组织复原力

专项要求

用户指南

Topical Requirement

The Institute of Internal Auditors

译者

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

目录

专项要求概述

《专项要求》（Topical Requirements）与《全球内部审计准则》（Global Internal Audit Standards™）和《全球指南》（Global Guidance）同为《国际专业实务框架》(International Professional Practice Framework®)的重要组织部分。国际内部审计师协会要求将《专项要求》与《全球内部审计准则》（标准 4.1 遵循《全球内部审计准则标准》）结合使用，为所要求的实务提供了权威依据。本指南全文均引用《准则》作为更详细信息的来源。

《专项要求》正式规定了内部审计人员如何应对常见的风险领域，以提升整个职业的质量和一致性。内部审计职责和权限明确规定了内部审计职能的服务范围和类型，包括对《专项要求》的考虑（标准 6.1 内部审计职责和权限）。《专项要求》为执行与其主题相关的确认服务确立了基准并提供了相关标准（标准 13.4 评价标准）。确认服务必须遵循《专项要求》，在咨询服务过程中则建议对其要求进行评估。《专项要求》并不打算覆盖开展确认业务时应考虑的所有潜在方面；相反，它的目的是提供一套最低要求，以便能够对有关内容进行一致、可靠的评估。

《专项要求》与国际内部审计师协会的“三线模式”和《准则》之间存在明确的关联。治理、风险管理和控制过程是《专项要求》的主要组成部分，与“标准 9.1 了解治理、风险管理和控制流程”保持了一致。根据“三线模型”，治理与董事会/治理机构相关，风险管理与第二线职能相关，控制或控制过程与第一线职能相关。管理层在一线和二线都有代表，而内部审计职能则作为第三线，以独立客观的方式提供确认，向董事会/治理机构报告（原则 8 接受董事会监督）。

适用性、风险和职业判断

当内部审计职能围绕《专项要求》的内容开展确认业务，或在其他确认业务中发现《专项要求》的某些内容时，必须遵循《专项要求》。

如《准则》所述，评估风险是首席审计执行官制定计划过程中的重要组成部分。要确定内部审计计划中应包括哪些确认业务，就必须至少每年评估一次组织的战略、目标和风险（标准9.4 内部审计计划）。在为某个确认项目制定计划时，内部审计人员必须评估与项目相关的风险（标准13.2 项目风险评估）。

如果在基于风险的内部审计计划过程中发现了《专项要求》的有关内容，并将其纳入审计计划，则必须使用《专项要求》中列出的要求来评估适用业务中的相关内容。此外，当内部审计人员开展审计业务（无论是否包含在计划中）时，如果出现了《专项要求》包含的要素，则必须将《专项要求》的适用性作为业务的一部分进行评估。最后，如果内部审计人员要求开展一项原本不在计划中的工作，但其中包含该相关内容，则必须对《专项要求》的适用性进行评估。(参见标准 9.4中有关审计计划变更的内容）。

职业判断在应用《专项要求》方面发挥着关键作用。风险评估促使首席审计执行官决定将哪些审计项目纳入内部审计计划（标准9.4）。此外，内部审计人员还须利用职业判断来确定每个审计项目将包含哪些方面（标准13.3 项目目标和范围、13.4 评价标准和13.6 项目工作方案），并确定实现工作目标所需的资源（标准13.5项目资源）。附录 A“应用场景”介绍了内部审计人员如何使用《专项要求》。

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《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。

