xxxx有限公司

标准操作政策与程序

SOPP

编 号	ISMS-SOPP-009		第1页共10页
文件名	信息安全风险评估管理程序		版 号：0
由管理会议推荐：			修改状态：
部门负责人制订： 日期：	总经理审核： 日期：	董事经理批准： 日期：	生效日期：

1．目的

在 ISMS 覆盖范围内对信息安全现行状况运用标准模式，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．范围

在 ISMS 覆盖范围内主要信息资产

3．定义

见程序中描述

4．职责

见程序中描述

5．程序

5．1 按照以下定义，使用 ISMS Tool 3 model 来收集信息资产数据，确定组织资产和方案。

5．1．1 定义纵深防御模型

物 理
网 络
主 机
应 用
数 据

a．网络防护：一个精心设计和正确实施的网络体系结构可提供高可用、安全、可扩展、易管理和可靠的服务。 组织中可能有多个网络，应对它们逐一评估以确保它们都得到了适

当的安全保护，或确保已保护了高价值网络免受未被保护的网络的影响。 实施内部网络防御包括正确的网络设计、无线网络安全，并可能使用 Internet 协议安全（IPSec）以确保只有受信任的计算机能够访问重要的网络资源。

b．主机防御：主机可分为两种类型：客户端和服务器。 有效地保护这两种主机的安全要求您在加强级别和可用性级别这两者之间找到一个平衡点。 尽管存在例外，但通常一台计算机的可用性降低时，其安全性提高。 主机防御可能包括禁用服务、删除特定的用户权限、使操作系统保持最新以及使用防病毒和分布式防火墙产品。

c．应用程序防御：应用程序防御对安全模型而言非常重要。 应用程序存在于整个系统的环境中，所以在评估应用程序安全性时，应考虑到整个环境的安全性。 在生产环境下运行每个应用程序之前，都应对其安全性进行彻底的测试。 实施应用程序防御包括正确的应用程序体系结构，其中包括确保应用程序以最低权限运行，暴露的受攻击面尽可能小。

d．数据防御:对于大多数组织，数据是最重要的资源。 在客户端级别，数据往往在本地存储，而且可能特别易受攻击。 可以用多种方式保护数据，包括使用加密文件服务（EFS）和

经常安全地进行备份。

5．1．2 按照纵深防御层定义，使用 ISMS Tool 1model 收集 ISMS 范围内信息资产。

ISMS 信息资产收集					
纵深防御层	信息资产名称	所有者	使用者	责任者	描述
物理					
网络					
主机					
应用					
数据					

ISMS Tool 1model

5．2 按照以下定义对信息资产进行定性评估资产类别、暴露程度和威胁可能性。

5．2．1 定性资产类别定义

a． 高度业务影响（HBI）：对信息资产的机密性、完整性或可用性的影响将对组织造成严重的或灾难性的损失。

b． 中度业务影响（MBI）：对信息资产的机密性、完整性或可用性的影响将对组织造成中度损失。

c． 低度业务影响（L BI）：未包括在 HBI 或 MBI 中的资产被分类为 LBI，且除了针对保护基础结构的标准最佳方法以外，没有正式的保护要求或附加的控制措施。

5．2．2 定义资产暴露程度

高度暴露 — 资产的严重或完全损失

中度暴露 — 有限或中度损失

低度暴露 — 极少或没有损失

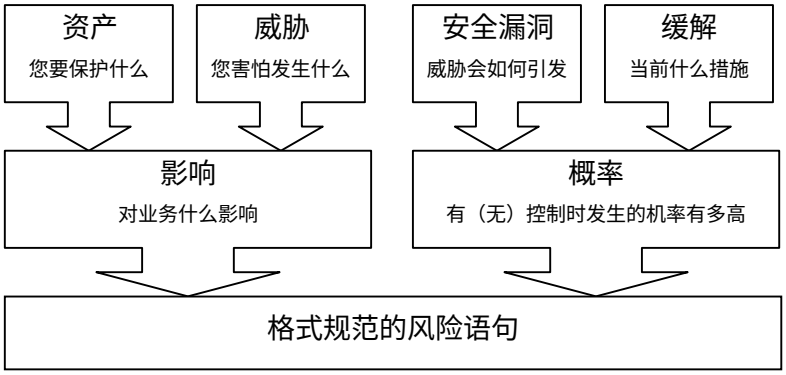
5．2．3 定义威胁的可能性

高 — 预计一个或多个影响可能在一年内发生

中 — 预计影响可能在两至三年内发生

低 — 预计影响不可能在三年内发生

5．2．4 定义格式正确的风险陈述



5．3 使用 ISMS Tool 2 model 来收集信息资产数据。确定信息资产威胁及可能发生的安全漏洞，信息资产暴露的级别及产生威胁的可能性。

资产名称			资产分类（高、中或低业务影响）			
纵深防御层	您害怕发生什么或尝试避免什么发生；（威胁）	什么情况下它可能发生：（安全漏洞）	暴露级别（高、中、低）	当前控制描述	概率（高、中、低）	控制问题，可能的新控制
物理						
网络						
主机						

