实。该流程应该主要覆盖：

1. 线上程序变更申请。
2. 申请需要测试团队sign off。
3. 大版本的变更申请，需要业务团队负责人组织UAT并sign off。
4. 初期主要通过流程管理书面记录，接下来需要建立完整的变更申请系统记录变更行为和过程。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 模块名称 | 子模块 | 功能描述 | 开发耗时 | 完成进度 | 备注 |
| 工作流--workflow | 项目管理 | 项目申请变更电子流 | 8~16小时 | 90% |  |
| 项目成员申请 | 项目成员角色申请电子流（只针对技术部人员角色） | 8~16小时 | 90% |  |
| 项目用户权限管理 | 项目系统用户权限申请电子流 | 16~32小时 | 50% | 需考虑对接项目系统用户，暂未定 |
| 项目用户管理 | 项目系统用户申请电子流 | 16~32 | 50% |  |
| 项目变更 | 项目发布变更申请电子流 | 8~16小时 | 80% |  |
| 数据库变更 | 项目数据库变更申请电子流 | 64~128小时 | 50% | 需考虑对接项目系统数据库，耗时较多 |
| 计划任务变更 | 项目任务计划变更申请电子流 | 8~16小时 | 50% |  |
| 密码策略 | 未实施 |  |  | 0% | 考虑系统对接，前期搁置 |
| 特权用户管理 | 未实施 |  |  | 0% | 考虑系统对接，前期搁置 |
| 异地备份 | 未实施 |  |  | 0% | 将把此功能放进数据库备份功能看 |

## 2 服务器操作系统/数据库维护管理机制

**金蝶EAS系统，SQL Server 2005数据库**

**观察所得**

* 在审计过程中，我们了解到公司未对系统维护升级制定相关的制度和流程。
* 审计期间，金蝶系统发生过从K3系统向EAS系统整体升级迁移的行为，但未保留数据迁移前的准备，实施，迁移后的校验等相关资料等资料，未形成正式的数据迁移报告。

**存在的风险**

规范的系统维护升级流程能有效的对操作系统、数据库进行维护管理，使系统符合安全的业务要求。制定编写管理系统维护升级操作能协助管理人员清楚的了解系统的更新周期和健康状况。

* + 如果缺乏相应的系统维护记录，将无法连续追踪系统进行过的操作，不便于发生问题时对系统进行排查。
  + 数据在系统间迁移不完整可能影响业务连续性，对于财务系统可能影响财务数据的完整性和可靠性。

**我们的建议**

以下建议同时建立以下流程制度并严格执行：

1. 公司应针对服务器操作系统及数据库的迁移、维护升级制定相应的流程规范，对迁移和维护操作的申请、授权、测试及上线审批进行记录，便于管理人员对系统的性能以及维护周期进行了解。
2. 需维护并妥善保留完整的维护变更清单，并保证变更清单与建议1中的变更流程记录有一一对应关系，便于后续进行跟踪。建议以下两种情况：
3. 如服务器操作系统及数据库支持导出维护日志的，需定期导出并签字确认其完整性；
4. 如服务器操作系统及数据库不支持导出维护日志的，需由专人维护完整的清单，并定期签字确认其完整性。

**管理层回复**

组织完善数据迁移报告，并在未来的数据迁移中注意保留完整的迁移报告。

## 3变更管理监控机制

**金蝶K3系统，E登系统，佰易系统**

**观察所得**

在审计过程中，我们了解到公司未对程序变更，配置/参数变更，紧急变更以及系统维护的流程进行相应的监控管理。

**存在的风险**

合理的程序变更监控机制可以有效的保证整个程序变更过程是按照公司既定程序执行，且变更是经过合理授权、测试和上线前审批。

* + 如果缺乏变更监控机制，则不能及时发现变更流程中不合理的操作，可能会导致在系统中引入不必要的风险。

**我们的建议**

以下建议需同时完善制度及执行流程：

1. 建议定期根据变更清单抽取一定的样本，检查这些样本的执行过程是否符合已设定的变更管理流程，并进行签字确认，建议频率为每月。
2. 定期根据实际的管理流程更新IT管理制度，建议频率为每半年，以及流程发生重大变化时，并归档保留更新的审批记录。

