硬件系统安全总体设计

系统建设严格遵循信息安全保障体系要求，按照国家法规实施安全等级保护，加强系统信息安全管理，并制定符合甲方制定的等保防护等级的防护方案，并以此进行建设。具体防护措施如下章节进行阐述。

系统安全防护方案

系统应用安全防护

系统可满足不同网络环境下正常访问，包括满足 SSLVPN 安全要求的 WEB 访问，并负责符合设备安全规则的代码修改。

充分考虑平台系统最大限度接收设备的数据量，保证不丢失数据。

整体安全设计：

对系统部署的环境，对与操作系统和数据库等相关软件定义了安全基线和加固策略，上线前进行安全漏洞扫描、基线检查，根据检查的结果进行安全加固。

系统提供自审计功能，能对所有人员对系统的操作信息进行记录。

内部安全设计：

系统采用了 SSL 等加密通讯协议传输，各模块之间通讯采用了安全通信协议，支持身份认证和传输加密。

应用安全设计：

系统采用统一身份认证技术，支持账户的登录失败锁定和超时退出等功能。

接口安全设计：

所有接口信息的传递均采用 SSL 加密传输，并结合身份认证相关信息进行验证。

系统数据安全防护

数据灾备设计：

数据库为分布式部署，如果单独数据出现故障，不影响系统运行，并能及时恢复。

数据安全防护：

系统的后端数据库采取了安全保护措施，数据库的访问以及对安全管控系统的操作都经过了严格的身份鉴别，并对操作者的权限进行严格划分，保证数据存储安全。重要数据均进行加密存储。系统严格的控制数据的删除权限。普通用户无法对数据进行篡改、删除等破坏日志的操作。

系统软硬件平台安全防护

对于通过各种措施发现的安全漏洞、安全弱点、安全风险，需要通过多方面的安全加固措施进行修补，确保整个系统的安全性。

硬件平台安全防护主要包括以下类型：

服务器加固服务：

对服务器的人工安全审计服务中，会发现服务器操作系统或应用软件的不安全配置，通过服务器加固服务的方式，消除各项不安全配置，确保服务器自身的安全性。服务器加固包括各项安全策略调整、补丁实施、应用软件升级等内容；

服务器加固服务是根据三级要求，对服务器操作系统和应用系统进行加固。

漏洞扫描发现的高风险：

通过每周漏洞扫描发现的各类高风险漏洞，需要进行安全优化，以消除高风险安全漏洞。

安全设备加固服务：

根据相关规范，调整安全设备的安全策略，如增加服务器、减少服务器而需要改变安全设备的通行端口等内容。

主机加固加固服务：

根据系统实际情况，结合现有杀毒软件集成的 HIPS、智能主机防火墙等功能，对每个系统主机进行安全加固，根据系统注册表、各种活动进程及程序指定规则，微调各种安全动作，以提高网络系统的总体安全。

高风险日志追踪服务：

本系统涉及重要网络安全设备日志的审计，及时发现高风险日志。对高风险日志在第一时间进行跟踪处理。如发现病毒、蠕虫，迅速查找源头，进行处理；发现攻击信息，迅速检查被攻击 IP 设备的安全性，并对攻击源进行隔离或其它方式处理等。

系统运维阶段安全管理

本完成建设阶段工作后，系统将进行运行维护阶段，根据相关安全规范要求，对系统运维阶段的安全管理提出如下设计：

（1）备份与恢复管理

识别系统中需要定期备份的重要业务信息、系统数据及软件系统等；

规定系统备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

根据备份方式，规定相应设备的安装、配置和启动的流程；

（2）系统变更管理

在系统进入运维阶段后，如需要对系统功能、架构、配置进行变更是，需要变更管理，主要包括：

确认系统中要发生的变更，并制定变更方案；

建立变更管理制度，重要系统变更前，管理人员应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更；

系统变更情况应向所有相关人员通告；

（3）应急预案管理

定制系统应急预案管理制度，在统一的应急预案框架下制定不同事件的应急预案，应急预案框架包括启动应急预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略。

系统建设安全管理方案

对信息系统的安全管理需要贯穿到信息系统整个生命周期中去，在系统审批、建设、使用等过程需要对其安全管理，在对系统建设的安全管理需要考虑如下几个方面：

软件开发安全管理解决方案

安全是一个整体，完整的安全解决方案应该包括网络安全、系统安全、应用安全和数据安全。其中网络安全、系统安全和数据安全的技术实现有很多固定的规则。而由于应用的千差万别，实现应用层面的安全难度要大得多。根据“木桶原理”，一个系统的安全强度等于它最薄弱环节的安全强度。应用安全往往成为整个安全体系中最为脆弱的部分，成为制约整个系统安全水平的关键因素。在安全体系设计时，要充分考虑“应用安全实现的可控性”，以便尽可能地降低安全系统与应用系统结合过程的风险。保持安全系统与应用系统的相互独立性，避免功能实现上的交叉或跨越。避免程序级别的低层接口，免除两者结合时应用系统的二次编程开发。增强安全系统的适用性，最大程度地提供便捷可靠的结合方式。建立完善的安全控制机制，包括：用户标识与认证、逻辑访问控制、公共访问控制、审计与跟踪等。

网络与信息系统的安全控制或安全性是通过系统的开发设计予以实现的，在设计阶段采取控制措施远比在实施过程中或者实施结束

之后落实控制措施更廉价。若在系统设计阶段未充分考虑系统的安全性，则系统本身就存在着先天不足。

因此，应在网络基础设施、应用系统（包括为最终用户开发的程序）的开发与维护阶段，正确识别、确认、批准所有安全需求（包括备用安排，如手工方式），并将之文档化。

软件安全需求管理

在建立新系统或扩展已有系统时，应首先明确业务需求，并将之作为系统设计开发的依据。业务需求不仅要包括系统的功能、性能、开发费用与周期等要求，还要明确规定系统的安全要求，并据此确定具体的安全控制措施，如系统的自动控制措施及是否需要手工控制措施等。

系统的安全需求主要包括两方面的内容：一方面是对系统本身的安全要求，即经开发设计的系统应具备一定的安全特性，如 AAA 功能；另一方面，对系统设计开发过程本身也 要进行控制，如在不同的设计开发阶段进行评审和验证，确保设计开发的系统满足规定的质量和安全要求。

系统的安全需求应能反映出所涉及的网络与信息资产的价值，以及故障或安全漏洞导致的潜在损失，即基于风险评估与风险管理来确定安全需求。

当涉及系统开发外包或合作开发时，安全需求应在双方认可的合同或协议中给予明确规定。

如果可能，可采用通过公正的第三方独立评估和认证的产品。

在进行具体的系统开发和软件维护时，还应注意以下几个方面：

必须在应用系统开发、修改或者投入使用之前指定应用系统责任人。

在应用系统开发、修改或者投入使用之前，必须完成风险评估、业务影响评估、备份和灾难恢复方案。

确保开发、测试与运行设备的分离。

应用系统责任人负责标明应用的信息分类级别，并确保运行应用的系统的信息分类级别不低于该应用的信息分类级别。

系统开发过程中应不断咨询操作部门及用户的意见，以提高所设计系统的操作效率。

软件设计安全管理

为避免应用系统中的用户数据丢失、修改和误用，应用系统应设计有适当的控制措施、审计跟踪记录或活动日志，如对输入数据、内部处理和输出数据的验证。针对用以处理敏感、脆弱或关键资产的系统，或者对此类资产有影响的系统，单位还应根据风险评估的结果确定安全要求，并采取额外的控制措施。

（1）输入数据检查

为了保证系统的安全性，必须在开发过程中对输入到应用系统中的数据进行严格的检查，以确保其正确性及适用性，避免无效数据对系统造成危害，如在 ASP 应用中，应过滤用户通过 WEB 提交的输入数据中的特殊字符。对输入数据的验证一般通过应用系统本身来实现，并应在系统开发中实现输入数据验证功能。

已被正确输入的数据可能受到错误处理或者故意破坏，系统应采取有效的验证检查措施来检测此类破坏，并在应用系统设计时引入数据处理控制，尽可能地减小破坏数据完整性处理故障的几率。可以采用的控制措施如下：

