保险公司的信息系统审计 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/87/2021_2022__E4_BF_9D_E9_99_A9_E5_85_AC_E5_c53_87923.htm 一、信息系统审计的内容 １．管理流程审计 信息技术管理流程审计主要评估与公司发展战略目标相一致的信息技术规划，评估信息技术工作条例或工作程序，评估信息技术部门的工作职责与工作分工，评估信息系统取得开发、购置、引进的制度和流程，评估生产系统的运行维护的制度和流程，评估项目管理、项目监理的制度和流程，评估信息系统的安全管理制度，评估开发、测试、生产系统分岗制衡管理制度等。 ２．技术平台审计 信息技术平台审计主要评估信息技术基础平台的运行与安全管理，包括网络运行与安全管理如路由器、网络设备、防火墙、通信线路等、硬件运行与安全管理如小型机、服务器、前置机、打印机、扫描仪、存储设备、ＰＣ、终端等、操作系统及数据库等运行平台的运行与安全管理如Ｕｎｉｘ、Ｗｉｎｄｏｗｓ、数据库、中间件、应用开发工具、应用发布工具、版本管理工具、项目管理工具、防/杀毒工具等。 ３．信息系统项目审计 信息系统项目审计主要评估信息系统项目管理与项目监理的有效性。 项目管理审计主要评估项目启动、立项、需求分析、系统设计、开发、测试、试点、验收、推广过程的有效性，评价系统开发生命周期中的每一个程序是否均被严格执行，评价系统迁移的方案与效果，评价各类项目文档是否齐全。其目的是控制项目进展过程中的风险。 项目监理审计主要评估项目监理在信息系统建设过程中发挥的作用，评估项目监理是否有效保证了信息系统建设的质量、

进度和成本符合项目立项时的要求。 评估项目管理与项目监理间的责职是否清晰，分工是否明确。 ４．生产系统审计 信息系统的上线与投产，仅仅是信息化的开始，大量的风险与问题将出现在信息系统的生产运行与维护阶段。保险公司内部一般均建立了核心业务系统、人员营销员等管理系统、财务系统、精算系统、再保系统等生产系统，公司的生产经营活动大多要通过生产系统进行，生产系统审计便显得更为重要。 生产系统的审计首先是信息系统与业务流程吻合审计，主要评估实际业务操作流程与信息系统操作流程的吻合情况，评估信息系统对需求的满足度及信息系统操作流程与业务操作流程的吻合度。以退保操作流程为例，退保的典型处理方式是在信息系统中产生应付信息，而财务支付退保款后不再在系统中确认已付款，这就导致系统信息与实际情况不一致，致使流程与数据均不完整，流程被短路、数据被割裂，最终导致数据可用性差，并留下安全隐患。其次是评估与信息系统相关的风险。评估数据访问授权、系统功能授权、业务操作授权、业务审批决定授权是否有效，是否拥有防止非法进行数据修改的措施。评估或测试信息系统中的关键控制点是否得到有效控制，如核赔中结案环节控制，需评估结案前的赔案信息状况，如资料是否完整，计算是否正确，会签、审批是否完成。同时需评估结案后的流程执行是否完整，如数据流是否与业务单证流一致。也可评估结案后对保单承保如结案后要求限制承保、保全如结案后要求扣还保单质押借款、生存给付如结案后要求中止生存给付或确保再给付几年等的影响，测试该关键点对保单生命周期各环节的影响是否合理与正确。 二、信息系统审计流程 信息系统审计的工作

