

第四节 风险评估

一、设计和实施风险评估程序的一般要求

由于有限保证和合理保证的保证程度不同，其风险评估程序也存在一定的区别。具体来说：

1. 在有限保证业务中，鉴证者设计和实施的风险评估程序应当到位，以识别和评估披露层次重大错报风险，包括舞弊和错误导致的重大错报风险，并设计和实施进一步程序。

2. 在合理保证业务中，鉴证者设计和实施的风险评估程序应当到位，以识别和评估披露认定层次重大错报风险，包括舞弊和错误导致的重大错报风险，并设计和实施进一步程序。

无论有限保证还是合理保证，在设计和实施风险评估程序时，鉴证者都应当执行以下工作：

1. 了解可持续事项和可持续信息；
2. 确定编制可持续信息所使用的标准是否适当；
3. 了解和评价被鉴证单位的报告政策；
4. 了解被鉴证单位及其环境；
5. 了解法律和监管环境；
6. 了解被鉴证单位内部控制体系。

在设计和实施风险评估程序时，鉴证者应当考虑在客户关系和业务的承接和保持过程中获取的信息。

项目负责人应当与项目组其他关键成员和关键外部专家讨论下列事项：

1. 可持续信息中的各项披露是否容易发生重大错报；
2. 根据被鉴证单位的实际情况运用披露标准。

针对上述事项，项目负责人应当确定需要向未参与讨论的项目组成员和外部专家告知哪些内容。

二、了解可持续事项和可持续信息

鉴证者应当了解可持续事项和可持续信息，包括可能导致披露发生重大错报的事项或情况通常具有的特征。

三、确定标准是否适当

鉴证者应当确定被鉴证单位编制可持续信息所使用的披露标准是否适当，包括该披露标准是否符合相关性、完整性、可靠性、中立性和可理解性。

四、了解和评价报告政策

鉴证者应当了解被鉴证单位的报告政策、政策变更及理由，并评价报告政策是否适当，是否与下列披露标准一致：

1. 被鉴证单位编制可持续信息所使用的披露标准；
2. 相关行业编制可持续信息所使用的披露标准。

五、了解被鉴证单位及其环境

鉴证者应当了解被鉴证单位及其环境，包括下列方面：

1. 被鉴证单位的经营性质、法律组织形式、组织结构、所有权和治理结构、业务模式；

2. 报告边界以及报告边界范围内的活动；
3. 与可持续事项相关的战略和目标以及评价被鉴证单位业绩或确定管理层薪酬的方法。

鉴证者应当向管理层、治理层、被鉴证单位其他人员或委托方询问下列事项：

1. 是否知悉任何影响可持续信息的舞弊或舞弊嫌疑、违反法律法规行为或疑似违反法律法规行为；
2. 被鉴证单位是否设有内部审计，如果是，则进一步询问内部审计针对可持续信息开展的工作和发现的情况。

六、了解法律和监管环境

鉴证者应当了解被鉴证单位所处的法律和监管环境，包括下列方面：

1. 针对被鉴证单位可持续信息披露领域，适用于被鉴证单位及所处行业的法律和监管框架；
2. 被鉴证单位是如何遵守这些法律和监管框架的。

七、了解被鉴证单位内部控制体系

无论有限保证还是合理保证，鉴证者都应当了解与可持续事项和可持续信息相关的内部控制体系各要素。在了解时，有限保证情形下通常实施询问程序，而合理保证情形下，除询问程序外，鉴证者还应当考虑实施其他必要的程序。

以下分别介绍在有限保证和合理保证情形下，鉴证者如何了解被鉴证单位内部控制体系各要素。

（一）内部环境

在有限保证业务中，鉴证者应当了解被鉴证单位与可持续事项和信息相关的内部环境（即控制环境，下同）。在合理保证业务中，鉴证者除了解被鉴证单位与可持续事项和信息相关的内部环境外，还应当评价下列事项：

1. 在治理层的监督下，管理层是否营造了诚实守信和遵守道德的组织文化；
2. 内部环境是否为内部控制体系的其他要素奠定了适当的基础；
3. 内部环境要素的控制缺陷是否会削弱内部控制体系的其他要素。

（二）风险评估

在有限保证业务中，鉴证者应当了解被鉴证单位与可持续事项和信息相关的风险评估工作的结果。

在合理保证业务中，鉴证者不能只了解风险评估工作的结果，而是应当了解被鉴证单位与可持续事项和信息相关的风险评估工作，包括下列方面：

1. 了解风险评估工作的下列步骤
 - （1）识别与实现可持续信息报告目标相关的风险；
 - （2）评估上述风险的重要程度和发生的可能性；
 - （3）应对上述风险
2. 了解风险评估工作的结果。
3. 评价风险评估工作是否适合被鉴证单位的实际情况。

