第 3 章

风险管理与安全管理体系

随着互联网和信息技术的快速发展，大数据和人工智能不断影响着人们的生活，在医疗、制造业、服务业、城市治理等领域数字化转型发挥着关键的作用，同时也引入了新风险。

风险管理的目的是以风险控制的合理成本，将风险可能带来的利益最大化，将风险可能导致的损失最小化，并在控制成本、潜在利益和潜在损失三者之间进行权衡。风险管理过程包括语境建立、风险评估、风险处置、批准监督、监控审查和沟通咨询等方面。作为风险管理的一个重要环节，风险评估使得组织能准确“定位”风险处置的策略、措施和实践，能将安全活动的重点放在重要问题上，能选择成本效益合理的和适用的安全策略。

本章以风险为主线，从理解风险、管理风险到建立安全管理体系，帮助读者树立数智安全风险管理意识，了解数智安全风险管理方法，理解和应用信息安全管理体系。

3.1 风险管理基础

3.1.1 基本概念

风险是事物可能面临特定情形发生的一种潜在状态。与之相对，事件是事物已经面临特定情形发生的一种显在状态。当特定情形处于未发生状态时是风险，而当特定情形处于已发生状态时便是事件。风险是事件产生的前提，事件是在一定条件下由风险演变而来的。由此可见，风险与事件是因果关系。风险的正面影响产生正面结果，即利益；负面影响产生负面结果，即损失。因此，风险既可以是正面的也可以是负面的，也就是人们常说的：机遇与挑战并存。所谓机遇是对正面结果而言，所谓挑战是对负面结果而言。

在管理学中，管理被定义为：通过规划、组织、领导、沟通和控制等环节来协调人力、物力、财力等资源，以期有效达成组织目标的过程。管理的特征表现为：在群体活动中，在特定环境下，针对给定对象，遵循确定原则，运用恰当方法，按照规定程序，利用可用资源，进行一组活动（包括规划、组织、指导、沟通和控制等），完成各项任务，评价执行成效，实现既定目标。

管理是一种过程，应采用过程方法。为了组织的有效运行，需要识别和管理许多活动。过程是指一组相互关联或相互作用的活动完成输入到输出的转换。这种转换通常是在计划和受控的条件下，使用一定的资源来进行。过程关联分为串联和分解两种形式。过程串联是指一个过程的输出可直接形成另一个过程的输入；过程分解是指过程中的活动也是一个过程，即一个过程可分解成多个子过程。

有了“风险”和“管理”的概念，“风险管理”可被定义为“对风险的管理”。风险管理的目

的是以风险控制的合理成本，将风险可能带来的利益最大化，将风险可能导致的损失最小化，并在控制成本、潜在利益和潜在损失三者之间进行权衡。而信息安全风险，指威胁主体可能利用信息、信息系统或支撑环境的脆弱性，对信息、信息系统和支撑环境实施威胁行为，可能造成负面影响。依据 ISO 31000:2018《风险管理指南》的定义，风险是指不确定性对目标的影响，风险管理是指组织指导和控制风险的协调活动。风险管理的目的是创造和保护价值，以提高绩效、鼓励创新和支持目标的实现。

3.1.2　原则

风险管理原则是风险管理的基础，在建立组织的风险管理框架和过程时应予以考虑，使组织能够管理不确定性对其目标的影响。图 3.1 给出了风险管理的原则，相关要素描述如下。

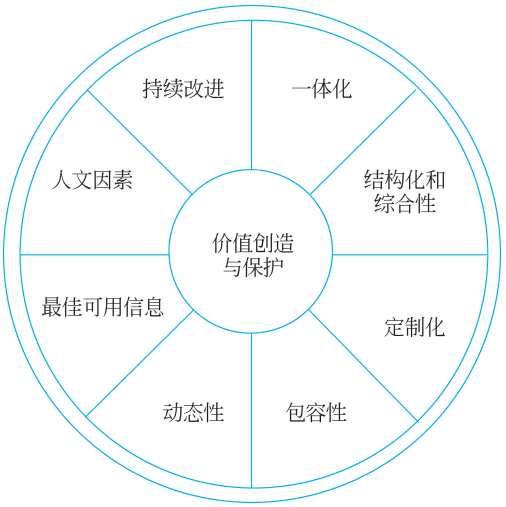

图 3.1　风险管理原则

（1）一体化，风险管理是所有组织活动的组成部分。

（2）结构化和综合性，结构化和全面的风险管理方法有助于形成一致和可比较的结果。

（3）定制化，对风险管理框架和过程进行定制，确保与组织相关外部和内部环境相适应。

（4）包容性，确保利益相关方能够适当、及时参与，并考虑其知识、观点和看法，以提高风险管理意识和水平。

（5）动态性，风险管理以适当和及时的方式对风险的动态变化和事件进行预期、检测、确认和响应。

（6）最佳可用信息，风险管理应基于历史和当前的信息以及对未来的预期，信息应及时、清晰并可供利益相关方使用。

（7）人文因素，人类行为和文化在每个层面和阶段会显著影响着风险管理的各方面。

（8）持续改进，通过学习和总结经验，不断提高风险管理水平。

3.1.3　框架

制定风险管理框架，协助组织将风险管理融入重要的活动和功能中。风险管理的有效

性将取决于能否将其有效整合到组织的治理中，这需要来自利益相关方的支持，尤其是高层管理人员。如图 3.2 所示，风险管理框架包括整合、设计、实施、评价和改进组织的风险管理。组织需要评价其现有的风险管理实践和过程，评价差距并解决框架内的这些差距。框架的组成部分和工作方式应根据组织的需要进行定制。

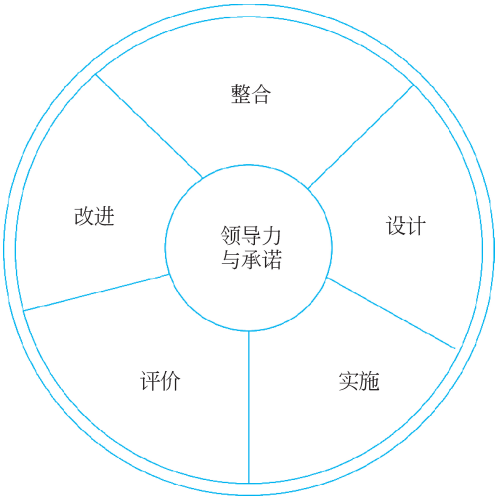

图 3.2　风险管理框架

（1）领导力和承诺：最高管理层和监督机构应确保将风险管理纳入所有组织活动。

（2）整合：将风险管理整合到组织中是一个动态的迭代过程，应该根据组织的需求和文化进行定制；风险管理应该是组织宗旨、治理、领导和承诺、战略、目标和运营的一部分。

（3）设计：在设计风险管理框架时，组织应检查并了解其外部和内部环境，阐明风险管理承诺，分配组织角色、权限、职责，分配资源，建立沟通和协商机制。

（4）实施：需要利益相关者的参与和意识，使组织能够明确解决决策中的不确定性，同时还确保可以考虑任何新的或后续的不确定性；如果设计和实施得当，风险管理框架将确保风险管理流程成为整个组织所有活动的一部分，包括决策制定，并充分捕捉外部和内部环境的变化。

（5）评价：评价风险管理框架的有效性。

（6）改进：持续监控和调整风险管理框架以应对外部和内部变化。

3.1.4　过程

风险管理过程涉及将策略、规程和实践系统地应用到风险的沟通与协商、语境建立以及评估、处置、监控、评审、记录和报告等活动中。这个过程如图 3.3 所示。

风险管理过程应该是管理和决策的一个组成部分，并整合到组织的结构、运营和过程中。它可以应用于战略、运营、计划或项目级别。一个组织内可以有许多风险管理过程的应用，这些应用被定制以实现目标并适应应用它们的外部和内部环境。在整个风险管理过程中，应考虑人类行为和文化的动态和可变性。尽管风险管理过程通常按顺序呈现，但实际上它是迭代的。

