国际内部审计师协会（IIA）三线模型

三道防线模型 升级版

The Institute of Internal Auditors | Global

目录

三线模型的原则 2

原则 1：组织治理 2

原则 2：组织治理机构的职责 2

原则 3：管理层和第一、二线的职能 3

原则 4：第三线的职能 3

原则 5：第三线的独立性 3

原则 6：创造和保护价值 3

三线模型的关键职能 5

组织治理机构 5

管理层 5

内部审计 6

外部确认提供方 6

核心职能之间的关系 7

组织治理机构和管理层（第一、二线职能）之间的关系 7

管理层（第一、二线职能）和内部审计的关系 7

内部审计和组织治理机构的关系 8

所有职能之间的关系 8

模型的应用 9

结构、职能和职责 9

监督和确认 10

相互配合并保持一致 10

简介

组织是一项人类的事业，其运行环境充满了不确定性，越来越复杂多变且相互关联。通常情况下，组织会有多个利益相关方，他们之间存在着复杂多样、不断变化、有时甚至会相互冲突的利益关系。利益相关方将组织监督权授予组织治理机构，治理机构将资源和权力分配给管理层，再由管理层执行具体的措施，例如对风险进行管理。

由于这一系列的原因，组织在加强治理和风险管理的能力的同时，还要建立有效的组织结构和流程来完成组织的目标。当治理机构收到来自管理层有关组织活动、成果和未来发展预测的报告时，治理机构和管理层都依赖内部审计部门为其提供有关上述事项的独立、客观的确认和咨询，从而推动和协助组织创新和发展。治理机构对治理活动承担最终责任，而组织治理是通过治理机构、管理层和内部审计共同努力达成的结果。

三线模型帮助组织对结构和流程是否能够发挥最大效用、协助完成组织目标并改善组织治理和风险管理的能力进行确认。该模型适用于所有类型的组织，需要做到以下几点来确保其发挥充分的效用：

- 采用基于原则的工作方法，并根据组织的具体目标和环境对模型进行调整。
- 重点关注风险管理在完成组织目标、创造价值以及在“防御风险”和保护价值方面做出的贡献。
- 对模型中的各个职能、各项职责以及彼此之间的关系有清晰的理解。
- 采取措施确保活动和目标与利益相关方的首要利益保持一致。

关键术语

组织 –由拥有共同目标的活动、资源和人员组成的有系统的集合。

利益相关方 –组织服务或影响其利益的集体和个人。

组织治理机构 –对利益相关者负责，负责领导组织实现成功。

管理层 –负责为组织客户提供产品和/或服务的个人、团体和支持性职能部门。

内部审计 –在管理层之外独立运行，为组织提供有关治理和风险管理（包括内部控制）的准确性和有效性的确认和观点的部门。

三线模型 –该模型之前被称为三道防线模型。

内部控制 –旨在为是否能够实现目标而提供合理确认的工作流程。

三线模型的原则

原则 1：组织治理

组织治理需要恰当的结构和流程，从而：

- 使利益相关方**信任**组织治理机构，并能够从诚信、领导能力和透明公开等方面对治理机构进行**问责**。
- 使管理层能够采取**行动**（含风险管理措施），通过基于风险的决策机制和对资源的应用来实现组织的目标。
- 使独立的内部审计职能部门能够提供**确认和咨询**，通过严格的询问和深度的沟通，为组织提供鉴证和树立信心，同时推动和协助组织实现不断进步。

关键术语

以风险为基础的决策机制 –一项经过审慎考虑的工作流程， 包含分析、计划、行动、监督和检查各个环节，并将在完成组织目标过程中可能存在的不确定因素考虑在内。

确认 –独立的鉴证并增加可信度。

原则 2：组织治理机构的职责

组织治理机构负责：

- 确保为有效的组织治理建立合理的结构和流程。
- 确保组织的目标和活动与利益相关方的首要利益保持一致。

组织治理机构：

- 向管理层分配职责，提供完成组织目标所需的资源，同时确保管理层遵守法律法规和道德要求。
- 建立并监督独立、客观且可靠的内部审计职能部门，使其在组织实现目标过程中针对工作流程提供明确的信息和确认可信度。

原则 3：管理层和第一、二线的职能

管理层肩负实现组织目标的职责，包含第一、二线的职能要求。[1]*第一线*是组织为客户提供产品和/或服务的前沿职能，包含支持性部门。[2]*第二线的职能部门*负责协助开展风险管理工作。

第一、二线的职能可能会存在相互交叉，也有可能彼此独立。第二线的一些职能可能会被分配给一些能够提供补充性专业知识、发挥支持或监督作用、并对第一线工作提出合理质疑的专业人员。第二线的相关职能部门可能会将工作重心放在风险管理的具体目标上，如对法律法规的遵循、可接受的职业道德行为、内部控制、信息和技术安全、业务可持续性以及质量确认。第二线的职能还可能会包含更广泛的风险管理职责，例如全面风险管理（ERM）。当然，第一线仍然需要承担风险管理的职责，并将其作为管理工作的一部分。

