X X X X网络安全技术有限公司	编　　号：NN-PD17
程　　序　　文　　件	版　　次：080501
	生效日期：2008.05.01

信息安全风险评估管理程序

编制：　　日期：

审核：　　日期：

批准：　　日期：

本版修改记录

修改状态	日期	修改原因及内容提要	修改人	审核人	批准人

信息安全风险评估管理程序

1.0目的

在ISMS 覆盖范围内对信息安全现行状况进行系统风险评估，形成评估报告，描述风险等级，识别和评价供处理风险的可选措施，选择控制目标和控制措施处理风险。

2.0适用范围

在ISMS 覆盖范围内主要信息资产

3.0定义（无）

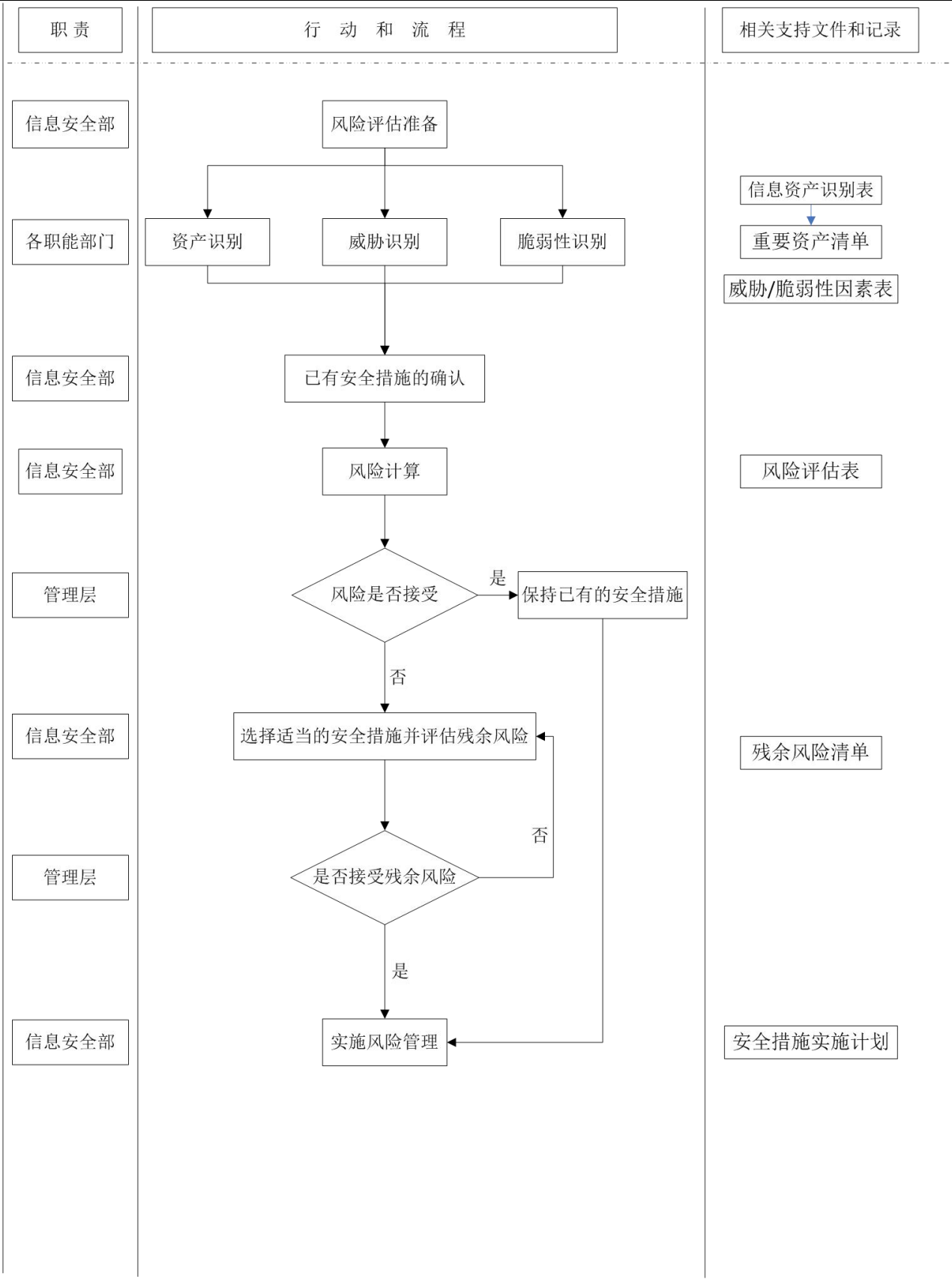
4.0职责

4.1各部门负责部门内部资产的识别，确定资产价值。

4.2信息安全部负责风险评估和制订控制措施。

4.3CEO负责信息系统运行的批准。

5.0流程图


职 责
行 动 和 流 程
相关支持文件和记录
信息安全部
风险评估准备
各职能部门
资产识别
威胁识别
脆弱性识别
信息资产识别表
重要资产清单
威胁/脆弱性因素表
信息安全部
已有安全措施的确认
信息安全部
风险计算
风险评估表
管理层
风险是否接受
是
保持已有的安全措施
否
信息安全部
选择适当的安全措施并评估残余风险
残余风险清单
否
管理层
是否接受残余风险
是
信息安全部
实施风险管理
安全措施实施计划

6.0内容

6.1资产的识别

6.1.1 各部门每年按照管理者代表的要求负责部门内部资产的识别，确定资产价值。

6.1.2 资产分类

根据资产的表现形式，可将资产分为数据、软件、硬件、文档、服务、人员等类。

6.1.3 资产（A）赋值

资产赋值就是对资产在机密性、完整性和可用性上的达成程度进行分析，选择对资产机密性、完整性和可用性最为重要（分值最高）的一个属性的赋值等级作为资产的最终赋值结果。资产等级划分为五级，分别代表资产重要性的高低。等级数值越大，资产价值越高。

1）机密性赋值

根据资产在机密性上的不同要求，将其分为五个不同的等级，分别对应资产在机密性上的应达成的不同程度或者机密性缺失时对整个组织的影响。

赋值	标识	定义
5	极高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性影响，如果泄漏会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	包含组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	包含仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成损害
1	可忽略	包含可对社会公开的信息，公用的信息处理设备和系统资源等

2）完整性赋值

根据资产在完整性上的不同要求，将其分为五个不同的等级，分别对应资产在完整性上的达成的不同程度或者完整性缺失时对整个组织的影响。