必须根据“标准14.6 项目文档”的规定，利用内部审计人员职业判断，来记录是否遵循了《专项要求》。

虽然《组织复原力专项要求》提供了需要考虑的控制过程的最低要求，但将相关风险水平评估为极高的组织可能还需要额外评估其他方面。

如果首席审计执行官认定内部审计职能不具备就《专项要求》有关内容开展审计业务所需的知识，则可将项目外包（标准3.1 胜任能力、7.2 首席审计执行官的资格、10.2 人力资源管理）。首席审计执行官可能会发现国际内部审计师协会发布的《内部审计胜任能力框架》（The IIA's Internal Auditing Competency Framework TM）是一个有用的资源。《准则》适用于所有提供内部审计服务的个人和团队，无论组织是直接聘用的内部审计人员，还是与外部服务提供方签订合同，亦或两种情况兼有。首席审计执行官负有确保遵循性的最终责任。此外，如果认定内部审计资源不足，首席审计执行官必须告知董事会资源不足的影响以及如何解决资源短缺问题（标准 8.2 资源）。

执行、归档和报告

在运用《专项要求》时，内部审计人员还必须遵守《准则》，按照“领域五：“实施内部审计业务”的要求开展工作。领域五中的标准描述了为审计项目制定计划（原则13 有效计划项目）、实施审计项目（原则14 实施项目）和沟通项目结果（原则15 沟通项目结果和监督行动计划的执行情况）。

《专项要求》的设计目的在于支持一致、高质量的内部审计实务。《专项要求》应与适用的当地法律、法规、监管预期和其他得到认可的框架一并适用，这些其他规定可能会提出额外或更加具体的要求。内部审计人员可能已经根据这些规定和框架制定了项目工作方案和测试程序。内部审计人员应将他们计划实施的有关组织复原力的控制测试，以及其他内部和外部确认提供方提供的的任何可靠测试（标准 9.5 协调与信赖）与《专项要求》进行比对，以确保所有要求得到覆盖。

根据内部审计人员的职业判断，《专项要求》的覆盖范围可记录在内部审计计划或项目工作底稿中。可以通过一个项目覆盖《专项要求》的所有内容，也可以通过多个项目达成这一目的。此外，并不一定所有要求都适用。必须保留对《专项要求》的适用性进行评估的证据，包括解释任何排除情况的理由。

附录D中的可选工具可作为参考，并用于记录内部审计人员的工作。

质量保证

《准则》要求首席审计执行官制定、实施和维护覆盖内部审计职能所有方面的质量保证和改进程序（标准8.3 质量、标准 8.4 外部评估、标准 12.1 内部评估）。审计结果必须向董事会和高级管理层通报。沟通内容中必须包含内部审计职能是否遵循《准则》以及绩效目标的实现情况。

在项目层面的督导活动中应考虑是否符合遵循《专项要求》（标准 12.3 监督和改进项目绩效），并在质量评估中对遵循情况进行评价。为准备接受质量检查，内部审计人员可使用附录D中提供的工具。

组织复原力

组织复原力指一个组织承受和适应变化的能力，尤其是充满颠覆性变革的时期。根据国际标准化组织的 ISO 22316 框架，它被定义为“一个组织在不断变化的环境中承受和适应的能力。”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。

实际上，具有复原力的组织能够更好地应对突如其来的挑战，并在面临挑战时不断发展壮大。

许多颠覆性因素可能会阻碍组织实现其战略目标和目的，包括但不限于：

- 自然灾害，如地震、火灾、洪水、飓风、海啸、热带风暴和其他极端天气事件。
- 网络攻击，如勒索软件、恶意软件、拒绝服务、数据泄露、内部威胁以及其他旨在伤害组织或阻碍其开展业务的恶意行为。

- 地缘政治冲突，如经济制裁、关税、恐怖主义、战争和国家间的其他冲突。
- 环境压力，如资源匮乏、公共卫生危机、可持续性因素或气候变化。
- 不断变化的外部因素，如不断发展的技术（包括人工智能）、合规要求（法律、监管和财务报告）的变化、就业水平、消费者需求和声誉。
- 金融挑战，如通货膨胀或通货紧缩、利率、货币汇率以及当前的市场状况，包括经济衰退或经济扩张。
- 运营方面的挑战，如复杂的流程、高度依赖第三方、地理位置、文化挑战、劳动力有限、领导力或风险管理不力。
- 供应链问题，如无法采购原材料、缺乏多样化的供应商以及商品价格波动。
- 内部事件，如关键员工流失和操作失误。

