# 组织复原力

## 专项要求

## *Topical Requirement*

The Institute of Internal Auditors

译者

中国内部审计协会 IIA China CHINA INSTITUTE OF INTERNAL AUDIT

# 组织复原力专项要求

国际内部审计师协会的《国际内部审计专业实务框架®》包括《全球内部审计准则》（Global Internal Audit Standards™）《专项要求》（Topical Requirements）和《全球指南》（Global Guidance）。《专项要求》应与《全球内部审计准则》结合使用，为所要求的实务活动提供了权威依据。

《专项要求》通过设定特定风险专项审计的最低基本要求，为内部审计人员提供明确的期望。组织的风险状况可能要求内部审计人员考虑该《专项要求》领域的其他方面，包括当地法规。

遵循《专项要求》将提高内部审计服务的一致性，并提高内部审计服务和结果的质量和可靠性。最终，《专项要求》将提升内部审计职业的水平。

内部审计人员在运用《专项要求》的时候必须遵循《全球内部审计准则》。确认服务必须遵循《专项要求》，咨询服务则推荐遵循《专项要求》。

《专项要求》在以下情况适用：

- 其覆盖领域是内部审计计划中包含的审计项目的审计对象。
- 在开展审计项目时发现与其覆盖领域属有关的问题。
- 其覆盖领域中包含未列入原内部审计计划的审计项目的审计对象。

并不是所有要求都必须在一个审计项目中全部得到满足，有些要求可以通过其他方法来满足。如果某项要求被其他监管规定或合同要求排除或取代，或通过实施符合《全球内部审计准则》的程序得以满足，则必须将理由记录在案并予以保存。质量评估期间将对遵循情况进行评估。

如需了解更多信息，请参阅《组织复原力专项要求用户指南》。

# 组织复原力

国际标准化组织将组织复原力定义为“组织在不断变化的环境中承受和适应的能力”（ISO 22316:2017）。虽然这一定义提出了明确的目标，但各组织在如何预测、应对、适应变革和干扰，并从中恢复的实践方面存在很大差异。由于组织复原力横跨战略、运营、技术、人力、社会和财务等多个层面，一些组织可以有效地吸收变革，而另一些组织则很难做到这一点，或者在面对不确定性时选择不同的方法。

组织复原力是一个总括术语，用于涵盖可能严重扰乱或损害组织提供核心产品和服务、维护利益相关方信任或实现战略目标的能力的风险。这些风险可能来自突发事件（如自然灾害、网络攻击和地缘政治冲突）、长期环境压力（如资源匮乏和公共卫生危机）或外部环境变化（如技术变革、监管变化和声誉受损）。

这些风险也可能是逐渐发生的变化或缓慢形成的压力，随着时间的推移，会损害组织的稳定性和适应能力。这类逐步积累的风险经常会被忽视。复原力强的组织能够预测和适应突如其来和细微的风险，从而取得成功。

对复原力构成威胁的固有风险因素包括：高度复杂的业务、全球化供应链、集中化的基础设施或数据系统、有限的劳动力可用性、动荡的市场条件以及对关键第三方或地理位置的高度依赖。由于公众影响和合规义务，高可靠性行业的组织或在严格监管下运营的组织也可能面对更高水平的固有风险。

组织复原力主要关注在发生业务中断之前、期间和之后管理风险。内部审计人员通常会围绕业务连续性和灾难恢复，来评估信息技术（IT）流程和控制措施。业务连续性计划详细说明了当灾难发生时，组织为维持关键职能和恢复正常运营功能而采取的步骤。灾难恢复计划描述了组织如何在破坏性事件发生后恢复其 IT 系统、关键数据和业务，以恢复正常业务运营。

组织复原力包括上述两项计划，需要战略规划、企业风险管理、有效的领导和文化以及全组织范围的控制流程。为组织复原力建立强健的控制流程，不仅能使组织不断预测、准备、应对和适应变化，还能帮助其生存和发展。

