ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 24364—2009

信息安全技术
信息安全风险管理指南

Information security technology—
Guidelines for information security risk management

2009-09-30 发布　　2009-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本指导性技术文件的附录A为资料性附录。

本指导性技术文件由全国信息安全标准化技术委员会提出并归口。

本指导性技术文件起草单位：国家信息中心信息安全研究与服务中心、中国电信股份有限公司北京研究院。

本指导性技术文件主要起草人：吴亚非、张鉴、范红、刘蓓、赵阳。

引　言

一个机构要利用其拥有的资源来完成其使命。在信息时代，信息成为第一战略资源，更是起着至关重要的作用。因此，信息资产的安全是关系到该机构能否完成其使命的大事。资产与风险是天生的一对矛盾，资产价值越高，面临的风险就越大。信息资产有着与传统资产不同的特性，面临着新型风险。信息安全风险管理的目的就是要缓解并平衡这一对矛盾，将风险控制到可接受的程度，保护信息及其相关资产，最终保证机构能够完成其使命。

信息安全风险管理是信息安全保障工作中的一项基础性工作，主要表现在以下几方面：

信息安全风险管理的思想和措施应体现在信息安全保障体系的技术、组织和管理等全方位。由于在信息安全保障体系的技术、组织和管理等方面都存在着相关风险，因此，在信息安全保障体系中，技术、组织、管理中均应引入风险管理的思想，准确地评估风险并合理地处理风险，共同实现信息安全保障的目标。

信息安全风险管理的思想和措施应贯穿于信息系统生命周期的全部过程。信息系统生命周期包括规划、设计、实施、运维和废弃五个阶段。每个阶段都存在着相关风险，同样需要采用信息安全风险管理的思想加以应对，采用风险管理的措施加以控制。

信息安全风险管理的思想和措施是贯彻信息安全等级保护制度的有力支撑。信息安全风险管理依据信息安全等级保护的思想和原则，区分主次，平衡成本与效益，合理部署和利用信息安全的保护机制、信任体系、监控体系和应急处理等重要的基础设施，选择并确定合适的安全控制措施，从而保证机构具有完成其使命所需要的信息安全保障能力。

为落实国家加强信息安全保障工作的要求，为实施信息安全等级保护制度的需要，制定本指导性技术文件。本指导性技术文件可与 GB/T 20984 结合使用，并可作为机构建立信息安全管理体系(ISMS)的参考。

本指导性技术文件参考了 ISO/IEC 27005 等国际信息安全风险管理的相关标准，并经过国家有关行业和地区的试点验证。标准针对信息安全风险管理所涉及的背景建立、风险评估、风险处理、批准监督、监控审查、沟通咨询等不同过程进行了综合性描述，对信息安全风险管理在信息系统生命周期各阶段的应用作了系统阐述。

本指导性技术文件条款中所指的“风险管理”，其含义均为“信息安全风险管理”。

本指导性技术文件中列出的带书名号的文档是示范性的，其格式和详细内容未作规范。

信息安全技术
信息安全风险管理指南

1 范围

本指导性技术文件规定了信息安全风险管理的内容和过程，为信息系统生命周期不同阶段的信息安全风险管理提供指导。

本指导性技术文件适用于指导组织进行信息安全风险管理工作。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求(ISO/IEC 15408-2:2005，IDT)

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则(ISO/IEC 27002:2005，IDT)

3 术语和定义

下列术语和定义适用于本指导性技术文件。

3.1

可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

[GB/T 20984]

3.2

保密性 confidentiality

数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[GB/T 20984]

3.3

信息安全风险 information security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

[GB/T 20984]

3.4

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

[GB/T 20984]

3.5

风险 risk

事态的概率及其结果的组合。

[GB/T 22081]

3.6

风险管理 risk management

识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。

3.7

风险处理 risk treatment

选择并且执行措施来更改风险的过程。

[GB/T 22081]

4 信息安全风险管理概述

4.1 信息安全风险管理的范围和对象

信息安全的概念涵盖了信息、信息载体和信息环境3个方面的安全。信息指信息系统中采集、处理、存储的数据和文件等内容;信息载体指承载信息的媒介,即用于记录、传输、积累和保存信息的实体;信息环境指信息及信息载体所处的环境,包括物理平台、系统平台、网络平台和应用平台等硬环境和软环境。

信息安全风险管理是基于风险的信息安全管理,也就是,始终以风险为主线进行信息安全的管理。从概念上讲,信息安全风险管理应该涉及信息安全上述3个方面(信息、信息载体和信息环境)中包含的所有相关对象。然而对于一个具体的信息系统,信息安全风险管理可能主要涉及该信息系统的关键和敏感部分。因此,根据实际信息系统的不同,信息安全风险管理的侧重点,即风险管理选择的范围和对象重点应有所不同。

4.2 信息安全风险管理的内容和过程

信息安全风险管理包括背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询6个方面的内容。背景建立、风险评估、风险处理和批准监督是信息安全风险管理的4个基本步骤,监控审查和沟通咨询则贯穿于这4个基本步骤中,如图1所示。

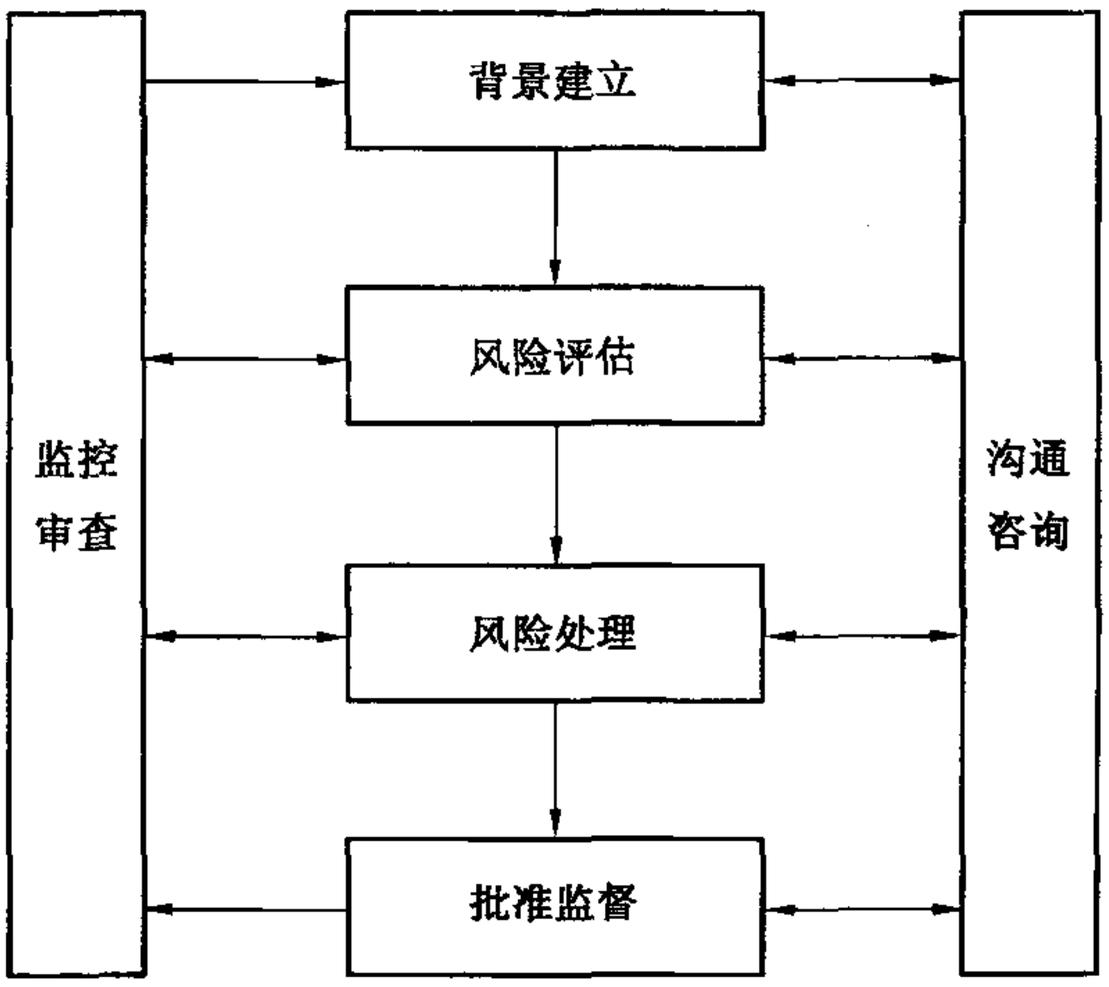

图1 信息安全风险管理的内容和过程

第一步骤是背景建立,确定风险管理的对象和范围,确立实施风险管理的准备,进行相关信息的调

查和分析。第二步骤是风险评估,针对确立的风险管理对象所面临的风险进行识别、分析和评价。第三步骤是风险处理,依据风险评估的结果,选择和实施合适的安全措施。第四步骤是批准监督,机构的决策层依据风险评估和风险处理的结果是否满足信息系统的安全要求,做出是否认可风险管理活动的决定。当受保护系统的业务目标和特性发生变化或面临新的风险时,需要再次进入上述4个步骤,形成新的一次循环。监控审查对上述4个步骤进行监控和审查。监控是监视和控制上述4个步骤的过程有效性和成本有效性;审查是跟踪受保护系统自身或所处环境的变化,以保证上述4个步骤的结果有效性和符合性。沟通咨询为上述4个步骤的相关人员提供沟通和咨询。沟通是为上述过程参与人员提供交流途径,以保持相关人员之间的协调一致,共同实现安全目标。咨询是为上述过程所有相关人员提供学习途径,以提高人员的风险意识和知识,配合实现安全目标。背景建立、风险评估、风险处理、批准监督、监控审查、沟通咨询构成了一个螺旋式上升的循环,使得受保护系统在自身和环境的变化中能够不断应对新的安全需求和风险。

在本指导性技术文件的第5章到第10章,对信息安全风险管理实施过程上述6个步骤的概念、过程、工作内容、输出文档等进行了阐述。

4.3 信息安全风险管理与信息系统生命周期和信息安全目标的关系

4.3.1 信息系统生命周期

信息系统生命周期是某一信息系统从无到有,再到扬弃的整个过程,包括规划、设计、实施、运行维护和废弃5个基本阶段。

在规划阶段,确定信息系统的目的、范围和需求,分析和论证可行性,提出总体方案。在设计阶段,依据总体方案,设计信息系统的实现结构(包括功能划分、接口协议和性能指标等)和实施方案(包括实现技术、设备选型和系统集成等)。在实施阶段,按照实施方案,购买和检测设备,开发定制功能,集成、部署、配置和测试系统,培训人员等。在运行维护阶段,运行和维护系统保证信息系统在自身和所处环境的变化中始终能够正常工作和不断升级。在废弃阶段,对信息系统的整体或信息系统过时或无用部分进行报废处理。当信息系统的业务目标和需求发生变化时,或技术和管理环境发生变化时,需要再次进入上述5个阶段,形成新的一次循环。因此,规划、设计、实施、运行维护和废弃构成了一个螺旋式上升的循环,使得信息系统不断适应自身和环境的变化。

4.3.2 信息安全目标

信息安全目标就是要实现信息系统的基本安全特性(即信息安全基本属性),并达到所需的保障级别。信息安全基本属性包括保密性、完整性、可用性、真实性和抗抵赖性等,每一属性都有相应的保障级别作为其强度的度量,如图2所示。

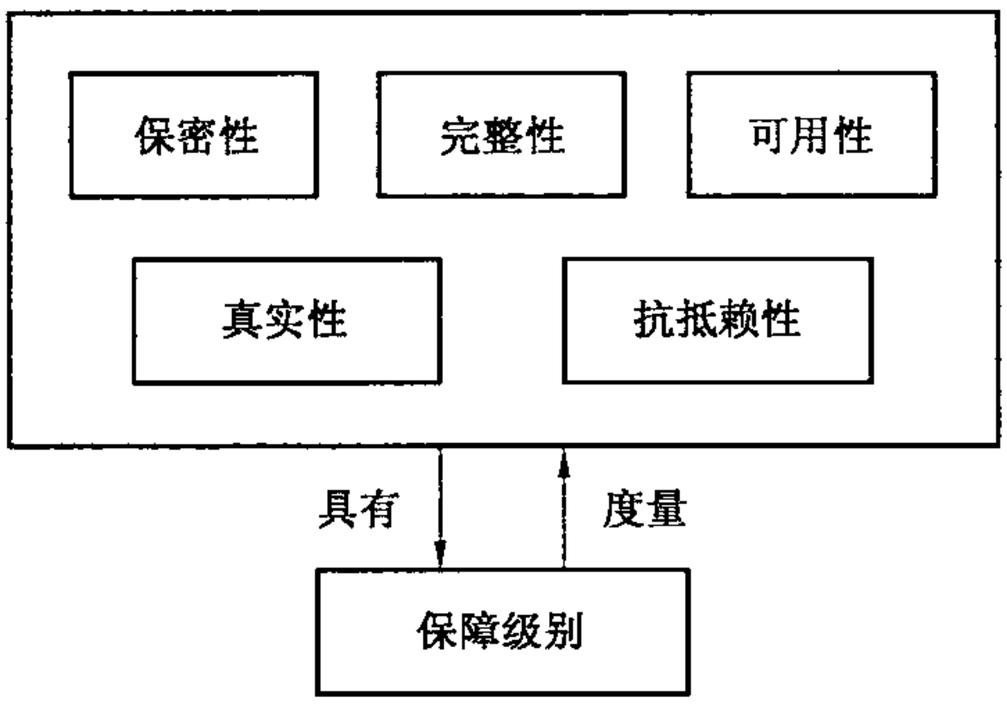

图2 信息安全基本属性及其保障级别

保密性指信息与信息系统不被非授权者所获取或利用的特性,包括数据保密和访问控制等方面。完整性指信息与信息系统真实、准确和完备,不被冒充、伪造和篡改的特性,包括身份真实、数据完整和系统完整等方面。可用性指信息与信息系统可被授权者在需要的时候访问和使用的特性。真实性指确保主体或资源的身份正是所声称的特性。抗抵赖性指一个实体不能够否认其行为的特性,可以支持责

任追究、威慑作用和法律行动等。保障级别指保密性、完整性、可用性、真实性和抗抵赖性在具体实现中达到的级别或强度，可以作为安全信任度的尺度。信息系统的安全保障级别主要是通过对信息系统进行安全测评和认证来确定的。

4.3.3 三者关系

信息安全风险管理与信息系统生命周期和信息安全目标之间的关系可简要表述为，信息系统生命周期的每个阶段，为了达到其信息安全目标，都需要相应的信息安全风险管理手段作为支持。

信息系统生命周期各阶段的特性及其信息安全目标的保障级别随行业特点和系统特性的不同而不同，也就是说，不同行业下的不同系统在信息系统生命周期的不同阶段，对信息安全基本属性（即保密性、完整性、可用性、真实性和抗抵赖性）的要求和侧重不同。因此，可在本指导性技术文件指导下开发行业的信息安全风险管理规范。对于信息安全目标的保障级别应遵循国家信息安全等级保护制度的要求，具体可参照 GB 17859—1999。

在本指导性技术文件的第 11 章到第 15 章，对信息系统生命周期各个阶段的安全需求和目标，以及相应的信息安全风险管理主要过程和活动进行了阐述。

4.4 信息安全风险管理相关人员的角色和责任

信息安全风险管理是基于风险的信息系统安全管理。因此，信息安全风险管理涉及人员，既包括信息安全风险管理的直接参与人员，也包括信息系统的相关人员。表 1 对信息安全风险管理相关人员的角色和责任进行了归纳和分类。

表 1 信息安全风险管理相关人员的角色和责任

层面	信息系统			信息安全风险管理		
	角色	内外部	责任	角色	内外部	责任
决策层	决策人员	内	负责信息系统的重大决策和总体规范	决策人员	内	负责信息安全风险管理的重大决策、总体规划和批准监督
管理层	管理人员	内	负责信息系统各方面的管理、组织和协调	管理人员	内	负责信息安全风险管理各过程中的管理、组织和协调
执行层	规划设计人员	内或外	负责信息系统的规划和设计	执行人员	内或外	负责信息安全风险管理的具体规划、设计和实施
	建设人员	内或外	负责信息系统的建设和实施			
	运行人员	内	负责信息系统的日常运行和操作			
	维护人员	内或外	负责信息系统的日常维护，包括维修和升级			
	监控人员	内	负责信息系统的监视和控制	监控人员	内	负责信息安全风险管理过程、成本和结果的监视和控制
支持层	支持人员	外	为信息系统提供专业技术支持，包括咨询、培训、测评和工具定制等服务	支持人员	外	为信息安全风险管理提供专业技术支持，包括咨询、培训、测评和工具定制等服务
用户层	使用人员	内或外	利用信息系统完成自身的任务	使用人员	内或外	遵循信息安全风险管理的原则和过程使用信息系统，并反馈信息安全风险管理的效果

5 背景建立

5.1 背景建立概述

5.1.1 背景建立的概念

背景建立是信息安全风险管理的第一步骤，确定风险管理的对象和范围，确立实施风险管理的准备，进行相关信息的调查和分析。

5.1.2 背景建立的目的

背景建立是为了明确信息安全风险管理的范围和对象，以及对象的特性和安全要求，对信息安全风险管理项目进行规划和准备，保障后续的风险管理活动顺利进行。

5.1.3 背景建立的依据

国家、地区或行业的相关政策、法律、法规和标准以及信息系统的业务目标和特性都是背景建立的必要依据。

5.2 背景建立过程

背景建立的过程包括风险管理准备、信息系统调查、信息系统分析和信息安全分析4个阶段。在信息安全风险管理过程中，背景建立过程是一次信息安全风险管理主循环的起始，为风险评估提供输入，监控审查和沟通咨询贯穿其4个阶段，如图3所示。

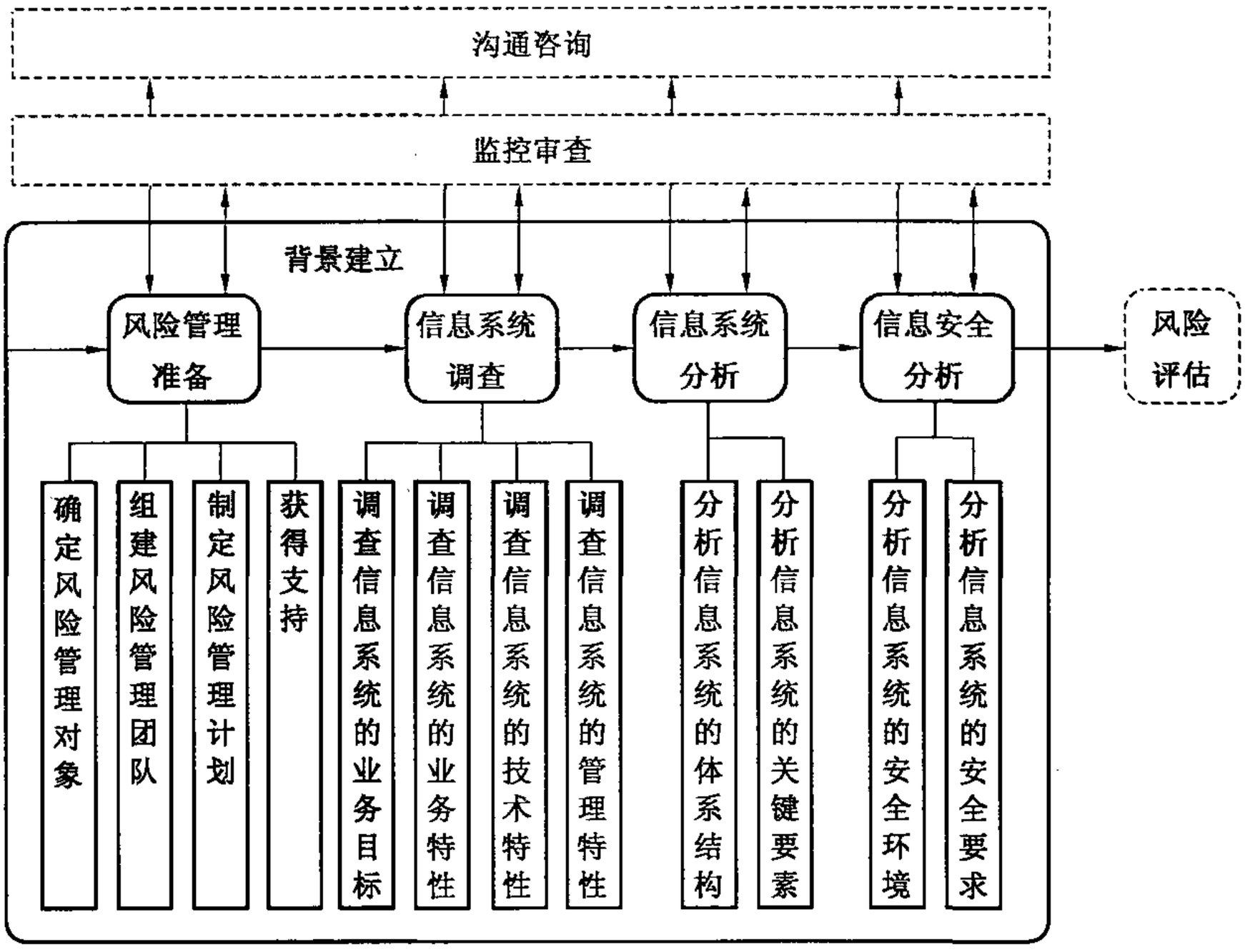

图3 背景建立过程及其在信息安全风险管理中的位置

5.2.1 风险管理准备

如图4所示，风险管理准备阶段的工作过程和内容如下：

a) 确定风险管理对象。依据机构的使命，并遵循国家、地区或行业的相关政策、法律、法规和标准的规定，确定将要实施风险管理的对象。

b) 组建风险管理团队。组建风险管理团队，确定团队成员、组织结构、角色、责任等内容。

c) 制定风险管理计划。制定风险管理的实施计划，包括风险管理的目的、意义、范围、目标、组织结构、实施方案、经费预算和进度安排等，形成风险管理计划书。

d) 获得支持。上述所有内容确定后，风险管理计划书应得到组织最高管理者的支持和批准；由决策层对管理层和执行层进行传达，在组织范围就风险管理相关内容进行培训，以明确有关人员在风险管理中的任务。

