上海艾雷电子商务有限公司

信息安全风险评估管理办法

2022 年 4 月 10 日

目　录

1 总则

为确保网络及信息系统安全、高效、可控的运行，提高业务系统安全运行能力，全面降低信息安全风险，特制定本管理办法。

2 组织与责任

IT 部负责信息安全风险评估的具体实施。

其他部门协助 IT 部开展信息安全风险评估工作。

3 信息安全风险评估规定

3.1 弱点分析

3.1.1 概述

弱点评估是安全风险评估中最主要的内容。弱点是信息资产本身存在的，它可以被威胁利用、引起资产或商业目标的损害。弱点包括物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各种资产的弱点。

3.1.2 弱点检查

IT 部应定期对公司 IT 系统进行全面的信息安全弱点检查，了解各 IT 系统的信息安全现状。

IT 系统安全检查的范围包括：主机系统、网络设备、安全设备、数据库系统、应用系统、邮件系统以及其它在用系统。

IT 系统安全检查的工具与方法如下：

1. 工具检查：针对 IT 设备建议采用专用的脆弱性评估工具进行检查，如 Nessus、BurpSuite 等工具，针对应用系统及代码安全检查，建议采用商业专用软件进行检查，如 IBM AppScan。
2. 手工检查：由 IT 部相关人员参照相关的指导文档上机进行手工检查。

信息安全检查工作开展前，IT 部需制定安全检查计划，对于部分可用性要求高的业务系统或设备，计划中要明确执行的时间，并且该计划要通知相关部门与系统维护人员，明确相关人员的及部门的职责与注意事项。

IT 部与外服公司针对信息安全检查须制定《安全检查方案》，方案中，针对工具扫描部分需明确扫描策略，同时方案必须提供规避操作风险的措施与方法。并且该方案必须获得 CEO 批准。

IT 部应对 IT 系统安全检查的结果进行汇总，并进行详细分析，提供具体的安全解决建议，如安全加固、安全技术引进等。

当发生重大的信息安全事件，IT 部应在事后进行一次全面的安全检查，并通过安全检查结果对重要的安全问题进行及时解决。

常见的弱点种类分为：

1. 技术性弱点：系统，程序，设备中存在的漏洞或缺陷，比如结构设计问题或编程漏洞；
2. 操作性弱点：软件和系统在配置，操作，使用中的缺陷，包括人员在日常工作中的不良习惯，审计或备份的缺乏；

3. 管理性弱点：策略，程序，规章制度，人员意识，组织结构等方面的不足；

识别弱点的途径包括审计报告，事件报告，安全复查报告，系统测试及评估报告，还可以利用专业机构发布的列表信息。当然，许多技术性和操作性弱点，可以借助自动化的漏洞扫描工具和渗透测试等方法来识别和评估。

在对生命周期敏感的资产评估过程中，应注意从创建，使用，传输，存储，销毁等不同的阶段识别弱点。

弱点的发现随着新应用,新技术的出现,需要不断更新完善弱点列表。

3.1.3 弱点赋值

信息资产弱点为 IT 设备自身存在的安全问题。根据弱点的严重性以暴露程度进行评价，即弱点被利用的难易程度，而弱点对资产安全影响的严重程度放在资产价值中去考虑，一个弱点可能导致多项不同价值资产的风险上升。参考业界的最佳实践，采用的等级划分如下：

将弱点严重性分为 4 个等级，分别是非常高（VH）、高（H）、中等（M）、低（L），并且从高到低分别赋值 4-1。赋值标准参照下表。

赋值	弱点等级	弱点赋值说明（弱点严重程度）
4	很高	弱点很严重，可直接、轻易的被非法者利用，并对信息资产生产破坏
3	高	弱点严重，可利用直接，但需通过一定的攻击手段，可对信息资产生产破坏
2	中	弱点严重一般，利用非常困难或不可利用，但通过与其它弱点进行组合利用，可对信息资产生产破坏
1	低	弱点不严重，弱点不能利用，但会泄露有限的资产信息

3.2 威胁分析

3.2.1 概述

安全威胁是一种对系统、组织及其资产构成潜在破坏的可能性因素或者事件。产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素包括有意因素和无意因素。环境因素包括自然界的不可抗力因素和其它物理因素。

