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。

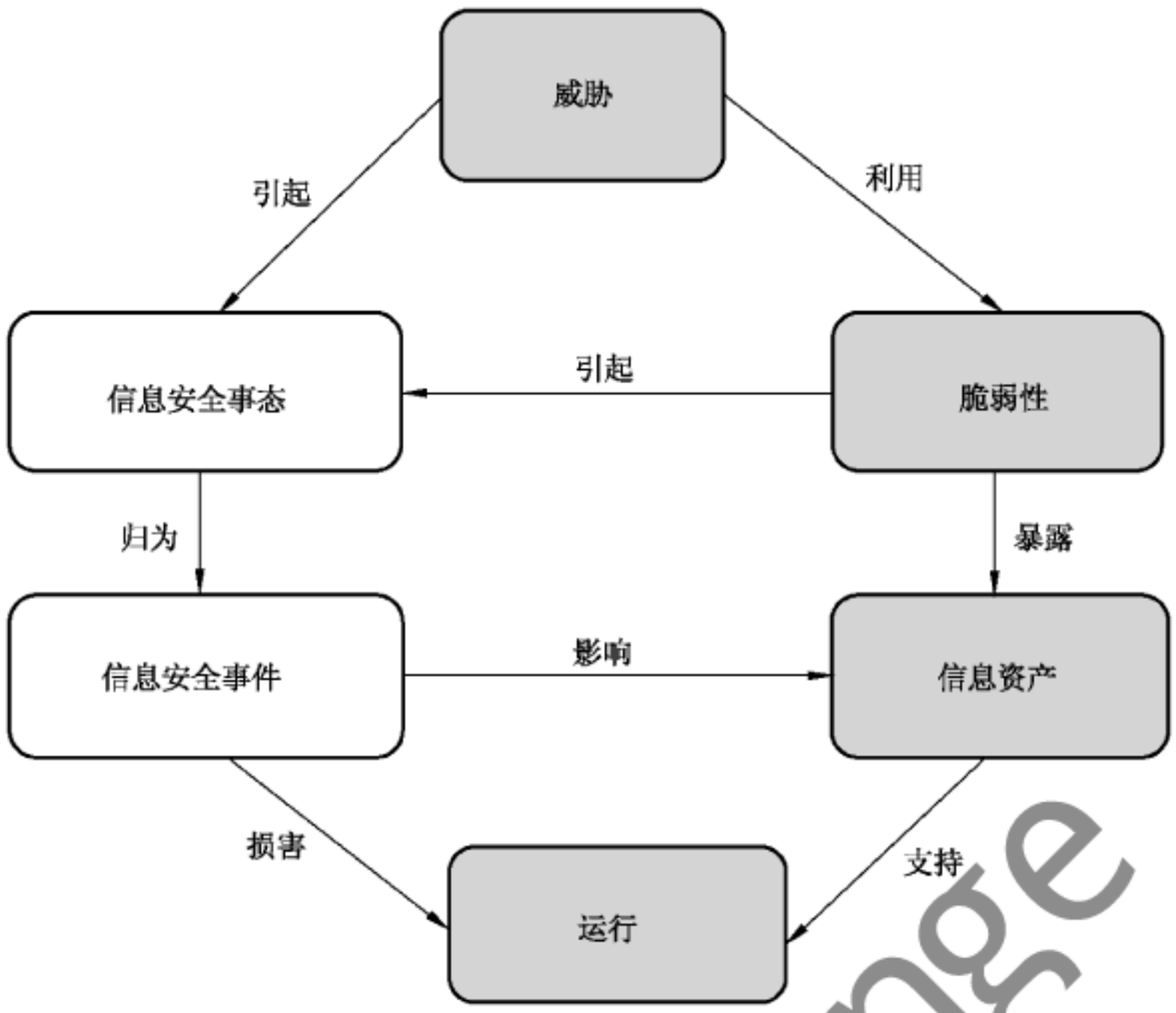

图 1　信息安全事件中对象的关系