虽然破坏性事件的性质可能各不相同，但组织应制定明确的复原力战略和正式流程，以持续预测、准备、应对和适应变化。组织复原力是一个总括术语，根据组织的不同，该战略可能包括业务连续性、灾难恢复、关键功能矩阵、继任计划和恢复测试等不同组成部分。

《组织复原力专项要求》的要求包括：

- **治理**-明确界定的最低复原力目标和战略，以支持实现组织的使命和愿景。
- **风险管理**-识别、分析、管理和监控复原力威胁的程序，包括及时上报复原力事件的流程。
- **控制**-管理层制定并定期评估的控制过程，以应对复原力风险。

考虑因素

内部审计人员可利用以下考虑因素来帮助评估《组织复原力专项要求》中的要求。以下考虑因素的字母标号均可与《专项要求》中的对应要求互相参照。这些考虑因素是说明性的，但不是强制性的。内部审计人员在确定将哪些内容纳入评估范围时应依据其职业判断。

立法、政府结构或政治环境对公共部门内部审计工作的限制可能会被认为是完成这项工作某些方面时的潜在障碍。公共部门的内部审计人员应将此类范围限制记录在案，作为其风险评估流程的一部分，并运用职业判断来明确界定和报告其根据实际情况定制的检查范围。

治理方面的考虑因素

为评估如何将治理程序应用于复原力目标，内部审计人员可检查以下内容：

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。它被正式传达给所有人员，并与组织的使命、愿景、文化和风险管理方法紧密结合，为其提供支持。复原力战略计划目标由董事会批准，与组织的风险管理总体方法保持一致，并定期进行测试和审查。该计划可包括业务、技术和财务要素，如：

- 业务 – 整个组织内部对复原力的协调、复原力风险评估流程、业务连续性计划（包括定期测试和报告）、危机管理、员工队伍的适应性（如远程应急能力、最低现场人员配备以及关键角色的交叉培训覆盖范围）、重要人员的继任计划、供应链复原力、关键绩效指标（KPI）的建立，以及为提高其认识对董事会成员进行的培训。
- 技术 – IT 基础设施要求、关键数据的识别（数据分类）、数据备份、网络安全加固和威胁监控、关键技术资产维护、为关键数据确定恢复点目标（RPO）和恢复时间目标（RTO）（通过恢复测试验证）。
- 财务 – 分配给复原力的预算资金、在业务中断期间维持运营的现金储备、准确记录与业务中断有关的交易的财务报告流程、降低业务中断风险的保险政策，以及用于紧急借款的信贷额度。

B. 领导组织复原力计划的人员或团队定期（如每月或每季度）向董事会提供有关复原力的最新信息，其中可能包括已定义的风险容忍度触发条件、KPI或其他信息，以反映观察结果或趋势。通报组织复原力战略目标的最新情况，包括战略监督、监测和长期规划。报告可包括以下方面的监测结果：

- 对复原力战略目标的实现情况以及可能阻碍实现目标的挑战。
- 支持复原力目标和目的的预算需求，如技术资产需求。
- 复原力风险状况，包括复原力风险环境中会影响既定风险容忍度的任何重大变化。
- 复原力内部控制的有效性，包括补救措施的进展情况。
- 衡量复原力计划成功与否的关键绩效指标。
- 招聘、培训和培养承担复原力责任的人员所需的人力资源。