1）应用系统不应在程序或进程中固化账户和口令。

2）系统应具备对口令猜测的防范机制和监控手段。

3）避免应用程序以错误的顺序运行，或者防止出现故障时后续程序以不正常的流程运行。

4）采用正确的故障恢复程序，确保正确处理数据。

5）采取会话控制或批次控制，确保更新前后数据文件的一致性，例如：检查操作前后文件打开和关闭的数目是否一致。

6）检查执行操作前后对象的差额是否正常，如：句柄处理，堆栈等系统资源的占用与释放等。

7）严格验证系统生成的数据。

8）在中央计算机和远程计算机之间，检查下载/上传的数据或软件的完整性。

9）检查文件与记录是否被篡改。例如通过计算哈希值（HASH）进行对比。

（2）消息认证

消息认证是一种用来检测对电子消息的非法修改或破坏的技术，如会话劫持（Session Hijack）、篡改和伪造。该技术可以用物理设备或软件算法实现。

（3）输出数据检查

尽管数据的输入和处理是正确的，输出仍然可能包含错误或有害的修改。因此，应用系统的输出数据应当被验证，以确保数据处理的正确性与合理性。输出验证包括：

用以测试输出数据是否合理的似真性检查；例如：输出数据应在规定的范围内。

为用户或后续处理系统提供充足的信息，以确定信息的准确性、完整性、精确性和分类级别；例如：在输出数据时提供帮助信息。

可以用来验证输出数据的测试程序。

规定数据输出过程中相关人员的职责。

（4）系统文件的安全

访问系统文件应当得到有效的控制。保证系统的完整性由拥有应用系统或软件的用户职能部门或者开发小组负责。

（5）操作系统控制

在操作系统中运行软件应当得到有效的控制。为了最大限度地降低操作系统遭受破坏的风险，单位应考虑采取如下控制措施：

1）程序运行库（operational program libaries）的升级只能由指定的程序库管理员在获取授权后予以完成。

2）操作系统应尽可能只保留应用程序的可执行代码。

3）在系统测试、用户验收结束之前，及相应的程序源代码库升级之前，可执行代码不得在操作系统中运行。

4）程序运行库的所有更新记录都应当予以保留。

5）历史版本的软件应当予以保留，用作应急措施。

6）任何版本更新都应考虑安全性，即应根据新版本具有的新型安全功能及带来的安全问题的数量和严重程度，确定是否更新版本。如果软件补丁有助于消除或削弱安全缺陷，则应采用软件补丁。

7）操作系统的软件版本更新，有可能对应用系统带来影响。另外，应与应用系统厂商签订合同，由其提供合适的支持与维护，例如兼容性测试、配合修改、技术支持等。

（6）系统测试数据的保护

系统和验收测试数据通常含有大量与操作系统相关的信息，因此，应对系统测试数据加以保护和控制，并避免使用含有个人隐私或敏感信息的数据去测试系统，确保测试数据的普遍性。可采用的控制措施如：

1）用于正式运营系统的访问控制程序，也应用于测试环境。

2）每当将测试数据加载到测试系统时，应进行独立授权。

3）在测试结束后，测试数据应当马上从测试系统中删除。

4）测试数据的加载和使用应当被记录在案，以便检查跟踪。

5）应用系统源代码访问控制

6）为降低系统程序遭受破坏的可能性，应严格控制对系统源代码的访问，具体控制措施如：

7）源代码尽量不要保留在操作系统内。

8）为每个系统指定程序库管理员。

9）控制系统支持人员对程序源代码库的访问。

10）处于开发和维护阶段的程序不得保留于运程序源代码库中。

11）程序源代码库的更新及发布只能由指定的程序库管理员在经过该应用的主管领导授权后实施。

12）程序清单应当保存在安全环境中。

13）对程序源代码库的所有访问都应保留审计日志。

14）老版本的源程序应当归档，并清楚记录其被正式使用的确切日期和具体时间，及所有相关的支持软件、功能说明、数据定义和程序（如流程图）等。

15）程序源代码库的维护和拷贝应当遵从严格的变更控制程序。

软件开发过程安全管理

（1）变更控制

为减少变更对系统安全造成的风险，单位应在系统开发与运行维护的所有阶段（如：计划需求、设计、编码、测试、运行和维护）强制实施严格的变更控制，对变更的申请、审核、测试、批准、执行计划与具体实施提出明确要求，确保系统安全性与控制措施不被损害，系统管理人员只能访问其工作必需的系统部分。应用软件的修改可能会影响运营环境，如若可行，应用软件和业务运营的变更控制程序应当结合起来实施。变更控制包括以下内容：

保留变更的授权级别记录。

确保由授权用户提交变更申请。

审查变更控制措施和流程的完整性，确保未被修改和破坏。

识别所有要求修改的计算机软/硬件、信息、数据库实体。

及时发布操作系统的变更通知。

在实施之前，详细的变更方案必须获得正式批准。

在实施之前，确保授权用户接受变更。

选择恰当的变更时间，确保在具体实施过程中最大限度地减少业务影响。

确保操作系统的更改不会对应用系统的安全性和完整性造成不良影响。

确保系统文档在每次修改后得到及时更新，并确保旧文档被正确归档和处置。

做好软件升级的版本控制，如保存历史版本。

保留所有变更的审计跟踪记录。

确保操作文档以及用户程序能在必要时被修改。

确保及时更新业务连续性计划。

（2）软件包变更控制

应尽量避免修改厂商提供的软件包，如必须修改，应注意以下几点：

评估软件包内置的控制措施和完整性流程遭受破坏的风险。

应征得原厂商的同意。

可能的话，由原厂商提供标准的升级程序来实现软件包的更改。

考虑变更带来的软件维护责任方面的潜在负面影响，如在修改之后需由本单位负责将来的软件维护工作。

若修改必不可少，则应保留原始软件，并在原始软件的清洁拷贝上进行。

全面测试所作的修改，并记录在案，以便必要时重新应用于将来的软件升级。

（3）恶意代码控制

后门、逻辑炸弹和特洛伊代码都属于恶意代码范畴，对网络与信息系统有重大的潜在威胁。在软件的原始采购、开发、使用和维护过程中，应采取如下防范控制措施：

1）仅从信誉卓著的厂商处购买软件。

2）购买提供源代码的软件，以便进行检验。

3）使用通过权威机构评估测试的软件产品。

4）在投入使用之前检查所有源代码。

5）一旦安装完毕，控制对源代码的访问和修改。

6）使用可靠人员操作关键系统。

7）不得随意运行未经检测的软件，如电子邮件附件。

8）安装并正确使用有关后门、特洛伊代码的检测和查杀工具。

9）外包开发的安全控制

10）在外包软件开发时，应注意以下几点要求：

11）选择信誉与质量保证能力好的软件承包商。

12）软件许可权协议、代码所有关系以及知识产权。

13）对外包工作质量和准确性的检验，并保留检查权利。

14）承包方违约时应该采取的措施。

15）代码质量的合同要求，如对编程标准的要求。

16）在安装之前进行测试，以检测后门、逻辑炸弹和特洛伊代码。

软件维护安全管理

用户是指使用网络与信息系统的人，既包括操作管理设备的内部人员或第三方，也包括享用服务的客户。

（1）用户注册、认证和注销

应用系统应该包括正式的注册、登录认证和注销模块，并且能够对不同用户的访问权限进行严格的访问控制。具体要求包括以下内容：

应用系统和操作系统账号分离。

应该根据应用程序采用合适的认证方式，对于安全要求较低的系统可以采取传统的用户名、密码认证方式，对于安全要求较高的应用系统应该采取安全性更高的认证方式，例如：指纹认证、智能卡、双因子认证等。

逐步统一所有应用程序的认证，建立企业的 PKI。

使用唯一的用户标识符（用户 ID），使用户与其操作相关联，并对其行为负责；确实必要时，作为例外情况，才允许使用用户组账号，并采取额外的控制措施。

检查授权访问的级别是否基于业务目的，且符合单位的安全策略，如不得违反职责分离原则。

用户访问权限应得到上级领导和责任人的批准。

向用户提供访问权限的书面说明，并要求用户签字确认，表明已了解访问的条件。

确保服务提供者不能在授权程序结束之前提供访问服务。

保留所有注册人员使用服务的正式记录。

马上修改或注销已经更换岗位或离开单位的用户的访问权限。

定期核查并删除多余、闲置或非法的用户 ID 和账户。

账户应能灵活设置，并可修改口令。

软件管理的安全管理

对应用系统进行某些特殊操作，例如：系统管理时，会用到一些特殊的账户，一旦这些帐户被攻击者窃取，对整个系统的危害是非常巨大的，对于这些管理帐户除了应该遵循一般用户的安全规定外，还需要进行如下限制：

确定不同系统的超级权限以及需要获得此类特权的人员类型。

超级权限应基于“使用需要”，逐个事件进行分配，即以完成其岗位职责的最低要求为依据，如某些超级权限在完成特定任务后应被收回。

保留所有超级权限的分配授权流程的记录。在授权流程结束之前，不得授予特权。

当某用户需要超级权限时，应在其原有的用户 ID 之外，另行设置一个授予了超级权限的特殊账户。

尽量对管理权限进行分割，把不同的管理权限赋予不同的账户。

应用系统应该做好管理账户登录和管理操作的记录。

定期对系统的日志进行审计，以发现异常登录、操作。

做好超级权限拥有者无法行使职责时的应急安排，如角色备份。

软件系统安全审计管理

应用系统应该具有完善的日志功能，能够记录系统异常情况及其他安全事件。审计日志应保留规定的时长，以便支持日后的事件调查和访问控制监控。审计日志包括以下内容：

1）用户创建、删除等操作。

2）登录和退出的日期和具体时间。

3）终端的身份或位置（如果可能的话）。

4）成功的和被拒绝的系统访问活动的记录。

5）成功的和被拒绝的数据与其他资源的访问记录。

6）成功的和被拒绝的管理操作记录。

安全事件处置与应急解决方案

在对信息的安全管理过程中，对于安全事件的处理和应急十分重要，该部分工作可以说决定系统安全运维的成败，我们建议对于安全事件处理与应急进行如下方面的建设：

安全事件预警与分级

根据网络与信息安全突发事件对网络与信息系统的直接危害表现，将突发事件的危害表象分为以下五种：

网络中断：指突发事件造成单位管理信息系统的局域网中断、不能正常使用网络的；或单位综合业务数据网络中断，影响管理信息系统主营业务正常运行的。

系统瘫痪：指突发事件造成主营业务系统主要功能不可用或不能正常使用的。

数据毁坏：主营业务数据毁坏后不能全部恢复的。

数据泄密：发生涉及单位秘密的数据泄漏。其它危害：除上述 4 种以外的危害。

根据网络与信息安全突发事件的起因、机理，将网络与信息安全突发事件分为以下七类：

有害程序类突发事件：指受到有害程序的影响而导致的信息安全突发事件。有害程序类事件包含计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件等。

