ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20985.1—2017/ISO/IEC 27035-1:2016
代替 GB/Z 20985—2007

信息技术　安全技术　信息安全事件管理
第 1 部分:事件管理原理

Information technology—Security techniques—Information security incident management—Part 1:Principles of incident management

(ISO/IEC 27035-1:2016,IDT)

2017-12-29 发布　　2018-07-01 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

GB/T 20985《信息技术　安全技术　信息安全事件管理》分为三个部分：

——第1部分：事件管理原理；

——第2部分：事件响应规划和准备指南；

——第3部分：事件响应操作指南。

本部分为GB/T 20985的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/Z 20985—2007《信息技术　安全技术　信息安全事件管理指南》，与GB/Z 20985—2007相比主要技术变化如下：

——由指导性技术文件改为推荐性国家标准，并拟分为三个部分；

——删除了“业务连续性规划”的术语和定义（见2007年版的3.1）；

——增加了“信息安全调查”“信息安全事件管理”“事件处理”“事件响应”和“联系点”的术语和定义（见3.1、3.5～3.8）；

——将术语“信息安全事件响应组（ISIRT）”改为“事件响应小组（IRT）”，并修改了其定义（见3.2，2007年版的3.4）；

——修改了术语“信息安全事态”和“信息安全事件”的定义（见3.3和3.4，2007年版的3.2和3.3）；

——将“规划和准备”“使用”“评审”和“改进”四个信息安全事件管理过程调整为“规划和准备”“发现和报告”“评估和决策”“响应”和“经验总结”五个信息安全事件管理阶段，并相应调整了其中的主要活动（见第5章，2007年版的5.2和第7章～第10章）。

本部分使用翻译法等同采用ISO/IEC 27035-1:2016《信息技术　安全技术　信息安全事件管理　第1部分：事件管理原理》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇（ISO/IEC 27000:2016，IDT）

本部分由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本部分起草单位：中国电子技术标准化研究院、中电长城网际系统应用有限公司、中国信息安全研究院有限公司。

本部分主要起草人：上官晓丽、闵京华、周亚超、许玉娜、蔡一鸣。

本部分所代替的历次版本发布情况为：

——GB/Z 20985—2007。

引　言

关于 ISO/IEC 27035

仅靠信息安全策略或控制不能保证信息、信息系统、服务或网络得到完全保护。即使采取了控制，仍可能存在残留的脆弱性，使信息安全效果降低，使信息安全事件易于发生，对组织的业务运行存在直接和间接的潜在负面影响。此外，以前未识别的新威胁将不可避免发生。若组织对处理这种事件未做好充分准备，将使任何响应的效果变差，却使对业务的潜在负面影响增加。因此，对于任何期望具有强健信息安全计划的组织，采用结构化和有计划的方法来开展如下活动十分必要：

——发现、报告和评估信息安全事件；

——响应信息安全事件，包括启动适当的控制来防止和降低影响并从中恢复；

——报告信息安全脆弱性，以便对其进行评估和适当处理；

——从信息安全事件和脆弱性中汲取经验教训，建立预防性控制，并改进整体信息安全事件管理方法。

为实现这种有计划的方法，ISO/IEC 27035 的如下部分在信息安全事件管理方面提供相应指南：

——ISO/IEC 27035-1 给出了信息安全事件管理的基本概念和阶段，以及如何改进事件管理。这部分将这些概念与结构化方法的原理相结合来发现、报告、评估和响应事件，并进行经验总结。

——ISO/IEC 27035-2 描述如何规划和准备事件响应。部分涵盖了 ISO/IEC 27035-1 中所给事件管理模型的“规划和准备”和“经验总结”阶段。

与其他标准的关系

ISO/IEC 27035 旨在对其他给出信息安全事件调查及调查准备指南的标准和文件进行补充。ISO/IEC 27035 并不是全部指南，而是某些基本原理的参考，旨在确保选择适当的工具、技术和方法并用于所需目的。

ISO/IEC 27035 涵盖信息安全事件管理的同时，也涵盖了信息安全脆弱性的某些方面。ISO/IEC 29147 和 ISO/IEC 30111 分别对脆弱性披露和供应商处理脆弱性提供了指南。

对于需要确定呈现在其面前的数字证据可靠性的决策者，ISO/IEC 27035 还意在提供指导。它适用于那些需要保护、分析和展示潜在数字证据的组织。它与创建和评价数字证据相关规程的策略决策机构相关，这些机构通常作为更大证据机构的组成部分。

有关调查类标准的进一步信息，参见附录 A。

信息技术　安全技术　信息安全事件管理
第1部分:事件管理原理

1　范围

GB/T 20985的本部分提出了信息安全事件管理的基本概念和过程阶段,并将这些概念与结构化方法的原理相结合来发现、报告、评估和响应事件,以及进行经验总结。

本部分给出的事件管理原理是通用的,适用于任何类型、规模或性质的组织。组织可根据其业务的类型、规模和性质,关联信息安全风险状况,调整本部分给出的指南。本部分也适用于提供信息安全事件管理服务的外部组织。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

ISO/IEC 27035-2　信息技术　安全技术　第2部分:事件响应规划和准备指南(Information technology—Security techniques—Information security incident management—Part 2: Guidelines to plan and prepare for incident response)

3　术语和定义

ISO/IEC 27000界定的以及下列术语和定义适用于本文件。

3.1

信息安全调查　information security investigation

为帮助理解**信息安全事件**(3.4)而进行的检查、分析和解释。

[ISO/IEC 27042,定义3.10,做了修改:将“事件”替换为“信息安全事件”]

3.2

事件响应小组　incident response team

IRT

由组织中具备适当技能且可信的成员组成的团队,负责在事件生存周期中处理事件。

注:IRT通常被称为CERT(计算机应急响应小组)和CSIRT(计算机安全事件响应小组)。

3.3

信息安全事态　information security event

表明一次可能的信息安全违规或某些控制失效的发生。

3.4

信息安全事件　information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的**信息安全事态**(3.3)。

3.5

信息安全事件管理　information security incident management

采用一致和有效方法处理**信息安全事件**(3.4)的行为。

3.6

事件处理　incident handling

发现、报告、评估、响应和处理**信息安全事件**(3.4)并从中汲取经验教训的行动。

3.7

事件响应　incident response

为缓解或解决**信息安全事件**(3.4)而采取的行动,包括为保护信息系统及其存储的信息并将其恢复至正常运行状态而采取的行动。

3.8

联系点　point of contact

PoC

被定义为事件管理活动的协调者或信息聚集点的组织功能或角色。

4　概述

4.1　基本概念和原理

信息安全事态是表明一次可能的信息安全违规或某些控制失效的发生。信息安全事件是达到了既定准则并与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

信息安全事态的发生并不意味着攻击成功或存在保密性、完整性或可用性问题,也就是说,并非所有信息安全事态都属于信息安全事件。

信息安全事件可能是故意的(例如,由恶意软件或故意违纪造成的)或意外的(例如,由意外的人为错误或不可避免的自然行为造成的),可能是由技术手段(例如,计算机病毒)或非技术手段(例如,计算机丢失或被盗)造成的。其后果包括信息未经授权的泄露、修改、破坏或不可用,或者组织信息资产的损坏或被盗。

