受控副本章	
发放编号	003
有效版本	A 版 0 次
实施日期	2010-05-01
使用部门	管理者代表

信息安全风险管理程序

1 范围

为了方便在考虑控制成本与风险平衡的前提下选择合适的控制目标和控制方式，将信息安全风险控制在可接受的水平，特制定本程序。

本程序适用于对信息安全管理体系信息安全风险的识别、评价、控制等管理。

2 职责

2.1 运管部负责牵头成立风险评估小组并组织协调信息安全风险管理工作。

2.2 风险评估小组负责编制[信息安全风险处置计划]，确认评估结果，形成[信息安全风险评估报告]。

2.3 各部门负责本部门使用或管理的资产的识别和风险评估，并负责本部门所涉及的资产的具体安全控制工作。

3 程序

3.1 风险评估前准备

3.1.1 运管部牵头成立风险评估小组，小组成员应包含信息安全重要责任部门的成员。

3.1.2 风险评估小组制定[信息安全风险评估计划]。

3.1.3 运管部协助各部门负责按[信息安全风险评估计划]，对影响本公司经营、服务和日常管理的重要业务系统以及涉及资产进行识别和风险评估。

3.2 风险评估的方法

3.2.1 运用 FEMA (评估潜在失效模式及影响的定量分析)方法从以下三个方面进行风险评价，然后算出风险值 RPN，以确定风险等级。

a) S－严重性：失效可能产生后果的严重程度；

b) O－可能性：预计出现的频率；

c) W－脆弱性：引起威胁脆弱点的脆弱程度；

计算公式：风险值 RPN=S×O×W

3.3 判定标准

a) 严重性(S)：INT｛影响（E）* 资产重要性分值（CIA）/10｝

影响（E）	分值

1） 不影响正常工作及客户的满意度，对公司运营影响不大----------2

2） 工作停止一个工作日以下，对公司运营有一定影响----------5

3） 工作停止一个工作日以上，严重影响公司运营、声誉、竞争力；

4） 违反法律法规或合同要求----------8

注：严重性分值取决于两部分，影响和资产的重要性，最后的分值如产生小数，直接进 1 取整，如 E=6 分，CIA=8 分，S=4.8 分，取整为 5 分。CIA 分值计算参考《资产识别管理程序》。

b) 可能性(O) ： 分值

5） 威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生----------2

6） 出现的频率较小；或一般不太可能发生；或没有被证实发生过----------3-4

7） 出现的频率中等（或> 1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过----------5

8） 出现的频率较高（或≥ 1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过----------6-7

9） 出现的频率很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过----------8

注：参考《GB/T 20984:2007 信息安全风险评估规范》

c) 脆弱性(W) ： 分值

10）现有系统能够自动识别，且有充分有效----------2

11）通过检查/监控能够看出趋势或有较充分----------5

12）现有条件下不能探测或一旦问题发生没有有----------8

3.4 风险等级判定

a) 风险按风险值 RPN，分为一、二、三级，其中一级为最高风险等级，三级为最低风险等级。风险等级判定标准见下表：

风险值（RPN）：（S×O×W）

RPN 分数值	风险程度	风险等级
126-512	高，需采取控制措施	一
51-125	中，需采取控制措施	二
8-50	低，可采取一般管理措施	三

*注：S=8（S 为最高分，表示影响最大，且资产重要性最大）的资产必须给予一级。

b) 各部门根据风险评估的结果，确定相关信息资产的风险等级，记入[信息资产风险评估表]。

3.5 风险评估的方法

可选的风险处置分为两大类：

a) 风险控制类

1） 降低风险，即采取适宜的控制措施降低风险至可接受的程度；

2） 回避风险，即不采纳可能导致风险的措施从而避免风险；

3） 转移风险，即将风险转嫁给其他方，如保险公司或供应商；

b) 风险接受类

接受风险，即遵守可接受风险准则，客观地并有意识地接受风险。

3.6 风险处置流程

a) 一二级风险的处置流程

对于评估为一级、二级风险的信息资产，责任部门应制定[信息安全风险处置计划]，将选择的风险处置方法及具体措施记入[信息资产风险评估表]，并向风险评估小组报告。风险控制措施可以是技术型的也可以是管理型的，选择风险控制措施应满足法律法规要求、合同方要求并考虑公司成本要求。