原则 4：第三线的职能

内部审计负责为组织治理和风险管理工作的适当性和有效性提供独立且客观的确认和咨询。[3]内部审计部门为了实现这一职能，需要充分应用系统且规范的工作流程、专业知识和观点。内部审计将审计发现报告给管理层和组织治理机构，从而推动和协助组织实现可持续的进步。在这一过程中，内部审计可能需要将其他内部和外部的部门或机构提供的确认成果一并纳入考虑。

原则 5：第三线的独立性

内部审计保持相对于管理层的独立性对于确保内部审计的客观性、权威性和可信度至关重要。内部审计的独立性是通过以下几种方式实现的：对组织治理机构负责；在完成其工作的过程中，可以不受限制地接触相关人员，获取资源和数据；以及在制定计划和提供审计服务的过程中避免偏见和免遭干涉。

原则 6：创造和保护价值

各项职能之间相互配合，并把利益相关方的利益放在首位，才能共同努力为组织创造价值并加以保护。只有充分沟通、配合和协作，才能实现各部门之间的协同，也只有这样才能为基于风险的决策机制提供值得信赖、相关、透明的信息。

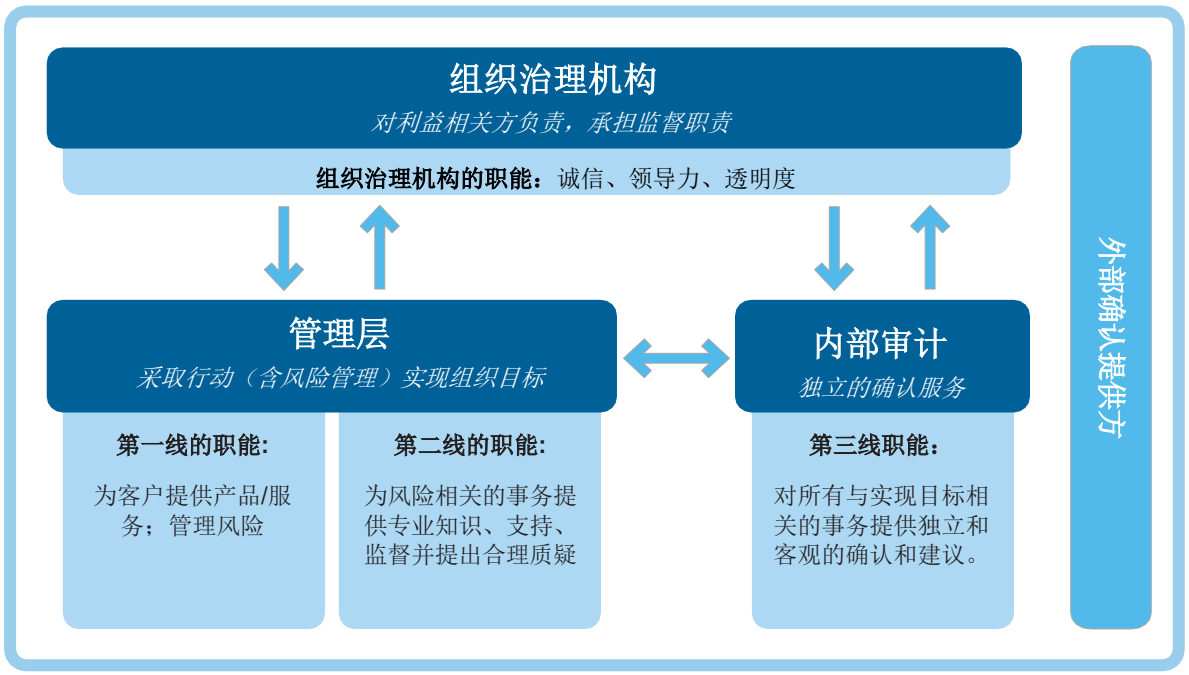
---

1. 为了与原来的模型保持一致，新模型也采用了“第一线”、“第二线”和“第三线”的说法。但是，“线”并非意指结构性元素，而是一项用于区分职能的标识。从逻辑上来讲，治理机构也构成了一道“线”，但是为了避免出现混淆，这一点并没有被采纳。各线的数位命名（第一、第二、第三）并不代表三者按数位顺序工作，相反，各项职能是同步运行的。

2. 一些人认为支持性职能部门（如人力资源和行政管理）应该属于第二线的职能范畴。为区分清楚，三线模型中的*第一线*既包括“前线职能”也包括“幕后职能”部门，*第二线*则涵盖关注风险相关领域的补充性活动。