出于资料性目的,附录 B 选择了一些信息安全事件及其起因的示例进行描述。需要注意的是这些示例并不是全部。

在信息系统、服务或网络中威胁利用脆弱性(弱点),对脆弱性所暴露的信息资产引起信息安全事态的发生并因此可能导致事件。图 1 示出了信息安全事件中对象的关系。

与外部 IRT 的信息共享与协调是重要的考虑方面。许多事件跨越组织边界且不能由单个 IRT 轻易解决。与外部 IRT 的信息共享与协调关系或伙伴关系,可显著提升响应和解决事件的能力。有关信息共享的更多细节,参见 ISO/IEC 27010。

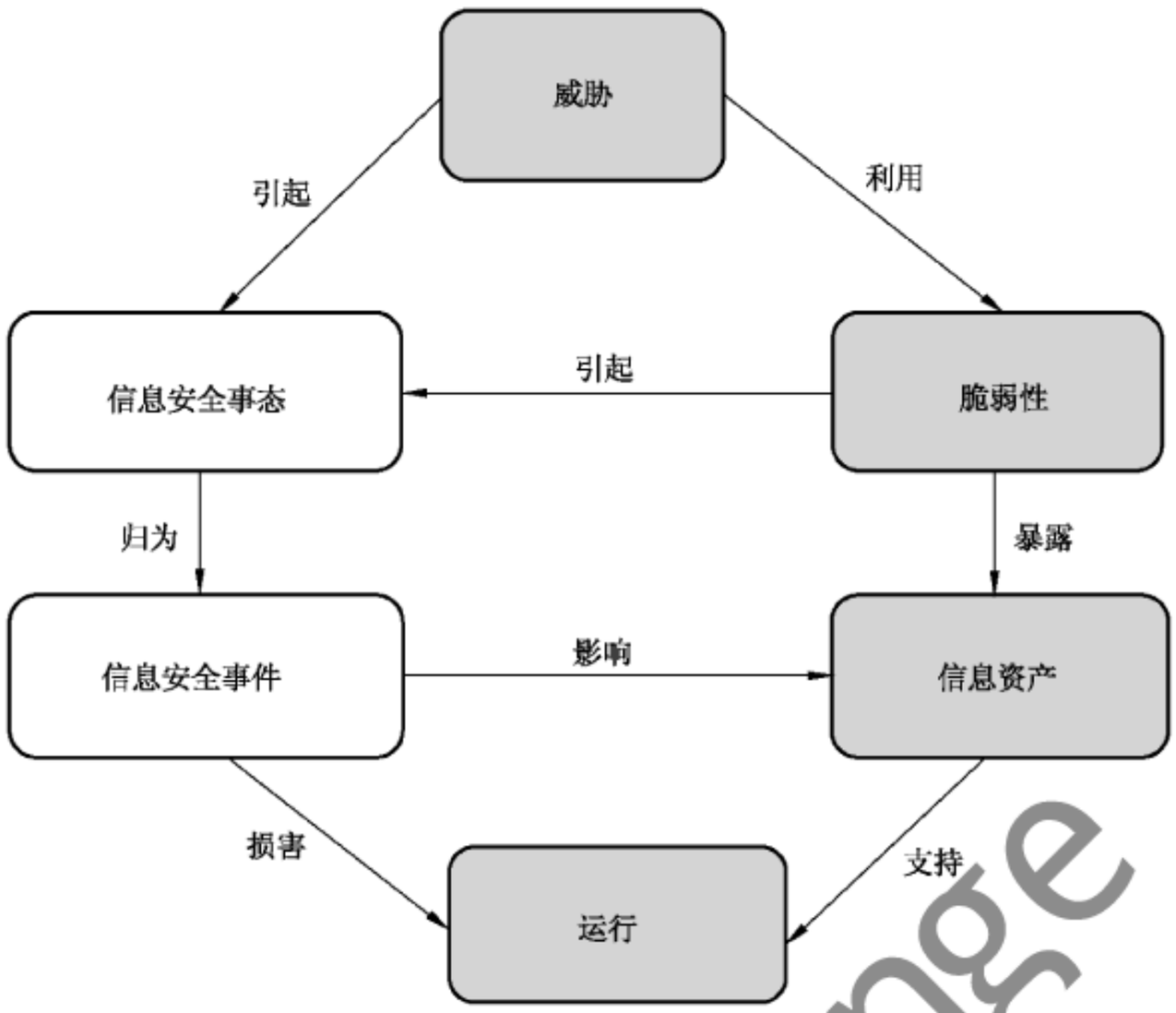

图 1　信息安全事件中对象的关系

4.2　事件管理目标

作为一个组织整体信息安全战略的关键部分，组织宜部署控制和规程来促使一种结构严谨、计划周全的方法进行信息安全事件管理。从组织的角度，其主要目标是避免或遏制信息安全事件的影响，以尽可能减少事件对其运行的直接或间接损害。由于损害信息资产会给运行带来负面影响，运行和业务的视角对于决定更加具体的信息安全管理目标会有重要影响。

一种结构严谨、计划周全的事件管理方法的更加具体目标宜包括：

a）　发现并有效处理信息安全事态，尤其是确定什么时候它们被归为信息安全事件；

b）　以最恰当和有效的方式，对已识别的信息安全事件进行评估和响应；

c）　作为事件响应的一部分，通过恰当的控制尽可能减少信息安全事件对组织及其运行的负面影响；

d）　建立在事件升级过程中与危机管理和业务持续性管理的相关要素的关联；

e）　评估并适当处理信息安全脆弱性，以防止或减少事件。根据职责分配，评估可由 IRT 或组织内其他团队完成；

f）　及时从信息安全事件、脆弱性及其管理中汲取经验教训。这种反馈机制旨在进一步防止信息安全事件未来发生的机会，改进信息安全控制的实施和使用，并整体改进信息安全事件管理方案。

为实现上述目标，组织宜确保信息安全事件以一种一致的方式被记录，并使用适当的标准对事件进行分类、分级和共享，以便经过一段时间后能够从聚合的数据中提取指标。这将为信息安全控制投资的策略决策过程提供有价值的信息。信息安全事件管理体系宜能够与相关外部伙伴和 IRT 共享信息。

本部分的另一个目标是，为致力于满足 ISO/IEC 27001 中规定的信息安全管理体系(ISMS)要求的组织提供指导，这些要求得到 ISO/IEC 27002 指南的支持。ISO/IEC 27001 包括与信息安全事件管理相关的要求。附录 C 给出了 ISO/IEC 27001 中信息安全事件管理条款与本部分条款之间的对照表。图 2 也展示了与 ISMS 的关系。本部分还支持 ISMS 以外的信息安全事件管理体系提出的要求。