**管理层回复**

和变更管理流程对应，组织每月1次的变更抽查。

每半年review一次变更管理流程。

# 二、逻辑访问管理缺陷

## 4系统安全设置

**E登系统，佰易系统**

**观察所得**

在审计过程中，我们了解到公司针对E登系统和佰易系统应用层面及其所在服务器的操作系统层面没有设置强密码安全策略：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **系统名 (应用系统/操作系统/数据库)** | **最小密码长度** | **初次登陆时使用一次性密码** | **密码**  **复杂性** | **强制变更**  **密码的**  **频率** | **锁定前允许的失败登录尝试的次数** | **用户指定自己密码的能力** | **再次使用某个密码前必须已使用的密码数目** | **空闲对话超时** | **记录失败的登录尝试** |
| E登系统  应用层面 | 6 | 是 | 是 | 未设置 | 未设置 | 能 | 未设置 | 未设置 | 是 |
| E登系统  应用服务器OS  &数据库服务器OS  Win server 2008 | 10 | 不适用 | 是 | 30天 | 未设置 | 能 | 2 | 未设置 | 是 |
| 佰易系统  应用层面 | 8 | 是 | 是 | 未设置 | 未设置 | 能 | 未设置 | 480分钟 | 是 |

**存在的风险**

密码安全策略是加强密码安全、防范密码破解的重要手段。缺乏密码安全策略的控制或密码安全策略设置不完整，将无法确保用户账号的安全，增加了应用系统或服务器遭受未经授权访问的风险。

**我们的建议**

以下建议需同时完善制度及执行流程：

我们建议在系统功能可实现的前提下，加强对系统应用层面和操作层面的密码设置（可参考附表中EY安全设置参考标准）。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 系统名称 | 最少密码长度 | 强迫修改初始密码 | 密码  复杂性 | 密码使  用期限 | 失败登录次数限制 | 用户能否修改密码 | 密码历史记录 | 空闲超时 | 失败登录记录 |
| XX系统 | 6 | 已  设置 | 已  设置 | 小于90天 | 5次 | 是 | 3次 | 15分钟 | 已设置 |

**管理层回复**

## 部分系统已经整改完毕，正在组织剩余系统的整改工作。5系统用户权限管理

**金蝶K3系统，E登系统，佰易系统**

**观察所得**

在审计过程中，我们了解到公司用户权限管理存在如下缺陷：

1. 尚未制定相关的制度和流程对系统的用户和权限进行定期审阅和确认。
2. 系统新建用户、用户权限变更、用户禁用或删除等的申请通过纸制申请单\邮件抄送部门领导\Tower平台提交审批的形式，尚未进行统一书面或电子档申请、审批管理，所申请的系统及权限描述不明确，以“参照XX员工”形式。
3. 尚未建立有效的流程以确保所有的离调职用户的权限均得到及时处理。包括岗位调动用户的原有权限及时禁用的流程，以及离职用户系统账号及时禁用的流程。
4. 公司目前尚未制定角色管理流程。

**存在的风险**

定期用户权限的清理可以保证业务部门人员始终拥有合理的系统权限。在发生人员离职或调职后，

* + 如果不及时将用户不需要的权限及时清理、调整，可能导致应用系统遭受被非授权人员恶意操作和系统数据泄漏的风险；
  + 如果权限申请没有书面或电子档形式进行管理，可能导致权限的授权没有经过应有的审批，无法保证授予的权限是否符合工作内容需要，是否符合“知所必需”“最小权限”原则。
  + 各系统的角色较多，如未设置合理的角色创建、角色所包含权限的增删改管理流程，可能会导致角色分配给的用户权限与实际业务不相符的情况

**我们的建议**

以下建议需同时完善制度及执行流程：

1. 建议公司实行定期对各系统用户进行权限清理工作，执行的频率可根据贵司的用户变动情况确定，建议半年至少执行一次。执行流程如下：
   * 复核发起者从系统中导出完整用户清单及角色功能表发给各业务部门负责人确认
   * 业务部门负责人将部门中岗位与权限不符合的情况反馈给复核发起人，由复核发起人对用户的角色权限进行处理。
   * 同时，信息部应对权限清理工作进行记录：包括系统导出的用户权限清单，各业务部门的反馈邮件等，反馈的结果，以及权限清理结果。
2. 设计有效的员工岗位调动的权限变更流程，并保留相关的变更记录。以下为可选的做法：

* 方法一：所有的员工岗位调动需要填写岗位调动表，并需经部门领导确认其新的系统权限，由信息部对其原有权限进行禁用。
* 方法二：人力资源部定期将岗位调动信息发送给信息部，信息部逐个与业务部门领导确认这些岗位调动用户的权限准确性，特别是原岗位的权限。并进行详细记录。
* 方法三：由人力资源系统自动触发变更授权。只要人力资源系统中的人员岗位进行变动，即触发相应的权限变更要求到OA系统进行审批或确认。

