该标准规定治理机构应通过**评估**、**指导**和**监督**三个主要任务来治理 IT。**【口诀：评指监】**

3.2 IT 审计（掌握）

为了有效控制 IT 风险，有必要对组织的信息系统治理及 IT 内控与管理等开展 IT 审计，充分发挥 IT 审计**监督**的作用，**提高**组织的信息系统**治理水平**，**促进**组织信息系统治理**目标的实现**。

1、IT 审计基础（掌握）

IT 审计重要性是指 **IT 审计风险（固有风险、控制风险、检查风险）对组织影响的严重程度**，如：**财务损失、业务中断、失去客户信任、经济制裁**等。

1. IT 审计定义

IT 审计经过多年的发展，国内外机构对 IT 审计从不同角度进行了描述，目前主流的 IT 审计定义如表所示。

机构/标准名称	定义
国际信息系统审计协会（Information Systems Audit and Control Association，ISACA）	IT 审计是一个获取并评价证据，以判断计算机系统是否能够**保证资产的安全、数据的完整以及有效利用组织的资源并有效实现组织目标**的过程
国际货币基金组织（International Monetary Fund，IMF）	IT 审计是对计算机化的系统进行审计，不仅是对现有信息系统的控制，还包括对系统建立过程、计算机设备和网络管理等方面的控制
最高审计机关国际组织（International Organization of Supreme Audit Institutions，INTOSAI）	IT 审计是一个通过获取并评估证据，以判断 IT 系统是否保护组织的资产，有效地利用组织的资源，保障数据的安全性和一致性，以及有效地达到组织业务目标的过程
GB/T 34690.4《信息技术服务 治理 第 4 部分：审计原则》	IT 审计是根据 IT 审计标准的要求，对信息系统及相关的 **IT 内部控制和流程进行检查、评价，并发表审计意见**

2. IT 审计目的

IT 审计的目的是指通过开展 IT 审计工作，了解组织 IT 系统与 IT 活动的总体状况，**对组织是否实现 IT 目标进行审查和评价**，**充分识别与评估相关 IT 风险**，**提出评价意见及改进建议**，促进组织实现 IT 目标。

组织的 IT 目标主要包括：①组织的 IT 战略应与业务战略保持一致；②保护信息资产的安全及数据的完整、可靠、有效；③提高信息系统的安全性、可靠性及有效性；④合理保证信息系统及其运用符合有关法律、法规及标准等的要求。

3. IT 审计范围

一般来说，IT 审计范围需要根据审计目的和投入的审计成本来确定。在确定审计范围时，除了考虑前面提及的审计内容外，还需要明确审计的组织范围、物理位置以及信息系统相关逻辑边界。IT 审计范围的确定如表所示。

IT 审计范围的确定

IT 审计范围	说明
总体范围	需要根据审计目的和投入的审计成本来确定
组织范围	明确审计涉及的组织机构、主要流程、活动及人员等
物理范围	具体的物理地点与边界