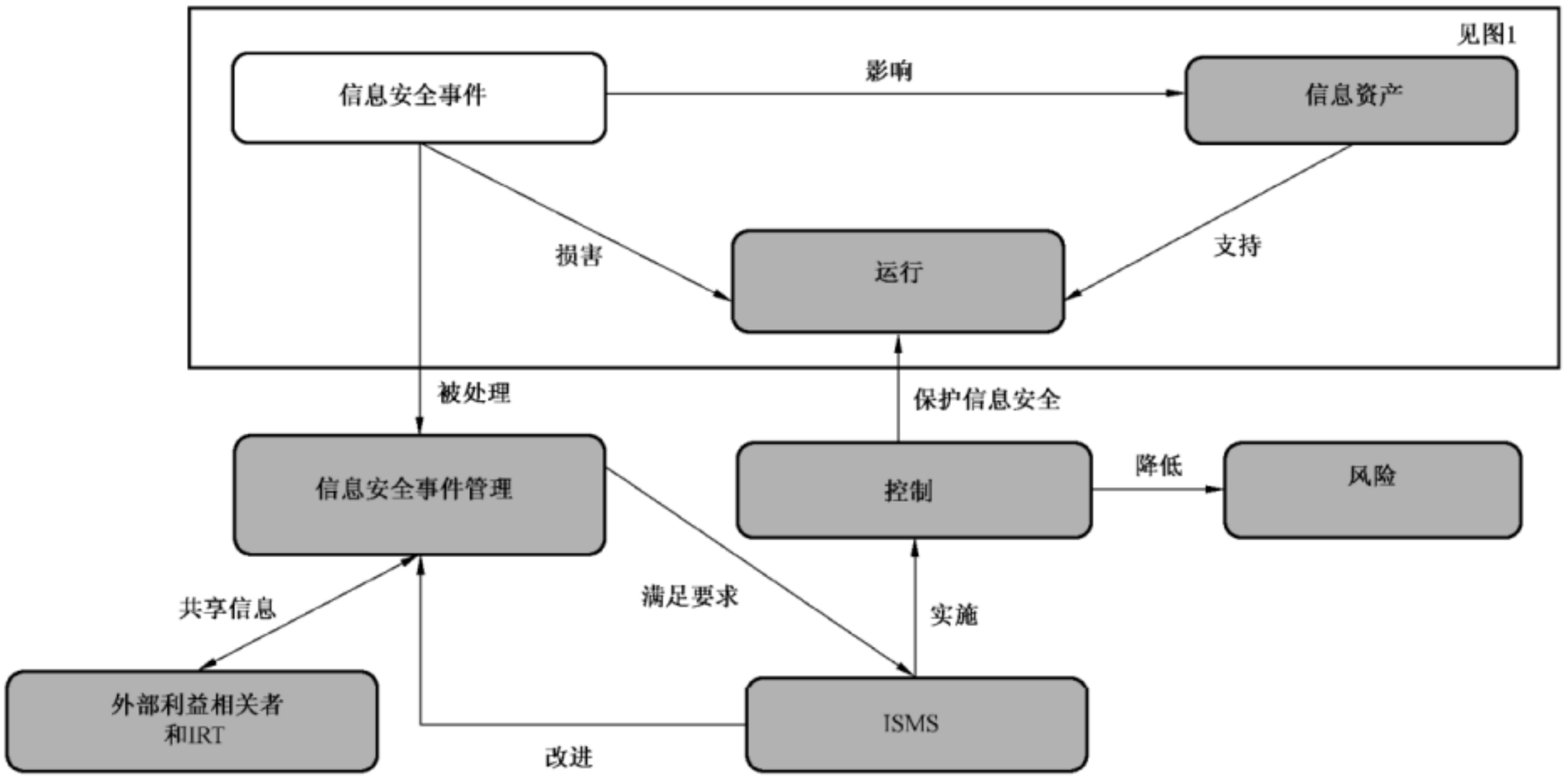

图 2　信息安全事件管理与 ISMS 和所应用控制之间的关系

4.3　结构化方法的益处

使用结构化方法进行信息安全事件管理能产生显著效益，可归纳为如下方面：

a)　改进整体安全

发现、报告、评估和决策信息安全事态和事件的结构化过程能促使快速的识别和响应。这将有助于快速识别和实施一致的解决方案，并因此提供防止将来类似的信息安全事件再次发生的手段，从而提高整体安全性。此外，指标、共享和聚合也带来益处。组织的公信力将通过证明其对信息安全事件管理最佳实践的实现得到提升。

b)　降低对业务的负面影响

结构化的信息安全事件管理方法有助于降低对业务潜在负面影响的程度。这些影响包括直接经济损失和由于声誉与公信力受损而造成的长期损失。有关业务影响分析指南，参见 ISO/IEC 27005。有关业务持续性的信息与通信技术就绪指南，参见 ISO/IEC 27031。

c)　强化对信息安全事件的预防

采用结构化的信息安全事件管理有助于在组织内创造一个以事件预防为重点的氛围，包括识别新的威胁和脆弱性的方法开发。对事件相关数据的分析能够识别事件的模式和趋势，从而帮助更准确地聚焦事件预防，并识别适当措施以防止事件再次发生。

d)　改进优先级

结构化的信息安全事件管理方法为信息安全事件调查时优先级的确定提供可靠基础，包括使用有效的分类和分级方法。如果没有清晰的规程，会存在调查活动可能采取极度反应模式的风险，即当事件发生时才响应并忽视了具有更高优先级的活动。

e)　支持证据收集和调查

必要时，清晰的事件调查规程有助于确保数据的收集和处理是证据充分的、法律允许的。如果随后要进行法律诉讼或纪律处分的话，这些是重点考虑事项。有关更多的数字证据和调查信息，参见附录 A 中列出的调查类标准。

f)　有助于对预算和资源的论证

定义明确且结构化的信息安全事件管理方法，有助于正确判断和简化所涉及组织部门的预算和资源分配。此外，对信息安全事件管理计划自身的益处将显现在更好的人员和资源分配计划。

例如，一种控制并优化预算和资源的方式是给信息安全事件管理任务加“时间戳”，来帮助定量评估组织的信息安全事件处理。它可以提供信息来说明解决不同优先级和不同平台上的事件需要多长时间。如果信息安全事件管理过程中存在瓶颈，也应该是可识别的。

g） 改进信息安全风险评估和管理结果的更新

使用结构化的信息安全事件管理方法有助于：

——收集更好的数据来帮助识别和确定各种威胁类型及相关脆弱性的特征；

——提供有关已识别威胁类型的发生频率的数据。

从信息安全事件中获取的有关对业务运行造成负面影响的数据，对于业务影响分析十分有用。识别各种威胁类型发生频率所获取的数据，有助于提高威胁评估的质量。同样，有关脆弱性的数据，有助于提高未来脆弱性评估的质量。有关信息安全风险评估与管理指南，参见 ISO/IEC 27005。

h） 提供增强的信息安全意识和培训教材

结构化的信息安全事件管理方法使组织能够收集它如何处理事件的经验和知识，这将为信息安全意识教育课程提供有价值的材料。含有实际经验总结的信息安全意识教育课程，有助于减少在未来信息安全事件中的错误或困惑。

i） 为信息安全策略及相关文件评审提供输入

信息安全事件管理计划所提供的数据能为事件管理安全策略（以及其他相关信息安全文件）的有效性评审及随后的改进提供有价值的输入。这可应用在既适用于整个组织又适用于单个系统、服务和网络的主题特定策略及其他文件。