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。

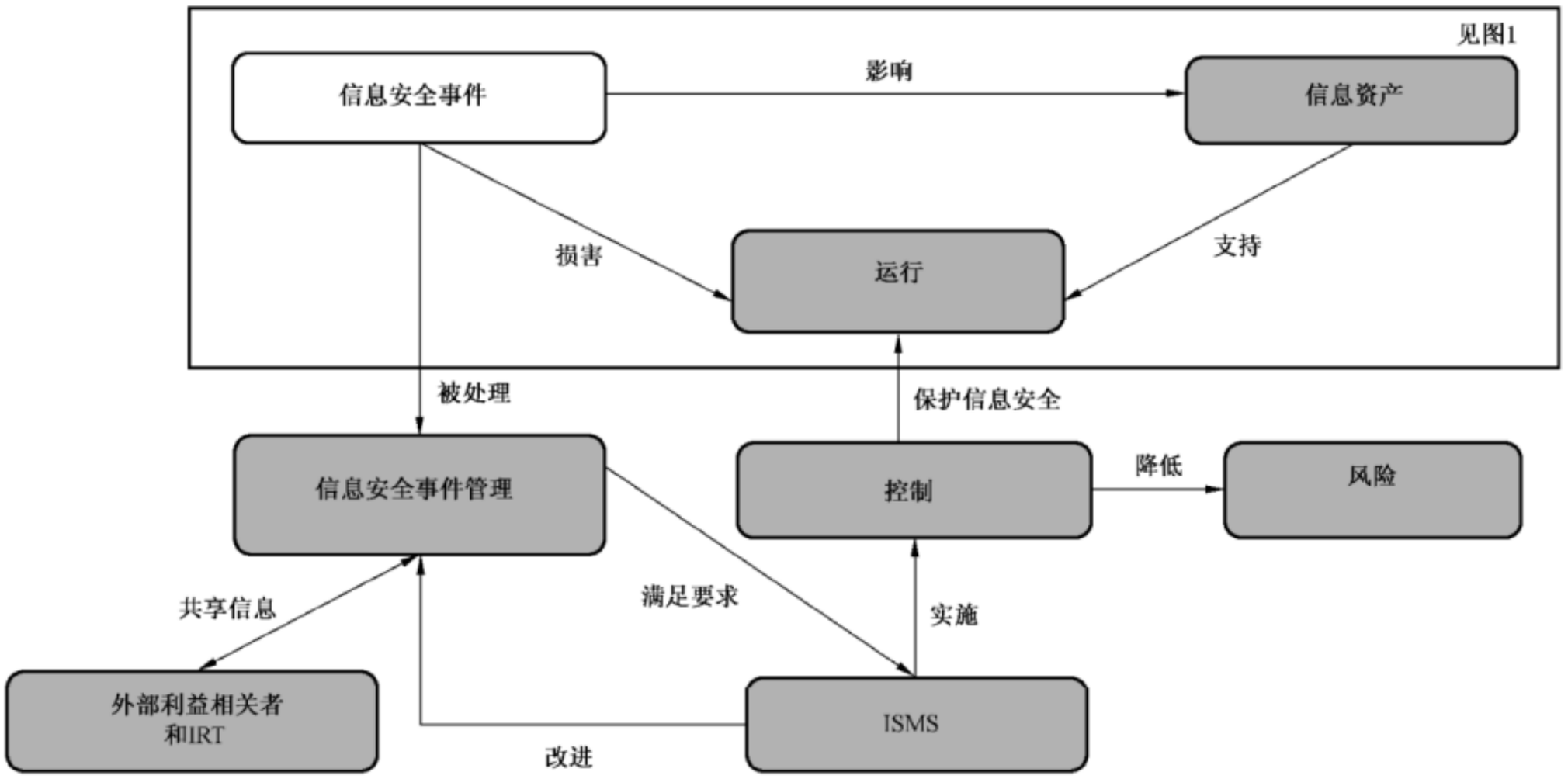

图 2　信息安全事件管理与 ISMS 和所应用控制之间的关系

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