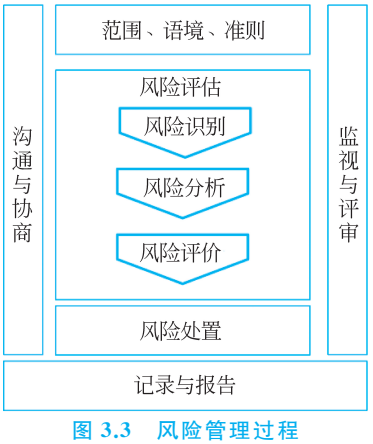

图 3.3　风险管理过程

（1）沟通和协商：目的是帮助利益相关者了解风险、决策依据以及需要采取特定行动的原因。

（2）范围、语境、准则：目的是定制风险管理流程，实现有效的风险评估和适当的风险处置。涉及定义过程的范围，以及理解外部和内部背景。

（3）风险评估：是风险识别、风险分析和风险评价的全过程。应以系统、迭代和协作的方式进行，并借鉴利益相关者的知识和观点。它应该使用最好的可用信息，并在必要时辅以进一步调查。

（4）风险处置：目的是选择和实施解决风险的方案。选择最合适的风险处置方案涉及平衡与实现目标相关的潜在收益与实施的成本、努力或劣势。

（5）监视与评审：目的是确保和提高过程设计、实施和结果的质量和有效性。应在该过程的所有阶段进行。包括规划、收集和分析信息、记录结果和提供反馈。结果应纳入整个组织的绩效管理、测量和报告活动。

（6）记录与报告：通过适当的机制记录和报告风险管理过程及其结果。

3.2　信息安全风险管理

信息安全风险管理围绕着信息安全的基本属性（简称“安全属性”，比如保密性、完整性、可用性）和信息安全风险的基本要素（简称“风险要素”）展开。首先，从每个安全属性的角度对各个风险要素及其相互关系进行识别、分析和评价，得出反映风险重要程度的风险等级（即“风险评估”）。然后，对照事先确定的风险接受准则，判断风险是否可接受；对于不可接受的风险，针对各个风险要素分别采取相应的控制措施，包括针对资产的保护和备份措施、针对威胁主体的威慑和打击措施、针对威胁行为的防范和抵御措施、针对脆弱性的加固和补丁措施、针对影响的抑制和弥补措施，从而改进和完善现有的控制措施（即“风险处置”，包括风险规避（risk avoidance）、风险修正（risk modification）、风险保留（risk retention）、风险分担（risk sharing））。

3.2.1　安全属性

相关安全概念如下。

ISO/IEC 27000:2018 中定义**信息安全**（information security）为：保持信息的保密性、完整性和可用性。除此之外，还可能涉及其他属性，如真实性、可核查性、抗抵赖性和可靠性等。

由于信息存在于信息系统中，信息系统进而存在于支撑环境（机房、场地等）中，故要保护信息的安全，也需要保护信息系统和支撑环境的安全。这里信息本身的安全性是目的，信息系统和支撑环境的安全性是手段。

ISO/IEC TS 27100:2020 中定义**网络安全**（cybersecurity）为：保护人民、社会、组织和国家，将面临的网络安全风险控制在可接受范围内。比如：社会、组织和国家的稳定性和连续性，人员和组织的资产（包括数据）安全，人的生命和健康安全。需要注意的是另外一个网络安全（network security）是指通信网络的安全，本书绝大部分的“网络安全”是cybersecurity。

ISO/IEC 2382:2015 中定义**隐私保护**（privacy protection）为：为确保隐私所采取的措

施，这些措施包括数据保护以及对收集、合并和处理个人数据的限制。

ISO/IEC 30145-2:2020 中定义**可信赖**(trustworthiness)为：以可验证的方式满足涉众期望的能力。根据上下文或行业，以及所使用的具体产品或服务、数据和技术，应用不同的特征，并需要验证，以确保利益相关者的期望得到满足。可信赖的特征包括可靠性、可用性、弹性、安全性、隐私性、安全、可核查性、透明度、完整性、真实性、质量、有用性和准确性等。可信赖是一种属性，可以应用于服务、产品、技术、数据和信息，在治理的上下文中，也可以应用于组织。本书以可信赖作为人工智能和算法、系统、服务等安全的属性之一，选取了常见的特征，如图 3.4 所示。

上述定义中涉及的各种属性定义如下。

(1) **保密性**(confidentiality)：不向未经授权的个人、实体或过程提供或披露信息的属性。[ISO/IEC 27000:2018，3.10]

(2) **完整性**(integrity)：准确性和完备性。[ISO/IEC 27000:2018，3.36]

(3) **可用性**(availability)：可被授权实体按需访问和使用的属性。[ISO/IEC 27000:2018，3.7]

(4) **真实性**(authenticity)：实体和所宣称的一致。[ISO/IEC 27000:2018，3.6]

(5) **质量**(quality)：在指定条件下使用时，数据特征满足规定和隐含需求的程度。[ISO/IEC TS 5723:2022，3.2.10]

(6) **可核查性**(accountability)：该属性确保实体的操作可以唯一地跟踪到该实体。[ISO/IEC 7498-2：1989]

(7) **不可抵赖性**(non-repudiation)：能够证明所声称事件或行动的发生及其发起实体的能力。[ISO/IEC 27000:2018，3.48]

(8) **有效性**(validity)：通过测量应该测量的内容和产生可用于预期目的的结果来评估达到其目的的程度。如果评估结果受到与评估既定目标无关技能的过度影响，则评估的效度较低。[ISO/IEC 23988:2007，3.25]

(9) **可靠性**(reliability)：与预期行为和结果一致。[ISO/IEC 27000:2018，3.55]

(10) **透明性**(transparency)：(1)确保所有与隐私相关的数据处理，包括法律、技术和组织设置都可以被理解和重构。[ISO/IEC TR 27550:2019，3.24](2)系统或过程的一种属性，其含义是公开和可核查。[ISO/IEC 27036-3:2013，3.3](3)开放、全面、可访问、清晰和可理解的信息呈现。[ISO/IEC TS 5723:2022，3.2.19]

(11) **有用性**(usability)：系统产品或服务能够被指定的用户在指定的使用环境中有效、高效和满意地用于实现指定的目标的程度。[ISO/IEC TS 5723:2022，3.2.21]

(12) **弹性**(resilience)：抵抗破坏影响的能力。[ISO/IEC 27031:2011，3.14]

(13) **隐私**(privacy)：不干涉个人私生活或事务的自由。[ISO/IEC TS 5723:2022，3.2.9]

(14) **安全**(safety)：一个系统的属性，在定义的条件下，它不会导致人类生命、健康、财产或环境受到威胁的状态。[ISO/IEC TS 5723:2022，3.2.17]

(15) **安全性**(security)：抵制旨在对系统造成伤害或损坏的故意的、未经授权的行为。[ISO/IEC TS 5723:2022，3.2.18]

(16) **可说明性**(explainability)：AI 系统的属性，以人类能够理解的方式表达影响 AI 系统结果的重要因素。[ISO/IEC 22989:2022，3.5.7]

(17) **可解释性**(interpretability)：理解底层(AI)技术如何工作的水平。[ISO/IEC TR

29119-11:2020，3.1.42]

(18) **可控性**(controllability)：允许人类或其他外部代理干预系统的功能运行。[ISO/IEC TS 5723:2022，3.2.5]

(19) **鲁棒性**(robustness)：系统在各种情况下保持其性能水平的能力。[ISO/IEC TS 5723:2022，3.2.16]

(20) **准确性**(accuracy)：对观察、计算或估计结果与真实值或公认为真实值的接近程度的度量。[ISO/IEC TS 5723:2022，3.2.2]