# 评价和评估有关组织复原力的治理、风险管理和控制过程

本《专项要求》为评估有关组织复原力的治理、风险管理和控制流程的设计和实施提供了一致、全面的方法。这些要求是评估组织复原力的最低要求。

## 治理

### *要求*

内部审计人员必须对组织复原力治理的以下方面进行评估：

A. 应对复原力问题的正式组织战略由管理层制定、董事会批准通过和监督实施，包括管理变革和继续运营所需的业务、技术和财务要素。复原力目标与本组织的风险管理总体方法相一致。

B. 应定期向董事会通报实现复原力目标的最新情况，供其审查。这可确保将复原力纳入战略监督、长期规划流程、继任计划和组织文化，包括支持关键业务活动所需的资源和预算中对其进行考虑。

C. 制定有关关键业务、技术和财务流程的政策和程序，并根据需要定期审查、测试和更新，以加强控制环境。

D. 建立事件指挥架构，用于监督和支持组织复原力目标。此架构包括了决策层级、沟通和上报规程，以及领导和运营角色与责任。

E. 建立相关流程，用于定期评估在复原力方面所需的能力，并重新评估在有关复原力的过程中发挥关键作用的个人的胜任能力。

F. 建立相关流程，用于确定所有内部和外部利益相关方，确定其优先次序，并使其参与建立信息和报告结构的过程，以实现机构复原力目标。利益相关方可能包括高级管理层、运营部门、风险管理部门、信息技术部门、供应链/采购部门、设施部门、人力资源部门、财务部门、法律部门、确认提供方（包括内部审计部门）、合规部门、公共关系部门、重要供应商、客户、监管机构及其他部门。

## 风险管理

### *要求*

内部审计人员必须对组织复原力风险管理的以下方面进行评估：

A. 在整个组织内定期识别、评估和管理与组织复原力有关的风险。将复原力风险对应到组织的战略目标。复原力风险管理流程包括评估关键流程。

B. 明确界定组织复原力风险管理的问责和责任制度。指派专人或专门的团队定期监测和报告组织复原力风险的管理情况，包括降低风险和识别组织复原力面临的新威胁所需的资源。

C. 建立相关流程，用于监测组织复原力风险（新出现的或以前确定的）水平，并迅速上报达到组织既定风险管理指引和风险容忍度或适用法律和监管要求所规定的不可接受水平的风险。考虑组织复原力风险的影响。

D. 管理层已实施并定期测试有关流程，以应对危机、业务中断和紧急情况并从中恢复。事件应对和恢复流程包括检测、确定优先级、遏制、恢复和事件后分析。事件应对方法包括针对一系列破坏性事件进行情景分析和定期压力测试。

## 控制过程

### *要求*

内部审计人员必须评估与组织复原力有关的控制过程的以下方面：

A. 建立了相关程序，以确定关键的第三方提供商（供应商和卖方），并确定维持基本运营所需的最低库存水平。这一流程还包括保存一份最新的备选供应商名单。

B. 确定对业务至关重要的数据并进行分类。数据分类包括确定数据存放在哪里、谁需要访问数据、如何访问数据，以及数据是否已备份并能在紧急情况下恢复。

C. 建立关键的信息技术控制和持续监测，以降低信息安全风险（包括网络相关风险），确保敏感数据在危机、业务中断和紧急情况下得到保护。控制和持续监控包括了实时威胁情报和仅允许授权用户访问。

D. 对关键 IT 资产进行了清查。这些资产包括在危机、业务中断和紧急情况下支持运营所需的硬件、软件和服务。

E. 制定了业务连续性和灾难恢复计划，并明确指定人员和恢复小组的职责。定期对计划进行测试（如“桌面演练”），并向董事会和高级管理层报告测试结果，包括改进机会。

F. 建立相关流程，以便在危机、业务中断和紧急情况下调整工作环境。

G. 建立相关流程，持续监测和报告可能影响组织复原力的新威胁和缺陷。该流程用于确定提升组织复原力运行的机会，对其按优先级进行排序并加以落实，包括举报或收集风险情报的系统等。

H. 建立相关流程，对人员进行有关组织复原力的教育和培训，确保他们了解在危机、业务中断和紧急情况发生时应遵循的政策和程序以及应采取的行动。这一流程包括模拟破坏性场景的培训演习。

I. 建立相关流程，确保必要的业务、人力、技术和财务资源被编入预算，并在危机、业务中断和紧急情况下可用。定期分析支持组织复原力所需的财务资源，并向董事会报告。

J. 建立危机、业务中断和紧急情况发生后的审查流程，并通过吸取经验教训进行事件后审查分析，包括将经验教训纳入未来的组织复原力计划。

## 关于国际内部审计师协会

国际内部审计师协会（IIA）是一家国际专业协会，为全球 265,000 多名会员提供服务，并在全球颁发了 20 多万张国际注册内部审计师® (CIA®) 证书。IIA成立于 1941 年，是全球公认的内部审计职业标准、认证、教育、研究和技术指导的领导者。如需了解更多信息，请访问 theiia.org。

## 版权



2026 年 4 月

The Institute of Internal Auditors

全球总部

1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
电话：+1-407-937-1111
传真： +1-407-1101