对于评估为一级、二级风险的可能需要采取接受风险处置的信息资产，责任部门必须提出残存风险申请，报告风险评估小组，并最终由总经理批准。

b) 三级风险的处置流程

评估为三级的信息资产，可直接提出残存风险申请，经总经理批准后，进行登记管理。

3.7 风险控制处置的跟踪

每半年责任部门应跟踪风险处置的结果并进行风险评估，记入[信息资产风险评估表]，并向风险评估小组报告。

对风险评估再次评定为一级、二级的信息资产，可申请为残余风险。

3.8 可接受风险

3.8.1 可接受风险的准则

符合以下条款的风险可以接受：

a) 满足法律法规或者合同方要求；

b) 对公司业务持续性影响较小。

3.8.2 可接受风险的水平

公司可接受风险水平如下：

a) 三级风险为可接受风险；

b) 在满足公司信息方针、法律法规要求、合同方要求的前提下，对被评估为一级、二级但处置成本太高的风险，可在经残存风险申请后，由总经理认可并接受风险。

3.9 残余风险的申请与批准

信息资产作为残余风险，责任部门必须提出申请，报告风险评估小组，并最终由总经理准。

对被列入风险接受或残余风险的信息资产，责任部门必须采取必要的管理措施以保持并改善目前的风险水平。

3.10 风险评估结果的运用

信息资产风险评估的登记结果，运用于以下事项：

a) 信息安全的目标、管理方案、运行控制及监视测量的实施和运行；

b) ISMS 紧急事态对应预案的制订；

c) 保证信息资产安全的设备、设施的设定；

d) 内外部的审核；

e) 风险预防、控制管理规定的设定。

3.11 变更评估与周期性评审

当输入的信息资产、适用的法律法规要求或合同方要求、公司的信息方针等发生重大变化时，各部门应重新进行风险评估和制定信息安全风险处置计划。风险评估小组每半年一次收集信息各部门变更信息并更新相应表格。

每年年末，各部门应对本部门信息资产的风险评估、风险处置、残余风险、可接受风险水平进行评审。

3.12 风险评估结果、风险处置的文件管理

a) 各部门根据《记录控制程序》要求，管理所属的风险评估结果、风险处置计划、结果跟踪、变更评估及年度评审结果，保存相应表格。

b) 风险评估小组对各部门报告的[信息资产风险评估表]进行汇总，形成信息资产风险评估汇总表。根据《记录控制程序》要求，保存相应表格。体系建立初期可考虑由风险评估小组直接进行评估，以后再指导各部门进行。

3.13 当企业发生以下情况时需及时进行风险评估：

a) 当发生重大信息安全事故时；

b) 当信息网络系统发生重大更改时。

4 相关文件和记录

《记录控制程序》

《资产识别管理程序》

［信息安全风险评估计划］	保存部门：使用部门	保存期限：2 年
［信息资产风险评估表］	保存部门：使用部门	保存期限：2 年
［信息安全风险处置计划］	保存部门：使用部门	保存期限：2 年
［信息安全风险评估报告］	保存部门：使用部门	保存期限：2 年
［信息资产风险接受、残余风险审批表］	保存部门：使用部门	保存期限：2 年