流程主要包括确定审计范围、做好审计准备、进行审计评估、出具审计报告、提供管理咨询等过程。 可根据审计目标，确定审计范围。例如，是进行全面审计还是专项审计；是进行全公司审计还是部分分公司审计。在此基础上制定审计预案，审计预案中要确定审计依据、人员分工、审计工作程序、方法技巧、审计工作文档模板与案例、审计时间表，并注明需重点关注的地方，也可以将审计预案制作成审计工作手册，让每一个审计人员得到同样的信息。 进行审计评估时，应对照审计依据，了解被审计单位的信息技术管理流程、技术基础平台、生产系统运行环境与管理制度，通过关键点测试等方式做出公正、合理的评估。完成后还需出具详细的审计报告，对被审计信息系统或专项被审计对象进行鉴证，并提出必要的管理建议书，也可主动为被审计单位提供管理咨询，促进或帮助被审计单位提高信息系统管理水平。对于公司内部审计，还有一个通过提供管理咨询帮助其提高管理水平的过程，如总公司对分公司的审计，或公司内部对信息系统的审计，更多的责任或义务是通过内部审计发现信息技术管理中的不足，提出改进建议，并督促或辅导职能部门改进、完善。 三、信息系统审计方法 １．信息系统审计机构 保险公司应有专门的机构负责信息系统审计工作，制定信息系统审计管理制度和工作程序、设计审计方案、制作审计计划、开发审计评估、出具审计报告、提出改进建议、提供管理咨询。 ２．常规审计与专项审计 信息系统审计也可分为常规审计和专项审计。常规审计为例行的全面审计，如每年一次对信息系统进行全面的审计，包括管理流程、技术平台、项目开发和生产系统审计，对信息系统做出全面的评估、鉴证，

提出管理建议。专项审计可以针对信息系统管理的某一方面进行专门的审计，可以视实际情况选择进行。如信息系统运行安全的专项审计，可以对公司在信息系统方面的安全管理措施、技术措施的实际应用情况进行审计评估、鉴证，提出管理建议。专项审计针对公司重点关心的专项问题，针对性强。专项审计也可用于高级信息技术管理人员的离任审计。

３．现场审计与非现场审计 信息系统审计可在现场进行，也可在非现场进行。现场审计适用于需在现场访谈、观察、测试、调查的情况。如对信息系统操作流程与实际业务操作流程吻合度的审计，需在现场观察数据流与实物流的流转情况。非现场审计主要借助非现场审计系统进行，通过计算机系统进行审计。如对万能险账户积数与账户余额的监控，可以通过计算机系统进行远程随机实时审计，也可要求被审计单位打印指定账户积数与余额后传真至审计机构进行审计。现场审计与非现场审计可以发挥定期审计与随机实时审计相结合的优势，使信息系统审计制度化。

４．外部审计、内部审计与自查审计 外部审计是指由公司外部独立的专业审计机构进行的审计，可对信息系统做出合理、公正的评价，可参照财务审计，每年进行一次。内部审计主要由保险公司内部的审计机构对信息系统进行审计，其目的在于帮助信息管理部门找差距，并督促和辅导信息管理部门提高信息系统管理水平。自查审计主要由各级信息技术管理部门对照信息技术管理标准自查、自纠，进行自我管理与自我完善。

５．通过审计系统进行审计 信息系统审计的常用方法有访谈、观察、现场测试、调阅文档、调查信息系统相关角色等，也可以开发审计系统对生产系统进行审计。

要实现通过审计系统对生产

系统进行审计，必须加强对生产系统建设的事前和事中审计，在生产系统立项、建设时，应明确审计要求，审计人员应参与生产系统的立项、需求分析、设计、验收等工作。在生产系统中，应设置审计接口，记录审计轨迹，由计算机自动记录审计线索，对于修改与删除的操作，应参照会计的红字更正法，在生产系统中留下可追溯的记录。在对生产系统进行验收的过程中，除评价系统是否达到了设计目标、是否满足需求外，还需强调生产系统的可审计性。在开发生产系统的同时，也要开发相应的审计系统，使生产系统投产后就有相应的审计系统投产运行。 开发相应的审计系统，应借鉴国际通用的审计软件，形成一套有保险公司自身特色的通用审计系统，通过对数据的采集、比对、分析，对关键审计点的跟踪、监控、反馈，保障生产系统健康、安全地运行。通过审计系统的应用，汇集大量的审计案例，分析其中的规律，强化已有的控制点，发现或部署新的控制点。这样，一方面进一步改进生产系统的运行状况；另一方面进一步完善审计系统自身功能，使生产系统与审计系统的应用水平共同提高。 四、信息系统审计的目标与任务 信息系统审计的根本目标是促进信息系统安全、稳定、有效、持续运行。通过对信息系统的安全性、稳定性和有效性进行审计、咨询，降低保险公司面临的信息系统风险，促使保险公司信息技术发展目标与其总体经营目标、战略相一致。其任务是完成对信息系统的鉴证、促进和咨询。 １．鉴证 信息系统审计的鉴证是指通过审计，合理地保证被审计单位信息系统及其处理、产生的信息的真实性、完整性与有效性，政策遵循的一贯性。在市场经济下，保险公司的信息资料对其生存、发展非常重要，