。

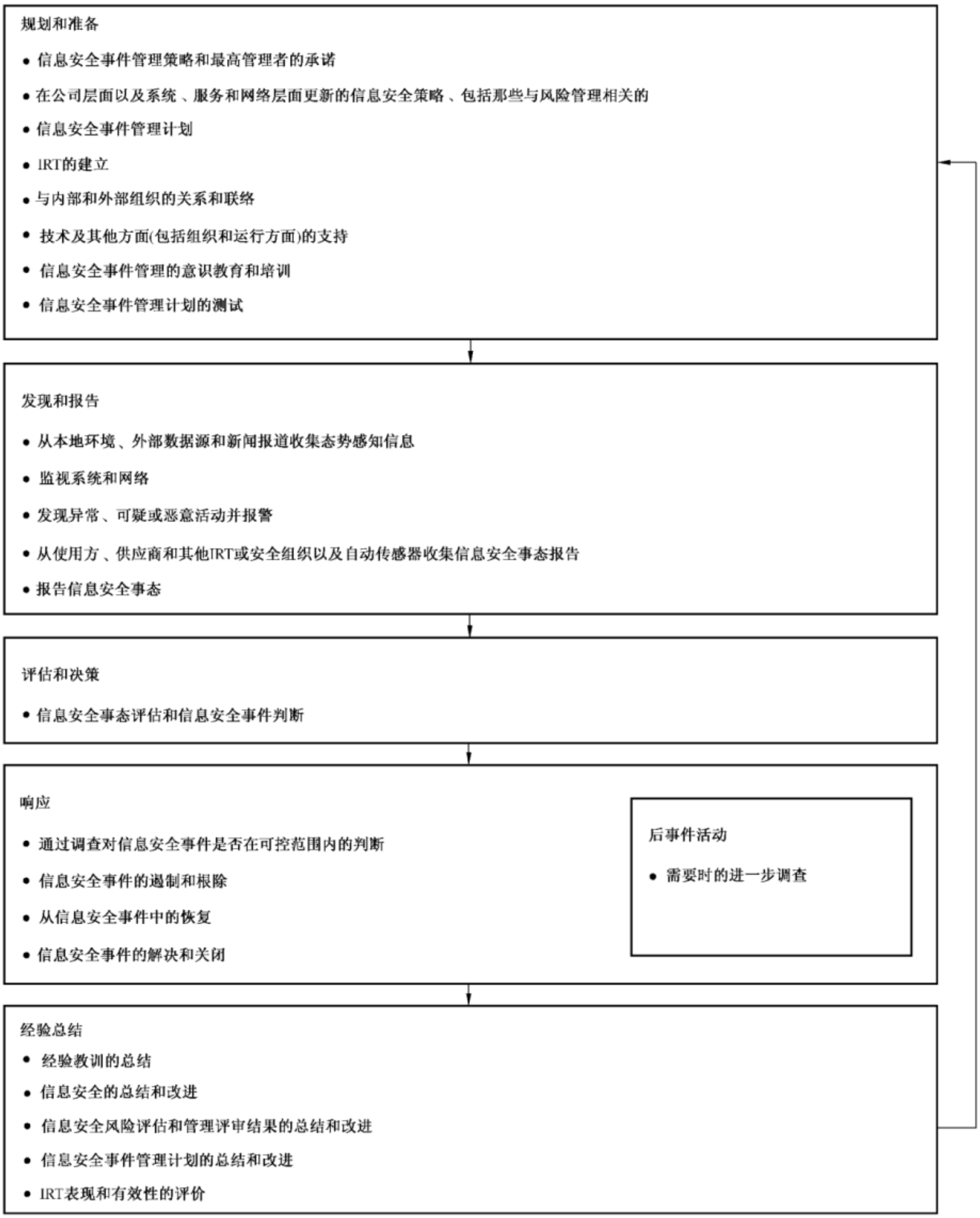

图 3　信息安全事件管理阶段

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;