(21) **偏见**(bias)：对某些物体、人或群体的系统性区别对待。[ISO/IEC TR 24368:2022，3.2]

(22) **公平性**(fairness)：处理、行为或结果尊重既定事实、社会规范和信仰，不受偏袒或不公正歧视的决定或影响。公平不等同于没有偏见。偏见并不总是导致不公平，不公平可能是由偏见以外的因素引起的。[ISO/IEC TR 24368:2022，3.7]

安全就是对保护对象相关安全属性的保持。数智安全涉及的安全属性如图 3.4 所示，虽然相比于信息安全有扩展，但信息安全风险管理的原则、方法、过程等仍然适用。

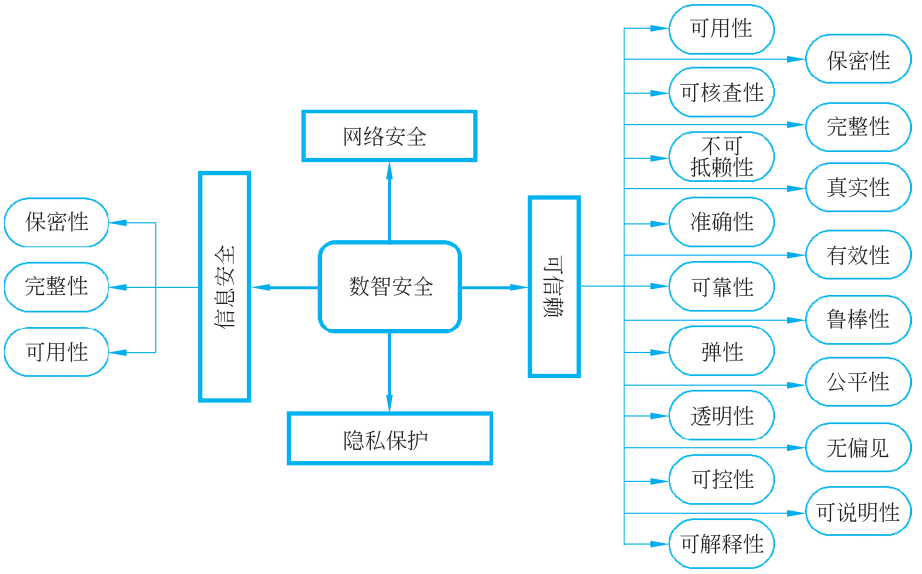

图 3.4　数智安全属性

3.2.2　风险要素

明确了要保护什么之后，就需要明确风险在哪里，信息安全风险的基本要素是指信息系统及其支撑环境从安全角度考虑所面临风险的基本组成成分，包括资产、威胁、脆弱性、影响和控制措施。

(1) 资产(asset)：对组织具有价值的任何东西。即保护对象。

(2) 威胁(threat)：导致对系统或组织伤害事件的潜在原因。

(3) 脆弱性(vulnerability)：可能被一个或多个威胁利用的资产或资产组的弱点。

(4) 影响(impact)：信息安全事件的结果。

(5) 控制措施(control)：处理风险的实践、规程或机制。

其中资产是核心要素，其他都是围绕资产而生的，即威胁是资产面临的威胁，脆弱性是资产自身的脆弱性，影响是资产损失带来的负面影响，控制措施是保护资产的措施。

风险表征的是不确定性，即威胁可能发生，可能产生负面的影响；一旦威胁已经发生，但尚未产生负面影响，风险即演变为了事态(event)；更进一步，如果已经产生了负面影响，则事态已演变为事件(incident)。

3.2.3 控制措施

明确了保护什么和相应风险之后，就可以有针对性地采取控制措施处置风险，包括任何过程、策略、设备、惯例或其他处置风险的措施。

控制措施包括：组织控制措施、人员控制措施、物理控制措施、技术控制措施。控制措施从不同角度有不同的属性分类。

(1) 类型：从控制何时以及如何处置与信息安全事件发生相关的风险的角度来查看控制的属性。属性值包括 preventive(在威胁发生前采取行动)、detective(在威胁发生时采取行动)和 corrective(在威胁发生后采取行动)；

(2) 安全属性：从控制措施将有助于保持哪些安全属性的角度来看。属性值包括保密性、完整性和可用性等；

(3) 网络空间安全概念：从网络空间安全框架中定义的网络空间安全概念与控制措施关联的角度来查看。属性值包括识别、保护、检测、响应和恢复；

(4) 操作功能：操作功能是从信息安全功能的实践者角度来查看控制措施的属性。属性值包括治理、资产管理、信息保护、人力资源安全、物理安全、系统和网络安全、应用安全、安全配置、身份和访问管理、威胁和漏洞管理、连续性、供应商关系安全、法律和合规性、信息安全事件管理和信息安全保障。

(5) 安全域：是从四个信息安全域的角度来看待控制的属性。属性值包括治理与生态系统、保护、防御和弹性。“治理和生态系统”包括“信息系统安全治理与风险管理”和“生态系统网络安全管理”；“保护”包括“IT 安全架构”“IT 安全管理”“身份和访问管理”“IT 安全维护”和“物理和环境安全”；“防御”包括“检测”和“计算机安全事件管理”；“弹性”包括“运营的连续性”和“危机管理”。

3.2.4 管理过程

依据 ISO/IEC 27005(对应国标 GB/T 31722)，信息安全风险管理过程可以迭代进行风险评估和/或风险处置活动。进行风险评估的迭代方法可以增加每次迭代评估的深度和细节。迭代方法最大限度地减少识别控制所花费的时间和精力，同时仍确保与适当评估风险之间的良好平衡。

语境建立是指综合信息安全的内部和外部语境用于信息安全风险管理或信息安全风险评估，需要确定风险管理的对象和范围、确定相关的基本要求、实施风险评估、建立和维护信息安全风险标准、选择合适的信息安全风险管理途径和方法。

风险评估包括以下活动。

(1) 风险识别：发现、识别和描述风险；回答风险是什么(What)、在哪里(Where)和何时(When)发生的问题；具体包括识别风险 5 要素：资产识别、威胁识别、脆弱性识别、影响识别、现有控制措施识别。

（2）风险分析：是理解风险类型和确定风险水平的过程，包括考虑风险的原因和来源、特定事件发生的可能性、该事件产生后果的可能性以及这些后果的严重性；回答风险为什么（Why）发生和相对级别（Level）的问题；具体包括：分析资产价值并赋值即资产价值分析，分析威胁主体动机和威胁行为能力并赋值，即威胁程度分析，分析脆弱性被威胁利用的难易程度并赋值即脆弱程度分析，分析资产因信息安全事件可能受到影响的严重程度并赋值，即影响程度分析，分析信息安全事件发生可能性，即可能性分析。

风险计算示例如下：

- 威胁潜力＝T（威胁主体动机＋，威胁行为能力＋）
- 信息安全事件发生的可能性＝P（脆弱程度＋，威胁潜力＋）
- 信息安全事件后果的严重性＝S（资产价值＋，影响程度＋）
- 信息安全风险值＝R（信息安全事件发生的可能性＋，信息安全事件后果的严重性＋，信息安全控制措施的有效性－）

其中，R、P、S 和 T 为计算函数，其表达方式既可以是数学公式也可以是计算矩阵；“＋”表示正相关参数（即与函数值正相关）；“－”表示负相关参数（即与函数值负相关）。

（3）风险评价：将风险分析的结果与风险标准进行比较，以确定风险和/或其重要性是否可以接受，基于这种比较，可以考虑是否需要处置。回答风险有多么（How）严重的问题。

风险评估应尽可能确保一致、有效和可重现的结果。此外，结果应该具有可比性，例如确定风险水平是否增加或减少。

组织应确保其信息安全风险管理方法与组织风险管理方法保持一致，以便任何信息安全风险都可以与其他组织风险进行比较，而不是单独考虑。有两种主要的评估方法：基于事件的方法和基于资产的方法。