网络攻击类突发事件：指通过网络或其它技术手段，利用配置缺陷、协议缺陷、程序缺陷等攻击信息系统，造成信息系统异常或不可用的信息安全突发事件。网络攻击类事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件等。

信息破坏类事件：指通过网络或其它技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致系统瘫痪、数据毁坏、数据泄密的信息安全突发事件。信息破坏类事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件等

信息内容安全类突发事件：指利用网络发布、传播危害国家安全、社会稳定和公共利益等违法内容的信息安全突发事件。信息内容包括违反宪法和法律、行政法规的信息，组织串连、煽动集会游行的信息等。

故障类突发事件：指网络与信息系统因自身或外围设备设施故障、以及人为误操作等导致的信息安全突发事件。故障类事件包括软硬件自身故障、外围保障设施故障、人为破坏事故、人为误操作事故等。

灾害类突发事件：指由于不可抗力对网络与信息系统造成物理破坏而导致的信息安全突发事件。灾害类事件包括水灾、台风、火灾、雷击、地震、坍塌、恐怖袭击、战争等导致的信息安全突发事件。

其它类事件：指不能归为以上 6 类的信息安全突发事件。

按照网络与信息安全突发事件的危害程度、影响范围和造成的损失，可将单位网络与信息安全突发事件分为特别重大突发事件（Ⅰ级）、重大突发事件（Ⅱ级）、较大突发事件（Ⅲ级）和一般突发事件（Ⅳ级）四个等级。

特别重大突发事件（Ⅰ级）：指网络与信息安全突发事件造成单位各单位因主营业务系统瘫痪，对单位各单位造成巨大经济损失的：

网络大面积中断：因综合业务数据网络中断，造成分单位、子单位内三分之二以上下属单位不能正常使用管理信息系统主营业务系统，持续时间达 0.5 小时以上的。

主营业务系统长时间瘫痪：因主营业务系统主要功能不可用，造成分单位、子单位内三分之二以上下属单位不能正常使用系统，系统瘫痪时间 0.5 个小时以上的。

重大突发事件（Ⅱ级）：指网络与信息安全突发事件造成单位各单位主营业务系统瘫痪，对单位各单位造成重大经济损失的。

网络较长时间中断：因综合业务数据网络中断，造成分单位、子单位内半数以上下属单位不能正常使用管理信息系统主营业务系统，持续时间超过 1 小时以上的。

主营业务系统较长时间瘫痪：因主营业务系统主要功能不可用，造成分单位、子单位内半数以上下属单位不能正常使用系统，系统瘫痪时间 1 个小时以上的。

较大突发事件（Ⅲ级）：指网络与信息安全突发事件造成单位各单位主营业务系统瘫痪、或主营业务系统数据毁坏、或经营管理数据泄密，对单位各单位造成较大经济损失的。

网络中断：因综合业务数据网络中断，造成分单位、子单位内四分之一以上下属单位不能正常使用管理信息系统主营业务系统，持续时间超过 2 小时以上的。

主营业务系统瘫痪：因主营业务系统主要功能不可用，造成分单位、子单位内四分之一以上下属单位不能正常使用系统，系统瘫痪时间 2 个小时以上的。

数据毁坏：主营业务数据毁坏后不能恢复的。

数据泄密：发生涉及单位秘密的数据泄漏。

一般突发事件（Ⅳ级）：指网络与信息安全突发事件造成单位各单位主营业务系统瘫痪、或部分主营业务系统数据毁坏，对单位各单位造成一定的经济损失。

网络中断：因综合业务数据网络中断而不能正常使用网络，造成分单位、子单位内至少 1 个下属单位不能正常使用管理信息系统主营

业务系统，持续时间超过 1 小时以上的。（持续时间超过 1 个小时过短，建议 4 小时）

主营业务系统瘫痪：因主营业务系统主要功能不可用，造成分单位、子单位内至少 1 个下属单位不能正常使用系统，系统瘫痪时间 1 个小时以上的。（持续时间超过 1 个小时过短，建议 4 小时）

数据毁坏：主营业务数据毁坏后只能部分恢复的。

参照网络与信息安全突发事件的分类原则，按照网络与信息安全威胁产生原因，将网络与信息安全预警信息分以下六类：

有害程序类预警信息：指发现的网络与信息安全威胁源于有害程序，有可能导致网络与信息安全突发事件的。有害程序包含计算机病毒、蠕虫、特洛伊木马、僵尸网络、混合攻击程序、网页内嵌恶意代码等。

网络攻击类预警信息：指发现的网络与信息安全威胁源于网络攻击，有可能导致网络与信息安全突发事件的。网络攻击包括拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼等。

信息内容安全类预警信息：指发现的网络与信息安全威胁为危害国家安全、社会稳定和公共利益等违法内容的信息，有可能导致网络与信息安全突发事件的。

故障类预警信息：指发现的网络与信息安全威胁源于软件、硬件自身的安全隐患、漏洞等，且同类软硬件或设施也有可能故障或不可用的，有可能导致故障类突发事件的。

灾害类预警信息：指发现的网络与信息安全威胁源于水灾、台风、火灾、雷击、地震、坍塌、恐怖袭击、战争等不可抗力因素，有可能导致灾害类突发事件的。

其它类预警信息：指不能归为以上 5 类的网络与信息安全预警信息。

按照网络与信息安全可能造成的危害、紧急程度和发展势态，将网络与信息安全预警信息分为四级，即特别严重（红色）、严重（橙色）、较重（黄色）和一般（蓝色）。

特别严重预警（红色）：指发现的网络与信息安全威胁，可能影响单位范围内所有网络和主营业务系统，并有扩散到单位全网的可能性。

严重预警（橙色）：指发现的网络与信息安全威胁，可能影响单位范围内多个单位的网络和主营业务系统，并有继续扩散的可能性。

较重预警（黄色）：指发现的网络与信息安全威胁，可能影响单位范围内多个单位的网络和主营业务系统，但无扩散性。

一般预警（蓝色）：指发现的网络与信息安全威胁，只可能影响单位范围内 1 个或个别单位的网络和主营业务系统，且无扩散性。

安全事件处理

（1）信息安全事件处置

各系统发生安全事件时，系统管理员、网络管理员应及时处理和汇报；各安全管理员应对信息安全事件的发生、处理办法进行记录，并把《信息安全事件记录单》提交给单位信息技术专业机构进行备案。

在处理安全事件过程中，系统管理、网络管理以及信息安全管理员需要根据信息安全事件的处置进程持续判断安全事件的严重程度，一旦达到设定的级别，立即启动应急处置程序。

（2）信息安全事件汇报

正常情况下，每日由单位信息技术专业机构值班人员总结一天来的信息安全状况，并将前一日信息安全事件处理结果进行汇报，每日信息安全报告通过电子邮件方式报告给单位信息技术专业机构领导和信息安全管理部门；信息系统管理人员及信息安全管理人员在值班过程中，监测到信息安全事件的发生，应初步判断信息安全事件的等级，并立即向部门领导报告；部门领导接到信息安全事件报告时，立即核实信息安全事件的等级，如果信息安全事件等级超过一般突发事件（Ⅳ级），则立即单位信息技术专业机构领导汇报。信息技术专业机构领导立即核实信息安全事件的等级，如果信息安全事件等级超过重大突发事件（Ⅱ级），则立即向单位信息安全管理员会主任汇报。

（3）事件处理程序

1）备份

完全备份所有受影响的系统，包括所有的日志和文件系统的“镜象备份”。

2）隔离

隔离是指立即切断信息安全事故的源头。从物理上完全阻止入侵或攻击的继续。例如，关闭主路由器或断开相关网络连接、物理隔离受攻击的服务器等。对于严重的信息安全事故必须采取紧急隔离措施。

3）监视

在断开受入侵或攻击设备和其他重要或敏感设备的网络连接后，可以对入侵者进行监控，记录入侵者在系统上所进行的所有活动，并在监控的基础上，跟踪入侵者，查出入侵或攻击源头（可以和其他网络或系统管理联系，以取得必要的技术协助）。

4）记录取证

应采集如下记录证据：

防火墙日志文件

入侵检测日志文件

防病毒系统日志文件

网络监控日志文件

路由器日志文件

主交换机日志文件

受影响计算机设备的安全审计记录

所有系统的进程、帐号、配置文件属性记录

进出受影响计算机设备的网络包

5）现场分析处理

调查分析是安全事故事后处理的核心，其主要目的在于找到发生安全事故的原因和相关解决方案。需要注意的是，整个调查分析工作不得不可信的单位进行全权处理。在没有找到安全事故的原因或相关解决方案前，在不影响系统可用性的情况下，须将受影响的计算机系统上线。