C. 用于管理业务、技术和财务复原力流程的政策、程序和其他相关文件，包括：

- 如何识别和定期分析关键的复原力流程，以确定这些流程是否继续准确反映最重要的工作流程。
- 政策至少每年审查和更新一次（或根据较高的风险级别进行更频繁的审查和更新），并根据新出现的复原力风险的要求或根据从测试或实际发生的破坏性事件中吸取的经验教训进行更频繁的审查和更新。
- 审查政策和程序是否足以支持复原力举措。
- 是否为相关流程使用得到广泛认可的框架（如风险管理、信息技术或治理框架等），来加强复原力流程和相关内部控制。可以考虑的示例包括 NIST、COSO 或 ISO 等组织发布的框架，特别是 ISO 22300 系列（22316 或 22336）。

D. 已建立并以书面方式明确了的应对事件的指挥架构，确定与实现复原力目标相关的领导角色和职责。有证据表明已建立决策层级，如在业务中断期间负责复原力相关决策的人员，以及业务决策所需的批准程序，如资金支付或在业务中断期间与第三方签订合同以协助组织的能力。其他考虑因素包括以书面形式确立的上报路径和业务中断期间的临时决策权限，包括财务授权和第三方承包阈值。

E. 定期（如每年或每半年）评估负责运营和管理机构复原力流程的个人的知识、技能和能力的既定程序。这一程序可能包括确定培训项目，如现场或线上学习、会议、定制课程或专业认证。已制定继任计划的证据，以确定复原力方面的关键角色，包括场景演练，以确定只能由某个人或少数几个人执行的关键人物。对替补人员需具备的资格进行了概述。

F. 建立既定流程，用以识别可能影响实现组织复原力目标的现有脆缺陷和新威胁，并酌情确定优先次序，让内部和外部利益相关方参与建立信息和报告结构。利益相关方参与对复原力缺陷进行讨论的证据。证据可以是电子邮件、会议记录或报告，包括在全组织范围内使用指标来衡量和监控复原力有效性的证明。

风险管理方面的考虑因素

为评估如何将风险管理流程应用于复原力目标，内部审计人员可检查以下内容：

A. 组织的风险评估和风险管理程序包括了对组织复原力风险的确定，持续执行和记录，并在整个组织通报结果。复原力风险管理流程包括评估关键流程，如运营、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。除了确定复原力风险外，这些流程还包括评估可能中断业务运营的威胁和缺陷：

- 如何被初步确定并报告。
- 如何被分析，以评估实现组织目标的风险。
- 如何被缓解，包括将风险降低到可接受水平的行动计划。
- 如何被监测，包括制定持续报告计划，直至威胁得到完全解决。

其他证据可包括：

- 通过报告、电子邮件或会议记录形成的文件，指明了参与其中的业务领域。影响、可能性、速度和其他方面的风险因素都可能包括在内。
- 分析高度相关或相互依存的风险因素，以确定多重风险暴露的累积影响。
- 风险评估包括对关键资产保护层和对资源的评估，以防止出现单点故障。
- 风险评估通过纳入从实际危机、业务中断以及测试和假设结果中吸取的经验教训进行更新。
- 组织根据业务影响分析得出的潜在影响和可能性，优先考虑构成最高风险的领域。

B. 组织为个人或团队分配监测和报告复原力风险的责任，并定期检查。个人或团队成员具有复原力管理经验，理想状态下具有组织所属的行业（如医疗保健、金融服务或公共部门）的相关经验。个人或团队定期参加培训，随时了解复原力风险的新趋势。

C. 组织已建立相关流程，用以监测组织复原力风险（新出现的或已经确定的），将达到组织既定风险管理准则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及时上报。考虑对组织复原力风险的影响，包括对财务和非财务指标的影响。财务指标的示例包括收入、支出、盈利能力、现金流、债务、股价和整体价值等。非财务指标的示例包括品牌声誉、客户满意度、环境影响和人员流动等。该流程包括：

- 初步识别风险并及时上报。
- 分析评估风险及其如何阻碍组织目标的实现。
- 提出并商定风险缓解行动计划，包括如何及时将风险降低到可接受的水平。行动计划以企业风险管理总体战略为基础。提案应包括必要的风险缓解资源，如资金、工时和提高能力所需的额外技术和软件。
- 对关键风险指标进行持续的风险监测和报告，直至威胁完全消除。