如果风险评估提供了足够的信息来有效地确定将风险处置到可接受水平所需的操作，那么任务就完成了，接下来就是风险处置。如果信息不充分，则应进行另一轮风险评估。这个可能涉及风险评估范围的改变、相关领域的专业知识，或通过其他方式收集所需信息，以将风险处置到可接受的水平。

风险处置涉及以下迭代过程。

（1）制定和选择风险处置方式（风险规避、风险修正、风险保留、风险分担）。

（2）规划和实施风险处置。

（3）评估该处置的有效性。

（4）判断剩余风险是否可接受。

（5）如不可接受则进一步处置。

有可能风险处置并不能立即达到剩余风险可接受的状态。在这种情况下，可以进行另一次尝试以找到进一步的风险处置，或者可以进行另一次风险评估的迭代，无论是整体还是部分。这可能涉及风险评估语境的变化（例如通过修改范围）和相关领域专业知识的参与。有关相关威胁或漏洞的知识可以在下一次风险评估迭代中就合适的风险处置活动做出更好的决策。

3.3 人工智能风险管理

基于风险管理基础标准 ISO 31000:2018《风险管理指南》,ISO/IEC 23894《信息技术 人工智能 风险管理指南》梳理了人工智能的风险,给出了人工智能风险管理的流程和方法。在人工智能风险管理中,语境建立、风险评估、风险处置和记录与报告 4 个基本步骤需要体现人工智能的特性,监视与评审和沟通与协商则贯穿于这 4 个基本步骤之中。

由于人工智能技术的潜在复杂性、缺乏透明度和不可预测性,应特别考虑人工智能系统项目级别的风险管理过程。这些系统项目级别的过程应该与组织的目标保持一致,并且应该与其他级别的风险管理同步。例如,人工智能项目的升级和经验应纳入到更高级别,如战略、运营和规划级别,以及其他适用的级别。

风险管理过程的范围、语境和准则直接受到 AI 系统生命周期影响。风险管理过程和 AI 系统生命周期的关系如表 3.1 所示。

表 3.1 风险管理过程和 AI 系统生命周期关系

<table>
<tr><th colspan="2">风险管理</th><th rowspan="2">AI 风险管理框架</th><th colspan="5">AI 风险管理过程</th></tr>
<tr><th>AI 系统生命周期</th><th>范围、语境、准则</th><th>风险评估</th><th>风险处置</th><th>监视与评审</th><th>记录与报告</th></tr>
<tr><td rowspan="2">与风险管理相关的组织活动</td><td rowspan="2">监管机构为人工智能风险管理指定方向。
高层管理人员参与。
建立高水平的风险管理偏好和一般标准</td><td colspan="5">接收和处理来自人工智能系统风险管理流程的反馈报告。
改进风险管理框架,依赖于扩展和细化风险管理工具:</td></tr>
<tr><td>风险准则目录</td><td>潜在风险源目录。
风险源评估和测量技术目录</td><td>缓解措施目录</td><td>用于监视和控制 AI 系统的技术目录</td><td>用于追踪、记录、报告内外部利益相关方共享关于 AI 系统的信息的既定方法和定义格式的目录</td></tr>
<tr><td>开始</td><td>根据组织和利益相关者的原则和价值观,监管机构检查人工智能系统的目标。全面分析确定 AI 系统是否可行,并定位组织寻求解决的问题</td><td>通过定制组织的风险管理框架,建立 AI 系统风险管理流程和系统风险标准</td><td>识别指定 AI 系统的风险来源(可能以多层方式)并详细描述</td><td>建立详细的风险处置计划</td><td>实施、测试和评估必要的“概念证明”方法</td><td>记录分析结果和建议,并传达给最高管理层</td></tr>
<tr><td>设计与开发

检验和确认</td><td>监管机构根据收到的反馈报告,不断重新评估系统的目标、有效性和可行性</td><td>根据反馈报告,可能会修改 AI 系统的风险标准</td><td>不断执行风险评估(可能是多层面的)</td><td>实施风险处置计划。
持续实施风险处置和风险评估,直到达到确定的风险准则</td><td>在测试、验证和证明期间,对系统组件和整个系统的风险处置计划进行评估和调整</td><td>结果被记录并反馈给相关的风险管理过程活动。
如必要,这些结论将被传达给管理层和监管机构</td></tr>
</table>

续表

风险管理 AI 系统生命周期	AI 风险管理框架	AI 风险管理过程 范围、语境、准则	风险评估	风险处置	监视与评审	记录与报告
部署	监管机构根据收到的反馈报告，不断重新评估系统的目标、有效性和可行性	AI 系统的风险准则和风险管理过程将根据必要的“配置”变更进行调整	不断执行风险评估（可能是多层面的）	风险处置计划可能会因“配置”的变化和实施而进行更新。 持续实施风险处置和风险评估，直到达到确定的风险准则	重新评估 AI 系统的风险处置计划，以便进行必要的调整	结果被记录并反馈给相关的风险管理过程活动。如必要，这些结论将被传达给管理层和监管机构
运行监视 持续确认	监管机构根据收到的反馈报告，不断重新评估系统的目标、有效性和可行性	AI 系统的风险标准可能会根据反馈报告而被修改	该系统的风险评估计划可能会根据风险准则的变化而进行调整	该系统的风险处置计划可能会根据风险评估结果中的风险变化进行调整	对系统组件的风险处置计划进行评估和调整	
再评价	监管机构重新审视 AI 系统的目标及其与组织和利益相关方的原则和价值观，通过分析，确定可行性	根据特定目的和范围、运行监控的结果和新的监管要求，重新评估 AI 系统的风险管理过程和系统的风险准侧	针对现有 AI 系统风险源清单，检查任何可能存在的相关性和差距	风险处置计划可能会更新。 持续实施风险处置和风险评估，直到达到确定的风险准则	重新评估 AI 系统的风险处置计划，以便进行必要的调整	
退役或更换 触发新的风险管理过程，实现新的目标、风险及其缓解措施。	监管机构重新审视 AI 系统的目标及其与组织和利益相关方的原则和价值观，通过分析，确定可行性	建立 AI 系统的风险管理、报废流程和系统报废风险准则	确定并详细描述了特定 AI 系统报废的风险来源	制定详细的风险处置方案	实施、测试和评估必要的“概念验证”方法	

3.3.1　语境建立

人工智能风险管理的第一步确定范围、语境和准则，目的是针对性设置风险管理过程，以便进行有效的风险评估和适当的风险应对。对于使用人工智能的组织，人工智能风险管理的范围、人工智能风险管理过程的背景以及评估风险对支持决策过程的重要性的标准应加以扩展，以确定组织中正在开发或使用人工智能系统的地方。这种人工智能开发和使用

的清单应被记录在案，并纳入组织的风险管理过程中。

1. 定义范围

组织应界定其风险管理活动的范围。由于风险管理过程可以在不同层面（例如，战略、运行、方案、项目或其他活动），因此必须明确所考虑的范围、相关目标以及它们与组织目标的一致性。在规划时，考虑事项包括：目标和需要做的决策、每一步流程取得的预期结果、时间、地点，具体的包含和除外的内容、适当的风险评估工具和技术、需要的资源、责任和记录，与其他项目、流程和活动的关系。该范围应考虑到一个组织不同级别的具体任务和责任。此外，应该考虑组织开发或使用的数智系统的目标和目的。

2. 外部和内部语境

外部和内部语境是组织寻求确定和实现其目标的语境。风险管理过程的语境应建立在对组织运行所处的外部和内部语境的理解之上，并应反映应用风险管理过程的活动的具体语境。理解语境很重要，因为风险管理是在组织的目标和活动的语境下进行的、组织因素可能是风险的来源、风险管理过程的目的和范围可能与整个组织的目标相关。