赋值	标识	定义
5	极高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补

4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，比较难以弥补
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，可以忍受，对业务冲击轻微，容易弥补
1	可忽略	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略

3）可用性赋值

根据资产在可用性上的不同要求，将其分为五个不同的等级，分别对应资产在可用性上的达成的不同程度。

赋值	标识	定义
5	极高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上
4	高	可用性价值较高，合法使用者对信息及信息系统的可用度达到每天 90%以上
3	中等	可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上
1	可忽略	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%

3 分以上为重要资产，重要信息资产由信息安全部确立清单

6.2 威胁识别

6.2.1 威胁分类

对重要资产应由 ISMS 小组识别其面临的威胁。针对威胁来源，根据其表现形式将威胁分为软硬件故障、物理环境威胁、无作为或操作失误、管理不到位、恶意代码和病毒、越权或滥用、黑客攻击技术、物理攻击、泄密、篡改和抵赖等。

6.2.2 威胁(T)赋值

评估者应根据经验和（或）有关的统计数据来判断威胁出现的频率。威胁频率

等级划分为五级，分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。威胁赋值见下表。

等级	标识	定义
5	很高	威胁出现的频率很高,在大多数情况下几乎不可避免或者可以证实经常发生过（每天）
4	高	威胁出现的频率较高,在大多数情况下很有可能会发生或者可以证实多次发生过（每周）
3	中	威胁出现的频率中等,在某种情况下可能会发生或被证实曾经发生过（每月、曾经发生过）
2	低	威胁出现的频率较小，一般不太可能发生，也没有被证实发生过（每年）
1	很低	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（特殊情况）

6.3 脆弱性识别

6.3.1 脆弱性识别内容

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性又可分为技术管理和组织管理两方面，前者与具体技术活动相关，后者与管理环境相关。

6.3.2 脆弱性(V)严重程度赋值

脆弱性严重程度的等级划分为五级，分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。脆弱性严重程度赋值见下表