D. 组织已实施相关流程，以应对危机、业务中断、紧急情况或其他事件，并从中恢复。定期对流程进行全面测试，如每季度或每年一次，也可能对特定部门进行更频繁的测试，如每月一次。关键服务可能需要更频繁的测试。事件应对和恢复过程可能包括：

- 检测 -- 持续监控网络事件。这可能包括使用入侵检测系统、威胁情报或安全信息和事件管理 （SIEM）。SIEM 可以使用人工智能来加强这一过程。在发生自然灾害或设施故障时，组织已建立沟通网络（如警报机制或通知），以便及时了解和共享信息。对于所有事件，组织都制定了通知相关应急人员和主管部门的程序。应根据事件的严重性确定优先级。
- 应对和遏制 – 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。例如，为防止在网络事件中造成进一步损害，组织实施了隔离受损资产的流程，如在事件期间重新路由网络流量或限制用户访问。对于物理事件，该组织已实施了相关程序，对破坏性事件进行物理隔离，以限制其影响，包括将员工转移到其他工作地点。
- 恢复 – 对于网络或 IT 相关事件，组织已制定程序，优先恢复重启运营所需的关键资产（如从备份中恢复数据或使服务器重新上线）。重启运营所需的其他非信息技术资源也应优先恢复。这可能包括规划关键人员或核心职能的逐步回归。
- 事件后分析 -- 组织对事件进行分析，以确定：
  - 破坏性事件的根本原因。
  - 所采取行动的效果。

- 为加强复原力流程而需要做出的改进，如更新政策、程序、风险或战略等。

通过桌面演练、模拟和演习对关键服务/职能及其依赖因素进行严格和有效的应对和恢复流程测试，可与组织的风险容忍度保持一致。这些事件可能来自内部，也可能来自外部。董事会和高级管理层可对这些活动的结果进行审查，并定期跟踪和报告改进行动。建议应具有可操作性，并有明确的负责人和时间表。

控制过程方面的考虑因素

为评估如何将控制过程应用于复原力目标，内部审计人员可检查以下内容：

A. 建立了相关程序，以确定和评估关键的第三方提供商（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。评估可考虑第三方复原力和业务连续性，并包括对每个供应商的风险评级。除了在签订正式协议前对供应商进行审查外，组织还可定期审查供应商，以持续评估风险评级。组织维护一份潜在替代供应商名单，以应对供应商关系终止。

B. 管理层进行了数据分类工作，特别是确定了从破坏性事件中恢复和维持运营所需的关键数据。该组织实施了有效的内部控制措施来保护关键数据，包括仅授予授权人员访问权限，确保关键数据得到及时备份和恢复。

C. 管理层建立了重要的信息技术控制和持续监测流程，以降低信息安全风险（包括与网络有关的风险），确保敏感数据在破坏性事件中得到保护。通过加密保护敏感数据。持续监控和实时威胁情报向管理层发出警报，并推动及时解决问题。可以使用 NIST、COSO、ISO 等组织发布的、得到广泛认可的控制框架。

D. 组织已清点关键 IT 资产，包括在危机、业务中断和紧急情况下支持业务所需的硬件、软件和服务。较难快速获取的 IT 资产被确定为高优先级资产。

E. 制定业务连续性计划和灾难恢复计划，并根据业务影响分析确定恢复小组的人员。通过桌面演练或压力测试对计划进行定期测试，如每季度或每年一次，在桌面演练或压力测试中模拟真实的紧急情况，包括测试与内部和外部利益相关方的沟通机制。向董事会和高级管理层报告测试结果，包括改进机会。