3.2.2 威胁来源分析

信息系统的安全威胁来源可考虑以下方面：

威胁来源表

威胁来源	威胁来源描述
环境因素、意外事故或故障	由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害；意外事故或由于软件、硬件、数据、通讯线路方面的故障。
无恶意内部人员	内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或被攻击；内部人员由于缺乏培训，专业技能不足，不具备岗位技能要求而导致信息系统故障或被攻击。
恶意内部人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主的或内外勾结的方式盗窃机密信息或进行篡改，获取利益。
第三方	第三方合作伙伴和供应商，包括业务合作伙伴以及软件开发合作伙伴、系统集成商、服务商和产品供应商；包括第三方恶意的和无恶意的行为。
外部人员攻击	外部人员利用信息系统的弱点，对网络和系统的机密性、完整性和可用性进行破坏，以获取利益或炫耀能力。

3.2.3 威胁种类分析

对安全威胁进行分类的方式有多种多样，针对上表威胁来源，需要考虑下述的安全威胁种类。表中列举的威胁种类随着新技术新应用的出现，需要不断更新完善。

威胁种类列表

威胁种类	威胁描述
软硬件故障	由于设备硬件故障、通讯链路中断、系统本身或软件 Bug 导致对业务高效稳定运行的影响。
物理环境威胁	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题和自然灾害。
无作为或操作失误	由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对系统造成影响。
制度不完善	相关制度不完善、合理，造成无章可循或无法遵循。
管理不到位	安全控制无法落实，不到位，造成安全控制不规范，或者管理混乱，从而破坏信息系统正常有序运行。
恶意代码和病毒	具有自我复制、自我传播能力，对信息系统构成破坏的程序代码。
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏信息系统的行为。
黑客攻击技术	利用黑客工具和技术，例如侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对信息系统进行攻击和入侵。
物理攻击	物理接触、物理破坏、盗窃。
泄密	机密泄漏，机密信息泄漏给他人。
篡改	非法修改信息，破坏信息的完整性。
抵赖	不承认收到的信息、所作的操作或交易。

3.2.4 威胁赋值

威胁发生的可能性是一个动态的，需要综合分析得出，在此可采用如下最佳实践的赋值标准，通过实际经验对威胁的可能性赋值。赋值标准参照下表：

威胁赋值列表

赋值	威胁	威胁赋值说明（威胁发生的可能性）
4	很高	在大多数情况下，很有可能会发生；或者可以证实发生过（发生可能性在 80%以上）
3	高	在多数情况下，可能会发生（发生可能性在 50%-80%）
2	中	在某种情况下或某个时间，可能会发生（发生可能性在 20% - 50%）
1	低	发生的可能性很小，不太可能（发生可能性在 20%以下）

3.3 风险计算

3.3.1 概述

风险是一种潜在可能性，是指某个威胁利用弱点引起某项资产或一组资产的损害，从而直接地或间接地引起组织的损害。因此，风险和具体的资产威胁等级以及相关的弱点直接相关。

风险评估包括风险的计算、风险的处置和风险的安全对策选择。

3.3.2 风险计算

采用下面的算术方法来得到信息资产的风险值：

风险值 ＝ 资产值 × 威胁值 × 弱点值

风险等级与风险值对应关系参考下图：

风险级别列表

风险等级		风险取值范围	
4	很高	48、64	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大。
3	高	24、27、32、36	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害。
2	中	12、16、18	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大，一般仅限于组织内部，通过一定手段就能解决
1	低	≤9	一旦发生造成的影响很小或几乎不存在，通过简单的措施就能弥补。

风险等级计算结果如下：

风险值计算矩阵																	
风险要素	威胁等级	1				2				3				4			
	弱点等级	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
资产等级	1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

根据计算出的风险值，对风险进行排序，并根据组织自身的特点和具体条件、需求，选择相应的风险处置方式。

3.4 风险处置

3.4.1 概述

风险的处置方法依照风险程度，根据风险等级来采取不同的处置方法。风险程度和遵照的处置方法建议见下表：

风险等级列表

符号	含义	建议处置方法
VH	很高风险	需要管理层的高度注意：避免？转移？减少？
H	高风险	需要管理层的注意：避免？转移？减小？
M	中风险	必须规定管理责任：避免？接受？转移？减小？
L	低风险	用日常程序处理：避免？接受？转移？减小？

选择处置措施的原则是权衡利弊：权衡每种选择的成本与其得到的利益。当风险已经定义后，必须决定如何处置这些风险。

3.4.2 风险处置方法

在考虑风险处理前，如果经评估显示，风险较低或处理成本对于组织来说不划算，则风险可被接受。这些决定应加以记录。

通常有四种风险处置的方法：

1. 避免风险：在某些情况下，可以决定不继续进行可能产生风险的活动来规避风险。在某些情况可能是较为稳妥的处理办法，但是在某些情况下可能会因此而丧失机会。例如，将重要的计算机系统与互联网隔离，使其免遭来自外部网络的攻击。