根据收集到的信息做处理

分析入侵方式

分析入侵过程

预测和确认入侵方法及时间

统计威胁造成的严重性

制定解决方案并处理

如果不能解决，则转入联系第三方

6）现场分析

调查分析是安全事故事后处理的核心，其主要目的在于找到发生安全事故的原因和相关解决方案。需要注意的是，整个调查分析工作不得不可信的单位进行全权处理。在没有找到安全事故的原因或相关解决方案前，在不影响系统可用性的情况下，须将受影响的计算机系统上线。

根据收集到的信息做处理

分析入侵方式

分析入侵过程

预测和确认入侵方法及时间

统计威胁造成的严重性

7）阻止

可以采用方式阻止更进一步的事件破坏：

对所有审计信息（如：系统日志文件）进行备份，并妥善保管；

获取所有进程的状态信息并将其存在一个文件里，安全存放文件；

所有可疑的文件都应该先转移到安全的地方或在磁带里存档，然后将其删除；

列出所有活动的网络连接，在分析员的帮助下获得系统的快照，记录所有的行为。

杀掉所有活动的黑客进程，并删除黑客在系统中留下的文件和程序；

改变所有黑客访问过的帐户的口令，删除黑客自己开的帐号。记录所有行为。

8）联系第三方

联系第三方安全咨询单位、安全顾问、安全专家和安全、系统厂商等。单位信息安全管理人员、相关信息系统管理人员和第三方共同找出解决方案。

9）恢复日常状态

恢复日常状态包括对遭受安全事故影响的系统进行恢复和安全修复两方面的工作，使受损的系统能恢复正常运作，并作必要的技术处理，当相同的安全事故再次发生时，系统将不受其影响。

重新安装操作系统和应用程序

恢复攻击前所有的正常数据

根据该系统的配置文档进行配置

10）加固处理

加固系统使系统同类问题的破坏，在采用这些措施之前，有必要对系统的损坏程度进行评估，对恶意代码进行分析提供相应的解决方

案。根据解决方案，按照系统、网络、数据库等安全配置标准进行加固处理。

11）重新入网

在经过加固处理后，确定系统恢复日常状态，可以重新接入网络，把隔离的系统重新加入网络，解除隔离。

12）反馈

根据安全事故的损失和后果，明确责任者，并由单位信息技术专业机构领导将安全事故的处理报告提交给单位信息安全管理委员会。对于涉及计算机犯罪的安全事故，安全事故的处理报告由单位信息安全管理委员会决定是否抄送给公安部门。

13）总结

对问题进行调查分析，务必找出原因，并制订相应的预防对策。

14）事件结束

系统恢复运行，事件结束。将安全事故处理报告抄送给单位文档管理员归档。

安全事件通报

（1）安全事件通报内容

安全事件的通报内容如下：

网络与信息安全突发事件信息；

网络与信息安全预警信息；

利用网络传播危害国家安全、社会稳定和公共利益等有害或违法信息的情况；

已经确定或可能发生的计算机病毒、网络攻击情况；

网络或信息系统通信和资源使用异常，网络和信息系统瘫痪、应用服务中断或数据篡改、丢失、泄露等情况；

网络安全状况、安全形势分析预测等信息；

其他影响正常生产的网络与信息安全信息。

（2）通报制度和方法

通报制度如下。

建立月报制度：每月应填写《网络与信息系统安全运行月报》，建议在每月第 2 个工作日前将上月的安全运行月报上报信息中心。

敏感时期执行日报制度：根据国家有关规定，例如在两会、“十一”、春节及特殊敏感时期，应设专人值守，。对于特殊敏感时期，由总部下发敏感时期信息安全通报通知，并明确日报的启动时间、截止时间。

建立网络与信息安全突发事件信息通报制度：当发生网络与信息安全突发事件时，应填写《网络与信息安全突发事件报告》，并按照突发事件不同等级要求，及时上报至信息中心。

建立网络与信息安全预警信息通报制度：各单位应通过各种途径收集网络与信息安全预警信息，当预警信息等级为特别严重或严重时，应在 24 小时内向信息中心上报

通报方法如下。

信息通报可通过单位数据上报平台完成上报。信息通报人负责信息通报的上报和接收。

对于网络与信息安全突发事件，还应通过信息中心的值班电话进行通知。

日报、月报执行零事件报告制度。

还应按照国家、单位保密规定，做好本单位网络与信息安全信息通报的保密工作。

应急响应流程

当系统出现安全事件后，必须启动应急响应，应急响应的流程如下图所示：

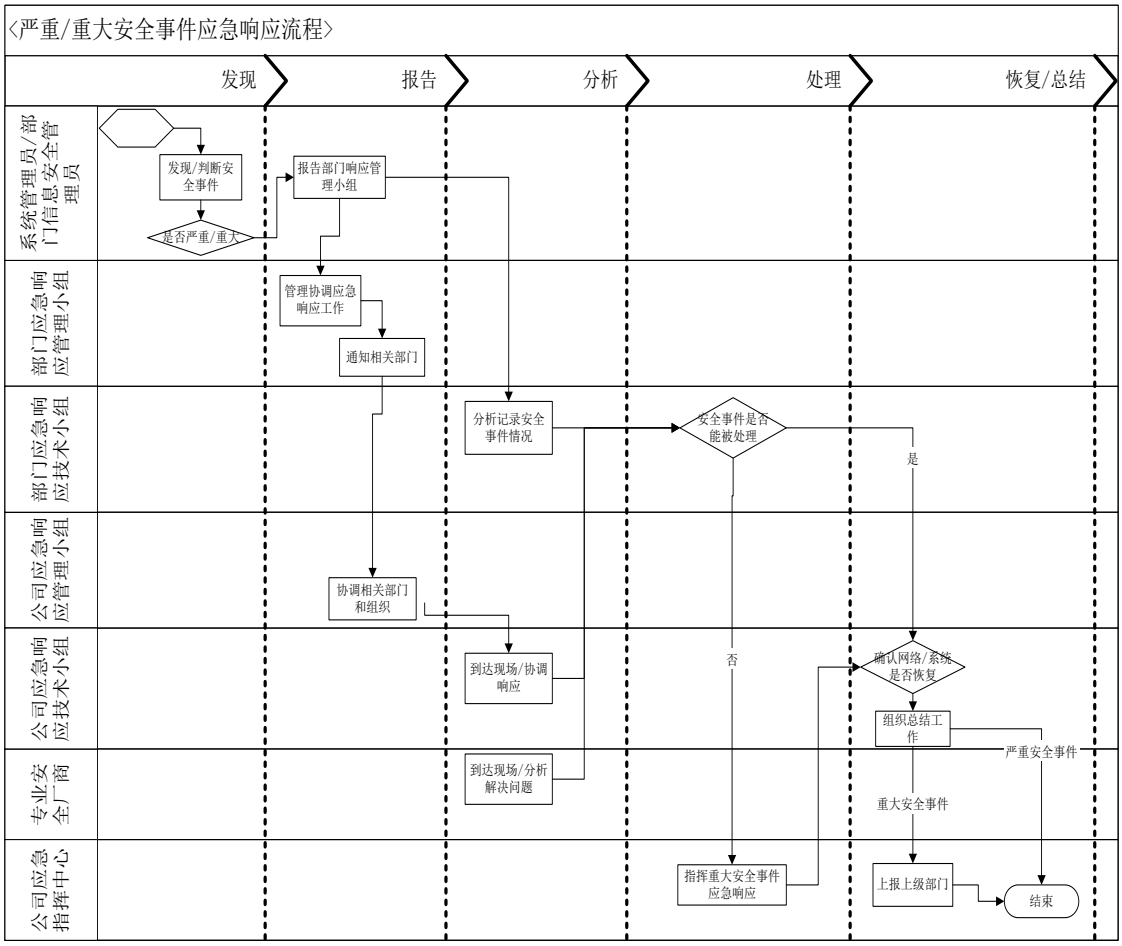

图 1 应急响应流程图

日常安全运维管理解决方案

运维管理

各系统管理员应根据单位的各类技术规范制定本系统的安全运行维护计划，并根据已经制定的安全运行维护计划进行日常操作和检查；部门信息安全管理员应定期检查各系统安全运行维护计划的执行情况，查看安全运行维护记录和实际的匹配情况，并进行记录；部门信息安全管理员应定期向单位信息安全办公室提交安全检查情况记录和报告，由信息安全办公室统一进行备案和审计。