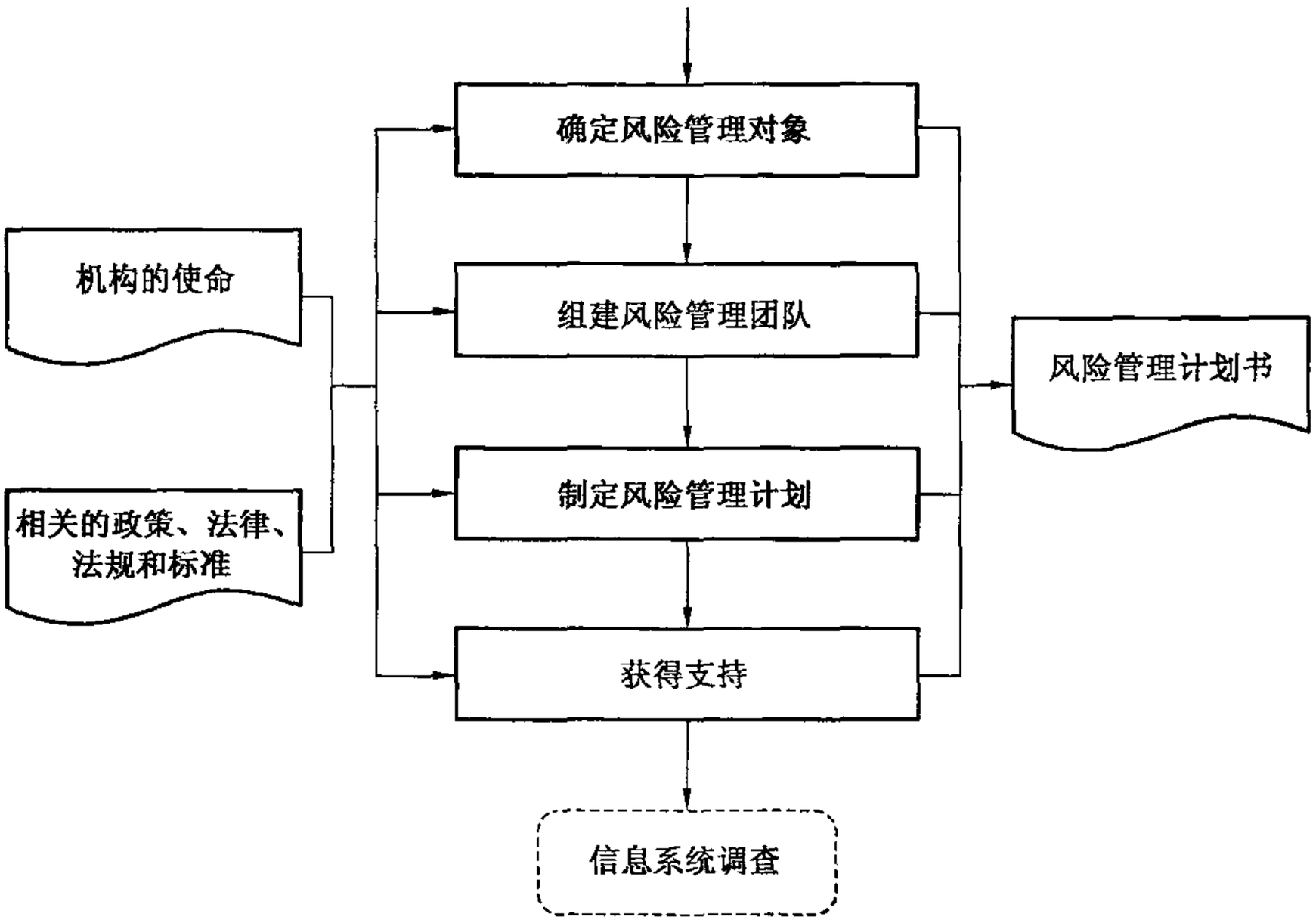

图 4 风险管理准备阶段的过程及其输入输出

5.2.2 信息系统调查

如图 5 所示，信息系统调查阶段的工作过程和内容如下：

a) 调查信息系统的业务目标。了解机构的使命，包括战略背景和战略目标等，从中明确支持机构完成其使命的信息系统的业务目标。

b) 调查信息系统的业务特性。了解机构的业务，包括业务内容和业务流程等，从中明确支持机构业务运营的信息系统的业务特性。

c) 调查信息系统的管理特性。了解机构的组织结构和管理制度，包括岗位设置、责任分配、规章制度、操作规程和人事管理等，从中明确支持机构业务运营的信息系统的管理特性。

d) 调查信息系统的技术特性。了解信息系统的技术平台，包括物理平台、系统平台、通信平台、网络平台和应用平台，从中明确支持业务运营的信息系统的技术特性。

e) 汇总上述调查结果，形成信息系统的描述报告，其中包含信息系统的业务目标、业务特性、管理特性和技术特性等方面的内容。

信息系统的调查方式包括问卷回答、人员访谈、现场考察、辅助工具等多种形式，可以根据实际情况灵活采用和结合使用。

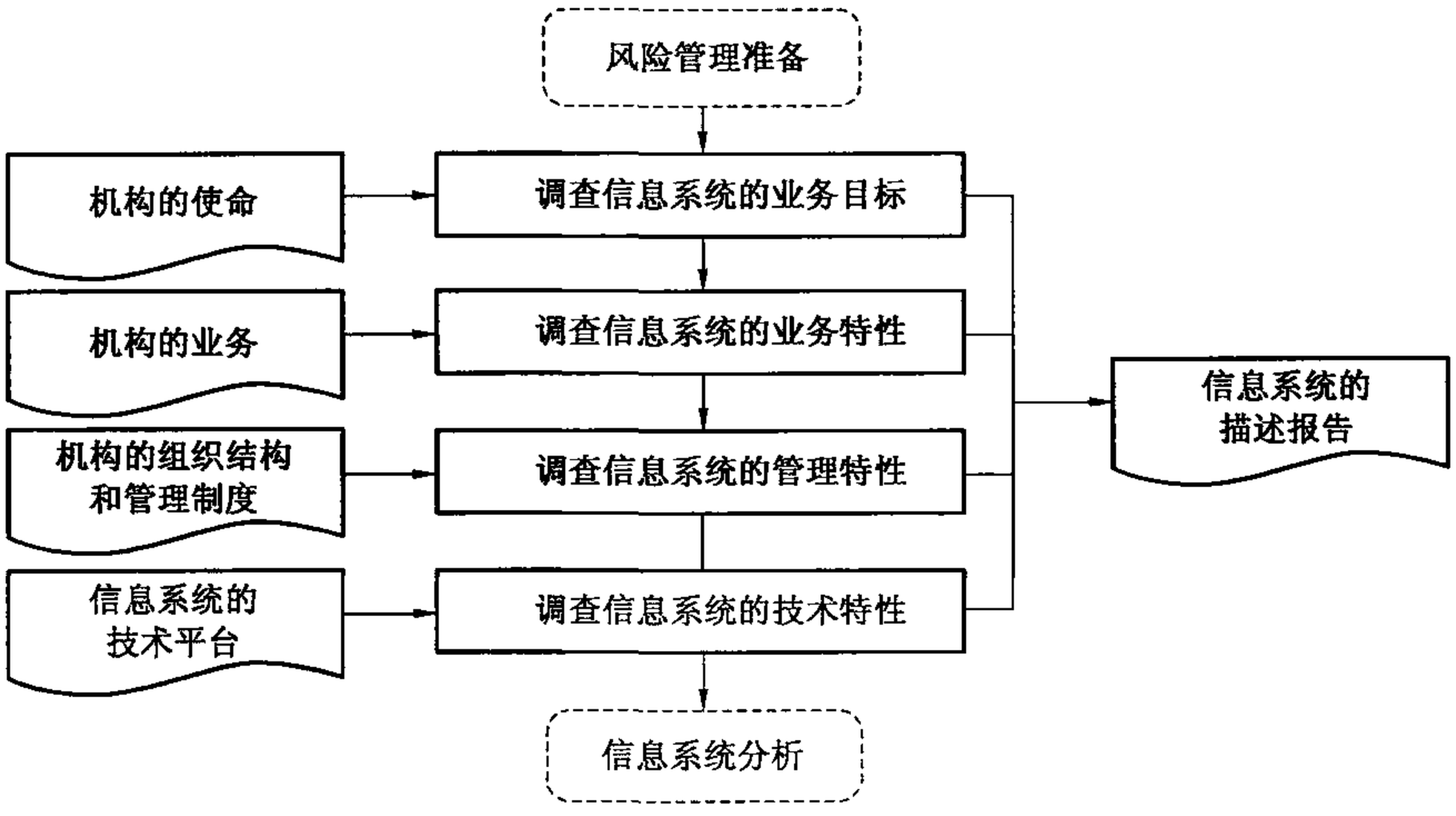

图 5　信息系统调查阶段的过程及其输入输出

5.2.3　信息系统分析

如图 6 所示，信息系统分析阶段的工作过程和内容如下：

a)　分析信息系统的体系结构。依据信息系统的描述报告，对信息系统的功能体系、数据体系、网络体系、运营体系和管理体系等方面进行分析，明确它们的内部结构和外部关系。

b)　分析信息系统的关键要素。依据信息系统的描述报告和上述体系结构的分析结果，找出信息系统中对机构使命具有关键和重要作用的部分，列出清单。

c)　汇总上述分析结果，形成信息系统的分析报告，其中包含信息系统的体系结构和关键要素等方面的内容。

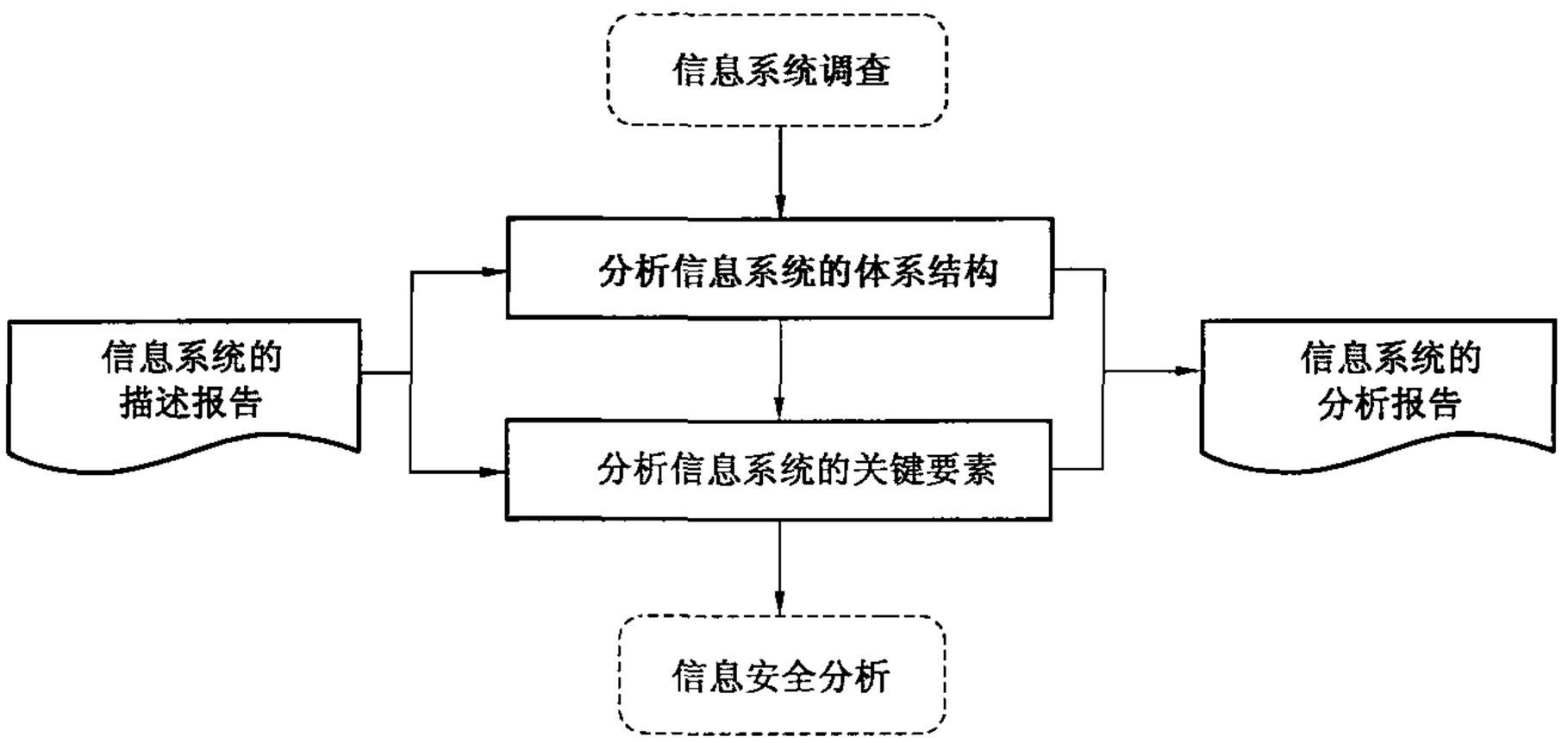

图 6　信息系统分析阶段的过程及其输入输出

5.2.4　信息安全分析

如图 7 所示，信息安全分析阶段的工作过程和内容如下：

a)　分析信息系统的安全环境。依据国家、地区或行业的相关政策、法律、法规和标准，考虑合作伙伴的合同要求，对信息系统的安全保障环境进行分析，明确环境因素对信息系统安全方面的影响和要求。

b)　分析信息系统的安全要求。依据信息系统的描述报告和信息系统的分析报告，结合上述安全

环境的分析结果，分析和提出对信息系统的安全要求，包括保护范围和保护等级等。

c) 汇总上述分析结果，形成信息系统的安全要求报告，其中包含信息系统的安全环境和安全要求等方面的内容。

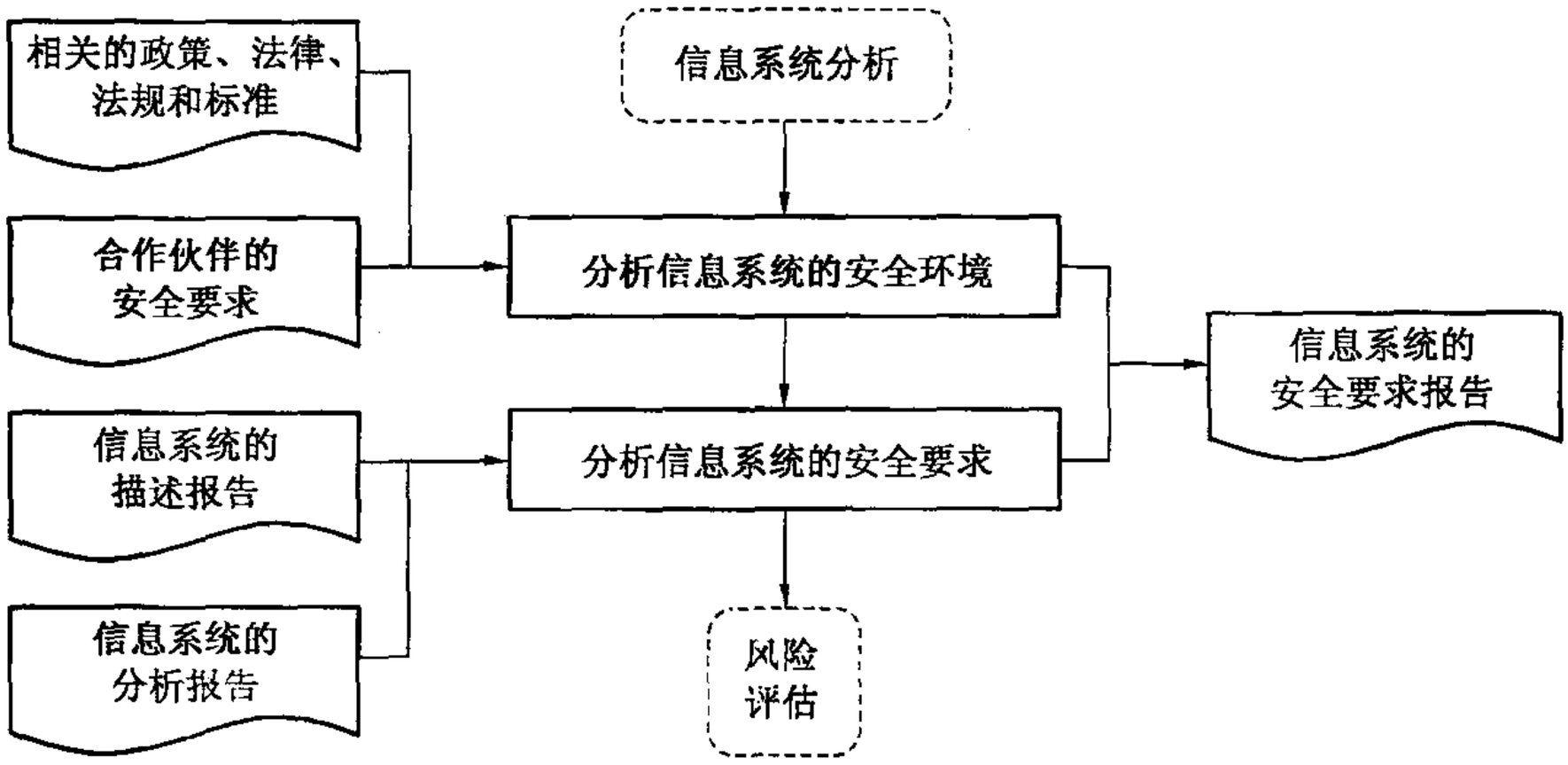

图 7 信息安全分析阶段的过程及其输入输出

5.3 背景建立文档

表 2 列出了背景建立过程的输出文档及其内容。输出文档的数量、名称和主要内容可以根据机构具体情况进行增加、删减或修改，但应涵盖表 2 中文档内容部分规定的内容。

表 2 背景建立过程的输出文档及其内容

阶 段	输出文档	文 档 内 容
风险管理准备	风险管理计划书	风险管理的目的、意义、范围、目标、组织结构、经费预算和进度安排等
信息系统调查	信息系统的描述报告	信息系统的业务目标、业务特性、管理特性和技术特性等
信息系统分析	信息系统的分析报告	信息系统的体系结构和关键要素等
信息安全分析	信息系统的安全要求报告	信息系统的安全环境和安全要求等