2. 降低风险：实施有效控制，将风险降低到可接受的程度，实际上就是力图减少威胁发生的可能性和带来的影响，包括：

   - 减少威胁：例如，建立并实施恶意软件控制程序，减少信息系统受恶意软件攻击的机会；
   - 减少弱点：例如，通过安全教育和意识培训，强化职员的安全意识与安全操作能力；
   - 降低影响：例如，制定灾难回复计划和业务连续性计划，做好备份。

3. 转移风险：这涉及承担或分担部分风险的另一方。手段包括合同、保险安排、合伙、资产转移等。

4. 接受风险：不管如何处置，一般资产面临的风险总是在一定程度上存在。当组织根据风险评估的方法，完成实施选择的控制措施后，会有残余的风险。残余风险可能是组织可以接受的风险，也可能是遗漏了某些信息资产，使其未受保护。为确保组织的信息安全，残余风险应该控制在可以接受的范围之内。

   风险接受是对残余风险进行确认和评价的过程。在实施安全控制措施后，组织应该对安全措施的情况进行评审，即对所选择的控制在多大程度上降低了风险做出判断。通过成本利益分析、影响分析及风险回顾，即在继续处置需要的成本和风险之间进行抉择。风险接受要符合风险可接受准则，即风险评估结果中风险值为 2 及以下，都是可以接受的风险，最终上报给最高领导，待领导批准是否选择接受风险。

3.4.3 风险处置流程

3.4.3.1选择控制项

在大多数情况下，必须选择控制项来降低风险。在完成风险评估之后，组织需要在每一个目标信息环境中，对选择的控制项进行实施，以便遵从 ISO/27001 标准。组织选择能够承受（经济上）的防护措施来防护面临的威胁。在最终风险处置计划出来前，组织可以接受或拒绝建议的保护方案。

3.4.3.2风险处置计划

风险处置计划包含所有相关信息：管理任务和职责、管理责任人、风险管理的优先等级等等（详见附录《风险处置计划表》）。对组织来讲，有一些附加控制在标准中没有描述，但也是需要的。一个由外部咨询顾问协助的风险评估会很有帮助。

3.4.3.3控制项的实施

通过风险处置计划的实施，组织应该尽其所能针对等级保护中的标准内容在管理、技术、逻辑、物理和环境控制方面进行劝止、防护、检测、纠正、恢复和补偿工作。如下表所示。表中所列举的风险问题及处置措施随着新应用，新技术的出现，需要不断更新完善。

部分风险处置建议表

风险及问题	控制措施类型	处置措施
缺乏防病毒系统	技术	1、 安装主机防病毒软件 2、 部署网络防病毒产品 3、 部署互联网出口防病毒墙
	管理	1、 制订病毒预防管理规定 2、 制订计算机安全使用意识规定
主机补丁不全	技术	1、 更新补丁 2、 集中补丁集中管理系统
	管理	1、 制订补丁维护管理制度
缺乏网络访问控制	技术	1、 部署防火墙，增加访问控制策略 2、 划分 VLAN，并增加 ACL
缺乏信息安全方针文件	管理	1、 制定信息安全方针文件并向所有员工公布 2、 按计划的时间间隔或发生重大事件时，对安全方针进行评审
缺乏有效的信息安全组织	管理	1、 成立有效的信息安全组织，明确规定所有信息安全职责 2、 定期与组织成员签署保密协议或责任书
缺乏对信息资产的整理和分类	管理	1、 制定详细的资产清单，并责任到人，定期做资产的统计和清查 2、 按资产的重要程度对信息进行分类，并对信息明确保密期限
	技术	1、 安装桌面管理软件或资产管理软件
缺乏对人员安全的考	管理	1、 对第三方用户进行背景验证检查 2、 要求第三方服务人员签署保密协议 3、 在员工的岗位职责中明确定义了信息安全的责任

