IIA实务公告2100-11：广泛性信息系统控制的效果 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/86/2021_2022_IIA_E5_AE_9E_E5_8A_A1_E5_c53_86846.htm 《国际内部审计专业实务标准》中第2100条标准的解释 相关标准：第2100条标准工作性质 内部审计活动应当通过应用系统的、规范的方法，评价并改善风险管理、控制和治理过程。 本实务公告源自国际信息系统审计和控制协会（ISACA）指引广泛性信息系统控制的效果，文件G11。该信息系统审计指引由ISACA于2000年3月发布。引用该文件经过ISACA的许可和确认。本实务公告与ISACA指引的任何差异，ISACA不保证其准确性或支持这些改变。 本实务公告性质：内部审计师实施信息系统控制检查时应当考虑以下建议。本实务公告无意囊括实施信息系统审计所需要的所有程序，仅推荐一系列高层次审计师责任，作为制定详细审计计划的补充。 1 控制框架概述COBIT将“ 控制 ”定义为“ 政策、程序、实务及组织结构的设计，用来合理确保组织目标的实现，并确保不希望发生的事件被预防或发现并纠正。 ”针对每一项信息系统审计，内部审计师应当区分影响所有信息系统和运营的一般控制（广泛性信息系统控制），以及在更为特定的层次运行的控制（详细信息系统控制），以便将审计力量集中在与审计目标相关的风险领域。以下描述的控制框架有助于内部审计师达成这一重点。 广泛性信息系统控制广泛性信息系统控制的例子包括COBIT“ 计划和组织 ”范畴及“ 监督 ”范畴所定义的信息系统过程控制，如，“ PO1订立IT战略性计划 ”及“ M1监督各项流程 ”。广泛性信息系统控制是一般控制的一个子集合，即侧重

于信息系统管理和监控的一般控制。广泛性信息系统控制的效果并不局限于财务系统应用控制的可靠性，广泛性信息系统控制也影响下列详细信息系统控制的可靠性，例如，l 程序开发l 系统实施l 安全管理l 备份程序薄弱的信息系统管理和监控（例如，薄弱的广泛性信息系统控制）应当警示内部审计师一项高风险，即设计用于详细层次运行的控制可能失效。详细信息系统控制详细信息系统控制是由应用控制和未包含于广泛性信息系统控制的一般控制所组成的。在COBIT框架中，详细信息系统控制是指与信息系统和服务的取得、实施、交付和支持有关的控制，例如对以下事项的控制：l 成套软件的安装l 系统安全参数l 灾难恢复计划l 数据输入验证l 例外报告的产生l 锁定试图无效存取的用户帐号应用控制是详细信息系统控制的一个子集合，例如数据输入验证，既是详细信息系统控制又是一项应用控制。安装及确认系统（AI5）属于详细信息系统控制，但并非应用控制。 信息系统控制之间的关系如下列大纲所示：l 信息系统控制l 一般控制l 广泛性信息系统控制l 详细信息系统控制l 应用控制 内部审计师应当考虑非信息系统控制对审计范围和程序的影响。 广泛性信息系统控制和详细信息系统控制之间的互动COBIT框架将信息系统控制区分为四个范畴：l 计划与组织l 取得与实施l 交付与支持l 监控 “ 取得与实施（AI） ” 和 “ 交付与支持（DS） ” 两个范畴的控制效果受到 “ 计划与组织（PO） ” 以及 “ 监控（M） ” 两个范畴的控制运营效果的影响。管理层的不当计划、组织和监督，意味着取得、实施、服务交付及支持方面的控制将失效。相反，强有力的计划、组织和监控可以识别并纠正关于取得、实施、服务交付及支持方面的无效控制。 例如，

“ 取得和维护应用软件 ”（COBIT 流程索引AI2）流程的有效详细信息系统控制受到下列广泛性信息系统控制的充分性的影响：l 订立IT战略性计划（COBIT流程索引PO1）l 项目管理（COBIT流程索引PO10）l 质量管理（COBIT流程索引PO11）l 监督各项流程（COBIT流程索引M1）应用系统取得的审计应当包括确认信息系统战略的作用，项目管理方法，质量管理以及监督的方法。例如，当项目管理不当时，内部审计师应当考虑：l 开展额外的工作，以保证该项目属于有效管理；l 向管理层报告广泛性信息系统控制的缺陷另一个例子为，“ 确保系统安全 ”（COBIT流程索引DS5）流程的有效详细信息系统控制受到下列广泛性信息系统控制的充分性的影响：l 定义信息技术组织及关系（COBIT流程索引PO4）l 沟通管理目的和方向（COBIT流程索引PO6）l 评估风险（COBIT流程索引PO9）l 监控流程（COBIT流程索引M1）对系统安全参数适当性的审计，例如，UNIX，WINDOWS NT，RACF，应当考虑管理层的安全政策（PO6），安全责任的分派（PO4），风险评估程序（PO9），安全政策遵循情况的监督程序（M1）。即使这些参数与内部审计师 “ 最佳实务 ” 的观点不一致，在考虑管理层认识到风险，以及指引如何应特定风险水平的管理政策的情况下，这些参数可能被评估为适当的。审计建议应针对风险管理或政策，以及详细的系统安全参数本身。