6 风险评估

6.1 风险评估概述

6.1.1 风险评估的概念

风险评估是信息安全风险管理的第二步骤，针对确立的风险管理对象所面临的风险进行识别、分析和评价。

本章仅对风险评估作框架性说明，详细内容可见 GB/T 20984。

6.1.2 风险评估的目的

信息安全风险管理要依靠风险评估的结果来确定随后的风险处理和批准监督活动。风险评估使得机构能够准确定位风险管理的策略、实践和工具，能够将安全活动的重点放在重要的问题上，能够选择成本效益合理的和适用的安全对策。基于风险评估的风险管理方法被实践证明是有效的和实用的，已

被广泛应用于各个领域。

6.1.3 风险评估的作用范围

风险评估只是为信息安全活动提供一个方向，并不会导致重大的信息安全改进。不管评估方法有多详细和多专业，也只能描述风险状态，而不会改进机构的安全状态。机构只有利用评估结果持续地进行改进活动，实现风险有效管理，才能使机构的安全状态得到改善。

6.2 风险评估过程

风险评估的过程包括风险评估准备、风险要素识别、风险分析和风险结果判定4个阶段。在信息安全风险管理过程中，接受背景建立的输出，为风险处理提供输入，监控审查和沟通咨询贯穿其4个阶段，如图8所示。

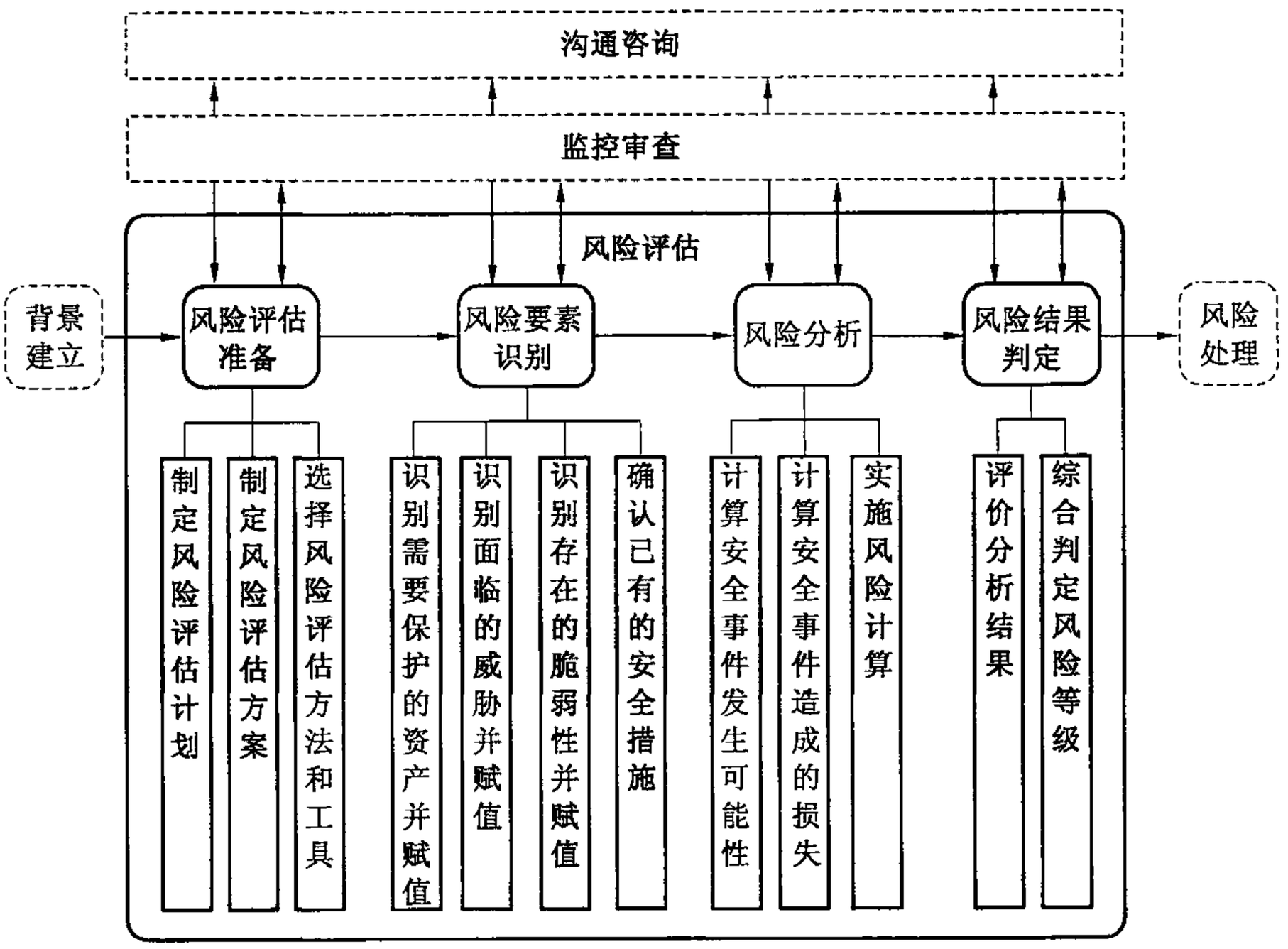

图8 风险评估过程及其在信息安全风险管理中的位置

6.2.1 风险评估准备

如图9所示，风险评估准备阶段的工作过程和内容如下：

a) 制定风险评估计划。依据背景建立输出的文档，制定风险评估的实施计划，包括风险评估的目的、意义、范围、目标、组织结构、经费预算和进度安排等，形成风险评估计划书。风险评估计划书需要得到信息系统和信息安全风险管理决策层的认可和批准。

b) 制定风险评估方案。依据背景建立输出的文档，确定风险评估的实施方案，包括风险评估的工作过程、输入数据和输出结果等，形成风险评估方案。风险评估方案需要得到信息系统和信息安全风险管理管理层的认可和批准。

c) 选择风险评估方法和工具。依据背景建立输出的文档以及风险评估计划和风险评估方案，从现有风险评估方法和工具库中选择合适的风险评估方法和工具，形成入选风险评估方法和工具列表。

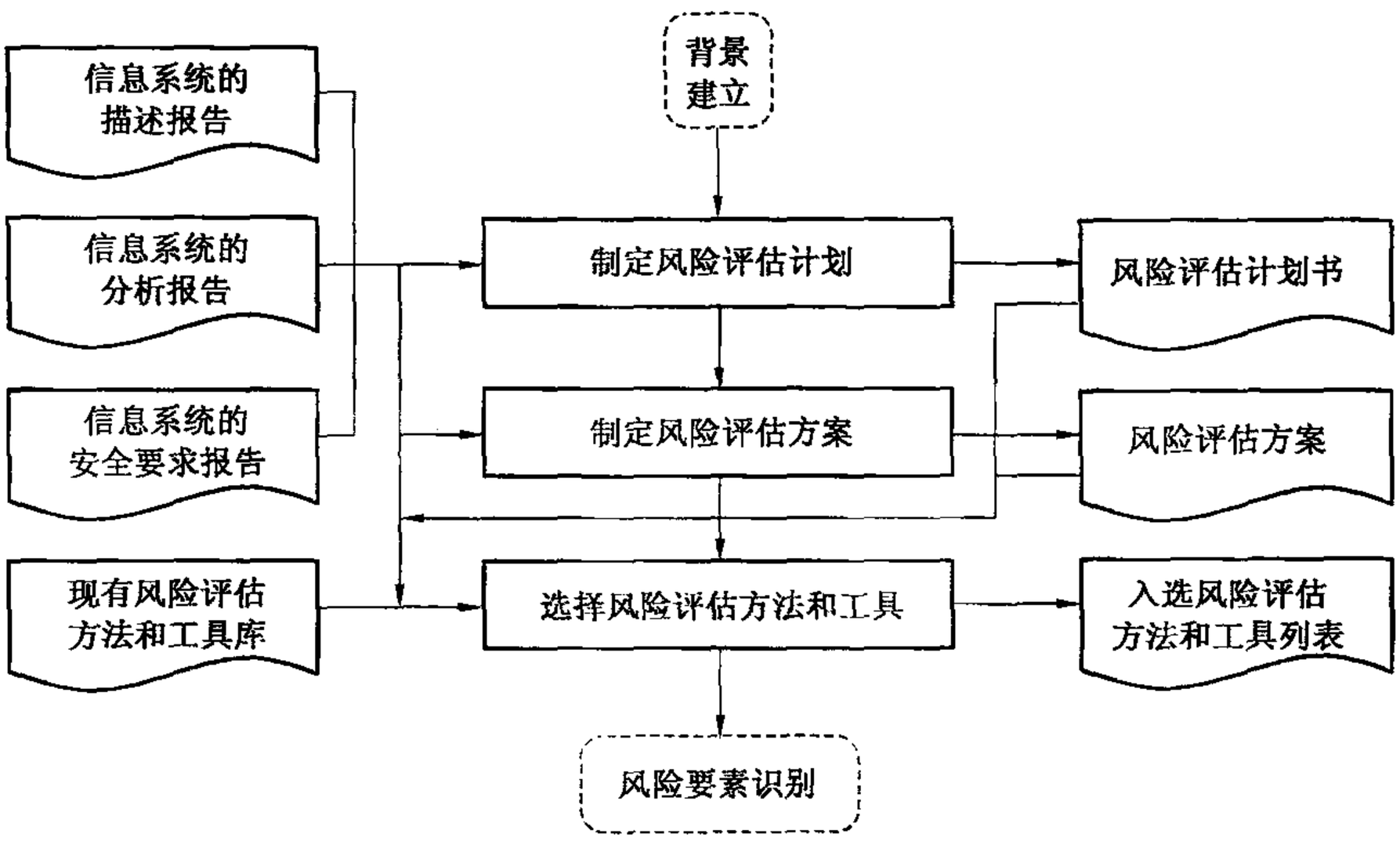

图 9　风险评估准备阶段的过程及其输入输出

6.2.2　风险要素识别

如图 10 所示，风险要素识别阶段的工作过程和内容如下：

a) 识别需要保护的资产并赋值。依据背景建立输出的文档，选择适当的资产识别方法，识别对机构使命具有关键和重要作用的需要保护的资产，并确定资产的重要性级别，形成需要保护的资产清单。

b) 识别面临的威胁并赋值。依据背景建立输出的文档，参照威胁库，选择适当的威胁识别方法，识别机构的信息资产面临的威胁，并确定威胁的属性等级，可参考的威胁属性包括威胁发生频度、威胁能力程度等，形成面临的威胁列表。威胁库是有关威胁的外部共享数据和内部历史数据的汇集。

c) 识别存在的脆弱性并赋值。依据背景建立输出的文档，参照漏洞库，选择适当的脆弱性识别方法，识别机构的信息资产存在的脆弱性，并确定脆弱性的属性等级，可参考的脆弱性属性包括脆弱性被利用程度、脆弱性严重程度等，形成存在的脆弱性列表。漏洞库是有关脆弱性/漏洞的外部共享数据和内部历史数据的汇集。

d) 确认已有的安全措施。依据背景建立输出的文档，即信息系统的描述报告、信息系统的分析报告和信息系统的安全要求报告，确认已有的安全措施，包括技术层面（即物理平台、系统平台、网络平台和应用平台）的安全功能、组织层面（即结构、岗位和人员）的安全控制和管理层面（即策略、规章和制度）的安全对策，形成已有安全措施列表。

风险要素的识别方式包括文档审查、人员访谈、现场考察、辅助工具等多种形式，可以根据实际情况灵活采用和结合使用。

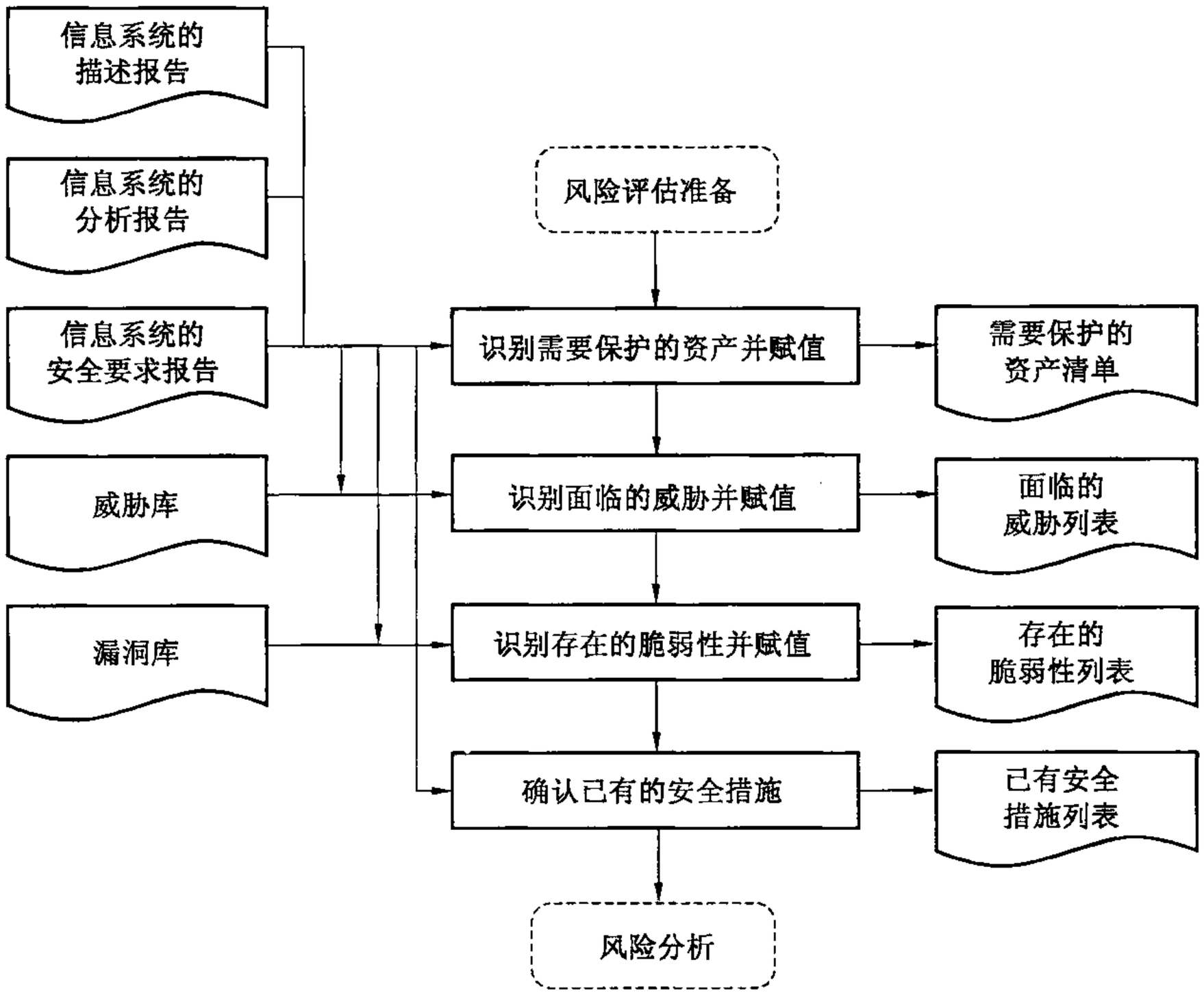

图 10　风险要素识别阶段的过程及其输入输出

6.2.3　风险分析

如图 11 所示，风险程度分析阶段的工作过程和内容如下：

a)　分析安全事件发生的可能性。依据面临的威胁列表和存在的脆弱性列表，根据威胁属性（威胁发生频率、威胁能力程度等）及脆弱性属性（脆弱性被利用程度等），计算威胁利用脆弱性导致安全事件发生的可能性。

b)　分析安全事件造成的损失。依据存在的脆弱性列表和需要保护的资产列表，根据资产属性（资产重要性程度等）及脆弱性属性（脆弱性严重程度等），计算安全事件一旦发生后造成的损失。

c)　实施风险计算。根据计算出的安全事件的可能性以及安全事件造成的损失，评估者可根据自身情况选择相应的风险计算方法实施风险计算，形成风险计算报告。风险评估算法库是各种风险评估算法的汇集，包括公认算法和自创算法。

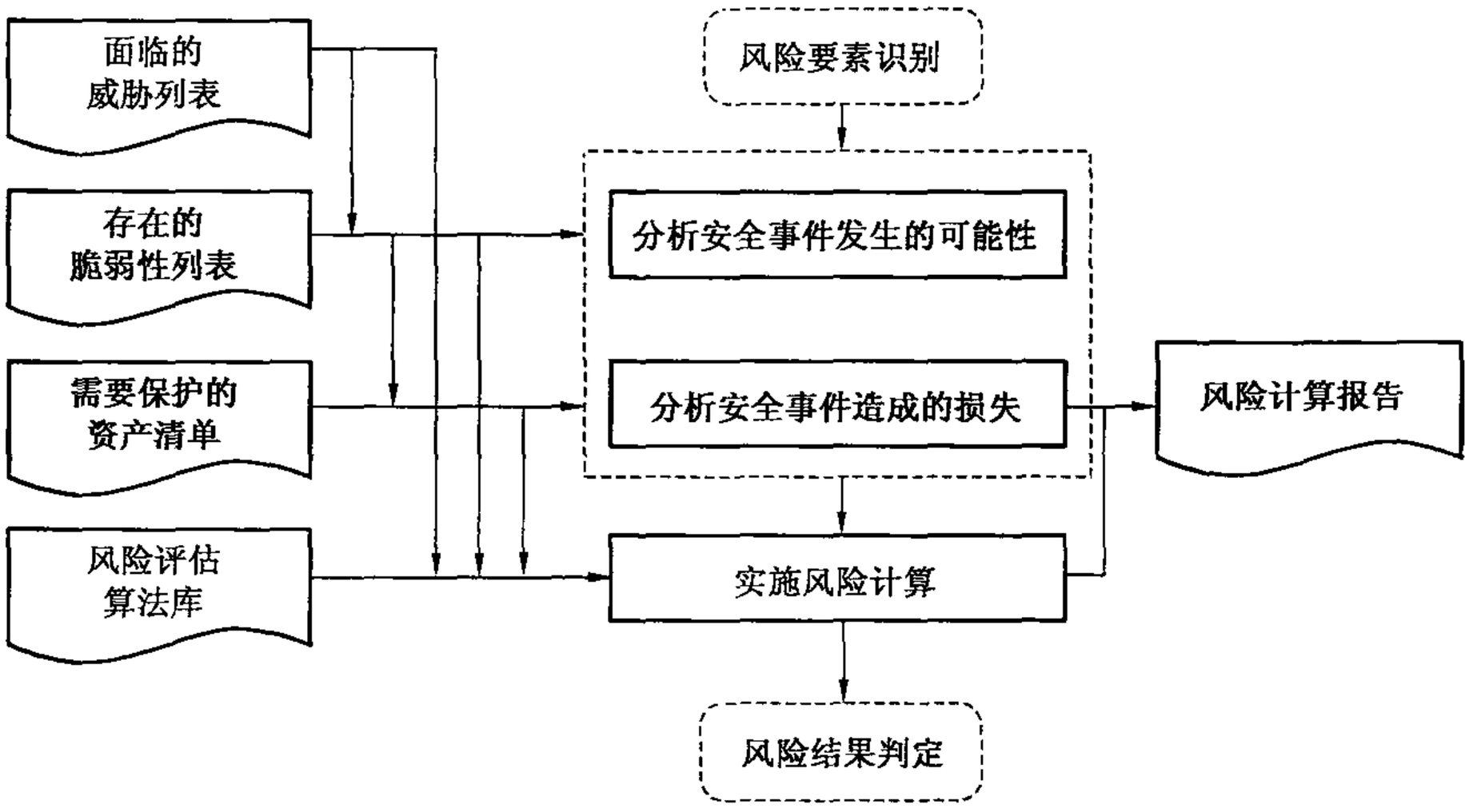

图 11　风险分析阶段的过程及其输入输出

6.2.4　风险结果判定

如图 12 所示，风险结果判定阶段的工作过程和内容如下：

a)　评价风险的等级。依据风险计算报告，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理，形成风险程度等级列表。

