公开征求意见稿
组织复原力专项要求

国际内部审计师协会的《国际专业实务框架®》包括《全球内部审计标准》（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了明确的期望。组织的风险状况可能要求内部审计人员考虑有关问题的其他方面。

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：

1. 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。
2. 在开展审计项目时发现与其覆盖领域属有关的问题。
3. 其覆盖领域属是中包含未列入原内部审计计划的审计项目的审计对象。

必须记录并保留对《专项要求》中每项要求的适用性进行评估的证据。具体要求可能并不适用于每一项审计业务；如果排除了某些不适用的要求，则必须记录并保留理由。《专项要求》是强制性的，质量评估中将对其遵循情况进行评估。

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

国际标准化组织发布的 ISO 22316:2017《安全与复原力--组织复原力--原则与属性》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”。组织复原力是一个宽泛的话题，涵盖了重要的战略、运营、技术、人力、社会和财务要素。组织复原力针对的是可能严重干扰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，随着时间的推移损害到了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。

对恢复能力构成威胁的固有风险因素包括：高度的业务复杂性、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审查下运营的组织也可能面对更高的固有风险。

内部审计人员通常会评估信息技术（IT）流程以及与业务连续性和灾难恢复有关的控制措施。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中断期间保护其 IT
系统和关键数据。组织复原力还需要战略规划、企业风险管理、有效的领导力和文化以及覆盖整个组织的控制过程。为组织复原力建立强健的控制过程，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、风险管理和控制过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. 董事会制定并记录正式的组织复原力战略，其目标应符合并支持组织的使命和愿景。该战略涉及在危机、中断和紧急情况下经受挑战和继续运行所需要的业务、技术和财务要素，以及随后如何恢复和适应。该战略与本组织的整体风险管理方法保持一致，并定期进行测试和更新。

B. 董事会会定期接受有关组织复原力战略和目标实现情况的报告，并对其进行审查，确保将复原力纳入战略监督、长期规划流程和组织文化，包括在支持关键业务活动所需的资源和预算中对其进行考虑。

C. 确定了与组织复原力有关的关键业务、技术和财务流程。制定了关键流程的政策和程序，并定期进行审查和根据需要更新，以加强控制环境。

D. 建立事件指挥架构，其中包括决策层级、沟通和上报规程以及领导和行动角色与责任。该架构用于监督和支持建立组织复原力目标。

E. 建立相关流程，用于定期重新评估在复原力流程中发挥关键作用的个人的胜任能力。制定了继任计划，并确定了关键职位和潜在的接替人选。

F. 建立相关流程，让内部和外部的有关利益相关方参与识别、分析和应对可能影响实现组织复原力目标的现有缺陷和新威胁。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、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. 组织的风险评估和风险管理程序包括了识别、分析、减轻和监控可能干扰业务的威胁。组织复原力风险管理战略在整个组织内进行了沟通，并定期接受审查。

B. 与组织复原力有关的风险在整个组织内得到定期评估和管理。风险评估和管理可包括以下领域：运营、企业风险管理、信息技术、供应链/采购、设施、人力资源、财务、法律、合规、监管、公共关系、关键供应商、声誉、新兴风险等。

C. 建立组织复原力风险管理的问责和责任制度。确定个人或团队定期监测和报告组织复原力风险的管理情况，包括减轻风险和识别新出现的组织复原力威胁所需的资源。

D. 建立有关流程，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财务和非财务影响。

E. 管理层已实施并定期测试有关流程，以应对危机、中断和紧急情况的发生并从中恢复。事件响应和恢复流程包括检测、控制、恢复和事件后分析。事件应对方法包括针对一系列看上去可信的破

坏性事件进行情景分析和定期压力测试。董事会和高级管理层对这些活动的结果进行审查，且改进措施得到定期跟踪和报告。建议具有可操作性，并有明确的责任人和时间表。

控制

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. 建立相关流程，以确定关键的第三方服务提供商（供应商和卖方）以及继续开展重要业务所需的最低库存水平。这一流程包括保存一份备选供应商名单。

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、中断和紧急情况下得到保护。控制和持续监控包括实时威胁情报和限制授权用户访问。

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

E. 制定业务连续性和灾难恢复计划。这些计划包括明确指派人员和恢复团队的职责。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、中断和紧急情况下改变工作环境。改变可能包括使用其他工作地点，如在家工作或及时有效地设立临时办公室。

G. 建立相关流程，以持续监测和报告与组织复原力有关的新威胁和缺陷，并确定、优先考虑和把握提高组织复原力的机会。该流程可能包括举报或收集风险情报的系统。

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、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。这一流程包括模拟中断情景的培训演习。

I. 建立相关流程，确保必要的人力、技术和财政资源编入预算，并在危机、中断和紧急情况下可用。该流程可能包括预先批准资金。

J. 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。分析包括评估流动性、保险覆盖范围和应急资金安排。

K. 建立危机、干扰和紧急情况发生后的审查流程，并通过吸取经验教训的流程对事件后审查进行分析，包括将经验教训纳入未来的组织复原力规划。

关于国际内部审计师协会

国际内部审计师协会是一家国际专业协会，为全球 265,000 多名会员提供服务，并在全球范围内颁发了 200,000 多张注册内部审计师® (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。欲了解更多信息，请访问 www.theiia.org.

版权

2025 年 9 月