（三）监督

在有限保证业务中，鉴证者应当了解被鉴证单位针对与可持续事项和信息相关的内部控制体系实施的监督工

作的结果。

在合理保证业务中，鉴证者应当了解被鉴证单位针对与可持续事项和信息相关的内部控制体系实施的监督工作及结果，并评价上述监督工作是否适合被鉴证单位的实际情况。

（四）信息系统与沟通

无论有限保证还是合理保证，鉴证者都应当了解被鉴证单位与可持续事项和信息相关的信息系统与沟通，包括了解下列方面：

1. 被鉴证单位识别拟报告可持续信息的流程；
2. 外部来源的信息（例如来自服务机构或被鉴证单位价值链上其他机构的信息）是如何记录、处理、进行必要的更正并纳入可持续信息的；
3. 针对估计和前瞻性信息，被鉴证单位如何根据所使用的披露标准，确定适当的方法、假设或数据来源以及是否需要作出调整。

鉴证者应当根据上述了解的情况，评价被鉴证单位的信息系统是否能够支持可持续信息的编制。

（五）控制活动

在**有限保证**业务中，如果计划测试控制运行有效性以获取鉴证证据，鉴证者应当了解下列控制：

1. 拟测试的控制，包括其他鉴证者的鉴证报告中指出的、与被鉴证单位相关的互补性控制；
2. 针对上述第1项中的控制，为应对运用信息技术导致的风险，被鉴证单位实施的信息技术一般控制。

鉴证者应当实施下列程序，以了解上述第1项和第2项所述的控制：

1. 评价控制是否得到恰当设计，以应对披露层次重大错报风险或支持其他控制的运行；
2. 实施除询问被鉴证单位人员以外的其他程序，以确定控制是否得到执行。

在**合理保证业务**中，鉴证者应当考虑下列问题，以识别需要了解的控制：

1. 鉴证者拟测试哪些控制的运行有效性以获取证据，其中应当包括以下控制：
 - （1）用于应对仅实施实质性程序不能提供充分、适当鉴证证据的风险的控制；
 - （2）其他鉴证者的鉴证报告中指出的、与被鉴证单位相关的互补性控制。
2. 针对上述第1项所述的控制，哪些信息技术应用程序和信息技术环境可能面临运用信息技术导致的风险。
3. 针对上述第2项明确的**信息技术应用程序和信息技术环境**，被鉴证单位采用了哪些信息技术一般控制来应对运用信息技术导致的风险。
4. 对于识别和评估披露认定层次重大错报风险，并设计进一步程序以应对这些风险而言，鉴证者认为适当的其他控制。

为了解上述第1-4项所述的控制，鉴证者应当实施下列程序：

1. 评价控制是否得到恰当设计，以应对披露认定层次重大错报风险或支持其他控制的运行；
2. 实施除询问被鉴证单位人员以外的其他程序，以确定控制是否得到执行。

（六）识别控制缺陷

鉴证者应当根据对被鉴证单位内部控制体系各要素的了解，考虑是否识别出控制缺陷。

八、管理层凌驾于控制之上的风险

与审计类似，实施风险评估程序的目的在于以此为基础设计和实施鉴证程序，以应对评估的重大错报风险。由于管理层凌驾于控制之上的方式具有不可预见性，在合理保证业务中，鉴证者应当将管理层凌驾于控制之上的风险作为舞弊导致的重大错报风险，并评估为最高风险等级。

九、评价风险评估程序获取的鉴证证据

鉴证者应当确定实施风险评估程序获取的鉴证证据能否为识别和评估重大错报风险提供充分的依据。如果不能，鉴证者应当追加风险评估程序，直至获取的证据能够提供充分的依据。

十、风险评估程序的工作底稿

针对风险评估程序，鉴证者应当在工作底稿中记录下列事项：

1. 项目负责人与项目组其他关键成员和关键外部专家开展的讨论及得出的重要结论；
2. 鉴证者在了解与可持续事项和信息相关的内部控制体系各要素时，了解、询问和讨论的关键内容；
3. 对控制是否得到恰当设计和执行的评价结果；
4. 识别和评估的披露层次重大错报风险或披露认定层次重大错报风险。