b)　综合评价风险状况。汇总各项输出文档和风险程度等级列表，综合评价风险状况，形成风险评估报告。

评价等级级数可以根据评价对象的特性和实际评估的需要而定，如〈高、中、低〉3 级，〈很高、较高、中等、较低、很低〉5 级等。

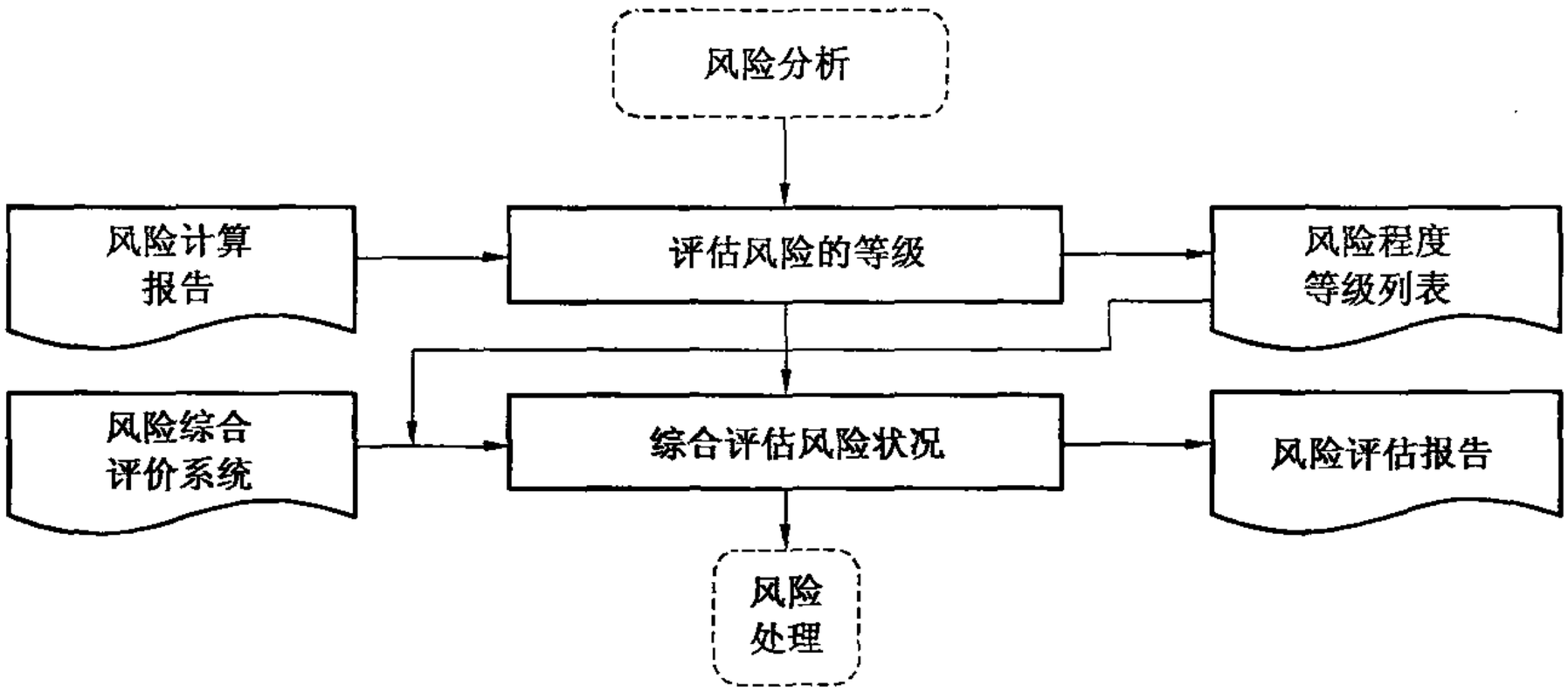

图 12　风险结果判定阶段的过程及其输入输出

6.3　风险评估文档

表 3 列出了风险评估过程的输出文档及其内容。输出文档的数量、名称和主要内容可以根据机构具体情况进行增加、删减或修改，但应涵盖表 3 中文档内容部分规定的内容。

表 3　风险评估过程的输出文档及其内容

阶　段	输出文档	文 档 内 容
风险评估准备	风险评估计划书	风险评估的目的、意义、范围、目标、组织结构、经费预算和进度安排等
	风险评估方案	风险评估的工作过程、输入数据和输出结果等
	入选风险评估方法和工具列表	合适的风险评估方法和工具列表
风险要素识别	需要保护的资产清单	对机构使命具有关键和重要作用的需要保护的资产清单，包括资产名称、描述、类型、重要程度、责任人/部门等
	面临的威胁列表	机构的信息资产面临的威胁列表，包括威胁名称、种类、来源、动机及威胁属性赋值
	存在的脆弱性列表	机构的信息资产存在的脆弱性列表以及脆弱性属性赋值
	已有安全措施列表	确认已有的安全措施，包括技术层面、组织层面和管理层面的安全对策
风险分析	风险计算报告	综合安全事件所作用的资产、威胁、脆弱性及其相应属性，进行风险计算，判断安全事件造成的损失对组织的影响，即安全风险值
风险结果判定	风险程度等级列表	风险程度的等级列表
	风险评估报告	对整个风险评估过程和结果进行总结，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险等级和结论等内容

7　风险处理

7.1　风险处理概述

7.1.1　风险处理的概念

风险处理是信息安全风险管理的第 3 步骤，依据风险评估的结果，选择和实施合适的安全措施。附录 A 中列出了常用的风险处理参考模型以及相应的处理措施。

7.1.2　风险处理的目的

风险处理是为了将风险始终控制在可接受的范围内。

7.1.3　风险处理的方式

风险处理方式主要有如下规避、转移、降低和接受 4 种方式。

a)　规避方式：通过不使用面临风险的资产来避免风险。比如，在没有足够安全保障的信息系统中，不处理特别敏感的信息，从而防止敏感信息的泄漏。再如，对于只处理内部业务的信息系统，不使用互联网，从而避免外部的有害入侵和不良攻击。

b)　转移方式：通过将面临风险的资产或其价值转移到更安全的地方来避免或降低风险。比如，在本机构不具备足够的安全保障的技术能力时，将信息系统的技术体系（即信息载体部分）外包给满足安全保障要求的第三方机构，从而避免技术风险。再如，通过给昂贵的设备上保险，将设备损失的风险转移给保险公司，从而降低资产价值的损失。

c)　降低方式：通过对面临风险的资产采取保护措施来降低风险。保护措施可以从构成风险的 5 个方面（即威胁源、威胁行为、脆弱性、资产和影响）来降低风险。比如，采用法律的手段制裁计算机犯罪（包括窃取机密信息，攻击关键的信息系统基础设施，传播病毒、不健康信息和垃圾邮件等），发挥法律的威慑作用，从而有效遏制威胁源的动机；采取身份认证措施，从而抵制身份假冒这种威胁行为的能力；及时给系统打补丁（特别是针对安全漏洞的补丁），关闭无用的网

络服务端口，从而减少系统的脆弱性，降低被利用的可能性；采用各种防护措施，建立资产的安全域，从而保证资产不受侵犯，其价值得到保持；采取容灾备份、应急响应和业务连续计划等措施，从而减少安全事件造成的影响程度。

d) 接受方式：接受风险是选择对风险不采取进一步的处理措施，接受风险可能带来的结果。采取不对风险进行处理的前提是：确定了信息系统的风险等级，评估了风险发生的可能性以及带来的潜在破坏，分析了使用每种处理措施的可行性，并进行了较全面的成本效益分析，认定某些功能、服务、信息或资产不需要进一步保护。

7.2 风险处理过程

风险处理的过程包括现存风险判断、处理目标确立、处理措施选择和处理措施实施4个阶段。在信息安全风险管理过程中，接受风险评估的输出，为批准监督提供输入，监控审查和沟通咨询贯穿其四个阶段，如图13所示。

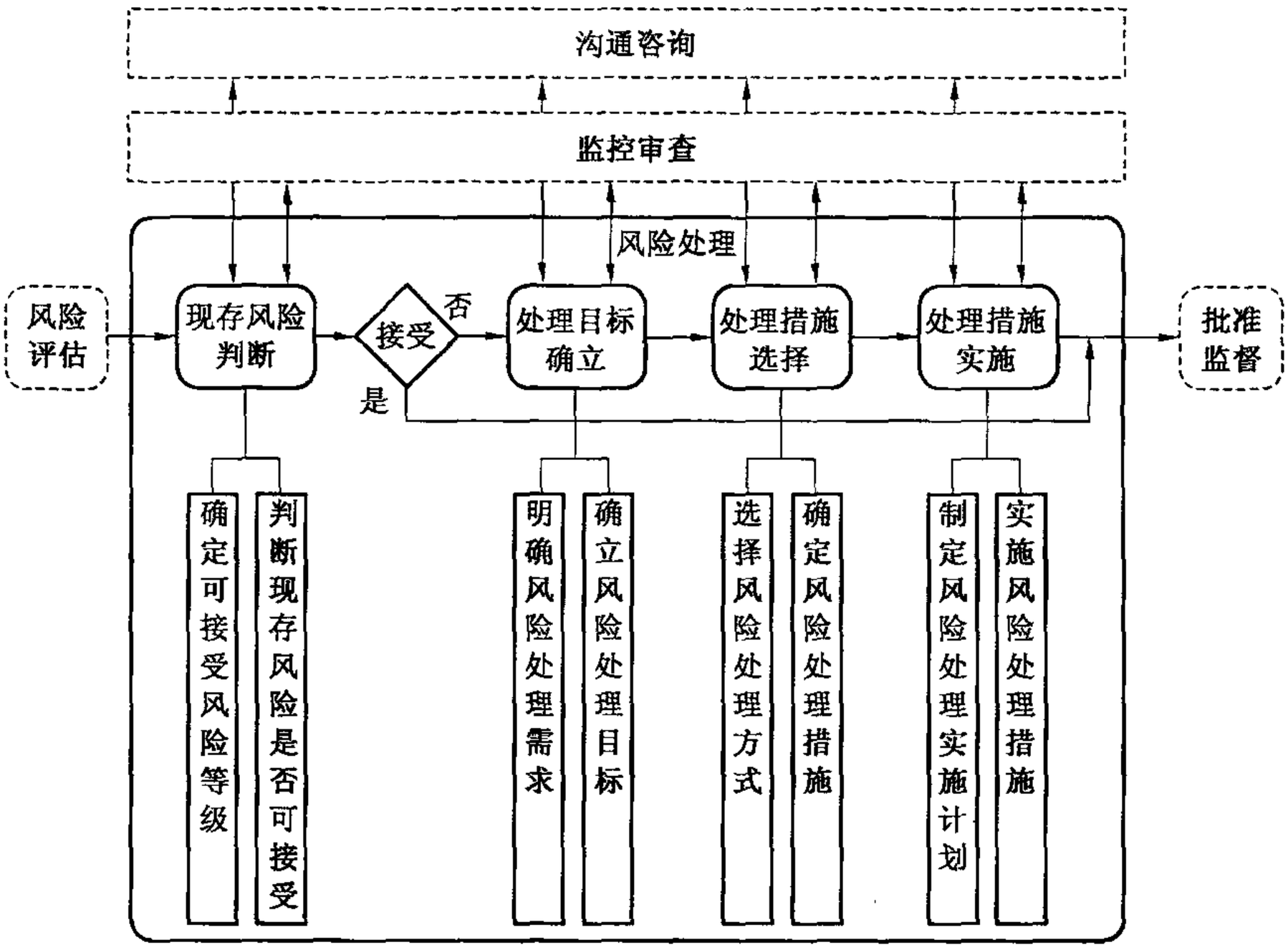

图13 风险处理过程及其在信息安全风险管理中的位置

7.2.1 现存风险判断

如图14所示，现存风险判断阶段的工作过程和内容如下：

a) 确定可接受风险等级。依据信息系统的描述报告、信息系统的分析报告、信息系统的安全要求报告和风险评估报告，确定可接受风险的等级，即把风险评估得出的风险等级划分为可接受和不可接受两种，形成风险接受等级划分表。

b) 判断现存风险是否可接受。依据风险评估报告和风险接受等级划分表，判断现存风险是否可接受，形成现存风险接受判断书。如果判断结果是可接受，则跳出风险处理过程，进入信息安全风险管理的批准监督；否则继续风险处理过程，进入处理目标确立阶段。现存风险接受判断书需要得到信息系统和信息安全风险管理决策层和管理层的认可和批准。

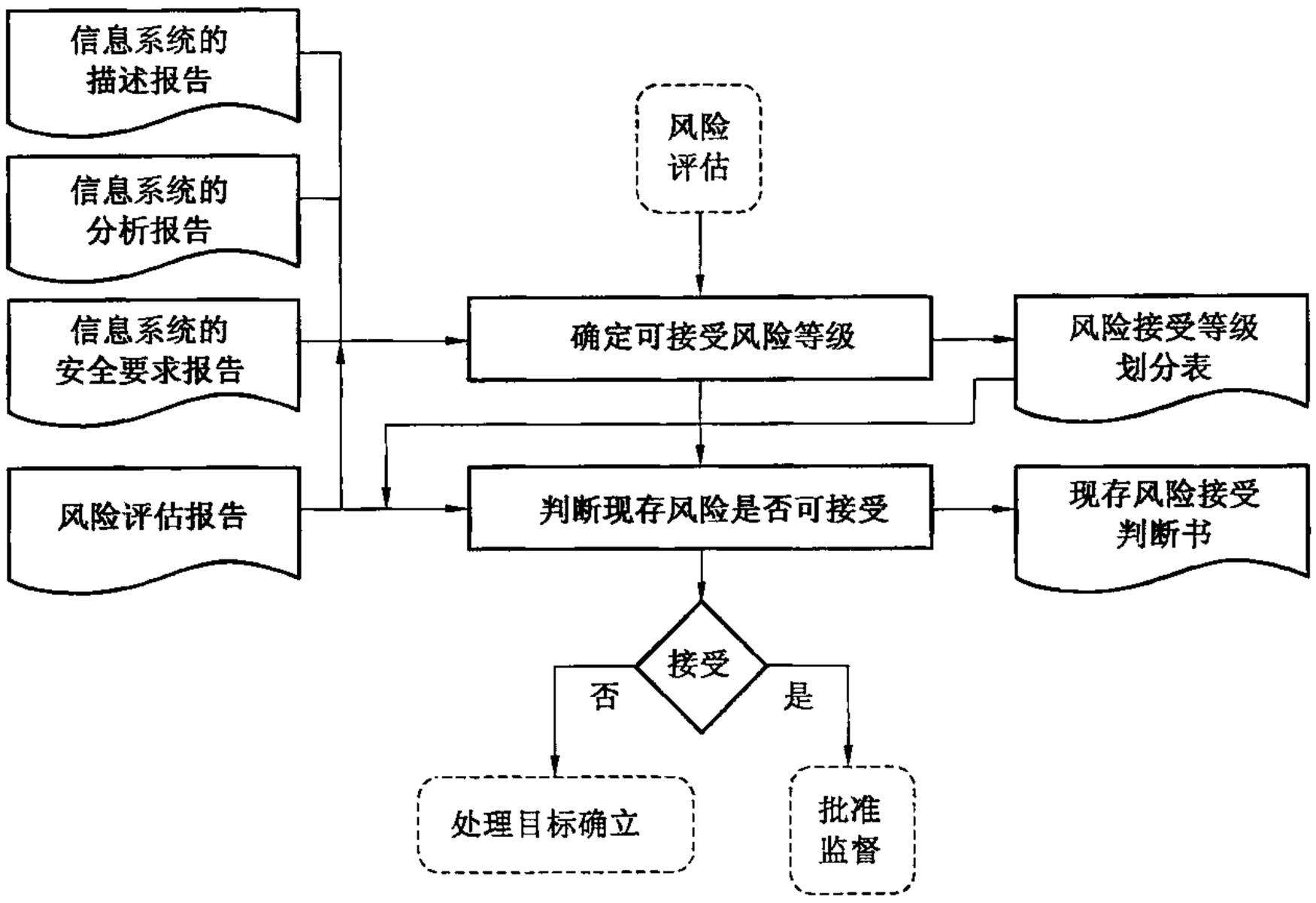

图 14　现存风险判断阶段的过程及其输入输出

7.2.2　处理目标确立

如图 15 所示，处理目标确立阶段的工作过程和内容如下：

a)　分析风险处理需求。依据信息系统的描述报告、信息系统的分析报告、信息系统的安全要求报告、风险评估报告和风险接受等级划分表，从技术层面（即物理平台、系统平台、通信平台、网络平台和应用平台）、组织层面（即结构、岗位和人员）和管理层面（即策略、规章和制度），分析风险处理的需求，形成风险处理需求分析报告；

b)　确立风险处理目标。依据风险接受等级划分表和风险处理需求分析报告，确立风险处理的目标，包括处理对象及其最低保护等级，形成风险处理目标列表。风险处理目标列表需要得到信息系统和信息安全风险管理管理层的认可和批准。

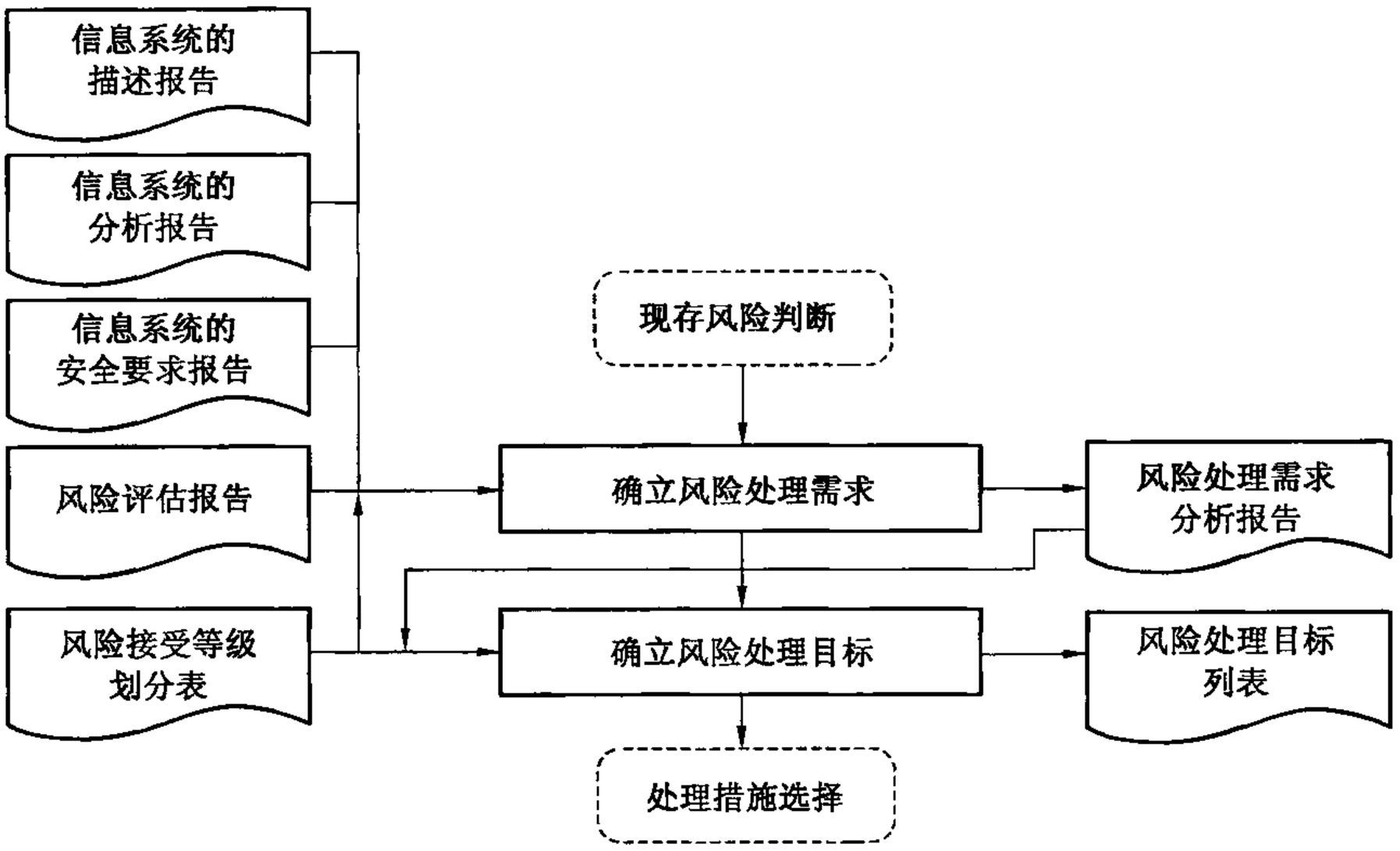

图 15　处理目标确立阶段的过程及其输入输出

7.2.3 处理措施选择

如图 16 所示，处理措施选择阶段的工作过程和内容如下：

a) 选择风险处理方式。依据信息系统的安全要求报告、风险处理需求分析报告和风险处理目标列表，选择合适的风险处理方式(包括接受方式、规避方式、转移方式和降低方式)，并说明选择的理由以及被选处理方式的使用方法和注意事项等，形成入选风险处理方式说明报告。

b) 选择风险处理措施。依据风险处理目标列表和入选风险处理方式说明报告，充分分析和平衡成本效益，选择合适的风险处理措施，并说明选择的理由以及被选处理措施的成本、使用方法和注意事项等，形成入选风险处理措施说明报告。风险处理措施说明报告需要得到信息系统和信息安全风险管理管理层的认可和批准。