F. 建立在发生破坏性事件时改变工作环境的程序。所需的调整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。组织可采用混合或远程工作方式来取代现场工作。其他方面可能包括及时有效地调动和重新分配资源（包括信息技术和人力资源）的机制。

G. 建立了相关流程，以持续监测和报告与机构复原力有关的新威胁和缺陷，以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。监测活动可包括关键风险指标（KRI）、风险仪表板和风险前瞻性扫描活动。组织可向全体员工提供有关新威胁的最新信息，包括缓解措施或控制措施，以提高员工的认识。对所有举报活动进行记录和分析，予以及时解决，并向高级管理层通报。为解决问题，可能有必要进行持续监测，这将需要额外的报告。

H. 建立相关流程，对人员进行有关组织复原力政策和程序的教育和培训，以便在发生危机、业务中断和紧急情况时加以遵循。这一流程包括模拟破坏性场景的培训演习。定期开展培训，如每季度或每年一次。关键服务可能需要更频繁地进行测试。

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。管理层定期（如每季度或每年一次）审查资源，以确保根据感知的风险水平提供充足的资源，并向董事会通报需求。关键服务可能需要更频繁地进行测试。分析包括评估流动性、保险范围和应急资金安排。根据组织的规模、复杂程度、行业和风险状况等因素规划财务资源需求。这一过程可能包括对资金的预先批准。

J. 建立危机、业务中断和紧急情况发生后的审查程序，并通过吸取经验教训进行事件后审查分析。应在正式报告中记录审查情况，并将吸取的经验教训纳入未来的复原力计划。

附录 A. 应用场景

以下场景描述了《组织复原力专项要求》的适用情况。此外，IIA的《专项要求应用指南》提供了关于遵循强制性要求、解决受限情况和确定关键风险阈值的实用建议。

情景 1：内部审计计划内的审计项目工作范围包含了组织复原力。

当内部审计职能部门完成其基于风险的计划流程，且在内部审计计划中包含一个或多个审计项目，覆盖了组织复原力，开展此类项目必须遵循《专项要求》。可通过在内部审计计划中的一项或多项审计业务中纳入相关要求来实现对《专项要求》的遵循。

组织复原力是一个宽泛的主题，《专项要求》中的所有要求并不一定都适用于每个项目。当内部审计人员运用职业判断，确定《组织复原力专项要求》中的一项或多项要求不适用，因此应排除在审计项目之外时，内部审计人员必须记录并保留排除这些要求的理由。例如，排除某些要求的理由可能是内部审计职能轮流开展各类有关组织复原力的审计项目，或者已确定复原力风险在某个审计项目中的重要性较低。

情景 2：在某个不以组织复原力为重点的审计项目中发现了组织复原力风险。

内部审计人员在评估与复原力没有直接关系的流程时，可能会发现复原力风险。例如，内部审计人员可能会在一项不以组织复原力为重点的工作中评估人力资源流程（如聘用和留任人员），并且在为审计项目制定计划时未将复原力风险纳入审计范围。然而，内部审计人员在进行初步检查后，认定此类风险应被纳入审计范围；例如，他们发现了与组织如何留任人员有关的继任计划风险（标准 13.2 项目风险评估）。

一旦确定存在相关风险，内部审计人员必须查阅《组织复原力专项要求》，并确定哪些要求适用。在这个例子中，他们可能只需要关注有关治理的要求 E，而排除其他风险管理和控制方面的要求。他们必须在项目工作文件中记录排除《组织复原力专项要求》中其他要求的理由，并保存该文件。

情景 3：要求开展最初未列入内部审计计划的组织复原力审计项目。

董事会、管理层或监管机构等利益相关方可能会要求内部审计人员在已确定的审计计划之外开展复原力评估。例如，当组织成为网络攻击的目标时，董事会可能会要求内部审计参与评估复原力控制，以评价组织为从网络攻击中恢复所作的准备是否充分。这种情况下，《专项要求》是适用的，必须对其要求进行评估，并记录排除任何要求的情况（标准 9.4 内部审计计划）。