4.4 适应性

ISO/IEC 27035（所有部分）所提供的指南内容丰富，如果全部实施，将占用大量的运行和管理资源。因此，重要的是组织在应用 ISO/IEC 27035 时宜保持一种整体观，并确保用于信息安全事件管理的资源和机制复杂度与以下方面相称：

a） 组织的规模、结构和业务性质，包括宜得到保护的关键资产、过程和数据；

b） 任何用于事件处理的信息安全管理体系的范围；

c） 事件的潜在风险；

d） 业务目标。

因此，组织在使用本部分时宜以一种与其业务规模和特点贴近的方式采用本部分给出的指南。

5 阶段

5.1 概述

为实现 4.2 所述的目标，信息安全事件管理由以下五个不同阶段组成：

——规划和准备（见 5.2）；

——发现和报告（见 5.3）；

——评估和决策（见 5.4）；

——响应（见 5.5）；

——经验总结（见 5.6）。

图 3 给出了这些阶段的高层视图。

一些活动可能发生在多个阶段中或整个事件处理过程。这种活动包括：

——记录事态和事件的证据及关键信息、采取的响应行动以及作为事件处理过程一部分的后续行动；

——在参与方之间进行协调和沟通；

——向管理层和其他利益相关者告知重大事件；

——在利益相关者与内部和外部协作者（诸如供应商和其他 IRT）之间共享信息。

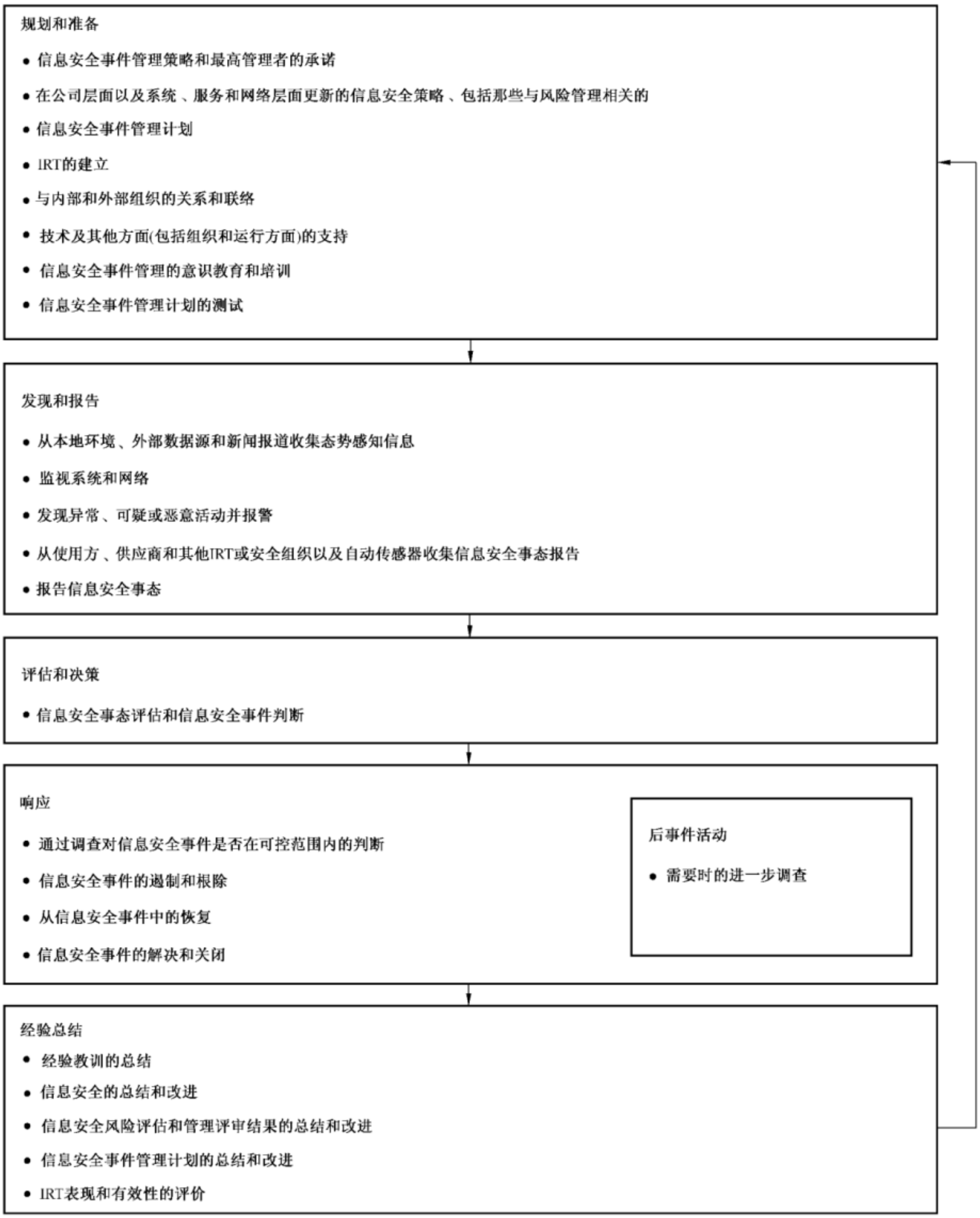

图 3　信息安全事件管理阶段

如引言所述,ISO/IEC 27035 目前分为如下两部分:

——ISO/IEC 27035-1 涵盖所有五个阶段。

——ISO/IEC 27035-2 涵盖:

- 规划和准备;