1. 设计有效的员工离职账号禁用流程，并保留相关的变更记录。以下为可选的做法：

* 方法一：所有的员工离职需要填写离职表，并需经部门领导确认其账号是否保留，保留的原因和期限，由信息部对其账号进行禁用或延期禁用的操作，并在相关系统中显示禁用日期。
* 方法二：人力资源部定期将离职信息发送给信息部，信息部逐个与业务部门领导确认这些离职用户的账号是否可禁用，并进行详细记录。
* 方法三：由人力资源系统自动触发离职授权。只要人力资源系统中的人员离职变动，即触发相应的系统账号变更要求到OA系统进行审批或确认。

1. 设计有效的新建账号申请流程，并保留相关的变更记录。以下为可选的做法：

* 方法一：所有的新建账号都需要填写申请表，并需经部门领导确认其申请是否符合工作需要，由信息部新建账号并赋权，且回复部门领导告知申请人提出的“参照XX员工权限”具体包括哪些权限。
* 方法二：由人力资源系统自动触发入职授权。只要人力资源系统中有新员工入职，即触发相应的系统账号新建要求到OA系统进行审批或确认。

**管理层回复**

同意意见。

## 6逻辑访问监控流程

**金蝶K3系统，E登系统，佰易系统**

**观察所得**

在审计过程中，我们发现公司尚未建立逻辑访问的监控流程，包含以下内容：

1. 未对各系统管理员的操作日志进行定期的检查和分析；
2. 尚未定期抽样检查用户账号新增、权限变更等操作是否经过合适的授权；

**存在的风险**

缺乏对逻辑访问的监控机制，将未能及时发现当前逻辑访问控制机制与实际业务不相符的情况，使得逻辑访问的控制未能起到维护系统访问安全性的功能。其中，缺乏对用户操作情况监督将导致用户的违规操作无法被察觉的风险，使系统安全存在隐患。

**我们的建议**

以下建议需同时完善制度及执行流程：

1. 制定逻辑访问控制相关制度并进行定期更新，确保制度要求与公司实际业务相符。
2. 定期导出用户权限或账号的变更操作日志，并抽样检查这些变更是否有相应的审批文件支持，以及时发现不合规操作的情况（需包含所有的管理员账号操作日志）。
3. 对具有系统特权（含用户权限修改）的用户的操作日志进行定期检查，以检查用户的系统操作行为与其岗位相符，且操作均经过合适的授权。

**管理层回复**

针对核心系统建立逻辑访问监控流程。对非核心边缘系统，采取日志分析的方式每半年集中做检查。

# 三、数据备份缺陷

## 7 备份恢复性测试及计划任务管理

**金蝶K3系统，E登系统，佰易系统**

**观察所得**

在审计过程中，我们发现公司已在设定了本地备份和异地备份机制。但仍有可改善之处：

* + 1. 尚未对系统异地备份数据定期执行恢复性测试及记录
    2. 未定期向异地云服务器供应商阿里云获取SOC1报告

在计划任务管理中，尚未建立计划任务设置和变更制定管理流程，且并定期对计划任务的完成情况进行检查。

**存在的风险**

有效的备份数据及定期的备份数据恢复性测试可以保证在重要业务数据丢失或业务运作中断时能有效地恢复应用系统和程序。若缺乏对恢复性测试，将无法及时发现恢复缺陷，从而导致当遇到突发事件时、系统数据或本地备份数据均不可用时，公司将没有后备数据支持，影响了公司业务的连续性和有效性。同时缺乏恢复性测试记录机制也不利于对系统数据恢复情况进行分析总结，以便对数据恢复机制进行升级。

公司各系统设置的计划任务较多，未对计划任务设置和变更进行管理可能导致计划任务不符合业务需求，或过分占用CPU影响系统正常的业务流程。

**我们的建议**

以下建议需同时完善制度及执行流程：

1. 创建对异地备份数据进行恢复性测试的机制。公司可根据业务数据的大小确定恢复性测试的频率(至少保证每半年1次)，并记录测试结果以便总结测试经验。
2. 建立计划任务管理流程，可参照程序变更管理。

**管理层回复**

半年进行一次异地备份恢复测试并记录结果。建立计划任务管理流程。