（1）操作程序和操作记录

各系统管理员在进行系统日常操作活动时应依照文档的程序进行，如计算机启动和关机程序、备份、设备维护、计算机机房和信息处理的管理和安全控制程序。

各系统管理员应将操作程序作为正式文件对待，经部门三级经理审批后才可修改。

为了严格日常运行的安全管理，便于落实和检查，运行部门的系统管理员应做日常记录和登记。

对于重要设备的各种操作行为，应保留审计记录。

（2）登录规程和口令管理

单位各系统制定相应的登录规程，包括：登录失败审核、账户锁定、登录连接时间超时控制和历史登录信息提示等。

单位各系统的账号、口令应根据《信息安全账号、口令及权限管理办法》中的规定严格执行。

（3）安全检查

单位网络与信息安全工作组要根据各等级业务系统定义的安全目标定期进行以下检查：

信息安全组织机构的组成及运作；

日常运行安全；

数据备份安全；

技术资料安全；

防病毒；

物理环境安全；

设备物理安全；

主机安全；

数据库系统安全；

应用系统安全；

网络系统安全；

信息安全应急；

黑客防范和计算机安全专用产品等。

介质管理

（1）介质的访问控制

介质的使用，需要严格执行介质管理制度，包括申请、审批、登记、归还等手续，介质的保管人和借用人有责任和义务保证介质的完整和安全，不得丢失和损坏。

对涉及含有单位秘密的介质原则上不能借用和复制。对确实因工作需要，如系统改造和维护等，必须由项目负责人提出申请。

介质保管理负责人有责任维护介质的完整性，一旦发现介质丢失或损坏，应立即报告技术资料的主管部门，由技术资料的主管理部门采取补救措施。

（2）介质的存储环境安全

介质存储室必须符合防火、防水、防震、防腐烂、防鼠害、防蛀虫、防静电、防磁场及防盗的安全要求。

介质存储室应指定明确的负责人，并明确管理人员的管理要求和责任，要求制定介质存储室管理办法。

介质存储室的管理员要严格、整齐、有序地管理好生产用各种数据和存储介质。

介质存储室管理员，应负责介质存储室的管理工作，并核查介质使用人员身份与权限。介质存储室严禁其他人员擅自进入、逗留。

应设立入库、转储、使用、销毁登记记录。对各类介质入库、使用、转储、销毁应有审批手续和传递记录。

（3）介质的分类和归档

介质应按照纸介质和电子介质分别集中分类管理、编制目录、造册登记。对同一内容以不同介质存储的技术资料要建立对应关系，以便于管理和使用。

对电子介质技术资料，要定期转储，并进行转储登记记录。

（4）介质的销毁和处置

对于纸文件、录音、复写纸、输出报表、一次性打印色带、磁带、可换的磁盘或盒式磁带、光盘（所有形式，包括所有生产商的软件光盘）、等介质，应安全销毁。

对于电子介质技术资料，要每半年进行转储，并进行转储登记记录。

应记录敏感信息的清除，如可能，保留一份审计跟踪记录。

恶意代码管理

所有计算设备用户应保证使用的计算设备按照单位要求安装了相应的病毒防护软件或采用了相应的病毒防护手段，并且应保证这些措施的可用性。如果自己无法对病毒防护措施的有效性进行判断，应及时通知单位 IT 服务部门进行解决；单位各系统防病毒系统应在遵循单位病毒防护系统整体规划的前提下由单位网络与信息安全办公室委托各系统自行建设和管理；单位各级人员在发现终端感染病毒的情况下，应首先拔掉网线，降低可能对单位网络造成的影响，然后向单位 IT 服务部门提交《病毒事件报告》；各系统管理员在生产和业务网络发现病毒，应及时进行处理，并依照相关规定进行汇报和备案。

（1）病毒响应时限

所有病毒防护的负责部门或人员应严格遵守病毒响应时限的要求。如无法在病毒响应时限内完成对病毒的响应工作，应及时上报单位信息安全管理部门进行协调解决并承担相应责任。

办公终端感染病毒的（非蠕虫类），应在发现时（防病毒系统记录或技术支持电话记录）起 2 小时内进行解决。

办公管理终端感染蠕虫的，应在发现时（防病毒系统记录或技术支持电话记录）起 30 分钟内进行解决。

服务器、监控平台等生产设备感染病毒的（非蠕虫类），应在发现时（防病毒系统记录）起 1 小时内进行解决。

服务器、监控平台等生产设备感染蠕虫的，应在发现时（防病毒系统记录）起 30 分钟内进行解决。如果该设备会对其他生产设备产生大于设备离网产生的影响时，应立刻切断该设备与网络的连接。

（2）监督和检查

单位病毒防护系统整体规划应由单位网络与信息安全工作组负责，定期组织各部门、各系统安全管理员对病毒防护系统现状进行检查、评估并提出改进建议。

单位各系统信息安全管理员应根据系统信息安全操作计划按时上报系统防病毒系统运行情况。

变更管理管理

（1）配置管理

单位各系统应对本系统的设备、系统等 IT 资产进行配置记录，并保存配置记录的信息。

单位各系统管理员对于系统配置操作的信息应进行记录并保存。

单位各部门信息安全组织应对各系统定制配置操作流程、并严格按照操作流程进行操作。

单位各系统应定制系统配置计划，根据配置计划定期进行设备和系统的配置。

（2）变更管理

单位各系统在发生变更操作时，应根据相关制度进行审批、测试。

单位各系统在发生配置变更操作时，系统管理员提出变更申请，并填写《配置变更申请单》和《配置变更参与人员信息表》。

单位各系统执行变更操作前，要对变更操作进行测试，确定无不利影响，并向部门信息安全组织提交测试计划、风险分析报告以及回退计划。

系统管理员测试完成后，连同申请单一并报部门三级经理审批，审批通过后可以进行配置变更操作。

单位各系统发生配置后，应在单位信息安全办公室进行备案。

单位各系统管理员应对变更操作的具体步骤进行记录并保存。

备份与恢复管理

（1）数据备份

数据管理牵头部门在技术支持部门的协助下制定备份策略和相应的操作规程。备份策略的制定应根据系统性能、存储容量、数据量增长速度、业务需求、备份方式、存储介质、存储介质型号、有效期等因素制定。

在特殊日、版本升级日增加特殊备份。

数据管理实施部门要根据备份策略按照操作规程做好数据备份。

实施数据备份时，要仔细检查备份作业或备份程序的执行结果，核实目标备份与源备份内容一致，确保备份数据的完整性和正确性。

数据管理实施部门应及时记录备份情况，包括备份作业（或名称），备份周期（定期或临时增加）、时间、内容、数据保存期限，磁带型号、磁带容量、业务种类、归档情况、异地备份记录、相关变更记录等信息，并进行当日备份的问题记录，以留档备查。

存放备份数据的介质必须具有明确的标识。标识必须使用统一的命名规范，注明介质编号、备份内容、备份时间和有效期等重要信息。

（2）数据恢复

数据恢复前，必须根据情况对原环境有用的数据进行必要的备份，防止有用数据的丢失。

数据恢复申请、审批要按照数据恢复流程和规范执行。

数据恢复过程中严格按照数据恢复手册执行，出现问题时由技术部门进行现场技术支持。

数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。

（3）数据保管、抽检

数据管理实施部门根据备份策略保存数据。

数据管理实施部门应编制所保管数据的清单，清单内容包括介质编号、备份内容、备份时间和保留期限等重要信息。采用自动化技术集中管理的备份数据须实现备份数据清单管理的电子化。

数据管理牵头部门必须对数据存储介质的异地存放、运输、交接和抽检等工作制定具体的管理规程。

数据管理牵头部门和技术支持部门共同制定数据抽检方法，包括抽检频度、验证方式等。

对备份数据超过保存期限的介质进行清理，清除介质上的原有数据后入库转作可用带使用。

数据存储介质的存放和运输要满足安全管理的要求，保证存储介质的物理安全。备份数据必须异地存放，并明确落实异地备份数据的管理职责。

（4）数据使用

信息系统中的数据不得随意查询、记录、携带、复制、传输、修改、删除和泄漏。

测试环境和研发环境需要使用生产环境的数据时，原则上要采用专用的处理程序进行适当的变形处理。

技术部门对数据磁带的借用严格遵守磁介质借用审批流程，进行审批、登记、交接和归还，并保证备份数据完好无缺。

（5）数据清理

数据管理牵头部门根据信息系统运行性能，运行成本和业务部门对数据使用的要求，制定数据清理规范，包括清理周期、清理内容等。

数据清理前必须对数据进行备份，在确认备份正确后方可进行清理操作。历次清理前的备份数据要根据备份策略进行定期保存或永久保存，并确保可以随时使用。

数据清理的实施应避开业务高峰期，避免对联机业务运行造成影响。

（6）数据归档

数据管理牵头部门和技术支持部门共同对归档的数据制定合理的归档方案及有效的查询、使用方法，保证数据的完整性和可用性。

需要长期保存的数据，数据管理实施部门根据归档方案和查询使用方法要在介质有效期内进行归档，防止存储介质过期失效。

归档的数据必须有详细的文档进行记录，记录信息包括：介质的编号、存储的内容、存储数据的记录时间、归档日期、保留期限、访问记录和操作、维护人员等。

（7）数据保密

任何单位和个人发现使用数据的违规行为都有权阻止或举报。

涉及加密环节的重要数据（例如各类密码和密钥、各类校验算法、加/解密算法和参数、终端设备识别算法和参数、身份识别算法和参数等）及其存放介质和技术资料等，必须同时按照有关法律、法规和单位有关规定严格管理。