- 经验总结。

图 4 示出了信息安全事件管理各阶段及相关活动中的信息安全事态和事件流。

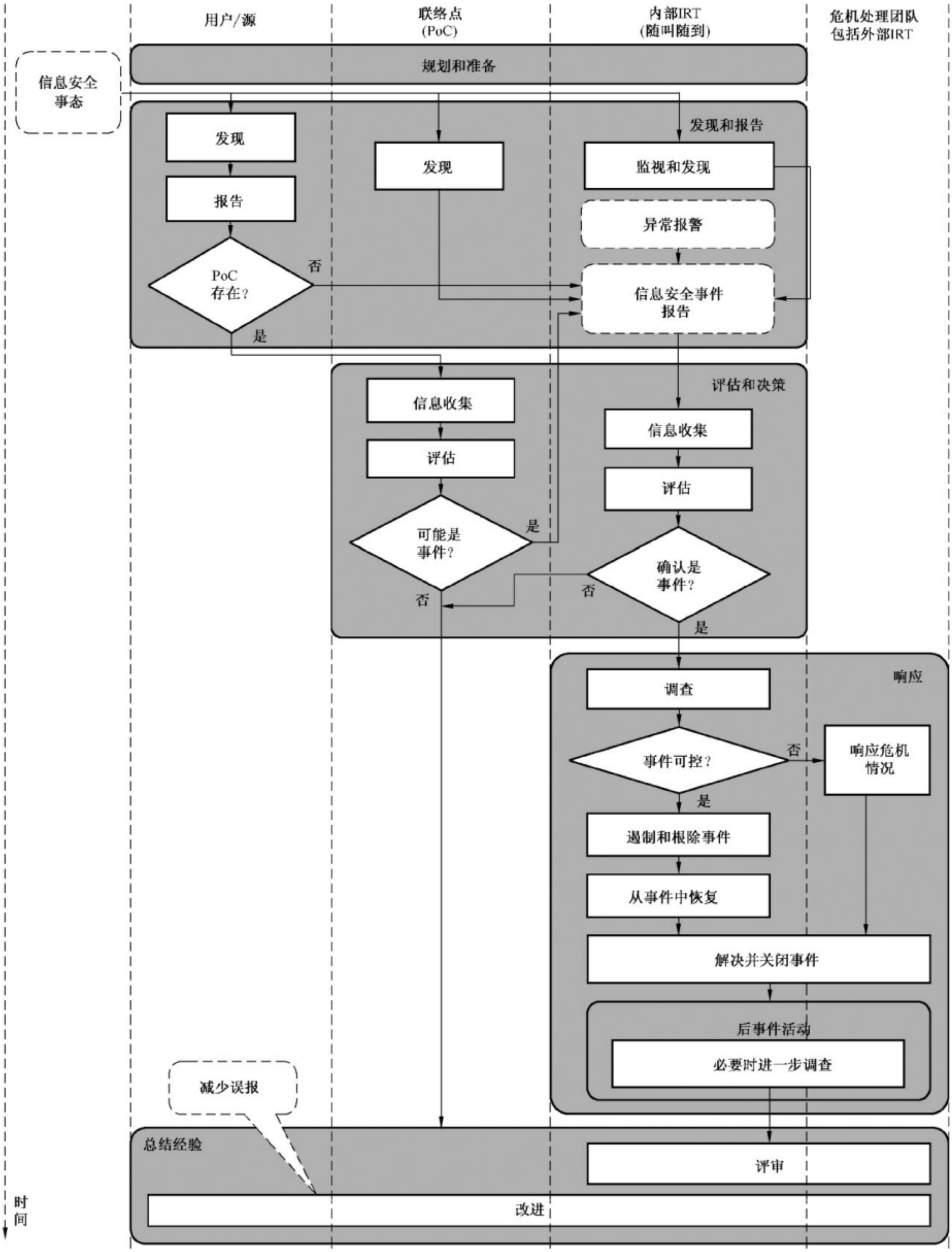

图 4　信息安全事态和事件流图

5.2 规划和准备

有效的信息安全事件管理需要适当的规划和准备。要将一个有效率和效果的信息安全事件管理计划投入运行,组织宜完成一些准备活动,即:

a) 制定和发布信息安全事件管理策略并获得最高管理者的承诺。

b) 在公司层面以及具体的系统、服务和网络层面更新信息安全策略,包括那些与风险管理相关的。

c) 制定详细的信息安全事件管理计划并形成正式文件,包括沟通和信息披露等方面。

d) 建立 IRT,并为其成员设计、开发和提供适当的培训课程。

e) 与直接参与信息安全事态、事件和脆弱性管理的内部和外部组织,建立并保持适当的关系和联络。

f) 建立、实施和运行技术上、组织上和操作上的机制,来支持信息安全事件管理计划和 IRT 的工作。开发和部署必要的信息系统来支持 IRT,包括信息安全数据库。这些机制和系统旨在防止信息安全事件发生或降低信息安全事件发生的可能性。

g) 设计和开发信息安全事态、事件和脆弱性管理的意识教育和培训课程。

h) 测试信息安全事件管理计划及其过程和规程。

本阶段完成后,组织宜对信息安全事件的妥当管理做好了已充分准备。ISO/IEC 27035-2 描述了上述每项活动,包括策略和规划文件的内容。

5.3 发现和报告

信息安全事件管理的第二阶段通过人工或自动手段发现信息安全事态的发生和信息安全脆弱性的存在,收集相关信息并报告。在本阶段中,事态和脆弱性可能尚未被归为信息安全事件。

按照组织的报告策略进行安全事态报告便于在需要时开展后续分析。

在发现和报告阶段,组织宜开展如下关键活动:

a) 适当时,监视并记录系统和网络活动。

b) 通过人工或自动方式,发现并报告信息安全事态的发生或信息安全脆弱性的存在。

c) 收集有关信息安全事态或脆弱性的信息。

d) 从内部和外部数据源收集态势感知信息,包括本地系统和网络的流量和活动日志、可能影响事件活动的当前政治、社会或经济活动的新闻报道、事件趋势的外部报道、新的攻击向量、现有攻击指标以及新的缓解对策和技术。

e) 确保正确地记录所有的活动、结果和相关决策,以便后续分析。

f) 确保安全地收集和存储数字证据,并且持续监控其保存安全,以备法律诉讼或内部纪律处分的证据之需。有关数字证据的识别、收集、获取和保全的更详细信息,参见附录 A 中列出的调查类标准。

g) 确保变更控制机制得到遵循,以使信息安全事态和脆弱性能够得到跟踪,报告得到更新,并保持信息安全数据库处于最新状态。

h) 本阶段需要的时候,升级去做进一步的评审或决策。

所有收集到的信息安全事态或脆弱性相关信息宜存储在由 IRT 管理的信息安全数据库中。在每项活动期间报告的信息宜尽可能做到当时是完整的,以支持评估、决策和所采取的行动。

5.4 评估和决策

信息安全事件管理的第三阶段对信息安全事态发生的相关信息进行评估,并判断是否将事态归为信息安全事件。

一旦信息安全事态被发现和报告，宜进行如下后续活动：

a) 对参与评估、决策和行动的人员（包括安全和非安全领域人员），通过适当的层次结构，分配信息安全事件管理活动的责任。

b) 为每一个被通知的人员提供遵从的正式规程，包括评审和修改报告，评估损害和通知相关人员。单个人的行动将取决于事件的类型和严重性。

c) 按照指南对信息安全事态以及在被归为信息安全事件后的后续行动进行完整的文档化。

在评估和决策阶段，组织宜进行如下关键活动：

d) 收集信息，可包括信息安全事态发现时采集到的测试、测量和其他数据。收集到的信息类型和数量将取决于已发生的信息安全事态。

e) 由事件处理者进行评估，来确定该事态是否可能是或被确认为信息安全事件，或者是一次误报。误报（即假阳性）表明所报告的事态是不真实的或无任何后果。如果需要的话，IRT 可进行质量评审以确保事件处理者的事件声明是正确的。

f) 确保所有参与方，特别是 IRT，正确地记录了所有活动、结果和相关决策以便后续分析。

g) 确保变更控制机制得到保持，以便涵盖住信息安全事态和脆弱性的跟踪以及事件报告的更新，并保持信息安全数据库处于最新状态。

所有收集到的信息安全事态、事件或脆弱性相关信息宜存储在由 IRT 管理的信息安全数据库中。在每项活动期间报告的信息宜尽可能做到当时是完整的，以支持评估、决策和所采取的行动。

5.5 响应

信息安全事件管理的第四阶段按照在评估和决策阶段所决定的行动响应信息安全事件。响应可能是立即的、实时的或接近实时的，并且一些响应可能包含信息安全调查，这些均取决于决策。

一旦信息安全事件被确认且响应被确定，宜进行如下后续活动：

a) 对参与决策和行动的人员（包括安全和非安全领域人员）通过适当的层次结构，分配信息安全事件管理活动的责任。

b) 为每一个参与人员提供遵从的正式规程，包括评审和修改报告，再评估损害和通知相关人员。单个人的行动将取决于事件的类型和严重性。

c) 按照指南对信息安全事件和后续行动进行完整的文档化。

在响应阶段，组织宜进行如下关键活动：

d) 根据需要并相对于信息安全事件分级的级别评分，对事件进行调查。必要时宜变更级别。调查可包括各种类型的分析来提供对事件更深入的理解。

e) 由 IRT 评审来确定信息安全事件是否在可控范围内，如果是，则执行所需的响应。如果事件不在可控范围内或将对组织运行产生严重影响，则通过升级到危机处理模式来执行危机响应活动。

f) 分配内部资源并识别外部资源来响应事件。

g) 本阶段需要的时候，升级去做进一步的评审或决策。

h) 确保所有参与方，特别是 IRT，正确地记录了所有活动以便后续分析。

i) 确保安全地收集和存储数字证据，并且持续监控其保存安全，以备法律诉讼或内部纪律处分的证据之需。有关数字证据的识别、收集、获取和保全的更详细信息，参见附录 A 中列出的调查类标准。

j) 确保变更控制机制得到保持，以便涵盖住信息安全事态和脆弱性的跟踪以及事件报告的更新，并保持信息安全数据库处于最新状态。

k) 按照组织及 IRT 沟通计划和信息披露策略，与其他内部的和外部的人员或组织，就信息安全事件的存在进行沟通，并共享任何相关细节（例如，威胁、攻击和脆弱性信息）。尤为重要的是，