附录 B. 基于应用场景的审计项目示例

情景 1：内部审计计划内项目涉及了有关主题。

负责中央批发市场的公共部门机构

在其基于风险的年度规划过程中，内部审计职能将基本市场业务的连续性确定为一个高风险领域，因为它可能受到后勤中断、公共卫生事件和关键基础设施依赖条件的影响。根据评估结果，内部审计人员确定《组织复原力专项要求》适用于计划内的审计项目。

为评估治理情况，内部审计人员会调阅了董事会会议记录、战略规划和预算文件，以确定是否正式制定并监督与复原力相关的目标。他们评估了管理层是否定期向治理机构报告重大缺陷，如运输依赖条件、基础设施限制和与健康有关的风险。在没有制定统一的复原力战略文件的情况下，内部审计人员评估了复原力要素是否始终贯穿于业务和战略文件中。

从风险管理的角度来看，内部审计人员检查了组织的风险登记册，并与业务管理人员进行访谈，以确认可能影响供应连续性的风险是否已被识别、评估并指派专人负责。他们测试了此前发生事件时是否启动了上报机制，如临时关闭或限制进入，并确定应对行动是否符合既定的风险容忍度参数。

控制程序包括检查业务连续性安排，检查定期测试演习的证据，以及检查在破坏性事件中与公共当局进行协调的文件。内部审计员还检查了事件发生后的报告，以确定是否将经验教训纳入更新后的流程。如果《专项要求》中的某些规定因立法或结构性限制不适用，内部审计人员依据《标准》对不适用的理由进行了记录。

情景 2：在实施审计项目时发现涉及了有关主题。

业务遍布全球的专业服务公司

在以治理和企业风险管理为重点的审计项目中，内部审计人员发现与决策权下放、依赖当地主要领导层以及跨辖区监管风险有关的漏洞。根据这些发现，内部审计人员确定《组织复原力专项要求》的某些要素适用于此审计项目。

为评估治理情况，内部审计人员查阅了全球政策、董事会报告材料和危机管理规程，以确定组织是否已明确在监管变化、关键人员重大变化或某一国家（地区）发生可能产生更广泛影响的声誉事件时如何维持运营。他们评估了治理机构是否收到关于各国家（地区）关键风险的综合报告，以及是否明确界定了监督复原力的责任。

从风险管理的角度来看，内部审计人员检查了企业风险框架，以确认与关键人物依赖性、跨境监管合规性和声誉风险相关的风险是否与公司的战略目标相匹配。他们对选定的事件进行抽样测试，以确定本地事件是否已适当上报给全球领导层，以及是否在规定的授权范围内做出了应对决定。

与控制相关的程序包括审查各管辖区的业务连续性安排，检查关键角色是否得到充分覆盖，是否有后备人员或结构合理的继任程序来应对突发事件，以及评估支持协调远程操作的技术基础设施是否完善。内部审计人员还检查了事后分析文件，以确认纠正措施是否得到落实。如果《专项要求》中只有某些要求适用，内部审计人员将纳入或排除的依据记录在案。

情景 3：内部审计被要求开展的项目涉及了有关主题。

负责国家关键基础设施的实体

邻近国家（地区）发生的一场破坏性飓风促使一名董事会成员要求内部审计职能在其审计计划中增加一项针对组织复原力的审计，以确认该实体面临的运营中断、对专业承包商的依赖、监管义务和严重环境事件等风险。在这种情况下，《组织复原力专项要求》得到了全面应用。

为评估治理情况，内部审计人员查阅了董事会批准的战略规划和相关文件，以确认关键服务的连续性已正式纳入长期规划。他们查阅董事会的报告，以确定与业务可用性、关键资产维护和财务应急计划（包括保险范围和储备金分配）有关的关键指标是否得到了定期审查。