外单位人员对单位存放数据的设备进行维修、维护时，必须由单位设备管理人员现场全程监督。有关设备或介质需送交外单位维修、维护前，设备管理部门应确认设备或介质内的数据已经清除。

设备管理管理

（1）信息资产分类

信息资产的识别是指按照规定属性对各类信息资产的辨认和区分，包括信息资产识别、分类和登记等项工作。

单位信息资产主要包括如下几类：

网络设备：无线 AP、AC、BAS、Hub、RAS、VoIP 网关、二层交换机、负载均衡、光纤转换器、路由器、缓冲服务器、调制解调器、多层交换机等构成信息系统网络传输环境的设备，软件和传输介质；

服务器：各类承载业务系统和软件的计算机系统及其操作系统，包括安装在服务器上各类应用系统以及构建系统的平台软件（数据库，中间件、群件系统、各商业软件平台等）；

存储设备：NAS、SAN、磁带机、磁带库、磁盘阵列、光纤交换机等构成信息系统存储环境的设备，软件和传输介质；

安全设备：VPN 网关、防火墙、内容过滤网关、入侵检测系统、防病毒网关、加密机、安全网闸等构成信息系统信息安全环境的设备和软件；

终端资产：指各级机构的办公终端和各信息系统的生产终端，包括一般用途的笔记本和 PC、柜台终端、监控终端、NC、on-demand 终端等；

单位专有资产：单位通信类专门设备，在信息安全管理的资产管理中，不将其作为资产管理的范畴；

其他资产：非以上信息资产。

（2）信息资产安全赋值

信息资产的安全价值有别于商品价值，由资产的机密性价值、完整性价值和可用性价值三部分组成。

信息资产安全性赋值按照如下规定进行：

每项资产的机密性价值、完整性价值和可用性价值分为一至三级；

根据资产所包含秘密信息被揭露时所可能造成后果的严重性可将资产的机密性价值分为“轻度损害”“中度损害”“严重损害”三级；

根据资产处于不正确、不完整或可依赖状态时所可能造成后果的严重性可将资产的完整性价值分为“轻度损害”“中度损害”“严重损害”三级；

根据资产不可用时所可能造成后果的严重性可将资产的可用性分为“个体不可用”“局部不可用”“整体不可用”三级。

（3）信息资产信息管理

信息资产信息的维护：各系统管理员识别管理的信息资产，并将信息资产的信息录入单位安全管理系统中的信息资产管理部分。

各部门信息安全管理员有责任协助本部门系统管理员核实和维护本部门系统信息资产的信息。

信息资产内部属性发生变更，系统管理员要及时更新到单位安全管理系统中。变更包括地理位置变动、信息资产配置信息、补丁信息等变动。

信息资产管理权限发生变更，系统管理员要及时通知本部门安全管理员或单位安全管理员，将信息资产状况及时更新到单位安全管理系统中。管理权限变更包括信息资产所属系统发生变更和信息资产所属部门发生变更。

应按规定要求对本系统信息资产进行调查，并建立信息资产清单和记录信息资产状况的档案。信息资产清单通过“单位网络信息安全管理系统”存储及管理。

（4）信息资产信息的检查

各部门信息安全管理员在部门季度评估中，检查本部门系统管理员信息资产信息与单位安全管理系统中信息是否一致，结果作为系统管理员安全考核的因素之一。

单位半年定期风险评估中，检查各部门信息资产与单位安全管理系统中信息是否一致，结果作为被管理部门信息安全员的考核因素之一。

单位及部门信息安全管理员随时抽检资产信息和单位安全管理系统中信息是否一致，结果将被作为检查系统管理员及该部门的考核因素之一。

（5）信息资产保护

信息资产保护管理：

信息资产设备由所属的系统管理人员负责安全防护。

信息资产所属部门安全管理组织，定期评估本部门所属系统信息资产的安全状况。

单位网络与安全工作办公室定期评估单位所有信息资产的安全状况。

信息资产保护内容：

信息资产要及时安装安全补丁，安全补丁的安装要符合业务影响最小原则。

信息资产设备每年定期进行信息安全评估及安全加固。

信息资产的信息要及时反映到单位安全管理系统中。

不同信息资产设备应根据系统及资产的重要性，部署不同程度的安全保护措施。

网络安全管理

在网络安全管理过程中，需要重点考虑如下内容：

各系统网络设备当前运行配置文件应和备份配置文件保持一致。

各系统网络设备的配置变更应根据《信息安全管理流程-安全配置变更管理流程》严格执行。

网络设备登录提示标识应适当屏蔽内部网络信息内容，并应有相关合法性警告信息。

各系统管理员应定期检查网络设备登录方式的开放情况，关闭没有使用的登录方式。

通过设备日志或外部认证设备维护对设备的登录状况，内容应当包括访问登录时间，人员，成功登录和失败登录时间和次数等信息。

严格控制对网络设备的管理授权。按照最小权限原则对用户进行授权。

各系统网络设备的密码应严格按照《信息安全账号、口令及权限管理办法》执行。

各部门应定期地收集设备运行状况，通过运行记录和供应商了解目前已有设备的硬件/软件缺陷，跟踪设备缺陷的修复情况，及时向部门信息安全组织和单位信息安全办公室汇报，作为设备选型/厂商选择的参考指标。

负责网络设备维护的人员应与网络设备厂商保持畅通的沟通联系，以便能及时从厂商处获取必要的技术支持。

严禁管理员透漏设备口令、SNMP 字符串、设备配置文件等信息给未授权人员。

所有网络必须具有关于拓扑结构、所用设备、链路使用情况等关于网络情况的详细说明文档，并保持文档内容和现有网络、设备连接和链路信息保持一致。

网络应具备冗余设计和规划，实现基本的冗余配置，预防关键点的网络故障。应配备冗余链路、核心和汇聚层的冗余设备，配置冗余路由以充分保障网络的可用性。

对重要区域实行冷备份与热备份相结合的方式，避免双重失效造成的影响。

网络冗余措施应根据预先制定的冗余配置、设备、线路等测试方案定期进行验证测试，以判别是否满足冗余要求。

网络管理员或安全管理员对网络链路应进行探测和监控，并对已经发生的安全事件进行及时响应和处理。

重要部门在网络上传输机密性要求高的信息时，必须启用可靠的加密算法保证传输安全。

在网络中选择和使用恰当的路由协议，并正确地进行配置和实施，保证网络的互联互通。

由统一的 IP 地址管理机构、人员负责对外部和内部各个部门、人员的 IP 地址进行规划、登记、维护和分配。确保各个部门有足够的地址容量并有一定的冗余供扩展使用。

对于重要区域应单独分配地址段，用于专门的网络设备互联，不与其他用户混用，以利于安全措施的使用。

维护和记录 IP 地址的使用情况，及时关闭和回收被废止的地址。

未经部门或单位信息安全组织批准，测试网络与单位内部网络不能直接连接。

未经部门或单位信息安全组织批准，严禁员工私自设立拨号接入服务。

未经部门或单位信息安全组织批准，严禁员工通过拨号方式对外部网络进行访问。

所有的远程访问必须具备身份鉴别和访问授权控制，至少应采用用户名/口令方式，通过 Internet 的远程接入访问必须通过 VPN 的连接，并启用 VPN 的加密与验证功能。

不同安全域之间应采用防火墙，路由器访问控制列表等方式对边界进行保护。只开放必要的服务和端口，减少暴露在网络外部的风险。

对于重要的系统需要在防火墙上对信息流的内容按照一定方式进行边界过滤。

根据业务变化及时检验更新现有的防火墙配置策略，满足新的安全需求。

采取逻辑或物理隔离方法对网络采取必要的隔离措施，以维护不同网络间信息的机密性，解决网络信息分区传输的安全问题。

在网络中的重要位置应部署网络监控设备或者采用人工手段，监控采集网络中的流量和事件，设备运行情况等信息，分析发掘异常事件。

网络中各设备应开启日志记录功能，对网络使用情况进行记录。

建立网络中的审计体系，应当对审计结果中的异常信息和长期性事件趋势进行分析。

系统安全管理

（1）帐号管理

在账号的管理过程，需要重点考虑如下内容：

单位各系统应根据不同的角色确定用户帐号，帐号至少应当分为以下角色：

系统管理员：负责维护系统的管理员；

普通用户：访问系统的普通用户，只具有相应访问内容和操作的最小权限；

信息安全管理员：对系统账号进行管理

信息安全审计员：对系统的安全进行审计

各系统管理员应当对系统中存在的帐号进行定期审计，系统中不应存在无用或匿名帐号。

应定期检查和审计账户信息，内容应包含如下几个方面：

遵守最小权限原则；

用户情况是否和安全部门备案的用户帐号权限情况一致；

是否存在非法帐号或者长期未使用帐号；

是否存在弱口令帐号。

各系统应开启系统安全日志功能，能够记录系统的登录和访问时间、操作内容。

各部门在创建帐号、变更帐号以及撤销帐号的过程中，都应进行备案。

（2）权限管理

用户访问权限由用户所在部门主管领导申请，经应用系统管理部门审批后，由应用系统管理员开通相应的权限；系统管理员开通用户权限后，需向用户提供访问权限的书面说明，并要求用户签字确认，表明已了解访问的条件；各系统应限制第三方人员的访问权限，对第三方的访问进行定期的检查和审计。