通知资产所有者(在影响分析期间确定的)以及内部和外部组织(例如,其他事件响应团队、执法机构、互联网服务提供商和信息共享组织),以便获得对事件管理和解决的帮助。由于同样的威胁和攻击经常影响多个组织,共享信息也会给其他组织带来益处。有关信息共享的更多细节,参见 ISO/IEC 27010。

l) 从事件中恢复后,宜根据事件的性质和严重性启动后事件活动,包括:

——事件相关信息的调查;

——其他相关原因(诸如涉及人员)的调查;

——调查结果的总结报告。

m) 一旦事件已得到解决,宜按照 IRT 或上级组织的要求关闭该事件处理,并通知所有利益相关者。

所有收集到的信息安全事态、事件或脆弱性相关信息宜存储在由 IRT 管理的信息安全数据库中。在每项活动期间报告的信息宜尽可能做到当时是完整的,以支持评估、决策和所采取的行动,包括潜在的进一步分析。

5.6 经验总结

信息安全事件管理的第五个阶段始于信息安全事件已得到解决。这个阶段从事件(和脆弱性)如何得到处理中汲取经验教训。

在经验总结阶段,组织宜进行如下关键活动:

a) 从信息安全事件和脆弱性中汲取经验教训。

b) 评审、识别和改进信息安全控制的实施(新的或更新的控制),以及信息安全事件管理策略。经验可来自一个或多个信息安全事件或报告的安全脆弱性。组织策略中有关信息安全控制投入的指标有助于改进。

c) 评审、识别和改进组织现有的信息安全风险评估和管理评审。

d) 评审过程、规程、报告格式和组织结构在响应和评估信息安全事件并从中恢复以及处理信息安全脆弱性方面的有效性。基于经验总结,识别和改进信息安全事件管理计划及其文档化。

e) 与可信团体沟通和共享评审结果(如果组织有此意愿的话)。

f) 决定事件信息、相关攻击向量和脆弱性是否可共享给合作伙伴组织,以为防止相同事件在他们的环境中重演提供帮助。有关更多细节,参见关于信息共享的 ISO/IEC 27010。

g) 对 IRT 表现和有效性进行周期性的综合评价。

需要强调的是,信息安全事件管理活动是迭代的,因此组织宜随时间推移定期改进一些信息安全要素。这些改进宜基于对有关信息安全事件、响应和报告的信息安全脆弱性的数据进行评审来提出。

ISO/IEC 27035-2 详细描述了上述每项活动。

附 录 A
（资料性附录）
与调查类标准的关系

本部分所描述的是综合调查过程的一部分。综合调查过程包括（但不限于）如下标准的应用：

——ISO/IEC 27037 数字证据的识别、收集、获得和保全指南

该标准描述了在调查初期（包括初始响应）介入的手段，以便能够确保获取充分的潜在证据来使调查恰当地进行。

——ISO/IEC 27038 数字脱敏规范

某些文件可能包含不宜向某些社群披露的信息。可以经过对原始文件进行适当处理后，将修改版向这些社群发布。移除不应披露信息的过程被称为“脱敏”。

文件的数字脱敏是文件管理实践中一个相对较新的领域，并由此引起独特问题和潜在风险。当数字文件被脱敏后，被移除的信息不宜被恢复。因此，需要小心从事，以使被脱敏的信息从数字文件中被永久移除（例如，不宜简单地隐藏在文件不可显示的部分中）。

该标准规范了数字文件的数字脱敏方法，还规范了对脱敏软件的要求。

——ISO/IEC 27040 存储安全

该标准为组织如何通过在规划、设计、记录和实现数据存储安全时，利用一种已被充分证明且一致的方法来确定适当的风险缓解程度，提供了详细的技术指导。存储安全应用于所存储信息的保护（安全）以及与存储相关的跨通信链路被传输信息的安全。存储安全包括在设备和介质有效期间及使用终结后设备和介质的安全、与设备和介质相关的管理活动的安全、应用和服务的安全以及与终端用户相关的安全。

像加密和清除这样的安全机制，因引入混淆机制，会影响一个人的调查能力，宜在调查前和调查中予以考虑。安全机制在确保调查中和调查后的证据材料存储得到充分的准备和保护方面也是重要的。

——ISO/IEC 27041 确保事件调查方法适宜性和充足性的指南

重要的是能够证明在调查中所采取的方法和过程是适当的。该标准为如何保证方法和过程满足调查的要求并得到适当的测试提供指导。

——ISO/IEC 27042 数字证据分析和解释指南

该标准描述了如何将调查中所使用的方法与过程设计和实现成能够正确评价潜在数字证据，解释数字证据，并有效报告调查结果。

——ISO/IEC 27043 事件调查原则和过程

该标准定义了事件调查背后关键的共同原则和过程，并为所有调查阶段提出了框架模型。

——ISO/IEC 27050 电子发现

该标准提出了电子发现中的活动，包括（但不限于）电子存储信息（ESI）的识别、保全、收集、处理、评审、分析和产出。此外，它还提供了从 ESI 初始生成至其最终处置的测量验证指导，组织可依此来降低电子发现的风险和开销。该标准与参与电子发现的某些或全部活动的非技术和技术人员均有关。值得注意的是该指南无意于与当地司法管辖区的法律法规冲突或取而代之。

电子发现常常会推动调查以及证据获取和处理活动。此外，数据的敏感性和重要性需要采取像存储安全这样的保护来防范数据泄露。

——ISO/IEC 30121 数字取证风险治理框架

该标准为组织治理者（包括所有者、董事会成员、主管、合作伙伴、高级管理人员，或同类人员）以最佳方式准备组织的数字调查提供了框架。该标准应用于制定有关数字证据披露的保留、可用性、访问和成本效益的战略过程（和决策），适用于所有类型和规模的组织，为组织的数字调查提供稳健的战略准

备。取证就绪确保组织为接受具有证据性的潜在事态做好了适当及相关的战略准备。当出现不可避免的安全违规、欺诈和名誉侵权时便可采用行动。在任何情况下,宜战略性地部署信息技术(IT),使证据的可用性、可及性和成本效益产生最大效果。

图 A.1 展示了围绕事件及其调查的典型活动。图中数字(例如,27037)表示上述列出的标准,其旁带有不同阴影的条表示该标准对调查过程或是最可能直接适用或是具有某种影响(例如,建立策略或产生约束)。建议在规划和准备阶段开始前和进行中都宜参考所有这些标准。图中所示的过程类在 ISO/IEC 27043 中有全面定义,与之匹配的各项活动在 ISO/IEC 27035-2、ISO/IEC 27037、ISO/IEC 27042 和 ISO/IEC 27041 中有更为详细的论述。