3. 对于一些组织而言，还存在其他属于第三线的职能，如监督、监察、调查、评估和补救等，这些可能属于内部审计职能的一部分，也有可能单独运行。

IIA 三线模型



图例： 向其负责、报告 | 授权、指导、提供资源和监督 | 保持一致、沟通、协调、相互协作

三线模型的关键职能

各个组织在职责分配方面可能存在较大差异。然而，按以下方式对相关职责进行划分可以满足“三线模型”各项原则的要求。

组织治理机构

- 受利益相关方的委托，监督组织运行情况。
- 与利益相关方一道监督其利益，并就实现组织目标与利益相关方保持公开透明的沟通。
- 建立一个鼓励职业道德行为和问责的组织文化。
- 建立组织治理的结构和流程，其中还包含根据需要建立辅助性委员会。
- 将职责分配给管理层，并为其提供完成组织目标所需的各种资源。
- 确定组织的风险偏好，并监督组织风险管理工作（包括内部控制）。
- 保持对合规工作的监督，确保各项工作符合法律、法规和道德规范的要求。
- 建立一个独立、客观、胜任的内部审计部门，并对其进行监督。

管理层

第一线的职责

- 领导并指挥各项业务（包括相关的管理风险），运用各种资源，完成组织目标。
- 与组织治理机构之间保持沟通，并向其报告与实现组织目标相关的计划、实际情况和预期，以及相关风险。
- 为组织的运营和风险管理（含内部控制）工作搭建适当的结构和流程，并对其进行维护。
- 确保各项工作符合法律、法规和道德规范的要求。

第二线的职能

- 提供补充性的专业知识，发挥支持或监督作用，并对风险管理相关工作提出合理质疑，其中包括：
    - 在工作流程、系统和整个组织层面上部署、实施并持续改进风险管理工作（含内部控制）。
    - 实现风险管理目标，如遵循法律法规和职业道德规范的要求、内部控制、信息技术安全、可持续性以及质量确认。
- 对风险管理（含内部控制）的准确性和有效性进行分析和报告。

内部审计

- 保持主要对组织治理机构负责的状态，独立于管理层的各项职能之外。
- 为管理层和治理机构就组织治理和风险管理工作（含内部控制）的准确性和有效性提供独立客观的确认和咨询，支持组织实现目标，推动并协助组织不断完善。
- 将有损内部审计独立性和客观性的情况报告给治理机构，并根据要求采取保护措施。

外部确认提供方

- 提供额外的确认服务，从而：
    - 满足有关保护利益相关方权益的法律和法规要求。
    - 作为内部确认服务的补充，满足管理层和组织治理机构的需求。

核心职能之间的关系

组织治理机构和管理层（第一、二线职能）的关系

一般情况下，组织治理机构会通过确定组织发展愿景、使命、价值以及风险偏好来为组织明确发展方向。确定发展方向之后，治理机构会将实现组织目标的各项职责和必要的资源分配给管理层。治理机构还要接受管理层关于计划、实际情况和预期结果的报告，以及关于风险和风险管理的报告。

关键术语

首席执行官（CEO） **–负责组织运营的最高级别的领导。**

对于不同的组织而言，治理机构和管理层之间可能会存在职能交叉或相互独立的情况，其程度也各不相同。治理机构或多或少都会“插手”组织战略和运营方面的事务。治理机构或管理层都有可能领导或共同承担组织战略规划制定工作。在一些地区，首席执行官（CEO）可能是治理机构的成员，甚至是治理机构的领导。无论在何种情况下，管理层和治理机构之间都需要保持充分的沟通。CEO 一般会是两者之间沟通的聚焦点，但其他的高级管理人员也会与治理机构保持频繁的互动。组织可能会希望分管第二线职能的领导，如首席风险官（CRO）和首席合规官（CCO）能够直接向治理机构报告，监管机构可能也会提出类似的要求。这一点与三线模型的原则是完全一致的。

管理层（第一、二线职能）和内部审计的关系

内部审计相对于管理层的独立性，能够防止其在制定计划和开展工作时受到阻挠或偏听偏信，并能够根据工作需要不受限制地接触相关人员，获取资源和信息。内部审计对组织治理机构负责。但是，独立性不意味着完全孤立。内部审计与管理层之间必须保持定期互动，从而确保内部审计工作的相关性，且能够与组织战略和运营需求保持一致。作为组织值得信赖的顾问和战略伙伴，内部审计通过以上所有活动来建立对组织的理解和认识，并据此提供确认和咨询服务。管理层的第一、二线职能部门和内部审计之间需要相互协作，保持沟通，从而避免不必要的职能交叉、重复和空白。