（3）用户注册、认证和注销

应用系统应该包括正式的注册、登录认证和注销模块，并且能够对不同用户的访问权限进行严格的访问控制。具体要求包括以下内容：

信息安全审计人员定期检查授权访问的级别是否基于业务目的，且符合单位的安全策略，如不得违反职责分离原则。

系统管理员开通用户权限后，需向用户提供访问权限的书面说明，并要求用户签字确认，表明已了解访问的条件。

保留所有注册人员使用服务的正式记录。

根据人力资源管理部门的通知，及时修改或注销已经更换岗位或离开单位的用户的访问权限。

定期核查并删除多余、闲置或非法的用户帐号。

（4）应用系统管理的安全控制

应用系统的运维管理安全，需要进行如下限制：

1）确定不同系统的超级权限以及需要获得此类特权的人员类型。

2）超级权限的使用授权应基于“使用需要”，按逐个事件进行分配，以完成其当前工作任务的最低要求为依据，在完成特定任务后超级权限用户帐号应被收回。

3）超级用户的使用必须严格按照超级权限分配授权流程进行审批、分配和授权，并保留所有超级权限的分配授权流程的记录，在未完成授权流程和手续之前，不得授予特权。

4）当现有用户需要超级权限时，应在其原有的用户帐号之外，另行设置一个授予了超级权限的特殊帐号。

5）尽量对管理权限进行分割，把不同的管理权限赋予不同的帐户。

6）应用系统应该具备管理员帐号登录和管理操作的记录。

7）定期对系统的日志进行审计，以发现异常登录、操作。

8）做好超级权限拥有者无法行使职责时的应急安排，如角色备份。

（5）应用系统安全审计

应用系统应该具有完善的日志功能，能够记录系统异常情况及其他安全事件。审计日志应保留规定的时长，以便支持日后的事件调查和访问控制监控。审计日志包括以下内容：

1）用户创建、删除等操作。

2）登录和退出的日期和具体时间。

3）终端的身份或位置（如果可能的话）。

4）成功的和被拒绝的系统访问活动的记录。

5）成功的和被拒绝的数据与其他资源的访问记录。

6）成功的和被拒绝的管理操作记录。

安全沟通与合作解决方案

沟通与合作为信息管理体系健康运作得主要方式。沟通是为人员提供交流途径，以保持他们之间的协调一致，共同实现安全目标。合作是为上述过程所有相关人员提供学习途径，以提高他们的风险意识和知识，配合实现安全目标。

为保证风险管理活动的顺利有效的进行，相关人员之间交流的畅通以及熟练的掌握相关知识是十分关键的因素，而这就是沟通与合作的意义所在：沟通，是为相关人员提供交流的途径，以保证相互之间的行动协调一致，共同实现安全目标；咨询，是为相关人员提供学习的途径，以提高风险意识与知识，帮助实现安全目标。

沟通与合作的分类

在安全管理活动中，安全相关人员保持不同角色之间交流畅通的重要一环：对上，安全员需要向主管领导说明风险管理的内容与作用，

以获得主管领导的理解与支持；对下，需要向系统使用人员灌输安全管理的理念和已实施控制措施的内容，以保证控制措施的顺利执行；对内，安全员必须和系统管理人员进行充分的交流，以保证相互之间的协调一致；对外，一方面需要紧密联系主管机构，获得及时的信息，另一方面需要向外部的安全专家以及安全评估机构咨询有关风险评估和控制的方法、技术以及工具。

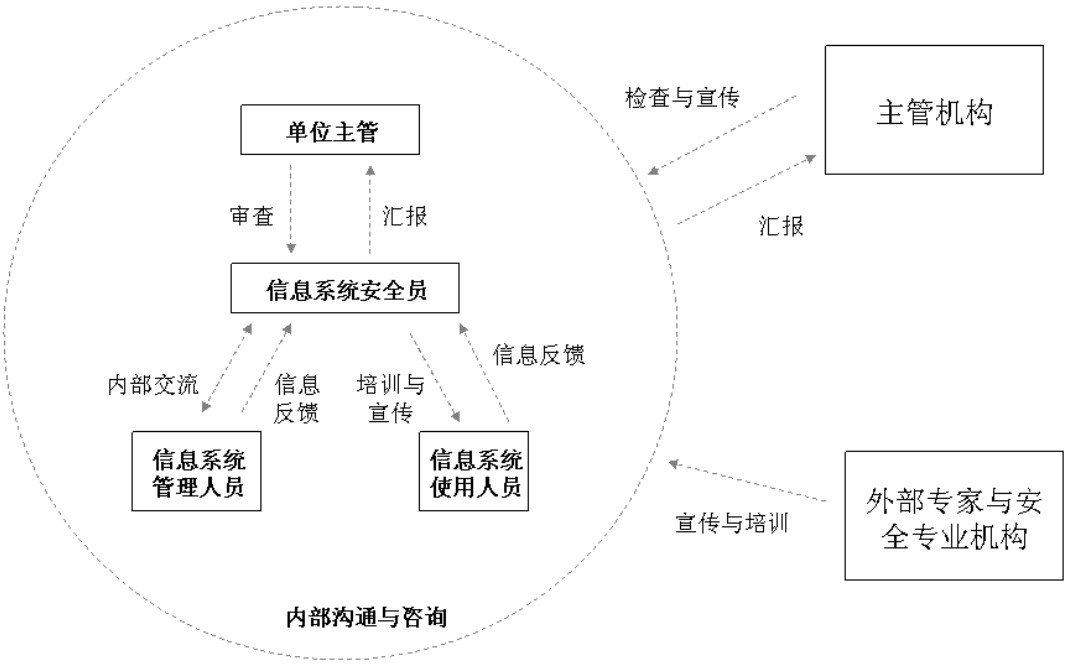

图 2 不同角色之间交流畅通

在完整的安全管理活动中，不同角色之间沟通与合作的内容主要可以分为以下几类：

信息系统安全相关人员和信息系统管理人员之间的交流，是保证风险管理过程顺利进行的重要因素。这种双向的交流有助于管理人员理解风险的意义以及风险评估和风险控制的基本方法与内容，从而提高自身分析问题的能力；同时，管理人员对于信息系统深刻的了解，

有助于安全员分析资产的价值、弱点的赋值以及威胁发生的可能性与影响，从而提高风险评估的可靠性和控制措施选取的有效性。

信息系统管理人员及时的向信息系统安全相关人员反映系统的改变和产生的安全事件，为安全员决定下一步行动提供了重要的依据。

信息系统安全相关人员对于系统使用人员的安全宣传和培训，是提高使用人员风险意识的主要途径。与安全员和管理人员之间相互的交流不同，由于系统使用人员为数众多，双向的交流很难实际开展起来，因此单向的培训与安全宣传是提高使用人员风险意识最有效的途径。

系统使用人员向信息系统安全相关人员反馈的系统运行状况以及控制措施执行情况，是安全员判断控制措施有效性的重要依据。

信息系统安全相关人员向主管领导准确、翔实的汇报，有助于获得主管领导的理解和支持。

在安全管理管理活动中，外部的安全专家或安全机构通过讲座和培训的方式，可以提高相关参与人员的知识与技能。

风险管理不同阶段中的沟通与合作

在系统建设的不同阶段中，沟通与合作的侧重点各有不同：

系统设计阶段。信息系统安全相关人员通过和信息系统管理人员的交流沟通，以及向系统设计人员了解相关信息，才能够准确的确定安全管理的对象和范围；同时，安全员向主管领导进行汇报，获得主管领导的理解与支持，是安全管理活动得以开展和进行下去的关键因素。

系统建设阶段。信息系统安全相关人员必须通过信息系统管理人员提供的信息，才能准确的确定资产、弱点和威胁的赋值；同时，只有当管理人员对于风险有了相当的理解，才能够提供有效的信息，这是一个双向互动的过程。另外，外部的安全专家和专业机构能够提供先进的评估方法、技术和工具，有助于提高风险评估结果的可靠性。

系统运维阶段。通过和信息系统管理人员的交流，信息系统安全相关人员能够更加准确的判断每一项控制措施实际的有效性以及相关成本，从而为控制措施的选取提供依据；同时，为保证选取的控制措施能够顺利的实施与执行，对于系统使用人员的安全宣传和培训是必不可少的。

贯穿于整个安全管理活动中，为更好的发挥监控与审查的作用，适当的沟通与合作是十分必要的。通过系统使用人员的反馈和与信息系统管理人员的交流，信息系统安全相关人员能够更好的掌握控制措施的有效性，了解系统变化和安全事件，从而为下一步采取的行动提供依据。

定期风险评估解决方案

系统在运维过程中，需要对系统进行定期的风险评估，定期风险评估是指按一定固定周期性，就约定的信息系统范围进行安全检查，来发现信息系统在日常运维过程中可能新增加的安全隐患，分析系统运维过程的不足，并给出相应的解决建议。