等级	标识	定义
5	很高	如果被威胁利用，将对资产造成完全损害（90%以上）
4	高	如果被威胁利用，将对资产造成重大损害（70%）
3	中	如果被威胁利用，将对资产造成一般损害（30%）
2	低	如果被威胁利用，将对资产造成较小损害（10%）
1	很低	如果被威胁利用，将对资产造成的损害可以忽略（10%以下）

6.4已有安全措施的确认

ISMS小组应对已采取的安全措施的有效性进行确认，对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对于确认为不适当的安全措施应核实是否应被取消，或者用更合适的安全措施替代。

6.5风险分析

完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，ISMS小组采用矩阵法确定威胁利用脆弱性导致安全事件发生的可能性，考虑安全事件一旦发生其所作用的资产的重要性及脆弱性的严重程度判断安全事件造成的损失对组织的影响，即安全风险。

6.5.1安全事件发生的可能性等级$P=(T*V)^{0.5}$，

6.5.2安全事件发生后的损失等级$L=(A*V)^{0.5}$，

6.5.3风险值R＝(L*P)，风险等级

风险值	1－5	6－10	11－15	16－20	21－25
风险等级	1	2	3	4	5

6.5.4风险管理策略

6.5.4.1完全的消除风险是不可能和不实际的。公司需要有效和经济的运转，因此必须根据安全事件的可能性和对业务的影响来平衡费用、时间、安全尺度几个方面的问题。公司在考虑接受残余风险时的标准为只接受中或低范围内的风险；但是对于必须投入很高的费用才能将残余风险降为中或低的情况，则分阶段实施控制。

6.5.4.2风险值越高，安全事件发生的可能性就越高，安全事件对该资产以及业务的影响也就越大，风险管理策略有以下：

- 接受风险：接受潜在的风险并继续运行信息系统，不对风险进行处理。
- 降低风险：通过实现安全措施来降低风险，从而将脆弱性被威胁源利用后可能带来的不利影响最小化（如使用防火墙、漏洞扫描系统等安全产品）。
- 规避风险：不介入风险，通过消除风险的原因和/或后果（如放弃系统某项功能或关闭系统）来规避风险。
- 转移风险：通过使用其它措施来补偿损失，从而转移风险，如购买保险。

6.5.4.3风险等级3（含）以上为不可接受风险，3（不含）以下为可接受风险。如果是可接受风险，可保持已有的安全措施；如果是不可接受风险，则需要采取安全措施以降低、控制风险。安全措施的选择应兼顾管理与技术两个方面，可以参照信息安全的相关标准实施。

6.6 确定控制目标、控制措施和对策

基于在风险评估结果报告中提出的风险级别，ISMS小组对风险处理的工作进行优先级排序。高等级（例如被定义为“非常高”或“高”风险级的风险）的风险项应该最优先处理。

- 评估所建议的安全措施
- 实施成本效益分析
- 选择安全措施
- 制定安全措施的实现计划
- 实现所选择的安全措施

6.7 残余风险的监视与处理

风险处理的最后过程中，ISMS小组应列举出信息系统中所有残余风险的清单。在信息系统的运行中，应密切监视这些残余风险的变化，并及时处理。

每年年初评估信息系统安全风险时,对残余风险和已确定的可接受的风险级别进行评审时，应考虑以下方面的变化：

- 组织结构；
- 技术；
- 业务目标和过程；
- 已识别的威胁；
- 已实施控制措施的有效性；
- 外部事件，如法律法规环境的变更、合同义务的变更和社会环境的变更。

6.8信息系统运行的批准

ISMS小组考察风险处理的结果，判断残余风险是否处在可接受的水平之内。基于这一判断，管理层将做出决策，决定是否允许信息系统运行。

如果信息系统的残余风险不可接受，而现实情况又要求系统必须投入运行，且当前没有其它资源能胜任单位的使命。这时可以临时批准信息系统投入运行。

在这种情况下，必须由信息系统的主管者决定临时运行的时间段，制定出在此期间的应急预案以及继续处理风险的措施。在临时运行的时间段结束后，应重新评估残余风险的可接受度。如果残余风险仍然不可接受，则一般不应再批准信息系统临时运行。

7.0相关文件

7.1《GB/T20984-2007信息安全风险评估规范》

7.2《信息资产管理制度》

8.0记录

8.1《信息资产识别表》

8.2《重要资产清单》

8.3《威胁/脆弱性因素表》

8.4《风险评估表》

8.5《安全措施实施计划》

8.6《残余风险清单》