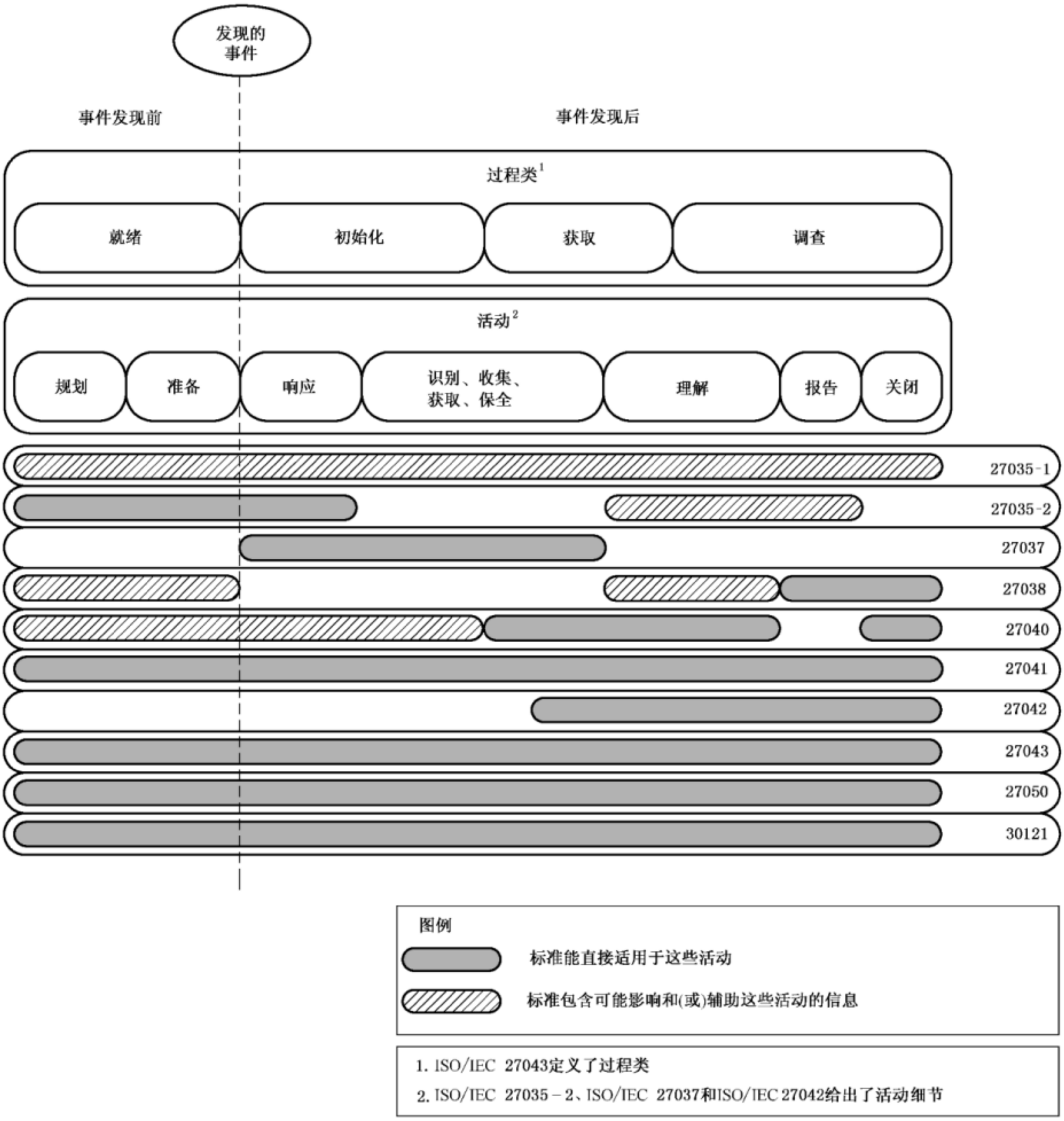

图 A.1 调查过程类和活动相关标准的适用性

附 录 B
（资料性附录）
信息安全事件及其起因示例

B.1 攻击

B.1.1 拒绝服务

拒绝服务(DoS)和分布式拒绝服务(DDoS)是事件的一个大类，具有共同点。这类事件导致系统、服务或网络失败，不能按其预期能力持续运行，经常导致合法用户完全不能访问。技术手段导致的DoS/DDoS事件类型主要有两种：资源消除和资源耗尽。

故意的技术型DoS/DDoS事件的典型例子包括：

——侦测网络广播地址，用响应流量占满网络带宽；

——向系统、服务或网络发送意外格式的数据，试图至其崩溃或扰乱其正常运行；

——开启特定系统、服务或网络的多个授权会话，试图耗尽其资源(即，至其慢速、锁定或崩溃)。

这种攻击经常通过僵尸工具来进行，即一个运行了恶意软件受僵尸网络控制的计算机系统。僵尸网络是受人集中控制的僵尸命令和控制网络。僵尸网络的规模可从数百台到数百万台受感染的计算机。

某些技术型DoS事件可能是意外造成的，例如，操作员的错误配置或应用软件的不兼容，但多数时候是故意的。某些技术型DoS事件是被有意发起的，目的在于导致系统、服务或网络崩溃，而其他那些仅是其他恶意活动的副产品。例如，某些较常见的隐形扫描和识别技术可能会导致旧的或错误配置的系统或服务在扫描时崩溃。值得注意的是，许多故意的技术型DoS事件往往是匿名执行的(即攻击源是“伪造的”)，因为它们通常不需要攻击者从受攻击的网络或系统接收任何反馈信息。

非技术手段导致的DoS事件，造成信息、服务和(或)设施损失，可能由如下示例引起：

——违反物理安全规定，造成设备的失窃或故意损坏和破坏；

——由火灾或水灾导致的对硬件[和(或)其位置]的意外损坏；

——极端的环境条件，例如，高运行温度(如因空调故障)；

——系统故障或过载；

——不受控的系统变更；

——软件或硬件故障。

B.1.2 未授权访问

通常，这类事件包括在实际未授权的情况下尝试访问或误用系统、服务或网络。技术型未授权访问事件的一些例子包括：

——试图找回密码文件；

——缓冲区溢出攻击，试图获得对目标的特权(例如，系统管理员)访问；

——利用协议漏洞，劫持或误导合法的网络连接；

——试图提升对资源或信息的访问特权，以致超出一个用户或管理员已经合法所拥有的。

非技术手段导致的未授权访问事件，造成直接或间接的信息泄露或篡改、责任违约或信息系统误用，可能由如下示例引起：

——违反物理安全规定，造成对信息的未经授权访问；

——由于系统变更不受控或者软件或硬件故障，致使操作系统配置不当和(或)错误。

B.1.3 恶意软件

恶意软件是指一个程序或一个程序的部分被插入另外一个程序中，意在修改原来的行为，通常进行恶意活动，诸如盗用信息和身份、破坏信息和资源、拒绝服务，发送垃圾邮件等。恶意软件攻击可分为五类：病毒、蠕虫、特洛伊木马、移动代码和混合攻击。其中，病毒旨在植入任何易受感染的系统，而其他恶意软件被用于针对特定目标进行攻击。这有时通过修改现有的恶意软件，生成不易被恶意软件检测技术认出的变体的方式进行。