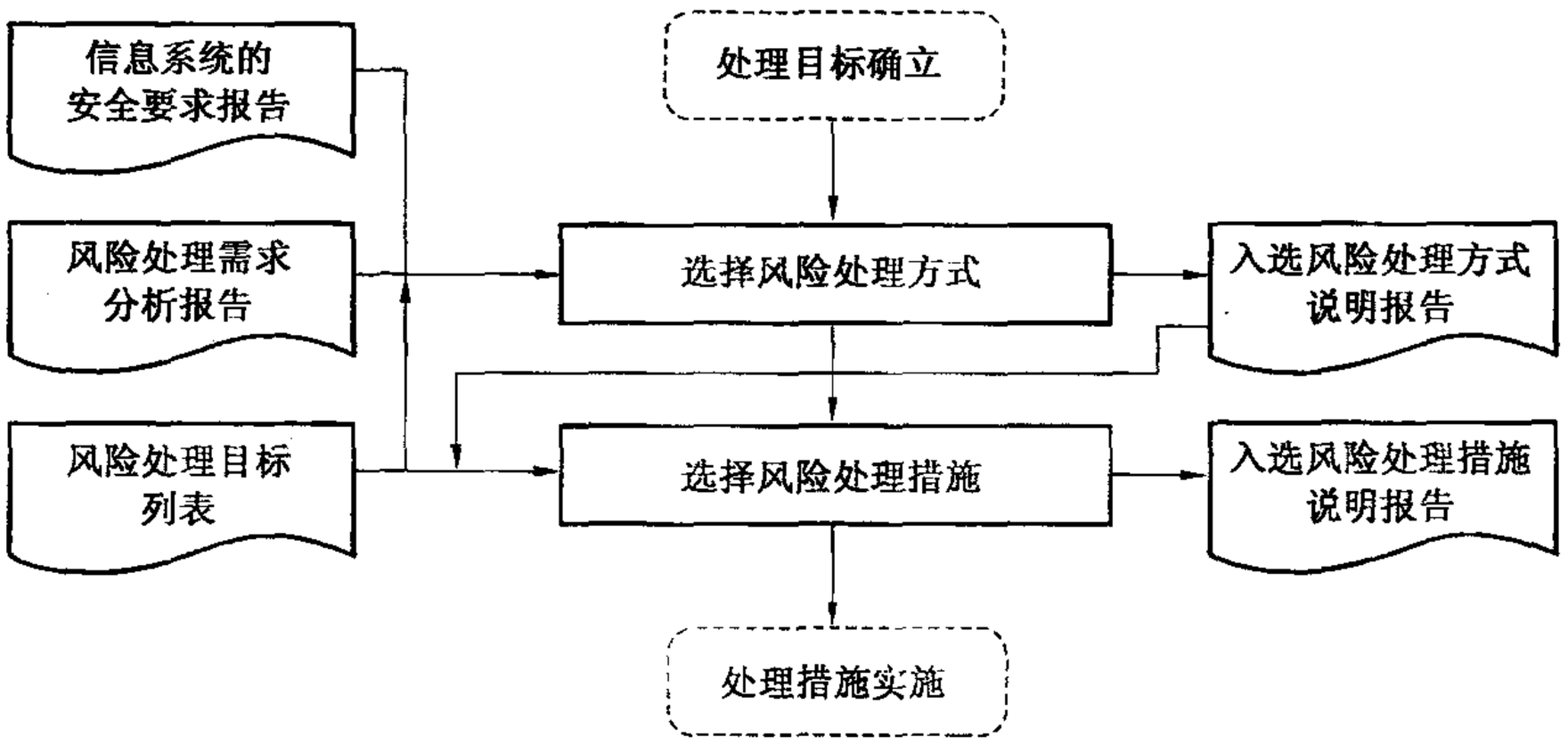

图 16 处理措施选择阶段的过程及其输入输出

7.2.4 处理措施实施

如图 17 所示，处理措施实施阶段的工作过程和内容如下：

a) 制定风险处理实施计划。依据风险处理需求分析报告、风险处理目标列表、入选风险处理方式说明报告和入选风险处理措施说明报告，制定风险处理的实施计划，包括风险处理的范围、对象、目标、组织结构、成本预算和进度安排等，形成风险处理实施计划书。风险处理实施计划书需要得到信息系统和信息安全风险管理决策层和管理层的认可和批准。

b) 实施风险处理措施。依据风险处理实施计划书、入选风险处理方式说明报告和入选风险处理措施说明报告，实施风险处理措施，并记录实施的过程和结果，形成风险处理实施记录。

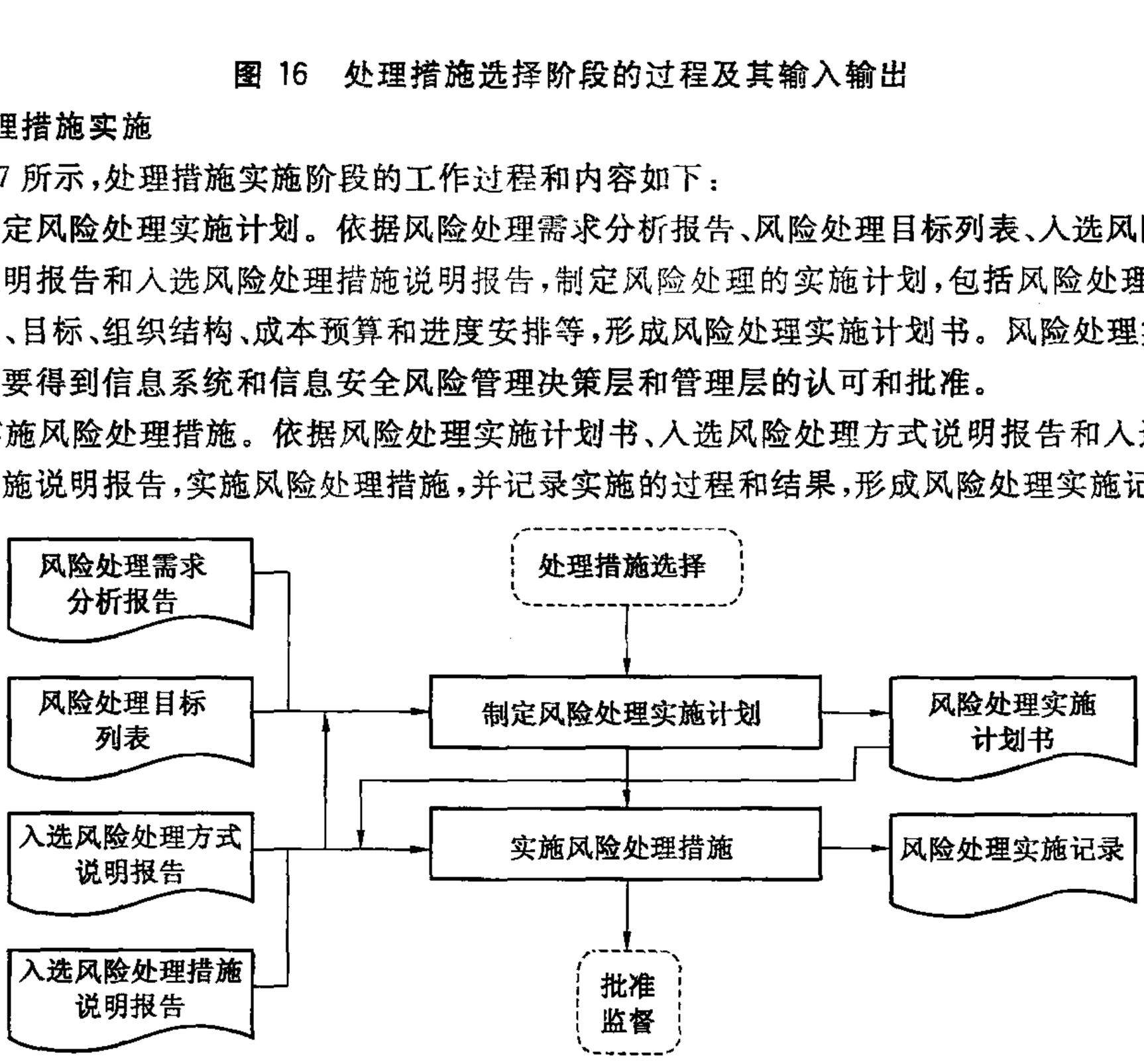

图 17 处理措施实施阶段的过程及其输入输出

7.3 风险处理文档

表 4 列出了风险处理过程的输出文档及其内容。输出文档的数量、名称和主要内容可以根据机构具体情况进行增加、删减或修改，但应涵盖表 4 中文档内容部分规定的内容。

表 4 风险处理过程的输出文档及其内容

阶 段	输出文档	文 档 内 容
现存风险判断	风险接受等级划分表	风险接受等级的划分，即把风险评估得出的风险等级划分为可接受和不可接受两种
	现存风险接受判断书	现存风险是否可接受的判断结果
处理目标确立	风险处理需求分析报告	从技术层面（即物理平台、系统平台、通信平台、网络平台和应用平台）、组织层面（即结构、岗位和人员）和管理层面（即策略、规章和制度），分析风险处理的需求
	风险处理目标列表	风险处理目标的列表，包括处理对象及其最低保护等级
处理措施选择	入选风险处理方式说明报告	选择合适的风险处理方式（包括规避方式、转移方式、降低方式和接受方式），并说明选择的理由以及被选处理方式的使用方法和注意事项等

8 批准监督

8.1 批准监督概述

8.1.1 批准监督的概念

批准监督是信息安全风险管理的第 4 步骤，包括批准和持续监督 2 部分：批准是指机构的决策层依据风险评估和风险处理的结果是否满足信息系统的安全要求，做出是否认可风险管理活动的决定；持续监督是指检查机构及其信息系统以及信息安全相关的环境有无变化，监督变化因素是否有可能引入新的安全隐患并影响到信息系统的安全保障级别。

批准应由机构内部或更高层的主管机构的决策层来执行。持续监督通常由机构内部管理层和执行层完成，必要时也可以委托支持层的外部专业机构提供支持，这主要取决于信息系统的性质和机构自身的专业能力。

8.1.2 批准监督的原则

对风险评估和风险处理的结果的批准和持续监督，不是仅依据相关标准进行僵化的比对过程，而是紧紧围绕着信息系统所承载的业务，通过对业务的重要性和业务遭受损失后所带来的影响来开展相关工作。批准通过的依据有两个：

a) 信息系统的残余风险是可接受的；

b) 安全措施（包括风险评估和风险处理）满足信息系统当前业务的安全需求。

8.2 批准监督过程

批准监督的过程包括批准申请、批准处理和持续监督 3 个阶段。在信息安全风险管理过程中，接受风险处理的输出，是一次信息安全风险管理活动的终点，监控审查和沟通咨询贯穿其 3 个阶段，如图 18 所示。

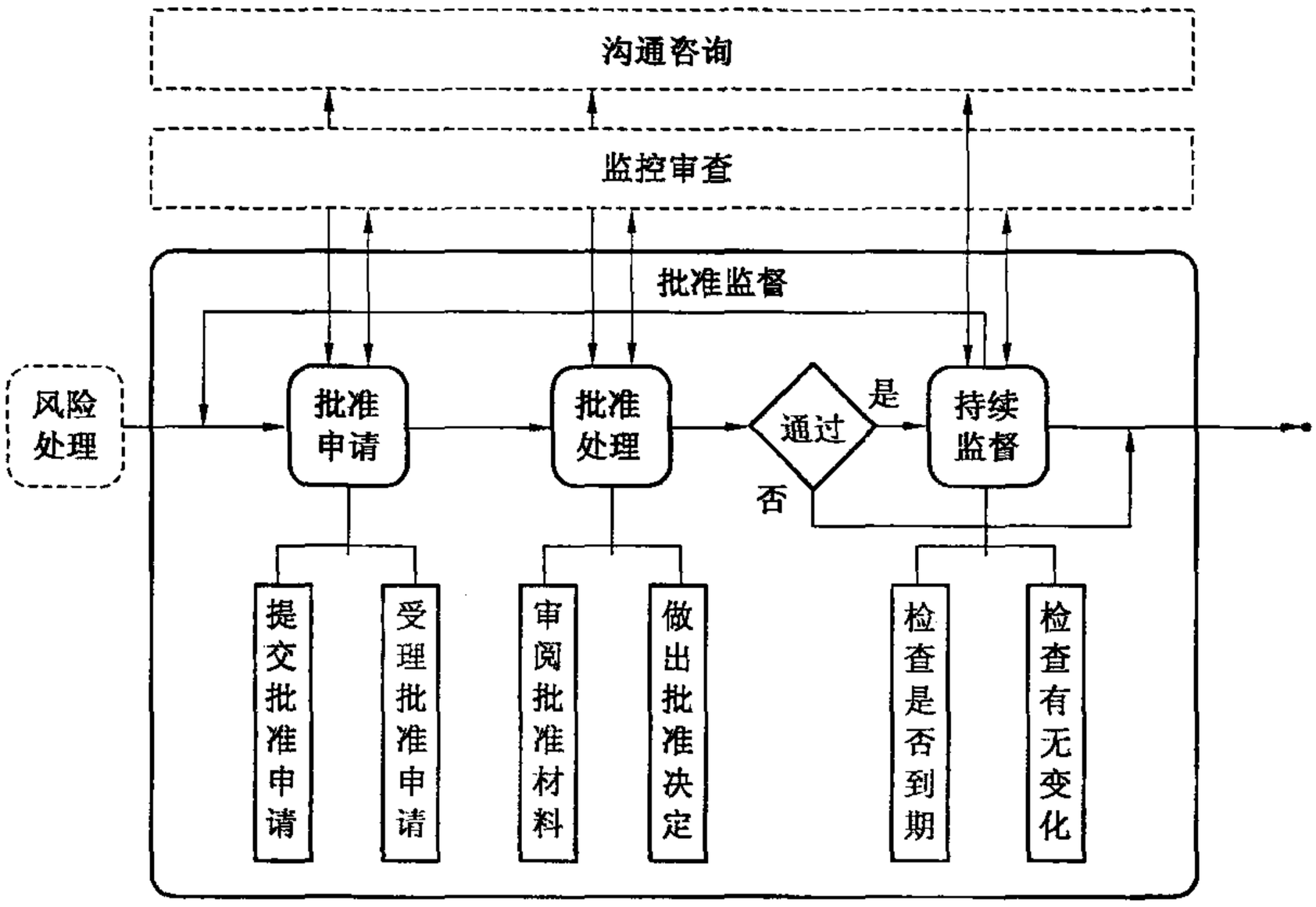

图 18　批准监督过程及其在信息安全风险管理中的位置

8.2.1　批准申请

如图 19 所示，批准申请阶段的工作过程和内容如下：

a）　提交批准申请。申请者填写批准申请书后，连同批准材料一并提交给批准机构。批准材料内容包括风险管理过程中输出的文档、软件和硬件等结果。批准申请书内容包括批准的范围、对象和期望，以及申请者的基本信息和签字等。批准机构由在信息系统和信息安全风险管理的决策层中负责重大决定的主管者构成。

b）　受理批准申请。批准机构接收批准申请书和审核结论报告并审查通过后，返回批准受理回执。批准受理回执内容包括同意受理、补充材料的要求和提交时间（如果需要），以及批准机构的名称和签章等。

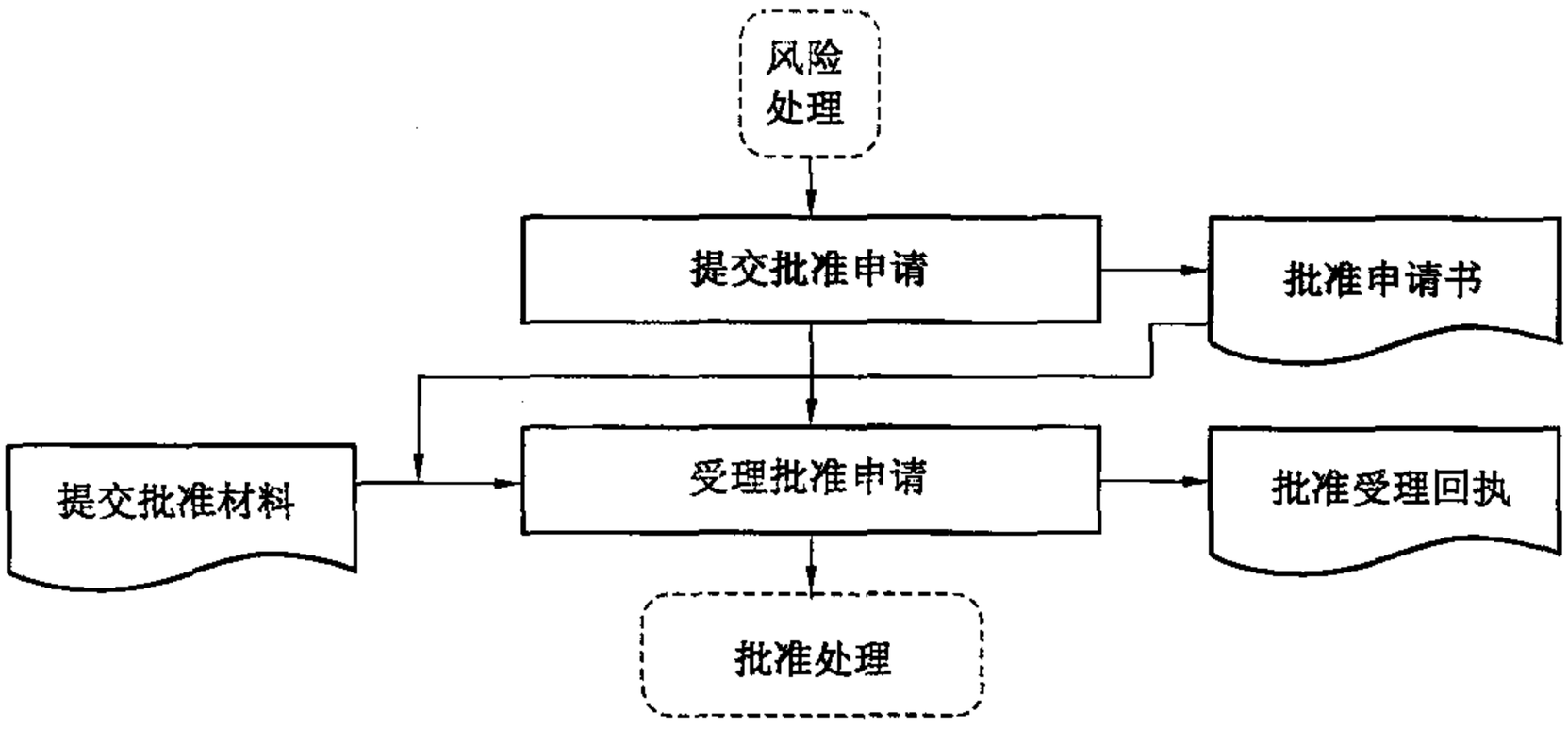

图 19　批准申请阶段的过程及其输入输出

8.2.2　批准处理

如图 20 所示，批准处理阶段的工作过程和内容如下：

a）　审阅批准材料。批准机构依据机构的使命和信息系统的安全要求报告，按照批准的原则、规定和程序，对批准材料进行审阅，与相关人员进行讨论和沟通，为批准决定做准备。

b）　做出批准决定。批准机构按照批准的原则、规定和程序，判断信息系统的安全要求是否得到

满足，机构的信息安全保障级别是否达到其使命所需要的等级，依此做出批准决定，形成批准决定书，交付申请者。批准决定书内容包括批准的范围、对象、意见、结论（即是否通过）和有效期，以及批准机构的名称和签章等。如果通过批准，则进入持续监督阶段；否则，结束本次信息安全风险管理的循环，启动新一轮循环进行改进。