是其重要的信息资产；同时对利益相关者如监管者、投资者、代理人或机构、团体客户、个人客户等也非常重要。信息系统审计以其独立的身份，对保险公司的信息系统进行审计，查出其中的各种错误、舞弊、风险、不足，有效地保证了被审计信息系统及其处理、产生信息的真实性、完整性、有效性，是维护保险公司正常生产经营不可或缺的重要手段。２．促进 信息系统审计完成后需出具审计报告，以鉴证被审计信息系统的真实、完整、有效。这可增强人们对保险公司信息系统的信任度。诚信即价值，经鉴证后的信息系统对信息的使用者是有价值的，高可信的信息系统可以吸引更多的投资者，这对积极争取上市的保险公司具有重要意义。信息系统审计还可出具管理建议书，对信息系统中存在的错误、舞弊、风险、不足提出控制或改进建议，以促进被审计单位对信息系统进行全面审视，并针对上述问题设计解决方案并努力完善。 ３．咨询 保险信息化产生的风险是多样的，数据大集中也将风险进一步集中起来，只有控制、化解风险才能保障信息系统安全、稳定、持续运行。通过外部的信息系统审计，可借助于其相对于信息系统建设者、使用者、服务提供厂商的独立性，依据其专业的风险管理经验或知识，在保险公司信息化过程中帮助其建立、健全内部控制制度，进行系统诊断、评估和咨询；也可根据实际情况，客观中立地提出合适的信息系统解决方案，帮助保险公司改进管理流程、优化信息系统，使信息系统能更好地服务于保险公司经营管理的需要。通过审计咨询，也使信息系统审计能更好地服务于保险公司信息化建设。 五、当前保险公司开展信息系统审计的建议 保险公司的信息系统审计尚处于探索、起步阶段，

需要一个渐进的过程。在当前情况下，信息系统审计人员应参与生产系统建设，使生产系统在建设过程中即得到专业的审计指导，从而为生产系统投产后的审计工作提供标准的审计接口，为今后审计系统自动进行生产系统审计打好基础。保险公司信息系统外部审计通过引入专业审计机构进行，可与外部财务审计相结合，在进行外部财务审计时进行信息系统审计，审计重点可集中在管理层所关注的局部问题。信息系统内部审计可在公司内部稽核工作中进行，在进行业务稽核、财务稽核时开展相应的信息系统审计，审计范围可确定为管理层所关注的风险控制点。信息系统自查、自纠式审计，可通过信息技术管理达标活动，对照标准，自查自纠；也可参照外部审计、内部审计的审计标准，进行自我评估与自我提高。信息系统审计也可从专项审计开始，如信息系统安全审计、生产系统运行流程审计，或更细的退保处理审计、间接佣金处理审计，在“点”、“线”基础上，不断积累审计要素、审计标准、审计方法、审计关键控制点，并以此为基础开发相应的审计系统，改进审计手段、提高审计效率，使信息系统审计工作有方法、有成果、有经验、有软件，以“点”带“面”，以“线”促“块”，从而分步演进，形成整体化的、程序化的、制度化的信息系统审计体系。 国际上信息系统审计已经体系化、标准化、程序化了。国内银行业也已从最初的内部非现场稽核发展为信息系统审计。相对而言，我国保险业的信息系统审计起步晚，通常在外部财务审计的过程中，附带少量的信息系统的抽查与稽核，与信息化的高度发展相比，信息系统审计相对滞后，应加快发展。信息系统审计的发展，关键在行动，通过探索、尝试、总结、

完善，使之成为保险公司信息化风险防范的制度化措施。通过对信息系统的外部审计、公司内部审计和自查审计促进信息系统特别是生产系统的安全、稳定、持续运行从而为保险公司的诚信服务和稳健经营提供强有力的技术保障。