应用						
数据						

ISMS Tool 2model

xxxx有限公司

标准操作政策与程序

SOPP

编 号	ISMS-SOPP-009		第4页共10页
文件名	信息安全风险评估管理程序		版 号：0
由管理会议推荐：			修改状态：
部门负责人制订： 日期：	总经理审核： 日期：	董事经理批准： 日期：	生效日期：

5．4 按照影响等级基准和简明风险程度等级基准来记录“ 汇总级风险 ”。

5．4．1 影响等级基准

业务影响	HBI	中等影响	高影响	高影响
	MBI	低影响	中等影响	高影响
	LBI	低影响	低影响	中等影响
		LBI	MBI	HBI
		资产暴露等级		

5．4．2 简明风险程度等级基准

影响	HBI	中等风险	高风险	高风险
	MBI	低风险	中等风险	高风险
	LBI	低风险	低风险	中等风险
		LBI	MBI	HBI
		概率值		

5．4．3 根据影响等级基准和简明风险程度等级基准，使用 ISMS Tool 3 model 收集所有信息资产的影响等级和简明风险级别。

数据收集过程期间收集的信息									
资产				暴露程度					
确定的	资产名	资产类	适用纵深	危险	安全漏	暴露等级	影响等级	概率（高/	简明风险级别

日期	称	别	防御层	描述	洞描述	（高/中/低）	（高/中/低）	中/低）	（高/中/低）

ISMS Tool 3 model

xxxx有限公司

标准操作政策与程序

SOPP

编 号	ISMS-SOPP-009		第5页共10页
文件名	信息安全风险评估管理程序		版 号：0
由管理会议推荐：			修改状态：
部门负责人制订： 日期：	总经理审核： 日期：	董事经理批准： 日期：	生效日期：

5．5 进行详细级风险优先级确定，按照风险定义（5．2．4）来记录“详细级风险”。

5．5．1 根据影响和暴露程度、可用性暴露程度来确定影响等级

a．机密性和完整性暴露程度图衡量因企业资产的机密性或完整性的危害而造成的影响程度。

暴露等级	资产的机密性和完整性
5	资产严重或完全损环，例如，从外部可见，并影响业务利润或成功
4	严重但对资产不造成完全损坏，例如，影响业务利润或取得成功,可从外部看到
3	中等损坏或损失，例如，影响内部业务实行，导致运作成本增加或利润减少
2	低损坏或损失，例如，影响内部业务实行，无法评定成本的增加
1	资产有轻微更改或无更改

b. 可用性暴露程度图衡量对企业资产可用性的影响。

暴露等级	资产的可用性	描述
5	停工	实质性支持成本或业务承诺被取消
4	工作中断	支持成本或者业务承诺延迟可量化增长
3	工作延迟	对支持成本和工作利具有显著的影响,无可评定的业务影响
2	工作分心	无可评定的影响，支持或基础结构成本有少量增加
1	由正常的业务操作吸收	对支持成本、工作效率或业务承诺无可评定的影响

c. 确定业务影响类别值

影响类别	影响类别值（V）
HBI	10
MBI	5
LBI	2

d. 影响等级值确定方法

暴露系数等级	暴露系数（EF）	影响等级（V*EF）	影响范围	简明级别比较
5	100%		7-10	高
4	80%		4-6	中
3	60%		0-3	低
2	40%			
1	20%			

xxxx有限公司

标准操作政策与程序

SOPP

编 号	ISMS-SOPP-009		第7页共10页
文件名	信息安全风险评估管理程序		版 号：0
由管理会议推荐：			修改状态：
部门负责人制订： 日期：	总经理审核： 日期：	董事经理批准： 日期：	生效日期：

5．5．2 描述当前控制措施

5．5．3 确定影响可能性

a. 评估漏洞

安全漏洞的概率定义
高
大量攻击者-“ script-kiddle”/hobbyist
可远程执行
需要匿名权限
外部发布利用方法
自动化
任一项适用时为“ 5 ”
中
中等数量攻击者-行家/专家
非远程可执行
需要用户级权限
非公式发布的利用方法
非自动化
任一项适用时为“ 3 ”
低
少量攻击者-有问必答知识
非远程可执行
需要管理员级权限
非公式发布的利用方法
非自动化
所有项适用时为“ 1 ”