内部审计和组织治理机构的关系

内部审计对组织治理机构负责，有时也被称为组织治理机构的“眼睛和耳朵”。组织治理机构负责对内部审计进行监督，这就要求治理机构履行以下职责：确保内部审计部门的独立性，包括负责首席审计执行官（CAE）的任免；作为 CAE[4]的主要汇报对象；审批审计计划并提供资源；接收并考量 CAE 的报告；保证 CAE 能够不受限制地接触治理机构，包括创造没有管理层出席的单独对话机会。

关键术语

首席审计执行官 (CAE) –组织内负责提供内部审计服务的最高级别领导，也被称为内部审计负责人或其他类似称谓。

所有职能之间的关系

组织治理机构、管理层和内部审计各自具有明确的职责，但是所有的活动都必须与组织的目标保持一致。保持一致的基础是各职能之间定期进行有效的协调、合作和沟通。

4. 为满足行政管理需求，CAE 可能也需要向适当的高管层成员报告工作。

模型的应用

结构、职能和职责

只有在符合组织目标和所处环境要求时，**三线模型**才能发挥最大的功效。管理层和组织治理机构负责确定组织结构和各项职责的分配。治理机构可以通过建立委员会来对特定领域的职责进行额外的监督，如审计、风险、财务、规划和薪酬委员会等。管理层中可能会发生具体的职责和等级分化，而且随着组织的规模扩大和复杂程度提高，管理层也会不断向专业化方向发展。

各职能部门、团队、甚至是个人都可能承担第一、二线的相关职责。然而，对第二线职能的指导和监督一定程度上也是为了确保第二线不受第一线（乃至高级管理层）的过度影响，保持一定的独立性。为此，组织需要建立一个第二线职能直接通向治理机构负责和汇报的通道。三线模型对管理层和治理机构之间搭建报告路径的数量没有限制，组织可以根据需求自行决定。一些组织，尤其是受监管的金融机构，会针对此类安排提出强制性的要求，从而确保具备充分的独立性。即便在这种情况下，那些属于第一线的管理部门依然要承担与其业务相关的风险管理职责。

第二线的职能可能会包含对风险管理相关的事务进行监督，提供建议、指导、测试、分析和报告。只要这些部门能够为第一线相关职能提供支持，提出合理质疑，并参与了管理层的决策及其实施，那么第二线的各项职能就属于管理层职能的一部分，无论报告和负责对象是谁，都不可能完全独立于管理层之外。

第三线的显著特征就是保持相对于管理层的独立性。三线模型的各项原则对内部审计独立性的重要性和本质特征进行了描述，将内部审计与其他职责进行了区分，明确提出了内部审计具备提供确认和咨询服务的独特价值。内部审计的独立性要求内部审计不能参与管理层职能（含风险管理）的决策和具体行动，也不能为内部审计目前或近期曾经承担过的职责或工作提供确认。例如，一些组织要求 CAE 承担额外的职责，为一些要求具备与审计类似的能力的活动（如强制性合规工作或全面风险管理）作决策。在这种情况下，内部审计无法保持相对于这些活动或者活动结果的独立性，因此当治理机构需要获得对这些领域提供独立客观的确认和咨询服务时，就有必要将这项工作交给具备相应资质的第三方机构。

监督和确认

组织治理机构依靠管理层（由第一、二线职能部门组成）、内部审计和其他部门的报告来履行监督职责，并实现既定目标，从而履行对利益相关方所负的责任。管理层利用第一手的实务经验和专业知识，针对工作计划、实际情况和预计结果、风险、风险管理提供有价值的确认（也可以视为其开展工作情况的证明）。属于第二线的部门负责对风险相关的事务提供额外的确认服务。由于内部审计则独立于管理层之外，因此与第一、二线部门相比，内部审计提供给治理机构的确认具有最高水平的客观性和可信度。组织可以通过外部确认提供方获得进一步的确认服务。

相互配合并保持一致

高效的组织治理要求对职责进行合理的分配，并通过相互合作和沟通，保持各项活动高度一致。治理机构希望通过内部审计的确认，能够了解组织治理结构和流程的设计和运行是否符合期待。

关于国际内部审计师协会（IIA）

国际内部审计师协会（IIA）是在内部审计行业得到最广泛认可的国际组织，是内部审计的倡导者，并提供教育服务、内部审计标准、实务指南和资格证书。国际内部审计师协会成立于 1941 年，如今会员人数超过 190,000，遍布 170 多个国家和地区。协会全球总部设在美国佛罗里达州的玛丽湖。更多信息，请登录 www.globaliia.org。

免责声明

版权

2020 年 7 月

全球总部
国际内部审计师协会
美国佛罗里达州玛丽湖，
格林伍德大道 1035 号 149 座
联系电话： +1-407-937-1111
传真： +1-407-937-1101
www.globaliia.org