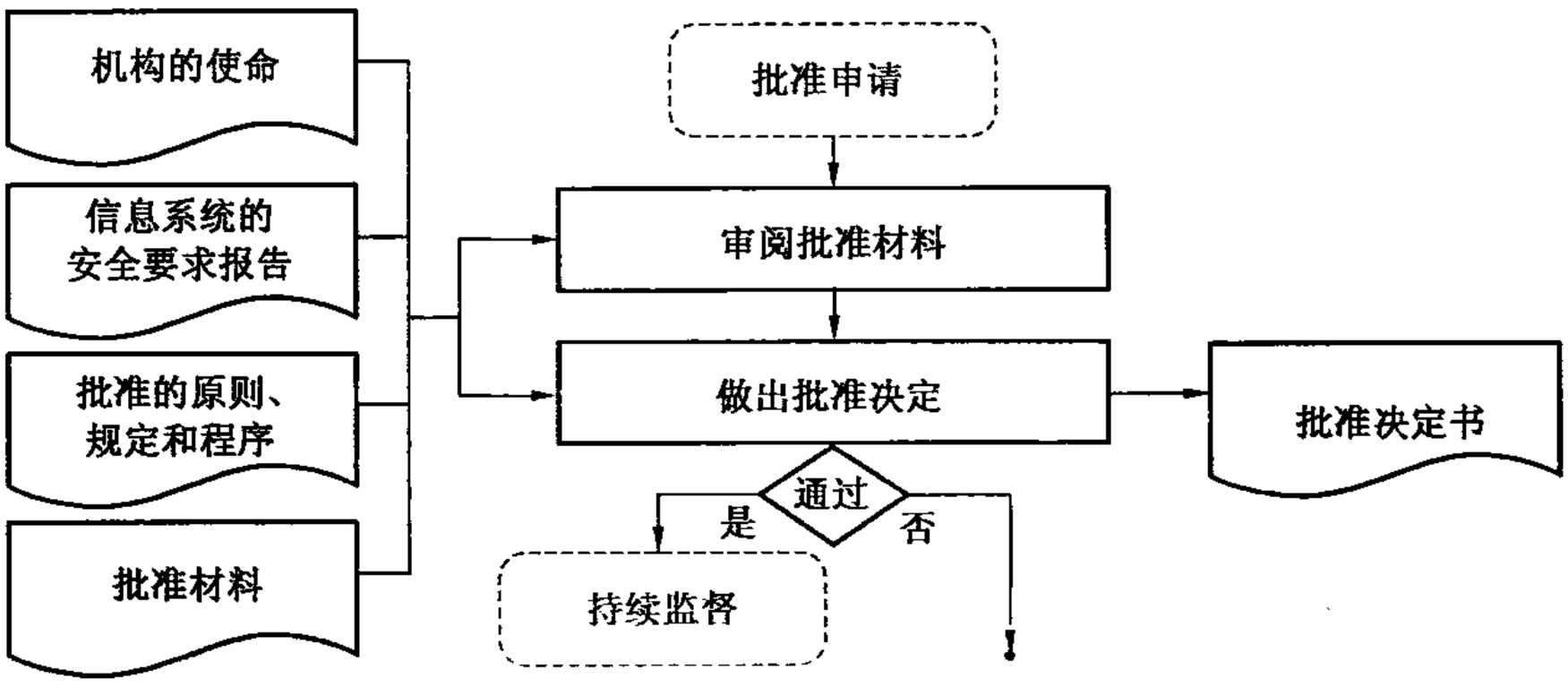

图 20　批准处理阶段的过程及其输入输出

8.2.3　持续监督

如图 21 所示，持续监督阶段的工作过程和内容如下：

a)　检查是否过期。如果批准有效期到期，则发出批准到期通知书。通知书的内容包括到期的时间和重新申请的要求，以及批准机构的名称和签章。批准有效期到期，需重新开始批准监督过程。

b)　检查有无变化。一是检查机构及其信息系统有无变化，比如，机构的使命、业务、组织结构、管理制度和技术平台等方面发展和变更；二是检查信息安全相关的环境有无变化，比如，新出台的安全相关的法律、法规、政策和标准，新的安全风险等。如果有变化，则分别给出机构变化因素的描述报告和环境变化因素的描述报告。描述报告的内容包括变化因素的列表、说明和安全隐患分析等。如果变化因素可能引入新的安全隐患并影响到安全保障级别，则结束本次信息安全风险管理的循环，启动新一轮循环进行风险评估和风险处理。

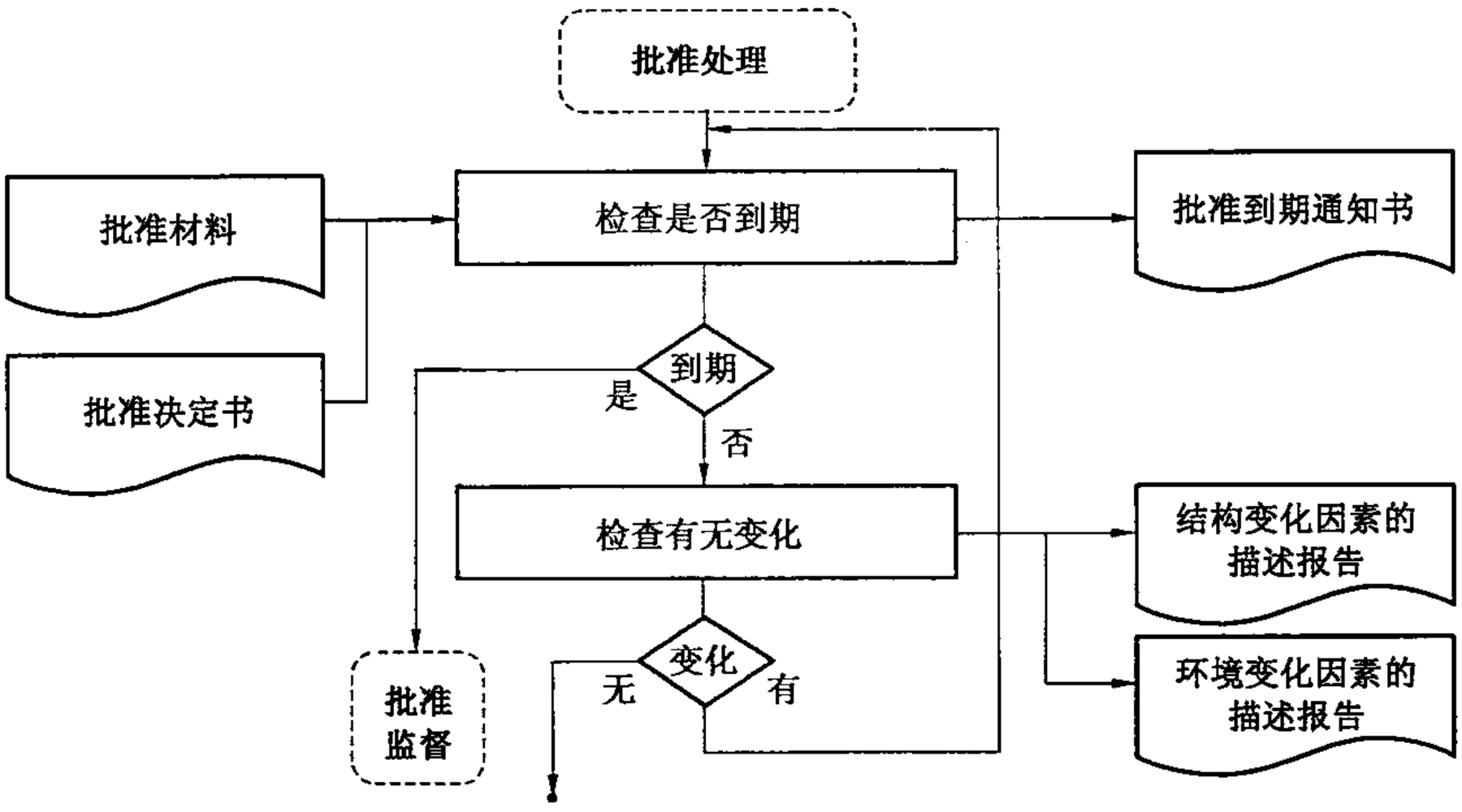

图 21　持续监督阶段的过程及其输入输出

8.3 批准监督文档

表5列出了批准监督过程的输出文档及其内容。输出文档的数量、名称和主要内容可以根据机构具体情况进行增加、删减或修改，但应涵盖表5中文档内容部分规定的内容。

表5 批准监督过程的输出文档及其内容

阶 段	输出文档	文 档 内 容
批准申请	批准申请书	批准的范围、对象和期望，以及申请者的基本信息和签字等
批准处理	批准决定书	批准的范围、对象、意见、结论（即是否通过）和有效期，以及批准机构的名称和签章等
持续监督	批准到期通知书	到期的时间和重新申请的要求，以及批准机构的名称和签章
	机构变化因素的描述报告	机构及其信息系统变化因素的列表、说明和安全隐患分析等
	环境变化因素的描述报告	信息安全相关环境变化因素的列表、说明和安全隐患分析等

9 监控审查

9.1 监控审查概述

9.1.1 监控审查的概念

监控审查对信息安全风险管理循环的4个主体步骤（即背景建立、风险评估、风险处理和批准监督）进行监控和审查。监控是监视和控制，一是监视和控制风险管理过程，即过程质量管理，以保证过程的有效性；二是分析和平衡成本效益，即成本效益管理，以保证成本的有效性。审查是跟踪受保护系统自身或所处环境的变化，以保证结果的有效性和符合性。

9.1.2 监控审查的意义

信息安全风险管理活动本身也会存在风险。监督与审查可以及时发现已经出现或即将出现的变化、偏差和延误等问题，并采取适当的措施进行控制和纠正，从而减少因此造成的损失，保证信息安全风险管理主循环的有效性。

9.1.3 监控审查的内容

监控审查包括以下方面和内容：

a) 监控过程有效性：

1) 过程是否完整和有效地被执行；

2) 输出文档是否齐全和内容完备。

b) 监控成本有效性：执行成本与所得效果相比是否合理。

c) 审查结果有效性和符合性：

1) 输出结果是否符合信息系统的安全要求；

2) 输出结果是否因信息系统自身或环境的变化而过时。

9.2 监控审查过程

监控审查的过程贯穿于信息安全风险管理的背景建立、风险评估、风险处理和批准监督这4个基本步骤，并分别输出相应的监控审查记录，如图22所示。监控审查记录内容包括监控和审查的范围、对象、时间、过程、结果和措施等。

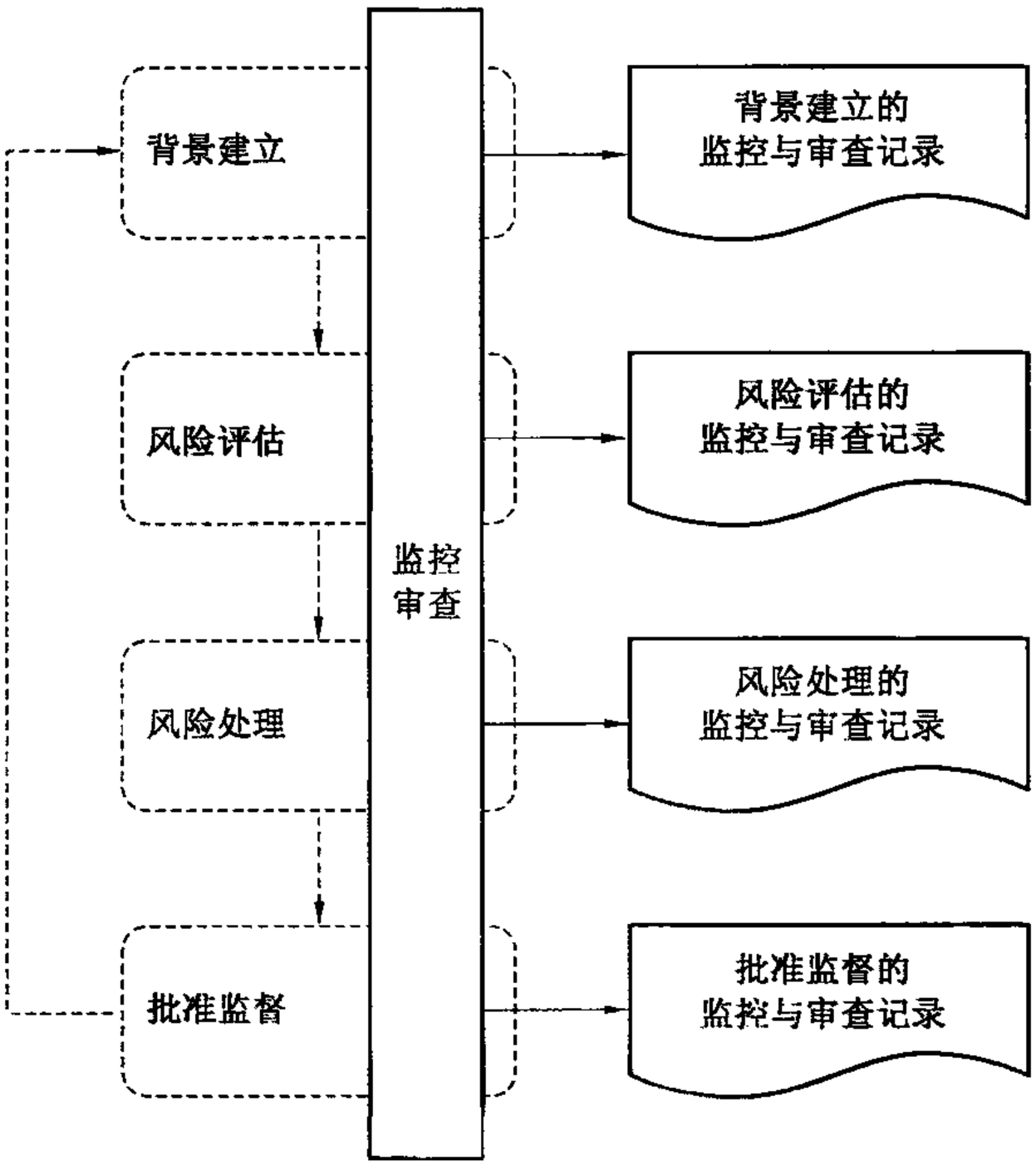

图 22　监控审查过程及其在信息安全风险管理中的位置

9.2.1　背景建立过程的监控审查

表 6 汇总了背景建立过程中各阶段的监控审查内容。

表 6　背景建立过程的监控审查

阶　段	监　控		审　查
	过程有效性	成本有效性	结果有效性和符合性
风险管理准备	风险管理计划制定的过程及其相关文档	风险管理计划的成本与效果	风险管理计划书的时效和符合性
信息系统调查	信息系统调查的过程及其相关文档	信息系统调查的成本与效果	信息系统的描述报告的时效和符合性
信息系统分析	信息系统分析的过程及其相关文档	信息系统分析的成本与效果	信息系统的分析报告的时效和符合性
信息安全分析	信息系统安全要求分析的过程及其相关文档	信息系统安全要求分析的成本与效果	信息系统的安全要求报告的时效和符合性

9.2.2　风险评估过程的监控审查

表 7 汇总了风险评估过程中各阶段的监控审查内容。

表 7　风险评估过程的监控审查

阶　段	监　控		审　查
	过程有效性	成本有效性	结果有效性和符合性
风险评估准备	风险评估的计划制定、方案确定以及方法和工具选择的过程及其相关文档	风险评估的计划、方案以及入选方法和工具的成本与效果	风险评估计划、风险评估方案和入选风险评估方法和工具列表的时效和符合性

表 7（续）

阶　段	监　控		审　查
	过程有效性	成本有效性	结果有效性和符合性
风险要素识别	资产、威胁列、脆弱性和已有安全措施识别的过程及其相关文档	资产、威胁、脆弱性和已有安全措施识别的成本与效果	需要保护的资产清单、面临的威胁列表、存在的脆弱性列表和已有安全措施列表的时效和符合性
风险分析	安全事件发生可能性分析、安全事件造成的损失分析、和风险计算的过程及其相关文档	安全事件发生可能性分析、安全事件造成的损失分析、和风险计算的成本与效果	风险计算报告的时效和符合性
风险结果判定	风险等级评价、风险状况综合评价以及风险评估报告生成的过程及其相关文档	风险等级评价、风险状况综合评价以及风险评估报告生成的成本与效果	威胁源等级列表、威胁行为等级列表、脆弱性等级列表、资产价值等级列表、影响程度等级列表和风险评估报告的时效和符合性

9.2.3　风险处理过程的监控审查

表 8 汇总了风险处理过程中各阶段的监控审查内容。

表 8　风险处理过程的监控审查

阶　段	监　控		审　查
	过程有效性	成本有效性	结果有效性和符合性
现存风险判断	可接受风险等级确定和现存风险接受判断的过程及其相关文档	可接受风险等级确定和现存风险接受判断的成本与效果	风险接受等级划分表和现存风险接受判断书的时效和符合性
处理目标确立	风险处理需求分析和风险处理目标确立的过程及其相关文档	风险处理需求分析和风险处理目标确立的成本与效果	风险处理需求分析报告和风险处理目标列表的时效和符合性
处理措施选择	风险处理方式和措施选择的过程及其相关文档	入选风险处理方式和措施的成本与效果	入选风险处理方式说明报告和入选风险处理措施说明报告的时效和符合性
处理措施实施	风险处理实施计划制定和风险处理措施实施的过程及其相关文档	风险处理实施计划制定和风险处理措施实施的成本与效果	风险处理实施计划书和风险处理实施记录的时效和符合性

9.2.4　批准监督过程的监控审查

表 9 汇总了批准监督过程中各阶段的监控审查内容。

表 9　批准监督过程的监控审查

阶　段	监　控		审　查
	过程有效性	成本有效性	结果有效性和符合性
批准申请	批准申请和受理的过程及其相关文档	批准申请和受理的成本与效果	批准申请书和批准受理回执的时效和符合性
批准处理	审阅批准材料和批准决定做出的过程及其相关文档	审阅批准材料和批准决定做出的成本与效果	批准决定书的时效和符合性

表 9（续）

阶　段	监　控		审　查
	过程有效性	成本有效性	结果有效性和符合性
持续监督	审核结论报告和批准决定书到期检查和机构及其环境变化检查的过程及其相关文档	审核结论报告和批准决定书到期检查和机构及其环境变化检查的成本与效果	机构变化因素的描述报告和环境变化因素的描述报告的时效和符合性

9.3　监控审查文档

表 10 列出了监控审查过程的输出文档及其内容。输出文档的数量、名称和主要内容可以根据机构具体情况进行增加、删减或修改，但应涵盖表 10 中文档内容部分规定的内容。

表 10　监控审查过程的输出文档及其内容

过　程	输出文档	文 档 内 容
背景建立	背景建立的监控审查记录	背景建立过程中监控和审查的范围、对象、时间、过程、结果和措施等
风险评估	风险评估的监控审查记录	风险评估过程中监控和审查的范围、对象、时间、过程、结果和措施等
风险处理	风险处理的监控审查记录	风险处理过程中监控和审查的范围、对象、时间、过程、结果和措施等
批准监督	批准监督的监控审查记录	批准监督过程中监控和审查的范围、对象、时间、过程、结果和措施等

10　沟通咨询

10.1　沟通咨询概述

10.1.1　沟通咨询的概念

沟通咨询为信息安全风险管理主循环的 4 个步骤（即背景建立、风险评估、风险处理和批准监督）中相关人员提供沟通和咨询。沟通是为直接参与人员提供交流途径，以保持参与人员之间的协调一致，共同实现安全目标。咨询是为所有相关人员提供学习途径，以提高风险意识、知识和技能，配合实现安全目标。

10.1.2　沟通咨询的意义

为保证信息安全风险管理活动顺利和有效地进行，相关人员行动的协调和一致以及相关知识和技能的熟练掌握是十分关键的因素。通过畅通的交流和充分的沟通，保持行动的协调和一致；通过有效的培训和方便的咨询，保证行动者具有足够的知识和技能，就是沟通咨询的意义所在。