建立风险管理过程的外部和内部语境，组织应该通过考虑包括但不限于表 3.2 所示因素。

表 3.2　风险管理过程的外部和内部语境

外 部 语 境	内 部 语 境
① 社会、文化、政治、法律、法规、金融、技术、经济和语境因素，无论是国际、国家、区域还是地方 ② 影响组织目标的关键驱动因素和趋势 ③ 外部利益相关方的关系、观念、价值、需求和期望 ④ 合同关系和承诺 ⑤ 网络及相关系统的复杂性	① 愿景、使命和价值观 ② 治理、组织结构、岗位和责任 ③ 战略、目标和方针 ④ 组织的文化 ⑤ 组织采用的标准、准则和模式 ⑥ 能力，从资源和知识（例如，资本、时间、人员、知识产权、过程、系统和技术）层面理解 ⑦ 数据、信息系统和信息流 ⑧ 与内部利益相关方的关系，考虑到他们的观念和价值 ⑨ 合同关系和承诺； ⑩ 相互的依存和互连性

由于人工智能系统的潜在影响巨大，在形成和建立风险管理过程的语境时应特别注意其利益相关者的环境。应谨慎考虑的利益相关方，包括但不限于：组织本身、客户、合作伙伴和第三方、供应商、最终用户、监管机构、民间组织、个人、受影响社区及社会。

其他涉及外部和内部语境因素，可包括：人工智能系统是否会伤害人类、拒绝提供基础服务（如中断将危及生命、健康或人身安全）或侵犯人权（例如通过不公平和有偏见的自动化决策）或造成环境危害；外部和内部对组织社会责任、环保责任的期望。

3. 确定风险准则

组织应规定其相对于目标可能承担或可能不承担的风险的数量和类型，确定风险准则以评估风险的意义和支持决策过程。风险准则应与风险管理框架保持一致，并根据所考虑的活动的具体目的和范围进行定制。风险准则应反映组织的价值、目标和资源，并与有关风险管理的方针和声明相一致。应该考虑组织的义务和利益相关方的观点来确定准则。

虽然风险准则应在风险评估过程开始时建立，但它们是动态的，必要时应不断检查修正。在定义风险准则时需要考虑的因素，如表 3.3 所示。

表 3.3　定义风险准则时需要考虑的因素

定义风险准则考虑因素 （根据 ISO 31000:2018，6.3.4）	其他考虑因素 （开发和使用人工智能系统）
影响结果和目标的不确定性的性质和类型（有形的和无形的）； 如何确定和测量结果（正负两方面）和可能性	组织应采取合理步骤，了解 AI 系统所有部分的不确定性，包括所使用的数据、软件、数学模型、物理扩展和系统方面的人机回圈（如数据收集和打标签期间的任何相关人类活动）
时间相关因素	参考 ISO 31000:2018
使用测量的一致性	组织应该意识到人工智能是一个快速发展的技术领域。根据运行中的人工智能系统有效性和适当性，测量方法保持一致
如何确定风险等级	组织应建立一致的方法来确定风险水平。方法应反映人工智能系统对不同目标的潜在影响。 （人工智能的 11 个目标：问责机制、专业知识、数据质量、环境影响、公平性、可维护性、隐私性、鲁棒性、人身安全、信息安全、透明度和可解释性）
如何综合考虑多个风险的组合和序列	参考 ISO 31000:2018
组织的能力	在确定组织的人工智能风险偏好时，应考虑组织的人工智能能力、知识水平和减轻人工智能风险的能力

3.3.2　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。风险评估应该系统、迭代和协调地进行，并利用利益相关方的知识和观点。它应该使用最好的可用信息，必要时补充进一步的查询。

人工智能安全风险应根据与组织相关的风险准则和目标进行识别、量化或定性描述，并确定优先级。在识别人工智能系统的风险时，应根据所考虑系统的性质及其应用环境考虑各种风险来源，包括：环境复杂性、缺乏透明度和可解释性、自动化程度、与机器学习相关的风险来源、系统硬件故障、系统生命周期故障、技术准备。虽然上述风险来源并不全面，但经验表明，对于首次执行风险评估工作或将人工智能风险管理集成到现有管理结构中的任何组织，将这些风险来源作为基线是有价值的。因此，从事 AI 系统开发、供应或应用的组织应将其风险评估活动与系统生命周期保持一致。不同的风险评估方法可以应用于系统生命周期的不同阶段。

3.3.3　风险处置

风险处置的目的是选择和实施解决风险的方案。风险处置涉及反复优化过程，制定和选择风险处置方案、策划和实施风险处置、评估处置的有效性、决定剩余风险是否可接受，如果不能接受则采取进一步措施。

1. 风险处置方案选择

选择最合适的风险处置方案包括平衡与实现目标有关的潜在利益与实现的成本。风险处置方案不一定在任何情况下都适用，处置风险的选择可能涉及以下一个或多个：决定不启动或停止实施有风险的活动来避免风险、承担或整合风险以追求机会、消除风险源、改变

可能性、改变后果、分担风险(例如通过合同,购买保险)、通过决策保留风险。

风险处置的理由不仅仅限于经济考虑,还应考虑到组织的所有义务、自愿承诺和利益相关方的观点。应根据组织的目标、风险准则和可用资源来选择风险处置方案。在选择风险处置方案时,组织应考虑利益相关方的价值、感知和参与能力,以及与其沟通和协商的最适当方式。虽然同样有效,一些风险处置可能比其他的更容易被一些利益相关方接受。即使精心设计和实施,也可能不会产生预期的结果,并可能产生意想不到的后果。监视与评审需要成为实施风险处置的一个组成部分,以确保不同形式的处置变得有效并保持有效。

风险处置也会引入需要管理的新风险。如果没有可供选择的处置方案,或者如果处置方案没有充分改变风险,则应记录风险并持续进行评审。决策者和其他利益相关方应该知道风险处置后剩余风险的性质和程度。剩余风险应记录下来,并进行监测、评审,并在适当的情况下做进一步处置。

2. 准备和实施风险处置计划

风险处置计划的目的是指明如何实施所选择的处置方案,以便相关人员理解安排,并且可以监测针对计划的进展。处置计划应清楚地确定应实施风险处置的顺序。

处置计划应与适当的利益相关方协商,纳入组织的管理计划和过程。处置计划中提供的信息应包括:选择处置方案的基本原理,包括获得预期的益处、负责批准和实施计划的人、建议的行动、所需资源,包括突发事件、绩效评估、制约因素、所需的报告和监测、何时开始和结束。风险处置计划一旦形成文件,就应实施其中所选择的风险处置措施。

3.3.4 监视与评审

监视与评审的目的是确保和提高过程设计、实施和结果的质量与有效性。在最开始规划风险管理流程时,应该将持续监视和定期评审作为其中的一部分内容,明确界定人员职责。流程的所有阶段都应该进行监视和评审。监视和评审包括计划、收集和分析信息、记录结果和提供反馈。监视和评审的结果应纳入整个组织绩效的管理、评估和报告等活动中。

3.3.5 记录与报告

应通过适当的机制记录和报告风险管理流程及其成果。记录与报告的目的是在整个组织内同步风险管理的活动和成果、为决策提供信息、改进风险管理活动、协助与利益相关方的互动,包括对风险管理活动有职责的相关方。关于建立、保留和处理文件化信息的决定应考虑但不限于:它们的用途、信息敏感性以及外部和内部环境。

报告是组织治理的组成部分,应提高与利益相关方沟通的质量,并支持最高管理和监督机构履行其职责。报告应考虑的因素包括但不限于:不同的利益相关方及其特定的信息需求和要求,报告的成本、频率和及时性,报告方法,信息与组织目标和决策的相关性。

组织应建立、记录并保持一种系统,用于从实施阶段和实施后阶段收集和验证产品或类似产品的信息。该组织还应收集和审查有关市场上类似系统的公开资料。然后应该评估这些信息与人工智能系统可信度的可能相关性。特别是,应评估以前未发现的风险,以及以前评估的风险的可接受程度。这些信息可以作为目标、用例或经验教训的调整,提供并纳入组织的人工智能风险管理过程。