定期风险评估体现了日常安全运维工作的规范化和专业化，根据客户信息系统的重要程度按不同周期持续的检查，使用户充分了解系

统安全的实时状况。避免了因为客户自身技术力量不足而影响信息系统的安全运行。

定期风险评估能使客户的信息系统安全运行，向合规化、专业化、体系化发展，使客户能清晰掌握自身信息系统的安全状况，轻松地管理系统的安全问题，有更多精力去更专注地开展业务，提高经营效益。

评估方式

定期风险评估的按照评估的频率主要有以下几种：

表 1　定期风险评估频率表

方式	内容
2 次/年	每六个月一次完全检查，二级粒度了解系统安全状况
4 次/年	每三个月一次安全检查，三级粒度了解系统安全状况
6 次/年	每两个月一次完全检查，四级粒度了解系统安全状况
12 次/年	每个月一次完全检查，五级粒度了解系统安全状况
自定义	根据客户需要，自定义评估周期，完全风险管理解决方案

以下是不同频率的定期风险评估方式对应的成本费用及风险控制精度：

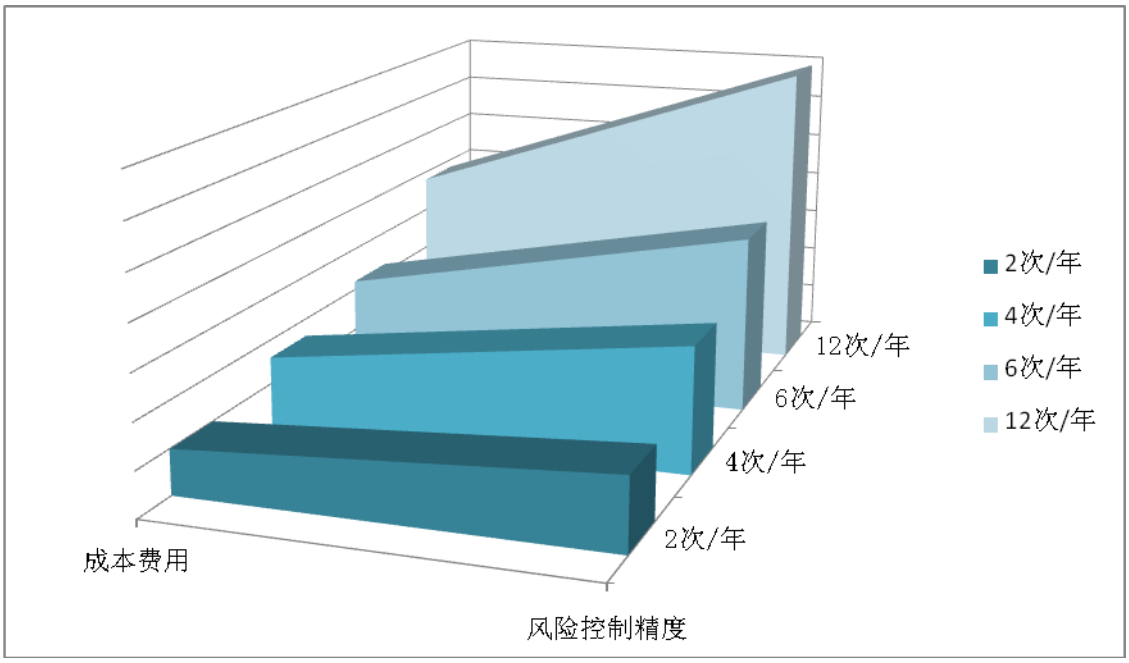

图 3 定期风险评估成本及风险精度示意图

评估内容

定期风险评估内容模块主要包括：

表 2 定期风险评估内容

类型	内容	方式
数据层面	业务分析、逻辑合理性	人工分析
应用层面	Web 容器、中间件、数据库	工具、手工
主机层面	通用系统日志，包括：应用程序日志、系统日志、安全日志等。	工具、手工
网络层面	网络设备日志、安全日志	工具、手工
管理层面	工作制度、业务流程、操作规范、人员安全	查阅分析 咨询建议
物理层面	主机设备、网络设备、安全设备、主机外设配电设备、防雷设备、	人工实地勘察

	温控设备、湿控设备、 电源线路、通讯线路	

评估流程

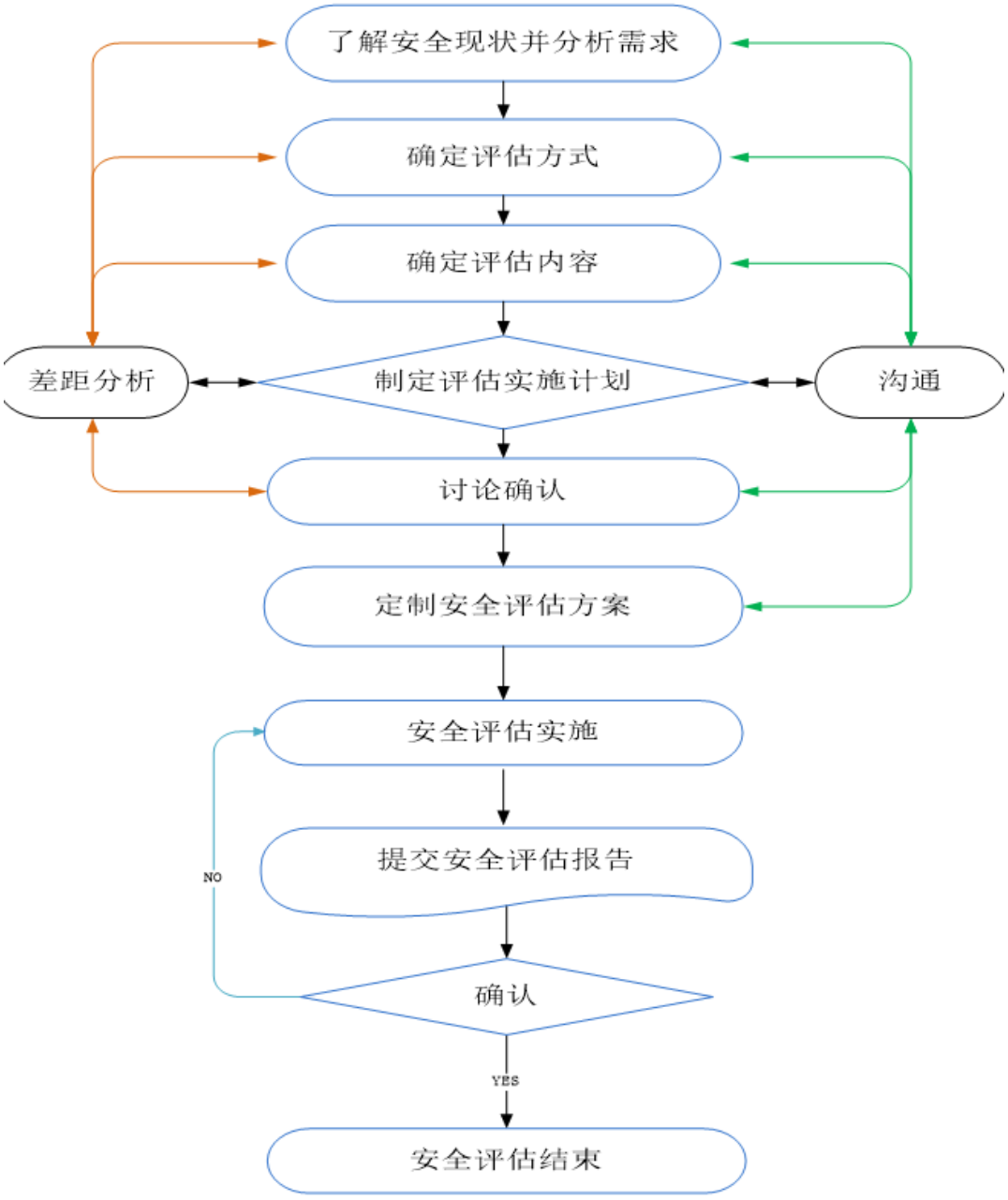

图 4 定期风险评估流程图

了解系统安全现状、分析需求：分析并解决的问题的前提是清晰地发现问题，通过对信息系统的安全状况的了解，和相关负责人员一起分析现阶段系统实际的安全需求，目的是发现并总结系统存在的安全问题；

选择定期风险评估模块：根据发现的首要安全问题，选择最适合当前状况的定期风险评估模块；

编写《评估计划》：根据系统的实际情况，定制适合执行并可以保证效果的定期风险评估计划，计划中应明确包括：定期风险评估的周期、定期风险评估的具体项目、执行过程中相关人员的责任分工、执行过程中的输入和输出及最终的工作成果；

相关负责人确认评估计划：评估计划作为整个项目实施的指导性文档，需要的相关负责人根据实际情况进行确认，予以批准实施；

执行评估计划：为了规避风险、保障系统的高可用性，定期风险评估必须严格按照相关计划进行，以防止计划外操作可能带来的问题；

生成周期性《评估报告》：根据定期风险评估执行的时间周期，在报告中说明本次的检查结果，并与以前历次检查结果进行综合分析，判断安全状况的发展趋势；

判断新的安全需求：企业的安全需求也应根据新的安全形势不断调整，当评估工作进行到一定阶段，对检查计划进行调整，以适应安全形势的需要。