10.1.3　沟通咨询的目标

沟通咨询包括以下方面和目标：

a）　面向参与人员的沟通：

1）　与决策层沟通，以得到理解和批准；

2）　与管理层和执行层沟通，以得到理解和协作；

3）　与支持层沟通，以得到了解和支持；

4）　与用户层沟通，以得到了解和配合。

b) 面向相关人员的咨询：为所有层面的相关人员提供咨询和培训等，以提高人员的安全意识、知识和技能。

10.1.4 沟通咨询的方式

沟通咨询的双方角色不同，所采取的方式有所不同。有关信息安全风险管理相关人员的角色和责任的划分参见表1。表11给出了不同层面人员之间沟通咨询的方式。

表11 沟通咨询的方式

方式		接受方				
		决策层	管理层	执行层	支持层	用户层
发出方	决策层	交流	指导和检查	指导和检查	表态	表态
	管理层	汇报	交流	指导和检查	宣传和介绍	宣传和介绍
	执行层	汇报	汇报	交流	宣传和介绍	培训和咨询
	支持层	培训和咨询	培训和咨询	培训和咨询	交流	培训和咨询
	用户层	反馈	反馈	反馈	反馈	交流

沟通咨询的各种方式说明如下：

a) 指导和检查指机构上级对下级工作的指导和检查，用以保证工作质量和效率，适用于决策层对管理层、决策层对执行层和管理层对执行层；

b) 表态指机构高层支持信息安全风险管理的对外表态，用以得到外界认同和支持，适用于决策层对支持层和决策层对用户层；

c) 汇报指机构下级对上级做工作汇报，用以得到上级认可，适用于管理层对决策层、执行层对决策层和执行层对管理层；

d) 宣传和介绍指机构的信息系统和信息安全风险管理的对外宣传和介绍，用以得到外界支持和配合，适用于管理层对支持层、管理层对用户层和执行层对支持层；

e) 培训和咨询指专业人员对信息安全风险管理相关人员的培训和咨询，用以提高人员的安全意识、知识和技能，适用于执行层对用户层、支持层对决策层、支持层对管理层和支持层对执行层；

f) 反馈指机构信息系统使用者对机构信息安全风险管理的意见反馈，用以了解实施效果和用户需求，适用于用户层对决策层、用户层对管理层、用户层对执行层和用户层对支持层；

g) 交流指同级或同行之间的对等交流，用以共享信息和协调工作，适用于决策层对决策层、管理层对管理层、执行层对执行层、支持层对支持层和用户层对用户层。

10.2 沟通咨询过程

沟通咨询的过程贯穿于信息安全风险管理的背景建立、风险评估、风险处理和批准监督这4个基本步骤，并分别输出相应的沟通咨询记录，如图23所示。沟通咨询记录内容包括沟通和咨询的范围、对象、时间、内容和结果等。

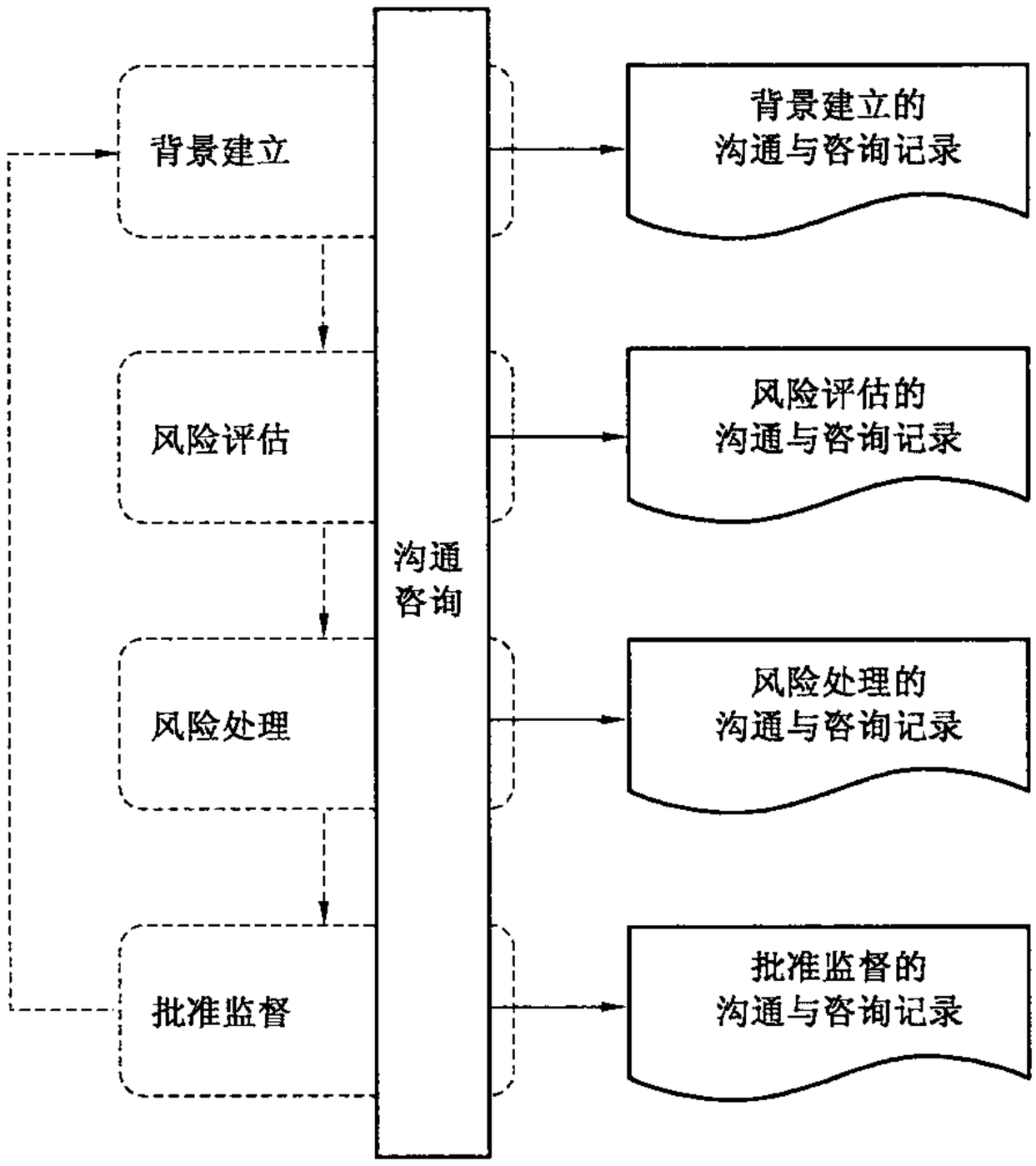

图 23　沟通咨询过程及其在信息安全风险管理中的位置

10.2.1　背景建立过程的沟通咨询

10.2.1.1　面向参与人员的沟通

表 12 汇总了背景建立过程中各阶段的沟通参与人员和涉及内容。

表 12　背景建立过程的沟通

阶　段	参与人员		涉及内容
	信息系统	信息安全风险管理	
风险管理准备	决策层	决策层 管理层	风险管理计划书
信息系统调查	管理层 执行层	管理层 执行层 支持层	信息系统的描述报告
信息系统分析	管理层 执行层	管理层 执行层 支持层	信息系统的分析报告
信息安全分析	管理层 执行层	管理层 执行层 支持层	信息系统的安全要求报告

10.2.1.2　面向相关人员的咨询

在背景建立的整个过程中，为所有相关人员提供有关背景建立的咨询和培训等。

10.2.2　风险评估过程的沟通咨询

10.2.2.1　面向参与人员的沟通

表 13 汇总了风险评估过程中各阶段的沟通参与人员和涉及内容。

表 13　风险评估过程的沟通

阶　段	参与人员		涉及内容
	信息系统	信息安全风险管理	
风险评估准备	决策层	决策层 管理层	风险评估计划
	管理层	管理层 执行层 支持层	风险评估方案 入选风险评估方法和工具列表
风险要素识别	管理层 执行层	执行层 支持层	需要保护的资产清单 面临的威胁列表 存在的脆弱性列表 已有安全措施列表
风险分析	管理层 执行层	执行层 支持层	风险计算报告
风险结果判定	管理层 执行层	管理层 执行层 支持层	风险程度等级列表 风险评估报告

10.2.2.2　面向相关人员的咨询

在风险评估的整个过程中，为所有相关人员提供有关风险评估的咨询和培训等。

10.2.3　风险处理过程的沟通咨询

10.2.3.1　面向参与人员的沟通

表 14 汇总了风险处理过程中各阶段的沟通参与人员和涉及内容。

表 14　风险处理过程的沟通

阶　段	参与人员		涉及内容
	信息系统	信息安全风险管理	
现存风险判断	决策层 管理层	决策层 管理层 执行层 支持层	风险接受等级划分表 现存风险接受判断书
处理目标确立	管理层	管理层 执行层 支持层	风险处理需求分析报告 风险处理目标列表
处理措施选择	管理层 执行层	管理层 执行层 支持层	入选风险处理方式说明报告 入选风险处理措施说明报告
处理措施实施	管理层 执行层	管理层 执行层 支持层	风险处理实施计划书 风险处理实施记录

10.2.3.2　面向相关人员的咨询

在风险处理的整个过程中，为所有相关人员提供有关风险处理的咨询和培训等。

10.2.4　批准监督过程的沟通咨询

10.2.4.1　面向参与人员的沟通

表 15 汇总了批准监督过程中各阶段的沟通参与人员和涉及内容。

表 15　批准监督过程的沟通

阶　段	参与人员		涉及内容
	信息系统	信息安全风险管理	
批准申请	管理层	决策层 管理层 执行层	批准申请书 批准受理回执
批准处理	决策层 管理层	决策层 管理层	批准决定书
持续监督	管理层 执行层	管理层 执行层	机构变化因素的描述报告 环境变化因素的描述报告

10.2.4.2　面向相关人员的咨询

在批准监督的整个过程中，为所有相关人员提供有关批准监督的咨询和培训等。

10.3　沟通咨询文档

表 16 列出了沟通咨询过程的输出文档及其内容。输出文档的数量、名称和主要内容可以根据机构具体情况进行增加、删减或修改，但应涵盖表 16 中文档内容部分规定的内容。

表 16　沟通咨询过程的输出文档及其内容

过　程	输出文档	文档内容
背景建立	背景建立的沟通咨询记录	背景建立过程中沟通和咨询的范围、对象、时间、内容和结果等
风险评估	风险评估的沟通咨询记录	风险评估过程中沟通和咨询的范围、对象、时间、内容和结果等
风险处理	风险处理的沟通咨询记录	风险处理过程中沟通和咨询的范围、对象、时间、内容和结果等
批准监督	批准监督的沟通咨询记录	批准监督过程中沟通和咨询的范围、对象、时间、内容和结果等

11　信息系统规划阶段的信息安全风险管理

11.1　安全目标和安全需求

信息系统规划阶段的安全目标是明确信息系统安全建设的目的，对信息系统安全建设实现的可能性进行分析论证并设计出总体安全规划方案。为了保证安全目标的实现，需要对信息系统规划阶段中可能引入安全风险的环节进行风险管理，从而降低在项目后期处理相同安全风险所带来的高额成本。

信息系统规划阶段所涉及的主要安全需求包括：

a)　明确安全总体方针；

b)　确保安全总体方针源自业务期望；

c)　清晰描述所涉及系统的安全现状；

d)　提交明确的安全需求文档；

e)　明确风险评估准则并达成一致；

f)　清晰描述从系统的那些层次进行安全实现；

g)　对系统规划中安全实现的可能性进行充分分析、论证。

11.2　风险管理的过程与活动

11.2.1　风险管理过程概述

依据信息系统规划阶段的安全目标和安全需求，该阶段的主要风险管理活动包括：明确信息系统安全总体方针、信息系统安全需求分析、风险评估准则达成一致、信息系统安全实现论证分析等，同时在上述过程中通过监控审查、沟通咨询来确保本阶段风险管理目标的实现。各项活动在风险管理过程中所

处位置如表 17 所示。

表 17　信息系统规划阶段的主要风险管理活动

序　　号	风险管理活动	所处风险管理过程
1	明确安全总体方针	背景建立
2	安全需求分析	背景建立
3	风险评估准则达成一致	风险评估
4	安全实现论证分析	风险处理、批准监督

对于上述风险管理活动，由于处于项目的起始阶段，因此特别需要重视沟通与监控的环节。确保在项目的规划阶段，就安全目标、管理范围、评价准则等在机构内达成一致是项目能否顺利进行和成功完成的关键。

11.2.2　明确安全总体方针

可通过以下方法来管理安全总体方针制定过程中可能引入的安全风险：

a）　应对安全总体方针文档的完整性、条理性、明确性等进行审查；

b）　应参考国家标准、相关国际标准、行业标准及公认安全管理实践等对安全总体方针文档的内容进行审查。

审查的内容至少应包括以下项目：

a）　是否已经制定并发布了能够反映机构安全管理意图的信息安全文件：

1）　审查机构当前业务期望；

2）　审查机构当前安全总体方针；

3）　审查机构当前安全策略。

b）　风险管理过程的执行是否有机构保障：

1）　审查组织机构的结构合理性；

2）　审查职责分工的合理性；

3）　审查监控审查过程的合理性。

c）　是否有专人按照特定的过程定期进行复审与评价：

1）　审查机构当前风险管理复查过程；

2）　审查复查情况及调整计划；

3）　审查能否确保当系统安全状态发生变化时及时地进入复审与评价的过程，以便及时地修改安全策略，恢复到机构可接受的安全状态。

d）　风险管理的范围是否明确。

以上项目需根据信息系统具体情况进行增加或删减，对于安全总体方针的审查过程需得到信息系统所属机构相关部门的批准监督。

11.2.3　安全需求分析

可通过以下方法来管理安全需求分析过程中可能引入的安全风险：

a）　应对安全需求分析文档的完整性、条理性、明确性等进行审查；

b）　应采用信息安全风险分析方法，通过对信息系统进行风险评估来发现当前安全保障体系中存在的不足。

以上过程中，缺少任何一个过程都将给风险评估结果带来较大的偏差，因此应重视过程的全面性并保证每个过程的正确实施。

对于安全需求分析文档的审查过程需得到信息系统所属机构相关部门的批准监督。

11.2.4　风险评估准则达成一致

可通过以下方法来管理风险评估准则制定过程中可能引入的安全风险：

a) 应对风险评估准则文档的完整性、条理性、明确性等进行审查。

b) 可通过问卷调查或专人访谈的方式审查风险评估准则是否得到信息系统所属机构一致性的认可。审查项目如下：

1) 风险管理的要素是否得到一致性认可；

2) 风险评估准则是否得到一致性认可。

对于风险评估准则，机构应保证准则文档的清晰性和明确性，以及是否得到机构的一致认可，如果风险评估准则不能达成一致，这将直接导致无法对风险作出公认的评价，从而导致风险评估的失败。

对于风险评估准则的审查过程需得到信息系统所属机构相关部门的批准监督。

11.2.5 安全实现可能性论证分析

可通过以下方法来管理系统规划安全实现论证过程中可能引入的安全风险：

a) 应对系统规划文档的完整性、条理性、明确性等进行审查。

b) 应对系统规划中安全实现方案进行详细的分析和论证。审查项目如下：

1) 系统规划中是否考虑信息系统的威胁、环境，并制定安全实现方案；

2) 系统规划中是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；

3) 系统规划中是否描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、组织安全策略、专门技术和知识等。

12 信息系统设计阶段的信息安全风险管理

12.1 安全目标和安全需求

信息系统设计阶段的安全目标是依据规划阶段输出的总体安全规划方案来设计信息系统安全的实现结构(包括功能划分、接口协议和性能指标等)和实施方案(包括实现技术、设备选型和系统集成等)。在设计信息系统的实现结构和实施方案时，在技术的选择、配合、管理等众多的环节均容易引入安全风险，因此对关键的环节应提出必要的安全要求并有针对性地进行安全风险管理。

信息系统设计阶段的主要安全需求包括：

a) 设计方案符合系统建设规划；

b) 设计方案中的安全需求符合规划阶段的安全目标；

c) 对用以实现安全系统的各类技术进行有效性评估；

d) 对用于实施方案的产品需满足安全保护等级的要求；

e) 对自开发的软件要在设计阶段就充分考虑安全风险。

12.2 风险管理的过程与活动

12.2.1 风险管理过程概述

依据信息系统设计阶段的安全目标和安全需求，该阶段的主要风险管理活动包括：信息系统安全设计方案分析论证、安全技术和安全产品选择、自开发软件设计风险处理等，同时在上述过程中通过监控审查、沟通咨询来确保本阶段风险管理目标的实现。各项活动在风险管理过程中所处位置如表18所示。

表18 信息系统设计阶段的主要风险管理活动

序　　号	风险管理活动	所处风险管理过程
1	设计方案分析论证	背景建立、风险评估
2	安全技术选择	风险处理
3	安全产品选择	风险处理
4	自开发软件设计风险处理	风险处理

对于上述风险管理活动，应该注重通过足够的外部咨询来学习、了解各种技术和产品的优缺点，并在充分的内部沟通的基础上得出技术选择说明、产品选型说明以及软件安全要求文档。

12.2.2 设计方案分析论证

可通过以下方法来管理系统设计方案分析论证过程中可能引入的安全风险：

a) 设计方案是否符合系统建设规划，并得到最高管理者的认可；

b) 设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析，制定信息系统的总体安全策略；

c) 设计方案是否对系统建设后面临的威胁进行了分析，重点分析来自物理环境和自然的威胁，以及由于内、外部人侵等造成的威胁；

d) 设计方案是否对设计原型中的技术实现以及人员、组织管理等方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性；

e) 设计方案是否考虑随着其他系统接入而可能产生的风险；

f) 设计活动中所采用的安全控制措施、安全技术保障手段对风险的影响。在安全需求变更和设计变更后，也需要重复这项评估。

12.2.3 安全技术选择

可通过以下方法来管理安全技术选择过程中可能引入的安全风险，从而构建符合要求的安全保障体系：

a) 参考现有国内外安全标准；

b) 参考国内外公认安全实践；

c) 参考行业标准；

d) 专家委员会决策。

在项目设计阶段，需充分考虑所选择的安全技术能够解决问题的程度，即技术选择的有效性。如果技术选择不合理，将直接导致相应安全弱点的暴露，安全风险的发生将是显而易见的。

对于技术选择文档的审查过程需得到信息系统所属机构相关部门的批准监督。

12.2.4 安全产品选型

可通过以下方法来管理安全产品选型过程中可能引入的安全风险：

a) 审查是否符合相关安全标准要求；

b) 审查是否通过相关认证机构的认证；

c) 审查是否满足当前安全保障等级的要求；

d) 审查产品的实用性；

e) 集中测试；

f) 专家会议决策。

安全产品选型的合理程度将直接影响原有设计方案所要求达到的安全防御效果。因此在项目设计阶段要做好安全产品选型的工作。

对于产品选型文档的审查过程需得到信息系统所属机构相关部门的批准监督。

12.2.5 自开发软件设计风险处理

可通过以下方法来管理自开发的非通用软件在前期设计过程中可能引入的安全风险：

a) 清晰描述软件的安全功能需求；

b) 在设计规格说明书中明确指出实现的方法；

c) 参考相关标准如 GB/T 18336.2—2008 对设计说明书的安全功能进行审查、补充；

d) 对各安全功能进行详细的功能测试。

对于自主开发的非通用软件，通常由于各种原因而存在众多的安全风险，这些风险直接影响了系统的正常运行。因此应在设计阶段对软件进行风险处理。

对于软件设计说明文档的审查过程需得到信息系统所属机构相关部门的批准监督。

13 信息系统实施阶段的信息安全风险管理

13.1 安全目标和安全需求

信息系统实施阶段安全目标是按照规划和设计阶段所定义的信息系统安全实施方案，采购设备和软件，开发定制功能，集成、部署、配置和测试信息系统的安全机制，培训人员，并对是否允许系统投入运行进行批准监督。

信息系统实施阶段的主要安全需求包括：

a) 确保采购的设备、软件和其他系统组件满足已定义的安全要求；

b) 确保定制开发的软件和系统满足已定义的安全要求；

c) 确保整个系统已按照设计要求进行了部署和配置，并通过整体的安全测试来验证系统的安全功能和安全特性符合设计要求；

d) 通过对相关人员的操作培训和安全培训，确保人员已具备维持系统安全功能和安全特性的能力；

e) 通过对系统投入运行前的批准监督，确保信息系统的使用已得到授权。

在实施阶段，风险管理的主要目标是确保上述安全需求已得到实现。

13.2 风险管理的过程与活动

13.2.1 风险管理过程概述

依据信息系统实施阶段的安全目标和安全需求，该阶段的主要风险管理活动包括：安全测试、检查与配置、人员培训及授权运行，同时在上述过程中通过监控审查、沟通咨询来确保本阶段风险管理目标的实现。各项活动在风险管理过程中所处位置如表 19 所示。