如果这些条件中的任何一个适用,组织应执行以下各项:评估对以往风险管理活动的影响,并将评估结果反馈到风险管理过程中。检讨人工智能系统的风险管理工作。如果存

在剩余风险或其可接受性发生变化的可能性，应评估其对现有风险控制措施的影响。评估的结果应该被记录。风险管理记录应允许通过所有风险管理过程对每个已识别的风险进行跟踪。记录可以利用组织所同意的公共模板。

除了记录范围、语境和准则、风险评估和风险处置外，记录应至少包括以下信息：对所分析系统的描述和识别、方法应用、人工智能系统的预期用途说明、进行风险评估的个人和组织的身份、风险评估的职权范围和日期、风险评估的发布情况、目标是否达到及达到何种程度。

3.3.6　沟通与协商

沟通与协商的目的是协助利益相关方理解风险、明确做出决策的依据以及需要采取特定行动的原因。沟通旨在提高对风险的认识和理解，而协商则涉及获得反馈和信息以支持决策。两者之间的密切协调应促进真实、及时、相关、准确和可理解的信息交换，同时考虑到信息的保密性和完整性以及个人的隐私权。

与适当的外部和内部利益相关方的沟通和协商，应贯穿风险管理过程的所有步骤内和整个流程中进行。

沟通和协商的目的是：为风险管理过程的每个步骤汇集不同领域的专业知识；确保在确定风险准则时适当考虑不同的观点；评价风险；提供足够的信息，促进风险监督和决策；在受风险影响的人群中树立一种包容性和主人翁意识。

可能受到数智系统影响的利益相关者可能比最初预期的要多，可能包括不被考虑的外部利益相关者，也可能扩展到社会其他群体。

3.4　信息安全管理体系

3.4.1　信息安全管理体系概述

1. 基本概念

1）信息

信息是一种资产，与其他重要的业务资产一样，对组织的业务至关重要，因此需要得到适当的保护。信息可以以多种形式存储，包括：数字形式（如存储在电子或光媒体上的数据文件）、物质形式（如纸上），以及以员工知识形式表示的未呈现信息。信息可能通过各种方式进行传输，包括：快递、电子或口头通信。无论信息采用何种形式，或以何种形式传输，它总是需要适当的保护。

在许多组织中，信息依赖于信息通信技术。这项技术通常是组织的一个基本元素，有助于促进信息的创建、处理、存储、传输、保护和销毁。

2）信息安全

信息安全确保信息的保密性、可用性和完整性。信息安全涉及应用和管理适当的控制措施，包括考虑到各种威胁，以确保业务的持续成功和连续性，并最大限度地减少信息安全事件的后果。

信息安全是通过实施一套适用的控制措施来实现的，这套控制措施通过选定的风险管理过程进行选择，包括策略、过程、规程、组织结构、软件和硬件，用以保护已识别的信息资

产。必要时，需要规定、实施、监视、评审和改进这些控制措施，以确保满足组织的特定信息安全和业务目标。相关的信息安全控制措施也是期望与组织业务过程无缝集成。

3）管理

管理涉及在适当的结构中指导、控制和持续改进组织的活动。管理活动包括组织、处理、指导、监督和控制资源的行为、方式或实践。管理结构从小型组织中的一个人扩展到大型组织中由许多人组成的管理层级。

信息安全管理涉及通过保护组织的信息资产来实现业务目标所需的监督和决策。信息安全管理通过制定和使用信息安全策略、规程和指南来表达，然后由与组织相关的所有个人在整个组织中应用这些策略、规程和指南。

4）管理体系

管理体系使用资源框架来实现组织的目标。管理体系包括组织架构、策略、规划活动、责任、实践、规程、过程和资源。

在信息安全方面，管理体系使组织能够满足客户和其他利益相关方的信息安全要求，改进组织的计划和活动，满足组织的信息安全目标，遵从法律法规、规章制度和行业规定，并且以有组织的方式管理信息资产，来促进持续改进和调整当前的组织目标。

5）过程方法

组织需要识别和管理许多活动，以便既有效果又有效率地运作。需要管理任何使用资源的活动，以便能够使用一组相互关联或相互作用的活动将输入转换为输出，这也称为过程。一个过程的输出可直接形成另一个过程的输入，通常这种转换是在计划和受控的条件下进行的。组织内过程系统的应用，以及这些过程的识别、交互及其管理，可称为“过程方法”。

2. 要素和原则

信息安全管理体系（Information Security Management System，ISMS）由策略、规程、指南及相关资源和活动组成，由组织集中管理，目的在于保护其信息资产。ISMS 是建立、实施、运行、监视、评审、维护和改进组织信息安全来实现业务目标的系统方法。它是基于风险评估和组织的风险接受程度，为有效地处置和管理风险而设计的。分析信息资产保护的需求，并根据需要应用适当的控制措施来切实保护这些信息资产，有助于 ISMS 的成功实施。

为保障 ISMS 的成功实施，可以遵循下列基本原则：认识到信息安全的必要性，分配信息安全的责任，明确管理者的承诺和利益相关方的利益，提升信息安全管理的社会价值，开展信息安全风险评估来确定适当的控制措施，以达到可接受的风险程度。在此基础上提升安全能力建设，将安全作为信息网络和系统的基本元素，主动防范和发现信息安全事件。同时，确保信息安全管理方法的全面性，并能够做到根据组织业务、外部环境和法律法规要求的变化，持续对信息安全进行再评估并酌情进行修改。

3. 作用和意义

实现信息安全需要管理风险，包括与组织内部或组织使用的所有形式的信息相关的物理、人为和技术威胁带来的风险。采用 ISMS 是期望其成为组织的一项战略决策，并且该决策有必要根据组织的需要进行无缝集成、扩展和更新。组织 ISMS 的设计和实施受组织的需要和目标、安全要求、采用的业务过程以及组织的规模和结构的影响。ISMS 的设计和运行需要反映组织的利益相关方（包括客户、供应商、业务伙伴、股东和其他相关第三方）的利益和信息安全要求。

在相互连接的世界中，信息和相关的过程、系统和网络组成关键业务资产。组织及其信

息系统和网络面临来源广泛的安全威胁，包括计算机辅助欺诈、间谍活动、蓄意破坏、火灾和洪水。恶意代码、计算机黑客和拒绝服务攻击对信息系统和网络造成的损害已变得更加普遍、更有野心和日益复杂。

ISMS 对于公共和私营部门业务都很重要。在任何行业中，ISMS 都使电子商务成为可能，对风险管理活动至关重要。公共和私营网络的互联以及信息资产的共享增加了信息访问控制和处理的难度。此外，包含信息资产的移动存储设备的分布可能削弱传统控制措施的有效性。当组织采用了 ISMS 标准体系，便可向业务伙伴和其他受益相关方证明其运用一致且互认的信息安全原则的能力。

在信息系统的设计和开发中，信息安全并不总是被考虑到的。而且，信息安全常被认为是技术解决方案。然而，能通过技术手段实现的信息安全是有限的，若没有 ISMS 的适当管理和规程支持，信息安全可能是无效的。将安全性集成到功能完备的信息系统中可能是困难和昂贵的。ISMS 涉及确认哪些控制措施到位，需要仔细规划并注意细节。例如，可能是技术（逻辑）、物理、行政（管理）或组合的访问控制提供了一种手段，以确保根据业务和信息安全要求授权和限制对信息资产的访问。

ISMS 的成功采用对于保护信息资产非常重要，它使组织能够更好地确保其信息资产得到持续的充分保护，免受威胁；保持一个结构化和全面的框架，来识别和评估信息安全风险，选择和应用适用的控制措施，并测量和改进其有效性。另一方面，可以持续改进其控制环境，有效地实现法律法规的合规性。