从风险管理的角度来看，内部审计人员评估了如何在企业风险管理框架内识别、评估和监控与基础设施中断、承包商集中、监管合规和自然环境有关的风险。他们检查了是否明确界定了监测这些风险的责任，以及在以前的服务中断期间是否遵循了上报规程，包括与监管机构和应急管理部门的协调。

控制测试包括核实是否建立了业务连续性和灾难恢复计划以及是否对其进行定期测试，检查关键资产的库存，检查与替代供应商的合同安排，以及评估事故后分析文件，以确定是否跟踪和实施了整改。当某些要求因监管规定而不适用时，内部审计人员会根据《准则》将理由记录在案。

附录 C. 与框架的映射

组织可以利用 ISO 等框架，开展自己的组织工作。内部审计人员可能已经根据这些框架制定了审计计划和测试程序。内部审计人员应将其计划开展的组织复原力控制测试与《专项要求》进行核对，以确保充分的覆盖范围（标准 13.4 评价标准）。下图将《组织复原力专项要求》与 ISO 22336 框架进行了映射对照。其他框架参考资料列于附录 E。

治理要求	ISO 22336 框架
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。	4.1、6.1、6.2、7.1、8.4、8.5、9.1、9.5
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。	6.4、8.6、10.2
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。	4.2、6.3、8.3、8.4、9.4
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。	5.4
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。	9.6
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。	9.2、9.5

风险管理要求	ISO 22336 框架
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。	4.4、5、7.3、7.4、7.5、7.6、9.2、9.3
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。	4.3、8.2、9.6
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。	7.2、7.6、10.1
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的发生并从中恢复。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。	7.2、7.6、7.8

控制过程要求	ISO 22336 框架
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。	7.7
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。	6.1
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。	7.5
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。	9.2
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。	8.6、9.6、10.3
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。	9.3

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。	7.6
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。	10.2、10.3
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。	6.4、7.6、9.6
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。	10.2、10.3

附录 D. 可选文档工具

内部审计人员应当运用其职业判断，来根据风险评估的结果确定哪些要求适用，并妥善记录排除了哪些要求。根据审计人员的职业判断，有关《专项要求》的内容可以被记录在内部审计计划或项目工作底稿中。可以通过一个项目覆盖《专项要求》的所有内容，也可以通过多个项目达成这一目的。此外，并非所有要求都一定适用。下方的可打印表格展示了记录对《组织复原力专项要求》遵循情况的一种方式，但对该表格的使用并不具有强制性。

组织复原力 - 治理

要求	已执行的覆盖范围或排除理由	文件参考
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。		

组织复原力 - 风险管理

要求	已执行的覆盖范围或排除理由	文件参考
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的发生		

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。		

组织复原力 - 控制

要求	已执行的覆盖范围或排除理由	文件参考
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。		

附录 E. 其他框架参考资料

领域	ISO 参考资料	范围/条款标题
治理：	ISO 22316:2017	政策和战略、领导承诺、共同愿景、文化、沟通、持续改进。
风险管理	ISO 31000:2018	范围/背景/标准、风险评估、处置、监测、沟通。
业务连续性/灾后恢复基础	ISO 22301：2019；ISO/TS 22317:2021	业务连续性管理体系的背景、领导、计划、运作；业务影响分析的活动和输出。
供应链复原力	ISO/T 22318:2021	供应商依赖性分析、连续性战略、替代方案、保证要求。
信息和通信技术准备度	ISO/IEC 27031	信息和通信技术的连续性、恢复目标、测试和改进、业务连续性管理体系的协调。

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.

免责声明

国际内部审计师协会出版本文件的目的是提供信息和开展教育。本资料无意为个人的具体情况提供明确的答案，因此仅供参考。国际内部审计师协会建议就任何具体情况直接寻求独立的专家建议。对于完全依赖本资料的任何人，国际内部审计师协会不承担任何责任。

版权

2026 年 4 月

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101