B.1.4 滥用

这类事件通常是因用户违背组织信息系统安全策略造成的。严格来说，这种事件并不是攻击，但通常作为事件来报告且宜由 IRT 管理。不当使用可包括：

——下载并安装黑客工具；

——利用企业电子邮件发送垃圾邮件或推广个人业务；

——利用公司资源建立未经授权的网站；

——利用对等网络(P2P)获取或发布盗版文件(音乐、视频、软件)。

B.2 信息收集

通常，信息收集类事件包括识别潜在目标，了解这些目标上运行的服务等相关活动。这类事件涉及以识别如下信息为目标的侦测：

——存在的目标及其周边的网络拓扑结构和与其日常通信的对象；

——目标或其即时网络环境中可能被利用的潜在脆弱性。

通过技术手段进行信息收集攻击的典型例子如下：

——镜像目标互联网域的域名系统(DNS)记录(DNS 区域传输)；

——侦测网络地址以发现活跃的系统；

——探测系统以识别(例如，采集痕迹)主操作系统；

——扫描系统上的可用的网络端口来识别网络服务[例如，电子邮件、文件传输协议(FTP)，网页等]，以及这些服务的软件版本；

——在网络地址范围中扫描一个或多个已知的易受攻击的服务(水平扫描)。

在某些情况下，技术型的信息收集可能会导致未授权访问。例如，攻击者在搜索脆弱性时还会试图获得未授权访问。这通常发生在使用自动化工具。自动化工具不仅搜索脆弱性，还自动地试图发现并利用系统、服务或网络中的脆弱性。

非技术手段导致的信息收集事件，会造成如下后果：

——直接或间接的信息泄露或篡改；

——电子化存储的知识产权的被盗；

——责任违约，例如，在账户记录中的责任违约；

——信息系统滥用(例如，违反法律或组织策略)。

信息收集事件可能由如下原因(示例)导致：

——违反物理安全规定，造成对信息的非授权访问，以及含有重要数据(例如，密钥)的数据存储设备失窃；

——由于系统变更不受控或者软件或硬件故障，致使操作系统配置不当和(或)错误，进而导致内部或外部人员获得额外的信息访问权限；

——社会工程，一种操纵人们行动或泄露机密信息的行为，例如，网络钓鱼。

附 录 C
（资料性附录）
ISO/IEC 27001 与 ISO/IEC 27035 对照表

ISO/IEC 27001 与 ISO/IEC 27035 对照表见表 C.1。

表 C.1 ISO/IEC 27001 与 ISO/IEC 27035 对照表

ISO/IEC 27001:2013	ISO/IEC 27035
A.16 信息安全事件管理	ISO/IEC 27035-1： 4 概述(信息安全事件管理概述)
A.16.1 信息安全事件的管理和改进 目标：确保采用一致和有效的方法对信息安全事件进行管理，包括对安全事态和弱点的沟通	ISO/IEC 27035-1： 5 阶段(信息安全事件管理阶段) 附录 B (资料性附录)信息安全事件及其起因示例 ISO/IEC 27035-2： 附录 A (资料性附录)法律法规方面 附录 B (资料性附录)信息安全事态、事件和脆弱性报告及其模板示例 附录 C (资料性附录)信息安全事态和事件的分类和分级方法示例
A.16.1.1 责任和规程 控制：应建立管理责任和规程，以确保快速、有效和有序地响应信息安全事件	ISO/IEC 27035-1： 5.2 规划和准备 5.4 评估和决策 a)，b) ISO/IEC 27035-2： 4 信息安全事件管理策略 5 更新信息安全策略 6 制定信息安全事件管理计划 7 建立事件响应小组(IRT) 8 建立与其他组织关系 9 确定技术及其他支持 10 创建信息安全事件意识教育和培训
A.16.1.2 报告信息安全事态 控制：应通过适当的管理渠道尽快地报告信息安全事态	ISO/IEC 27035-1： 5.3 发现和报告
A.16.1.3 报告信息安全弱点 控制：应要求使用组织信息系统和服务的员工和合同方注意并报告任何观察到的或可疑的系统或服务中的信息安全弱点	ISO/IEC 27035-1： 5.4 评估和决策
A.16.1.4 信息安全事态的评估和决策 控制：应评估信息安全事态并决定其是否属于信息安全事件	ISO/IEC 27035-1： 5.4 评估和决策
A.16.1.5 信息安全事件的响应 控制：应按照文件化的规程响应信息安全事件	ISO/IEC 27035-1： 5.5 响应

表 1（续）

ISO/IEC 27001:2013	ISO/IEC 27035
A.16.1.6　从信息安全事件中学习 控制：应利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响	ISO/IEC 27035-1： 5.6　经验总结 ISO/IEC 27035-2： 12　经验总结
A.16.1.7　证据的收集 控制：组织应确定和应用规程来识别、收集、获取和保存可用作证据的信息	ISO/IEC 27035-1： 5.3　发现和报告　d)，g) 5.4　评估和决策　d)，g) 5.5　响应　d)，i)，l)

参 考 文 献

[1] ISO/IEC 20000 (all parts) Information technology—Service management

[2] ISO/IEC 27001 信息技术 安全技术 信息安全管理体系 要求(Information technology—Security techniques—Information security management systems—Requirements)

[3] ISO/IEC 27002 信息技术 安全技术 信息安全控制实践指南(Information technology—Security techniques—Code of practice for information security controls)

[4] ISO/IEC 27003 信息技术 安全技术 信息安全管理体系实施指南(Information technology—Security techniques—Information security management system implementation guidance)

[5] ISO/IEC 27004 信息技术 安全技术 信息安全管理 测量(Information technology—Security techniques—Information security management—Measurement)

[6] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理(Information technology—Security techniques—Information security risk management)

[7] ISO/IEC 27010 信息技术 安全技术 行业间和组织间通信的信息安全管理(Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications)

[8] ISO/IEC 27031 Information technology—Security techniques—Guidelines for information and communication technology readiness for business continuity

[9] ISO/IEC 27033-1 Information technology—Security techniques—Network security—Part 1:Overview and concepts

[10] ISO/IEC 27033-2 Information technology—Security techniques—Network security—Part 2:Guidelines for the design and implementation of network security

[11] ISO/IEC TS 27033-3 Information technology—Security techniques—Network security—Part 3:Reference networking scenarios—Threats,design techniques and control issues

[12] ISO/IEC 27037 Information technology—Security techniques—Guidelines for identification,collection,acquisition and preservation of digital evidence

[13] ISO/IEC 27039 Information technology—Security techniques—Selection,deployment and operations of intrusion detection systems (IDPS)

[14] ISO/IEC 27041 Information technology—Security techniques—Guidance on assuring suitability and adequacy of incident investigative method

[15] ISO/IEC 27042 Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence

[16] ISO/IEC 27043 Information technology—Security techniques—Incident investigation principles and processes

[17] ISO/IEC 29147 Information technology—Security techniques—Vulnerability disclosure

[18] ISO/IEC 30111 Information technology—Security techniques—Vulnerability handling processes

中华人民共和国
国家标准
信息技术　安全技术　信息安全事件管理
第1部分：事件管理原理
GB/T 20985.1—2017/ISO/IEC 27035-1:2016
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2018年1月第一版
*
书号：155066·1-59301

GB/T 20985.1-2017