3.4.2　信息安全管理体系过程

组织在建立、监视、保持和改进其 ISMS 时，需要采取如下步骤。

（1）识别信息资产及其相关的信息安全需求，评估信息安全风险和处置信息安全风险。

（2）选择并实施相关控制措施，以管理不可接受的风险。

（3）监视、保持和改进组织信息资产相关控制措施的有效性。

同时，为确保 ISMS 持续有效地保护组织的信息资产，有必要不断重复上述步骤，以识别风险或组织战略或业务目标的变化。

1. 识别信息安全需求

在组织的总体战略和业务目标、规模和地理分布的范围内，可通过了解如下方面来识别信息安全需求，包括已识别的信息资产及其价值，信息处理、存储和通信的业务需要，法律法规、规章制度和合同要求。根据风险评估工作需要，对与组织信息资产相关的风险进行有条不紊的评估包含分析信息资产面临的威胁、信息资产存在的脆弱性、威胁实现的可能性，以及任何信息安全事件对信息资产的潜在影响。期望相关控制措施的支出与感知到的风险成为现实所造成的业务影响相称。

2. 评估信息安全风险

管理信息安全需要一种适合的风险评估和风险处置方法，该方法可包括对成本和收益、法律要求、利益相关方的关切以及其他适合的输入和变量的判断。风险评估可以根据风险接受准则和与组织相关的目标来识别、量化并按重要性排列风险。评估结果宜指导和确定适当的管理行动及其优先级，以管理信息安全风险，并实施为防范这些风险而选择的控制措施。

需要注意的是，有必要定期进行风险评估，以应对信息安全要求和风险状况的变化，例

如，资产、威胁、脆弱性、影响、风险评价以及发生重大变化时的变化。这些风险评估宜以能够产生可比较和可重现结果的有条不紊的方法进行。为保障信息安全风险评估的有效性，建议具有明确界定的范围，以便有效，还包括与其他区域风险评估的关系。

ISO/IEC 27005（对应国标 GB/T 31722）提供信息安全风险管理指南，包括关于风险评估、风险处置、风险接受、风险报告、风险监视和风险评审的建议。风险评估方法的例子也包括在内。

3. 处置信息安全风险

以风险管理为核心，在考虑风险处置之前，需要确定风险是否可接受。例如，如果评估风险较低或处置成本对组织不具有成本效益，则可接受风险。此类决定要予以记录。

对于经过风险评估后识别的每个风险，需要做出风险处置决策。风险处置的可能选项包括：一是采用适当的控制措施来降低风险；二是明知而客观地接受风险，前提是这些风险明确地满足组织的风险接受策略和准则；三是通过不允许可能导致风险发生的行为来规避风险；四是与其他方共担相关风险，例如，保险公司或供应商。对于那些已决定采用适当控制措施来处置的风险，可以选择和实施这些控制措施。

4. 选择和实施控制措施

一旦识别了信息安全需求，确定和评估了所识别信息资产的信息安全风险，并做出了处置信息安全风险的决定，则选择和实施风险降低的控制措施。控制措施宜确保将风险降低至可接受的程度，同时考虑到以下因素：国家和国际法律法规的要求和约束；组织目标；运行要求和约束；风险降低相关的实施和运行成本，并保持与组织要求和约束相称；监视、评价和改进信息安全控制措施的效果和效率以支持组织目的的目标。控制措施的选择和实施宜记录在适用性声明中，以满足合规要求以及控制措施的实施和运行投入与信息安全事件可能导致的损失之间平衡的需要。

宜在系统和项目需求规划和设计阶段考虑信息安全控制措施。如果不这样做，可能会导致额外的成本和低效的解决方案，并且在最坏的情况下，无法实现足够的安全性。控制措施可从 ISO/IEC 27002（对应国标 GB/T 22081）或其他控制措施集中选择。或者，可设计新的控制措施，以满足组织的特定需要。有必要认识到，某些控制措施可能不适用于每个信息系统或环境，也不适用于所有组织。有时，实施所选择的一组控制措施需要时间，在此期间，风险程度可能高于长期所能容忍的程度。风险准则宜涵盖控制措施实施期间短期风险的可承受性。随着控制措施的逐步实施，宜将在不同时间点估算或预计的风险程度告知利益相关方。

5. 监视、保持和改进 ISMS 有效性

组织需要根据其策略和目标监视和评估 ISMS 的执行情况，并将结果报告给管理层审查，从而保持和改进 ISMS。这种 ISMS 审查检查 ISMS 是否包括适用于处置 ISMS 范围内风险的特定控制措施。此外，根据所监视区域的记录，提供对纠正、预防和改进措施进行验证和追溯的证据。

6. 持续改进

ISMS 持续改进的目的是提高实现信息保密性、可用性和完整性目标的可能性。持续改进的重点是寻找改进的机会，而不是假设现有的管理活动已经足够好或已尽其可能。

采取改进措施，首先分析和评价现状，以识别改进的地方。在此基础上，制定改进的目标，寻找实现目标的可能解决方案，评价这些解决方案并做出选择。继而，实施选定的解决方案，测量、验证、分析和评价实施结果，以确定目标已实现。最后，正式确认实施方案并予

以改进。必要时，对结果进行评审，以确定进一步的改进机会。因此，改进是一个持续活动，即经常重复行动。客户和其他利益相关方的反馈、信息安全管理体系的审核和评审也可用于识别改进机会。

3.4.3　信息安全管理体系要点

1. 组织语境

首先，要理解组织及其语境，组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

其次，理解相关方的需求和期望，组织应确定信息安全管理体系相关方，这些相关方与信息安全相关的要求，相关方的要求可包括法律、法规要求和合同义务。

最后，确定信息安全管理体系范围，组织应确定信息安全管理体系的边界及其适用性，以建立其范围。在确定范围时，应考虑组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。

2. 领导力

最高管理层应通过以下活动，证实对信息安全管理体系的领导和承诺：确保建立了信息安全策略和信息安全目标，并与组织战略方向一致；确保将信息安全管理体系要求整合到组织过程中；确保信息安全管理体系所需资源可用；沟通有效的信息安全管理及符合信息安全管理体系要求的重要性；确保信息安全管理体系达到预期结果；指导并支持相关人员为信息安全管理体系的有效性做出贡献；促进持续改进；支持其他相关管理角色，以证实其领导按角色应用于其责任范围。

最高管理层应建立信息安全方针，该方针应与组织意图相适宜并包括对满足适用的信息安全相关要求的承诺，形成文件化信息并可用。最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通，并向最高管理者报告信息安全管理体系绩效。

3. 规划

组织应在相关职能和层级上建立信息安全目标。信息安全目标应与信息安全方针一致，考虑适用的信息安全要求，以及风险评估和风险处置的结果，并适当时更新。组织应保留有关信息安全目标的文件化信息。

组织应确定并提供建立、实现、维护和持续改进信息安全管理体系所需的资源。确定在组织控制下从事会影响组织信息安全绩效的工作人员的必要能力，确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作。适用时，采取措施以获得必要的能力，并评估所采取措施的有效性，保留适当的文件化信息作为能力的证据。

在组织控制下工作的人员应了解信息安全方针，其对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；不符合信息安全管理体系要求带来的影响。在沟通方面，组织应确定与信息安全管理体系相关的内部和外部的沟通需求。

4. 运行

开展运行规划和控制，组织应规划、实现和控制所需要的过程，保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

开展信息安全风险评估。按计划的时间间隔，或当重大变更提出或发生时，执行信息安全风险评估。实现信息安全风险处置计划，保留信息安全风险处置结果的文件化信息。

5. 绩效评价

（1）评价信息安全绩效以及信息安全管理体系的有效性。分析和评价监视和测量的结果，包括信息安全过程和控制；适用的监视、测量、分析和评价的方法，以确保得到有效的结果。