附加说明：

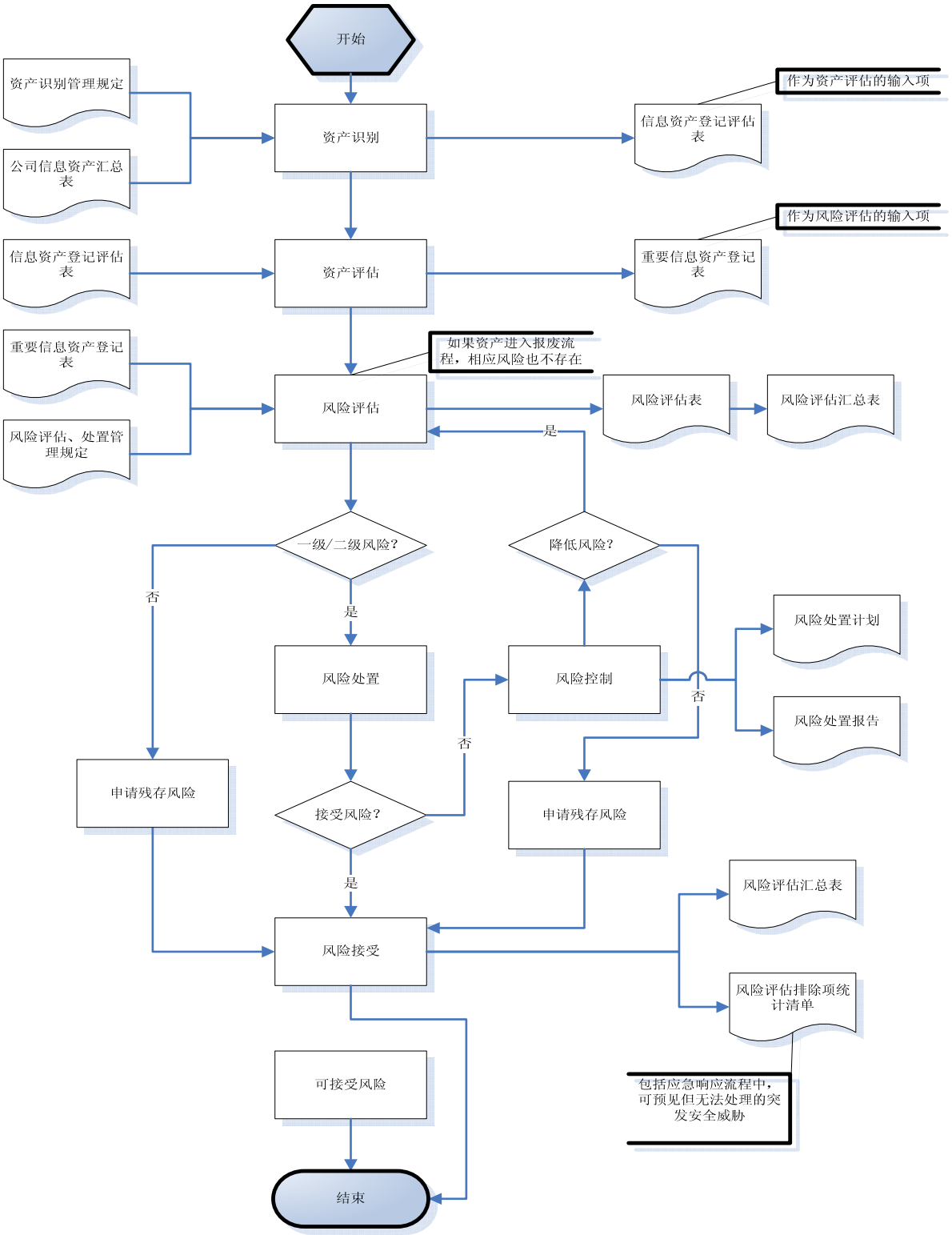
本标准由湖南丰汇银佳科技有限公司提出。

本标准由湖南丰汇银佳科技有限公司运管部起草。

起草：熊文群　　审核：杨彬　　批准：刘熙　　日期：2010-04-28

附录 A

风险评估流程图


开始
资产识别管理规定
公司信息资产汇总表
资产识别
信息资产登记评估表
作为资产评估的输入项
信息资产登记评估表
资产评估
重要信息资产登记表
作为风险评估的输入项
重要信息资产登记表
风险评估、处置管理规定
如果资产进入报废流程，相应风险也不存在
风险评估
风险评估表
风险评估汇总表
是
一级/二级风险？
降低风险？
否
是
风险处置
风险控制
风险处置计划
风险处置报告
否
否
申请残存风险
接受风险？
申请残存风险
是
风险评估汇总表
风险接受
风险评估排除项统计清单
可接受风险
包括应急响应流程中，可预见但无法处理的突发安全威胁
结束