核		4、 工作人员离职时交还资产，并接受检查
	技术	1、 取消即将离任的工作人员相关访问权限
缺乏对人员的安全教育培训	管理	定期对工作人员进行安全教育培训、培训内容包含安全方针、各种安全技术，根据工作人员从事的安全岗位不同，提供专业技能培训
缺乏对第三方人员的访问控制	管理	1、 对第三方（第三方包括产品提供商，软件提供商，服务商、集成商和顾问等）访问（进出机房、接入网络、访问系统等）的安全性进行风险评估 2、 对外包的业务，在双方合同中明确规定安全风险、安全控制程序的要求
缺乏对机房的安全区域的划分	管理	1、 对机房安全区域的划分：如机房、监控室、办公室 2、 机房帐台记录相关的出入、进入时间、进入事由等相关信息
	技术	1、 物理安全访问边界设置门禁或监控室
缺乏对设备安全的考虑	管理	1、 考虑盗窃、火灾、化学、灰尘、震动、电子干扰等环境威胁产生的潜在风险等 2、 禁止在重要信息处理设施附近饮食、饮水和吸烟 3、 提供多路供电、不间断电源或发动机 4、 对设备定期维护、检查和更新
缺乏统一的操作规程	管理	1、 制定统一安全操作规程：如变更管理规程、问题管理规程、事件管理规程、测试评估规程等
缺乏信息备份策略	管理	1、 制定备份策略对信息和软件进行备份并定期测试
缺乏用户管理	管理	1、 定期对用户访问权限进行检查 2、 记录访问权限的授权、维护 3、 立即取消已经变更工作或离开公司的用户访问权力
缺乏对移动设备 的接入和远	管理	1、 制定对移动设备接入和远程控制的管理办法
	技术	1、 远程接入用户数量、时间控制

程控制		
缺乏对介质的管理	管理	1、 对介质进行适当的访问控制，以合理的方式进行介质的保存，传送和废弃必要保证信息的安全性 2、 只允许授权人员进行介质的获取，接收，转移和交付 3、 系统存储介质废弃时,清除其存储的信息或将其销毁，防止未经授权的人通过废弃的介质得到其中的信息
	技术	1、 终端管理软件
缺乏应用系统开发中对安全要求分析和规范	管理	1、 系统设计阶段提出 对安全的要求，包含系统 本身的安全要求和开发过程中的控制要求 2、 应用系统开发过程中对应用系统口令使用策略、以及数据传输过程中数据加密安全策略
缺乏应急预案	管理	1、 建立安全应急响应管理制度 2、 建立安全应急响应领导机构 3、 建立安全应急预案，并进行应急响应演练，记录演练操作。
缺乏数据备份机制	管理	1、 建立有效的备份与恢复机制 2、 建立完备份工作操作技术文
	技术	1、 备份软件

3.4.3.4控制措施及其定义的原则

1. 防护：保护或降低资产的脆弱性；
2. 纠正：降低风险和影响的损失；
3. 检测：检测攻击和安全的脆弱性，针对攻击建立防护和纠正措施；
4. 恢复：恢复资源和能力；
5. 补偿：对控制措施的替代方案。

同时应该咨询信息安全专家和法律专家，确保控制措施的选择和实施是正确、有效的。

3.5 IT 需求评估决策流程

在评估一个需求（资产）的风险时，应从两个角度分别进行评估。通常的风险评估是针对该资产本身所面临的风险，采取的处置方式也是出于保护该资产信息安全的目的。同时还需要考虑随着该资产的应用所引入的新威胁，可能会导致现有的资产风险等级提升。

因此在评估一个需求是否符合安全要求时，应遵循以下步骤：

1. 全面识别需求中所涉及的 IT 资产等级，分析这些资产的脆弱性，面临的威胁和问题，评估资产的风险等级，给出相应的处置措施。
2. 全面识别需求所引入的新威胁，分析这些威胁对已经经过评估的现有资产所造成的影响，如果这些新威胁导致某项资产的风险等级超过了 2 级，则必须采取相应的处置措施。
3. 对需求进行评估决策，分析自身存在的风险和引入的风险，以及需要采取的处置措施，措施所需要增加的投资，以及业务的重要性。根据信息安全方针策略中所定义的基本原则策略来决策对需求的处理方式。

4 奖惩管理规定

1. 本办法要求定期执行相关安全评估工作。相关组织与部门应在 IT 部进行风险评估时提供相关的支持与帮助，积极配合信息安全风险评估工作，

如果部门不配合相关的风险评估工作，而发生信息安全事件，综合部门应视情况对该部门进行教育、批评、罚款等处理。

2. 在信息安全风险评估过程中，发现某部门或系统高风险事项较多，IT 部应视情况对部门或相关维护人进行通报批评。
3. 在风险评估过程中，发现上次风险未进行加固或解决，IT 部应进行通报批评，如果多次评估发现安全风险未解决，应报告综合部进行相关处罚。
4. 如违反本管理办法，造成公司严重损失，公司视情况终止该员工劳动合同或移交公安机关。

5 附则

本办法发布之日起生效，由 IT 部负责编制。本办法的解释和修改权属于 IT 部。定期统一检查和评估本制度，并做出适当更新。在业务环境和安全需求发生重大变化时，也将对制度进行检查和更新。

上海艾雷电子商务有限公司

2022 年 4 月 10 日