国际内审协会IIA实务公告2100-9：应用系统检查 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__E5_9B_BD_E9_99_85_E5_86_85_E5_c53_86840.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）指引应用系统检查，文件G14。该信息系统审计指引由ISACA于2001年11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：内部审计师实施应用系统检查时应当考虑以下建议。本实务公告无意囊括与应用系统检查相关的综合性确认或咨询业务所需要的所有程序，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 首席审计执行官应当确定内部审计活动具备或者可以取得独立[1]并且胜任的审计资源，开展应用系统检查并评估相关的风险暴露。 审计计划的考虑 2 审计计划的一部分内容是充分了解组织的信息系统环境，便于内部审计师确定系统的规模和复杂程度，以及组织对信息系统的依赖程度。内部审计师应当了解组织的目的和业务目标，运用信息技术和信息系统的水平和方式，与组织的目的及其信息系统相关联的风险和披露情况。此外，还需要了解组织结构，包括主要信息系统人员和应用系统业务处理负责人的职权和责任。审计计划过程中还应当考虑业务领域的风险。 审计计划的主要目的是确定应用水平的风险。相关水平的风险影响所需要的审计证据的水平。系统

层面和数据层面的应用水平风险包括以下内容：l 与缺乏系统操作能力相关的系统可获得性风险 l 与未经授权进入系统或取得数据相关的系统安全性风险 l 与处理数据不完整、不准确、不及时和未经授权相关的系统完整性风险 [1] 独立指内部审计师未介入应用系统的开发、收购、运行或维护等工作。l 在要求持续提供系统的可获得性、安全性和完整性的情况下，与无法更新系统相关的系统维护风险 l 与数据全面、完整、保密、准确、及时相关的数据风险 针对应用水平风险的应用控制可以采用系统内置的计算机化控制，或者手工实施的控制，或者两者结合的形式。例如计算机化文件核对（采购订单、发票和收货报告），核对和签署机打票据，由高级管理人员对特殊报告进行检查。 在选择信赖程序控制的情况下，应当考虑相关的总体信息技术控制以及与审计目标有关的控制。总体信息技术控制可以是一项单独的检查，主要包括：物理控制、系统层的安全、网络管理、数据备份以及应变计划。根据检查的控制目标，内部审计师可以不需要检查总体控制，例如，对应用系统进行评估用于收购的情况。 应用系统检查可以在一整套应用系统用于收购目的进行评估的时候开展，可以在系统投产之前（运行前）和投产之后（运行后）进行。运行前应用系统检查的涵盖范围包括应用水平的安全构造，执行安全措施的计划，系统和用户记录的充分性，实际或计划的用户接受测试的充分性。运行后应用系统检查的涵盖范围包括运行后的应用水平安全，如果存在数据和主文件信息从旧系统向新系统转换的情况，则包括系统转换的检查。 