（2）按计划的时间间隔进行内部审核，以提供信息，确定是否符合组织自身对信息安全管理体系的要求，是否得到有效实现和维护。管理评审应考虑以往管理评审提出的措施的状态，与信息安全管理体系相关的外部和内部事项的变化，风险评估结果及风险处置计划的状态以及持续改进的机会。

6. 改进

当发生不符合时，组织应评价采取消除不符合原因的措施的需求，评审任何所采取的纠正措施的有效性；必要时，对信息安全管理体系进行变更，持续改进信息安全管理体系的适宜性、充分性和有效性。

7. 安全控制措施

控制的选择取决于组织决策，该决策基于风险接受准则、风险处置选项、组织采用的通用风险管理方法；控制的选择也必须遵守所有相关的国家法律法规。同时控制的选择也取决于控制交互方式以提供纵深防御。有关控制选择的更详细信息以及其他的风险处置选项，可参见 ISO/IEC 27005。控制措施详见 ISO/IEC 27002《信息技术 安全技术 信息安全控制实用规则》。

8. 实施信息安全管理体系

ISMS 的实施是一种重要活动，通常作为组织的一个项目来执行。图 3.5 给出了规划 ISMS 项目的 5 个阶段以及主要输出文档，包括：获得管理者对启动 ISMS 项目的批准；定义 ISMS 的范围和 ISMS 的方针策略；进行组织分析；进行风险评估和规划风险处置；设计 ISMS。

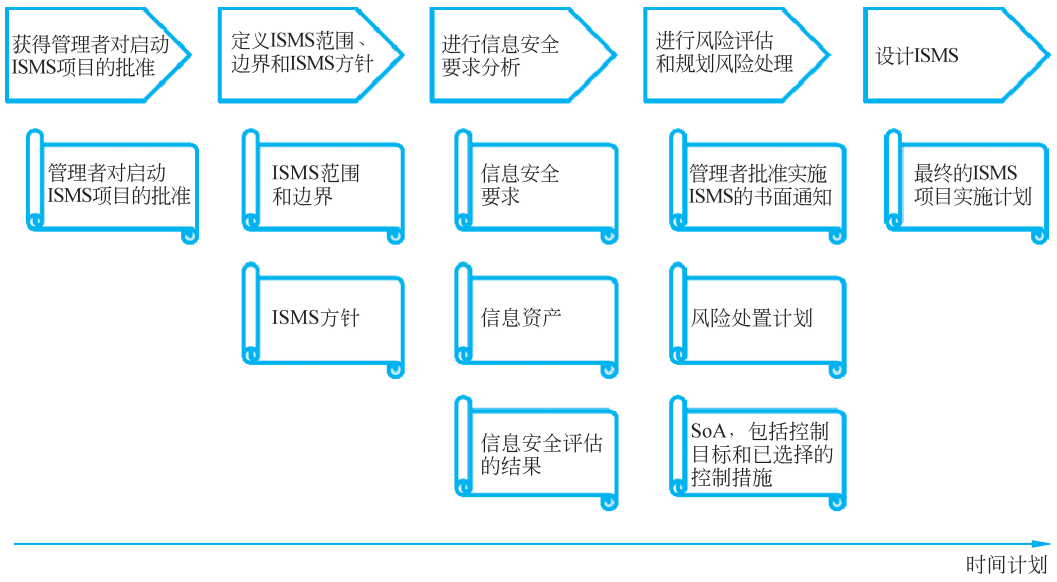

图 3.5　ISMS 项目的各个阶段

3.4.4　信息安全管理标准体系

信息安全管理体系（ISMS）标准体系由已发布或制定中的相互关联的标准组成，并包含

许多重要的结构组件。这些组件的重点是规定如下要求的标准：一是 ISMS 的要求(ISO/IEC 27001)；二是对进行 ISO/IEC 27001 符合性认证的认证机构的要求(ISO/IEC 27006)；三是对具体行业 ISMS 实施的附加要求框架(ISO/IEC 27009)。其他文件为 ISMS 实施的各个方面提供指导，包括通用过程以及具体行业指导。ISMS 标准体系中各标准之间的关系如图 3.6 所示，对于已转国家标准的国际标准，加括号标出对应的国家标准编号。

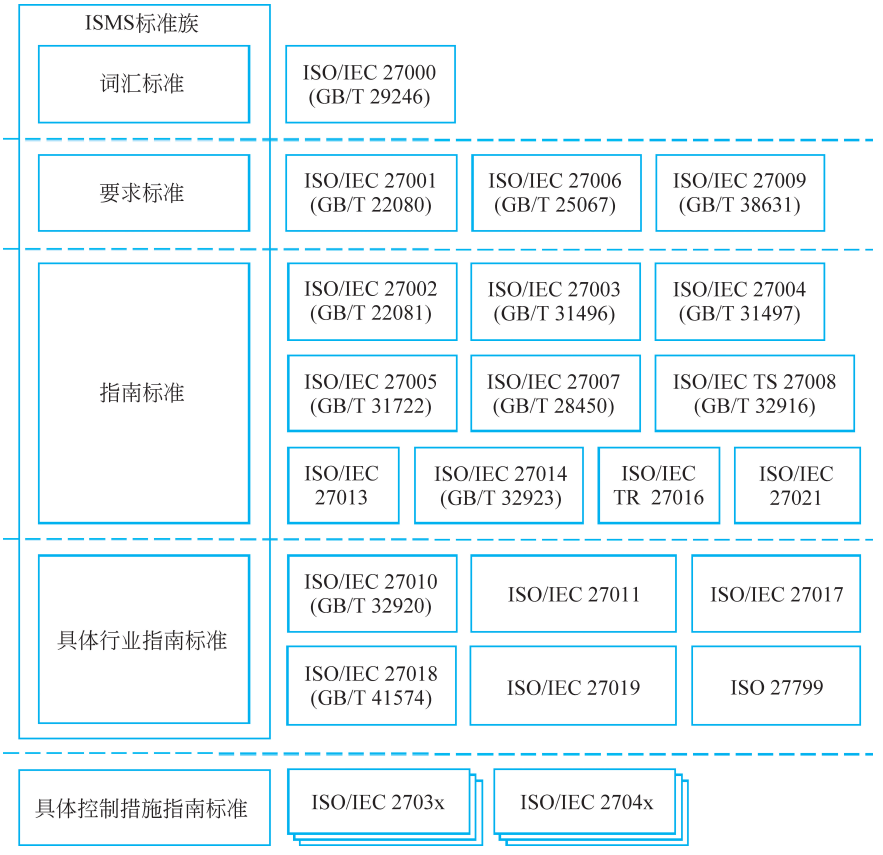

图 3.6　ISMS 信息安全管理标准体系

通过采用 ISMS 标准体系，降低信息安全风险(即降低信息安全事件发生的可能性和/或造成的影响)。具体而言，实施 ISMS 标准体系可以形成一个结构化框架，支持规范、实施、运行和保持一个全面、经济有效、创造价值、集成和一致的 ISMS，以满足组织跨不同运行和场所的需要。在企业风险管理和治理的语境下，协助管理层以负责任的方式持续管理和运用其信息安全管理方法，包括就信息安全的整体管理对业务和系统所有者进行教育和培训。促进全球公认的良好信息安全实践，使组织有自由采纳和改进适合其具体环境的相关控制措施，并在面对内部和外部变化时保持这些控制措施。提供信息安全的共同语言和概念基础，使其更容易信任符合 ISMS 的业务伙伴，特别是如果其需要由一个被认可的认证机构根据 ISO/IEC 27001 进行认证。增加利益相关方对组织的信任，对信息安全投资进行更有效的经济管理。

一方面，ISMS 提高了组织持续实现其信息资产所需关键成功因素的可能性。另一方面，许多因素对于 ISMS 的成功实施至关重要，以使组织能够实现其业务目标。ISMS 管理