表 19 信息系统实施阶段的主要风险管理活动

序　　号	风险管理活动	所处风险管理过程
1	安全测试	风险评估
2	检查与配置	风险处理
3	人员培训	风险处理
4	授权系统运行	批准监督

在检查与配置、安全测试活动中，信息系统安全员应与系统使用人员、系统管理人员在系统安全功能和安全特性、测试计划和测试过程方面进行充分沟通，并相互配合来完成风险处理的工作。信息系统安全员还应监控上述实施过程，如发现问题及时向主管领导汇报。

13.2.2 安全测试

系统安全测试是对所开发或采购的系统特定部分的测试和整个系统的测试，内容包括：

a) 采购的设备和软件、定制的软件和系统各部分安全功能和安全特性的测试；

b) 对集成后整个系统的整体安全测试；

c) 对安全管理、物理设施、人员、流程、业务或内部服务（如网络服务）的使用，以及应急计划等进行测试。

如果在开发或采购阶段增加了新的处理措施，应进行重新测试。安全测试可以由信息系统所属机构内部实施，也可以聘请第三方专业机构实施。

测试之前应制定测试计划，并对测试过程和测试结果进行记录。

13.2.3 检查与配置

应对采购的设备、软件、定制开发的软件和系统进行检查并正确配置，内容包括：

a) 检查采购的设备和软件是否具有国家主管部门的生产和销售许可证，以及是否通过了国家有

关部门的测评和认证；

b） 检查采购的设备和软件、定制的软件和系统所具备的安全功能和安全特性；

c） 按照产品说明书和设计说明书正确配置设备、软件和系统，确保符合设计要求。

如果在系统实施的过程中增加了新的安全处理措施，还应对新增加的措施给原有系统带来的风险进行分析，确保增加的处理措施与原有设计保持协调和一致。

13.2.4 人员培训

培训的对象包括系统的使用人员、系统维护人员和安全管理人员，培训过程是沟通咨询的重要体现，培训内容包括：

a） 系统的操作流程和操作方法；

b） 安全意识、基本安全技术知识和安全管理知识；

c） 系统维护和安全功能的使用；

d） 安全管理制度和管理流程；

e） 系统安全事件的应急处理流程和恢复流程。

13.2.5 授权系统运行

信息系统在投入运行前应进行批准监督。负责审批的管理者应与系统安全员、系统管理人员、系统使用人员进行充分沟通，必要时还可以聘请专家进行咨询，以便对系统是否可以投入运行做出正确决策。管理者对信息系统可以有以下 3 种授权方式：

a） 授权系统全面运行——在对安全测试的结果进行评估之后，如果系统的残余风险被认为是完全可以接受的，那么就可以为系统发布一个全面运行的授权。这时信息系统已被认可，可以没有限制地或制约地投入运行。

b） 临时批准运行——在对安全测试的结果做出评估之后，如果系统的残余风险被认为不能完全接受，但是又迫切需要将信息系统投入运行，或机构的使命需要其继续运行，那么就会为信息系统发布一个临时的运行批准。临时批准提供的是一种有限制的授权，允许信息系统在特定时限和条件下投入运行，并使相关人员了解到机构的运行和资产在限定时间内具有相对更高的风险。

临时运行批准允许时限应与信息系统的风险等级相关联，最长不应超过一年。在临时批准运行结束前，信息系统应满足全面批准运行的条件，开始全面批准的运行，否则应停止系统运行。

c） 拒绝对运行进行授权——在对安全测试的结果做出评估之后，如果系统的残余风险被认为是不可以接受的，那么就要拒绝批准信息系统投入运行。对于被拒绝运行的系统，信息系统拥有者应与授权管理者和其他相关方进行沟通，重新制定风险处理措施和改进计划，将信息系统的安全风险降低到可接受的程度后，再进行授权审批。

14 信息系统运行维护阶段的信息安全风险管理

14.1 安全目标和安全需求

信息系统运行维护阶段安全目标是在信息系统经过授权投入运行之后，确保在运行过程中，以及信息系统或其运行环境发生变化时维持系统的正常运行和安全性。

信息系统运行维护阶段的安全需求包括：

a） 在信息系统未发生更改的情况下，维持系统的正常运行，进行日常的安全操作及安全管理；

b） 在信息系统及其运行环境发生变化的情况下，进行风险评估并针对风险制定处理措施；

c） 定期进行风险再评估工作，维持系统的持续安全；

d） 定期进行信息系统的重新审批工作，确保系统授权的时间有效性。

在运行维护阶段，风险管理的主要目标是确保上述安全需求已得到实现。

14.2 风险管理的过程与活动

14.2.1 风险管理过程概述

依据信息系统运行维护阶段的安全目标和安全需求，该阶段的主要风险管理活动包括：安全运行和管理、变更管理、风险再评估、定期重新审批，同时在上述过程中通过监控审查、沟通咨询来确保本阶段风险管理目标的实现。各项活动在风险管理过程中所处位置如表 20 所示。

表 20 信息系统运行维护阶段的主要风险管理活动

序　　号	风险管理活动	所处风险管理过程
1	安全运行和管理	风险评估、风险处理
2	变更管理	风险评估、风险处理
3	风险再评估	风险评估、风险处理
4	定期重新审批	批准监督

图 24 描述了运行维护阶段风险管理活动的过程。

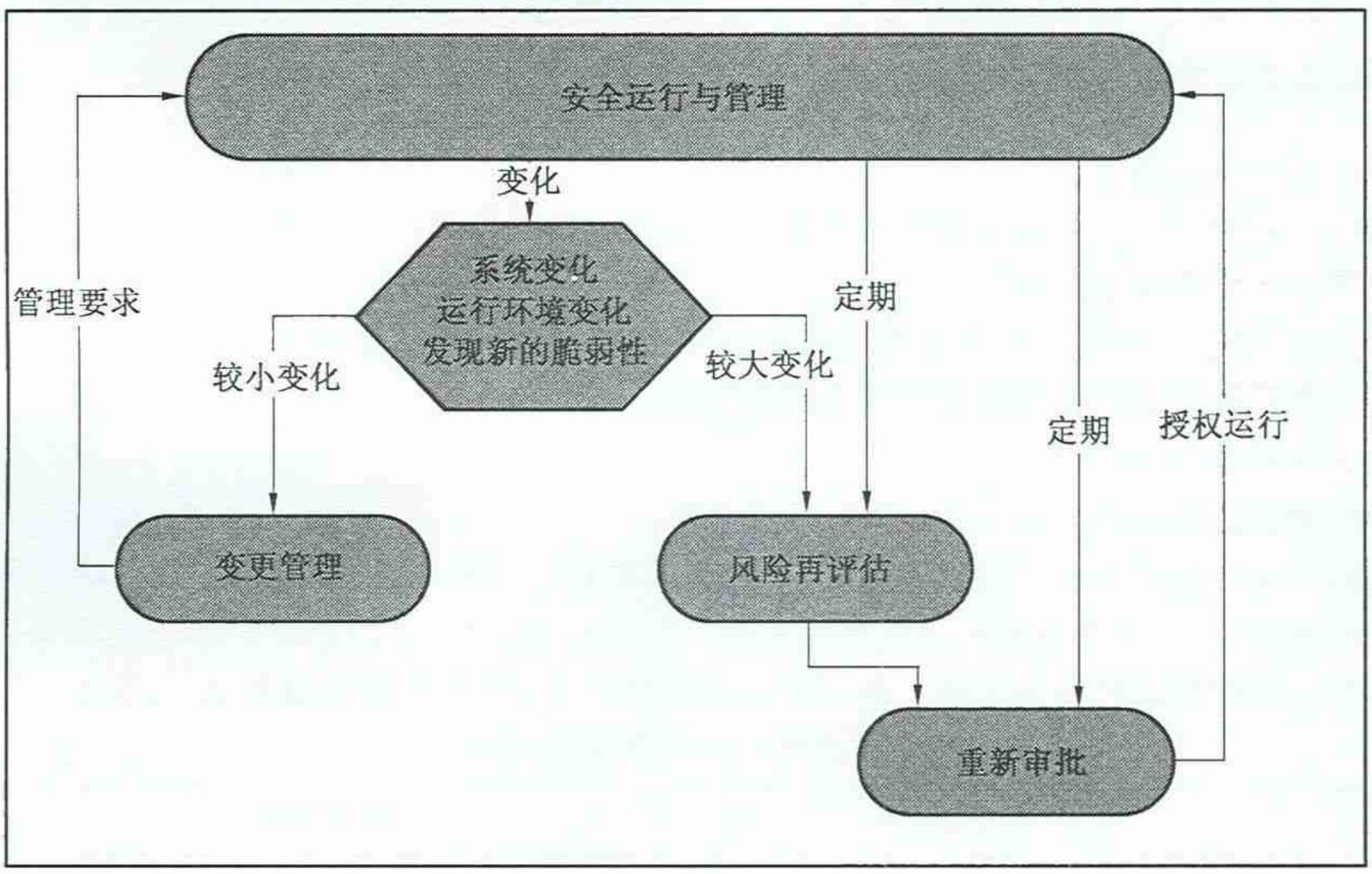

图 24 运行维护阶段的风险管理活动

安全运行和管理活动贯穿于整个运行维护阶段，在系统发生变化、运行环境发生变化以及发现新的脆弱性的情况下，应进行系统变更管理，并将管理要求反馈到安全运行与管理活动中；在变化较大的情况下，应进行风险再评估，再评估活动也应定期进行；系统授权运行的重新审批工作也应定期进行，保证系统的授权维持时间有效性。

14.2.2 安全运行和管理

信息系统在开始运行之后，应按照处理措施所定义的系统操作要求、运行要求和管理要求，进行安全操作和安全管理，保证系统的安全功能的实现。安全运行和管理的例子包括执行备份、举办培训课程、管理密钥、更新用户管理和访问特权、以及更新安全软件等。

14.2.3 变更管理

在信息系统及其运行环境发生变化时，应评估其风险，并制定和实施相应的处理措施来控制风险。变更管理包括以下几个方面：

a) 信息系统的变更：包括系统升级、增加新功能、发现新的系统威胁和脆弱性等；

b) 系统运行环境的变更：包括系统的硬环境、软环境的变化以及法律法规环境的变化。

在信息系统及其运行环境发生变化时，应执行风险管理过程中的风险评估过程和风险处理过程，分析可能出现的新风险，并制定和实施处理措施对风险进行处理。

变更管理主要用于信息系统及其运行环境发生变化不大的情况，变更管理无需对系统运行进行重新授权。

14.2.4 风险再评估

风险再评估是重新对系统进行风险评估的过程。应定期进行系统的风险再评估，在信息系统及其运行环境发生重大变化时，也应适时进行风险再评估。定期风险评估的周期一般应为一年，最长不应超过2年。

风险再评估后应执行风险处理过程，针对风险制定和实施处理措施。

14.2.5 重新审批

重新审批是重新执行信息系统批准监督的过程。信息系统在运行一段时间之后，系统及其运行环境、风险环境都会发生变化，应重新确认系统风险是否仍在可接受的范围内。

信息系统授权的重新审批应以风险再评估的结果为依据，根据系统风险再评估后的风险状况和残余风险，重新审批信息系统是否可以继续运行。

15 信息系统废弃阶段的信息安全风险管理

15.1 安全目标和安全需求

信息系统废弃阶段安全目标是确保对信息系统的过时或无用部分进行安全报废处理，防止信息系统的安全要求和安全功能遭到破坏。

废弃阶段涉及信息、硬件和软件的安全处置，应防止将敏感信息泄漏给外部人员。在这一阶段主要的风险管理活动是对系统废弃的风险评估和风险处理。

15.2 风险管理的过程与活动

15.2.1 风险管理过程概述

依据信息系统废弃阶段的安全目标和安全需求，该阶段的主要风险管理活动包括：确定废弃对象，对废弃对象的风险评估，对废弃对象及废弃过程的风险处理，同时在上述过程中通过监控审查、沟通咨询来确保本阶段风险管理目标的实现。各项活动在风险管理过程中所处位置如表21所示。

表21 废弃阶段的主要风险管理活动

序　　号	风险管理活动	所处风险管理过程
1	确定废弃对象	背景建立
2	废弃对象的风险评估	风险评估
3	废弃过程的风险处理	风险处理
4	废弃后的评审	批准监督

15.2.2 确定废弃对象

信息系统在经过一段时间的运行及使用之后，系统的部分或全部可能不再需要。这时需要对废弃的部分进行分析，确定系统的哪些部分需要废弃。废弃对象的考虑范围包括被废弃的信息、硬件、软件、或者是整个系统。

应建立废弃对象的清单，并进行标识。

15.2.3 废弃对象的风险评估

废弃系统的风险评估主要应考虑被废弃的信息、硬件和软件的安全要求，分析废弃对原有系统造成的威胁和脆弱性，评估不安全废弃可能带来的影响和可能性。

废弃系统的安全要求应在保证原有系统的保密性、完整性和可用性的前提下，重点考虑废弃信息与系统的保密性要求，确保敏感信息不会泄漏。

15.2.4 废弃过程的风险处理

废弃过程的风险处理应考虑建立废弃系统的安全处置程序，可考虑以下处理措施：

a) 对载有敏感信息的媒体应加以安全妥当的保存或采用安全的方式加以处置，如焚烧或碎片，或在清空数据后供本组织内的其他方面使用。

b) 把所有的媒体收集起来并进行安全的处置，比试图分离出敏感的物品可能更加容易。

c) 许多组织对文件、设备和媒体提供收集和处置的服务。应注意选择一个适当的具有足够的处理措施和经验的承包商。

d) 若可能，对敏感物品的处置应进行记录，以便保持审核踪迹。

在堆积媒体等候集中处理时，应当考虑到聚集效应，即大量未分类信息堆置在一起可能比少量已分类的信息更敏感。

15.2.5 废弃后的评审

在执行完废弃过程后应对系统废弃后的残余风险进行评审，确保残余风险是在信息系统的可接受范围内。

评审的内容包括确认废弃后系统中的敏感信息已被有效清除，系统废弃的安全要求已得到满足等。

附 录 A
（资料性附录）
风险处理参考模型及其需求和措施

A.1 风险处理参考模型

风险处理按照演进路线可参考以下模型：传统安全防护处理模型、PDR 模型、P2DR 模型以及 P2DR2 模型等四种。说明如下：

a) 传统安全防护处理模型。该方法对信息系统进行审计分析，制定相应的安全策略，采取一定的安全防护措施。采用该模型的前提是，要保证信息系统的正确设置、比较完善的防御手段、威胁及弱点相对固定。适用于规模较小，安全要素相对没有动态变化的网络或信息系统，无需检测和反应机制。

b) PDR 模型。该模型的风险处理模型包含防护、检测、反应等 3 个过程，对三者的时间要求满足：Dt + Rt < Pt，其中，Dt 是系统能够检测到网络攻击或入侵所花费的时间，Rt 是从发现对信息系统的入侵开始到系统做出足够反应的时间，Pt 是系统设置各种保护措施的有效防护时间，也就是外界入侵实现对安全目标侵害目的所需要的时间。此模型着重强调 PDR 行为的时间要求，可以不包含风险分析及相关安全策略的制定。

c) P2DR 模型。在 PDR 模型的基础上，通过对系统的审计分析得出贯穿整个 PDR 过程的安全策略，形成安全审计、策略、防护、检测、响应的动态安全处理循环系统。

d) P2DR2 模型。PPDRR 模型是典型的、公认的安全处理模型。它是一种动态的、自适应的安全处理模型，可适应安全风险和安全需求的不断变化，提供持续的安全保障。PPDRR 模型包括策略(Policy)、防护(Protection)、检测(Detection)、响应(Response)和恢复(Recovery)5 个主要部分。防护、检测、响应和恢复构成一个完整的、动态的安全循环，在安全策略的指导下共同实现安全保障。风险处理就是基于风险的安全处理，所以，PPDRR 模型同样适用于风险处理。该模型是随着现代风险评估理论趋于成熟后形成的全网动态安全防护模型，一般应包含动态的风险评估体系、动态的安全策略制定、动态的防御系统、实时的监控系统、实时的响应及灾难恢复机制以及健全的安全管理体系。

根据各类信息系统的差异化安全保护要求，建议对不同等级的信息系统采取不同要求的风险处理模型，对于安全保护等级为 4 及以上者，建议采用 P2DR2 模型，安全保护等级为 3 者，建议参考 P2DR2 模型，安全保护等级为 2 及以下者，不作要求。

A.2 风险处理的需求和措施

表 A.1 根据 P2DR2 模型列出了主要的风险处理需求及其相应的风险处理措施。

表 A.1 主要的风险处理需求及其相应的风险处理措施

P2DR2	风险处理需求	风险处理措施
策略 Policy	设备管理制度	建立健全各种安全相关的规章制定和操作规范，使得保护、检测和响应环节有章可循、切实有效
	机房出入守则	
	系统安全管理守则	
	系统安全配置明细	
	网络安全管理守则	
	网络安全配置明细	

表 A.1（续）

P2DR2	风险处理需求	风险处理措施
策略 Policy	应用安全管理守则	建立健全各种安全相关的规章制定和操作规范，使得保护、检测和响应环节有章可循、切实有效
	应用安全配置明细	
	应急响应计划	
	安全事件处理准则	
保护 Protection	机房	宜按照 GB 50174—1993、GB/T 9361—1988、GB/T 2887—2000 等国家标准建设和维护计算机机房
	门控	安装门控系统
	保安	建设保安制度和保安队伍
	电磁屏蔽	在必要的地方设置抗电磁干扰和防电磁泄漏的设施
	病毒防杀	全面部署防病毒系统
	漏洞补丁	及时下载和安装最新的漏洞补丁模块
	安全配置	宜遵守各系统单元的安全配置明细，避免配置中的安全漏洞
	身份认证	根据不同的安全强度，分别采用身份标识/口令、数字钥匙、数字证书、生物识别、双因子等级别的身份认证系统，对设备、用户、服务等主客体进行身份鉴别
	访问控制	根据不同的安全强度，分别采用自主型、强制型等级别的访问控制系统，对设备、用户等主体访问客体的权限进行控制
	数据加密	根据不同的安全强度，分别采用由国家密码管理部门认可的数据加密系统，对传输数据和存储数据进行加密
	边界控制	在网络边界布置防火墙，阻止来自外界非法访问
	数字水印	对于需要版权保护的图片、声音、文字等形式的信息，采用数字水印技术加以保护
	数字签名	在需要防止事后否认时，可采用数字签名技术
	内容净化	部署内容过滤系统
	安全机构、安全岗位、安全责任	建立健全安全机构，合理设置安全岗位，明确划分安全责任
检测 Detection	监视、监测和报警	在适当的位置安置监视器和报警器，在各系统单元中配备监测系统和报警系统，以实时发现安全事件并及时报警
	数据校验	通过数据校验技术，发现数据篡改
	主机入侵检测	部署主机入侵检测系统，发现主机入侵行为
	主机状态监测	部署主机状态监测系统，随时掌握主机运行状态
	网络入侵检测	部署网络入侵检测系统，发现网络入侵行为
	网络状态监测	部署网络状态监测系统，随时掌握网络运行状态
	安全审计	在各系统单元中配备安全审计，以发现深层安全漏洞和安全事件
	安全监督、安全检查	实行持续有效的安全监督，预演应急响应计划

表 A.1（续）

P2DR2	风险处理需求	风险处理措施
响应 Response 恢复 Recovery	故障修复、事故排除	确保随时能够获取故障修复和事故排除的技术人员和软硬件工具
	设施备份与恢复	对于关键设施，配备设施备份与恢复系统
	系统备份与恢复	对于关键系统，配备系统备份与恢复系统
	数据备份与恢复	对于关键数据，配备数据备份与恢复系统
	信道备份与恢复	对于关键信道，配备信道备份与恢复系统
	应用备份与恢复	对于关键应用，配备应用备份与恢复系统
	应急响应	按照应急响应计划处理应急事件
	安全事件处理	按照安全事件处理找出原因、追究责任、总结经验、提出改进

参 考 文 献

[1] GB/T 19715.1—2005 信息技术 信息技术安全管理指南 第1部分:信息技术安全概念和模型(ISO/IEC 13335-1:1996,IDT)

[2] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全(ISO/IEC 2382-8:1998,IDT)

[3] ISO/IEC FCD 27005:Information technology—Security techniques—Information security risk management

[4] NIST Special Publication 800-26:Security Self—Assessment Guide for Information Technology Systems

[5] NIST Special Publication 800-30:Risk Management Guide for Information Technology Systems