安全漏洞总计	
暴露程度属性（从上面选择一项）	
高	5
中	3
低	1
概率值（1、3、5）	

b. 评估控制措施有效性

当前控制的有效性如何？	
是（0），否（1）	
是否规定了责任并有效实施？	1，0
是否传达了意识并有效地跟进？	1，0
是否规定了过程并有效地实行？	1，0
现有技术或控制是否有效地减少了威胁？	1，0
当前审核操作是否足以检测滥用或控制缺陷	1，0
控制属性总和（0-5）	

c. 所有控制措施特性的总和：

安全漏洞等级与控制措施有效性总计（0-10）	

5．5．4 确定详细风险级别

a. 详细风险基准

风险级别=影响等级范围*概率范围				
属性	影响等级范围	概率范围	整体风险等级	风险级别
高	7-10	7-10	41-100	高
中	4-6	4-6	20-40	中
低	0-3	0-3	0-19	低

xxxx有限公司

标准操作政策与程序

SOPP

编 号	ISMS-SOPP-009		第8页共10页
文件名	信息安全风险评估管理程序		版 号：0
由管理会议推荐：			修改状态：
部门负责人制订： 日期：	总经理审核： 日期：	董事经理批准： 日期：	生效日期：

b． 使用 ISMS Tool 3 model 收集详细级风险

资产		暴露							
资产名称	影响类别等级	纵深防御层	危险描述	安全漏洞描述	暴露等级（1-5）	影响等级（1-10）	当前控制描述	采用控制的概率等级（1-10）	采用控制的风险等级（0-100）

ISMS Tool 3 model

5．6 量化风险

5．6．1 为公司指定各个资产类别的货币值

使用实质性指导原则来构建资产评估的基线，计划在获得经验后修改估计值。通过应用年净收的 5%实质性指导原则，基准值为

HBI=$M

MBI=$M/2

LBI=$M/4

5．6．2 依据 5．6．1 确定资产价值。

5．6．3 确定单一预期损失（SLE）

商业务影响值 = $M			暴露等级	暴露系数 %
			5	100
资产类别			4	80
HBI 值	$ M		3	60
MBI 值	$ M/2		2	40
LBI 值	$ M/4		1	20
估计风险值 =	资产类别值 * 暴露系数 % = SLE			

5．6．4 确定年发生率（ARO）

定性等级	描述	ARO 范围	描述示例
高	很可能	>= 1	每年影响一次或多次
中	可能	0.99 到 0.33	每 1-3 年至少 1 次
低	不可能	< .33	每 3 年不到 1 次

5．6．5 确定年预期损失（ALE）

年预期损失（ALE）=SLE*ARO

风险描述	资产类别值	暴露等级	暴露程度值	SLE	ARO	定量估计(ALE)
LAN 主机风险	$ 10	4	80%	$ 8	0.5	$ 4
远程主机风险	$ 10	4	80%	$ 8	1	$ 8

5．7 识别和评价供处理风险的可选措施

5．7．1 定义功能要求

功能安全要求是描述降低风险所需控制措施的语句。应以希望的功能而不是所述的技术来表达控制措施。

5．7．2 确定控制解决方案

a．组织性控制措施

组织性控制措施是定义组织内的人员应如何履行其职责的程序和流程。

b．操作性控制措施

操作性控制措施定义组织中的人员应如何处理数据、软件和硬件。

c．技术性控制措施

技术性控制措施在复杂性方面有很大的不同。 它们包括系统体系结构设计、工程、硬件、软件和固件， 是用于建立组织之信息系统的所有技术性组成要素。

5．7．3 根据要求审查解决方案

5．7．4 评估风险降低程度

5．7．5 评估解决方案成本

a．购买成本

这些成本由与提议的新控制措施有关的软件、硬件或服务组成。

b．实施成本

这些支出与安装和维护提议的新控制措施的人员或顾问有关。

c．持续成本

这些成本与新控制措施的持续活动有关，例如管理、监控和维护。

d．通信成本

此支出与向用户通知新的策略或程序有关。

e．IT 员工的培训成本

这些成本与需要实施、管理、监控和维护新控制措施的 IT 员工有关。

f．用户的培训成本

此支出与必须根据新的控制措施进行工作的用户有关。

g．生产力和方便性成本

这些支出与其工作会受到新控制措施影响的用户有关。

5．7．6．选择风险缓解方案

将实施缓解方案后面临的风险程度与缓解方案自身的成本进行比较。