附件

# 第3205号内部审计实务指南—信息系统审计

## 目 录

# 前　言

随着我国信息技术的不断发展，相关组织根据实际工作需要开展建设的信息系统也越来越多。而实务工作中信息系统由于标准不一，建设和应用的要求不同，使得信息系统审计实践工作缺乏统一的依据和参考。为了规范信息系统内部审计实务工作，中国内部审计协会组织编写了本指南。作为内部审计准则体系的一部分，指南为广大内部审计机构和人员提供指导性的操作规程和方法，便于规范信息系统审计行为，控制审计工作风险，提高审计工作效率和质量。

本指南根据《内部审计基本准则》《内部审计人员职业道德规范》《第 2203 号内部审计具体准则——信息系统审计》《信息技术服务、治理、安全审计》（中国电子工业标准化协会）《中华人民共和国国家标准信息技术服务治理第 4 部分：审计导则》（GB/T34960. 4-2017）、《COBIT 5. 0》(信息系统审计与控制协会（ISACA）2012)《全球技术审计指南 GTAG》（国际内部审计师协会）《中华人民共和国网络安全法》《网络安全等级保护基本要求》（GB/T22239-2019）《关键信息基础设施网络安全保护基本要求》（报批稿）等标准制定。

本指南力求结合国内信息系统审计现状，参考相关组织内部信息系统审计管理规定、信息化评价办法、信息系统审计指

导意见、规范等，围绕组织信息系统涉及的组织层面、一般控制、应用控制三方面内容，梳理信息系统审计可能涉及管理环节的关键控制点，结合信息系统建设业务流程中的立项、开发、应用及运维全过程，选取信息系统审计所涉及的建设需求分析、立项管理、预算管理、成本管理、招投标管理、采购管理、合同管理、进度管理、安全管理、质量管理、应用及运维管理、运行的效果及效率等方面，全面系统地提出信息系统审计的内容框架及实务操作指南。

由于当前信息化对新技术应用的逐步深入，信息系统审计不可避免地会涉及对新技术应用（例如云计算、物联网等）的审计和某些常见专题（IT 外包、业务连续性等）的审计，本指南把这部分内容汇总在一起，单独形成一个信息系统专题审计的章节，以便于当前使用和未来扩展。

本指南共分六章，其中：第一章介绍了信息系统审计的基本概念、内容体系和审计程序等基础知识，提供关于信息系统审计的总体概念框架；第二章介绍了组织层面信息系统管理控制审计；第三章介绍了信息系统一般控制审计；第四章介绍了信息系统应用控制审计；第五章介绍了信息系统相关专项审计；第六章介绍了信息系统审计的质量控制；附录中涉及了本指南中的相关术语、主要法规参考标准及相关实务案例。

本指南突出以内部控制为基础的流程审计及以风险管理为基础的风险导向审计，以评价信息系统建设程序和内容的合法合规性，信息系统数据的真实性、准确性，信息系统的安全性，以及信息系统应用的效果性、效率性等为目标，帮助内部审计人员确定适用的审计依据、审计流程、审计方法等，力求达到简明、易懂、易操作的目的。其内容是开放性的，将随着信息系统审计实践工作的不断深入做进一步充实和完善。

本指南适用于各类组织的内部审计机构、内部审计人员开展的信息系统审计活动。其他组织或者人员接受委托、聘用，承办或者参与内部审计业务的，应当参照本指南。

本指南自 2021 年 3 月 1 日起施行。

# 第一章　概 述

## 第一节　信息系统审计总体要求

### 一、信息系统审计基本概念

信息系统审计是指内部审计机构和内部审计人员对组织信息系统建设的合法合规性、内部控制的有效性、信息系统的安全性、业务流程的合理有效性、信息系统运行的经济性所进行的检查与评价活动。

信息系统审计包括审计计划、审计依据、审计方法、审计技术、审计人员配置、审计实施流程、审计报告以及审计质量控制等内容。内部审计机构应建立信息系统审计的相应组织管理体系，对信息系统审计的流程和质量进行管控，并依照规章制度开展信息系统审计。

### 二、信息系统审计一般原则

组织应建立信息系统审计组织管理体系，并根据有关制度、标准和要求开展信息系统审计活动。其一般原则包括：

1. 信息系统审计需结合所在组织的战略目标、业务目标、治理要求和管理授权开展审计。

2. 信息系统审计应合理保证信息系统的运行符合法律法规以及相关监管要求。

3. 信息系统审计应在充分了解组织信息系统治理、管理和应用的基础上做出客观评价。

4. 信息系统审计应结合组织的业务流程、信息系统及应用数据开展审计工作。

5. 信息系统审计应不断提升内部审计人员技能，严格履行审计程序，提高审计工作质量。

**三、内部审计机构在组织信息系统审计中的职责和义务包括但不限于：**

1. 编制组织信息系统审计中长期规划。

2. 编制组织信息系统审计年度计划、预算及审计资源计划。

3. 制定组织的信息系统审计相关制度及流程等。

4. 按信息系统审计规章制度、有计划地开展相关业务。

5. 承担对信息系统控制设计和执行有效性评估的责任。

6. 做好与组织内、外相关机构和人员的沟通协调工作。

**四、内部审计机构在信息系统审计过程中的权力包括但不限于：**

1. 有权参加或者列席信息系统治理及管理的重要会议。

2. 有权进行现场实物勘查，或就与审计事项有关的问题对有关机构和个人进行调查、质询和取证。

3. 若审计过程中审计范围受到限制影响审计目标和计划的实现，有权就范围受到的限制及其潜在影响与治理主体进行沟通。

4. 有权向治理主体提出提高信息系统绩效的改进意见和建议。

5. 有权对审计发现的违反信息系统法律、法规等规定或内部管理制度行为予以制止，并对相关机构和人员提出责任追究或者处罚建议。

## 第二节　信息系统审计目标与特点

### 一、信息系统审计的目标

#### （一）信息系统审计总体目标

通过对信息系统的审计，揭示信息系统面临的风险、评价信息系统技术的适用性、创新性、信息系统投资的经济性、信息系统的安全性、运行的有效性等内容，合理保证信息系统安全、真实、有效、经济。

#### （二）信息系统审计的具体目标

1. 保证信息系统建设符合国家有关法律法规和组织内部制度。保证信息系统建设方案、规划内容充分体现组织的战略目标，对信息系统建设、应用与公司的经营目标的一致性作出评价。

2. 信息系统审计应促进信息系统在购置、开发、使用、维护过程中，以及数据在生产、加工、修改、转移、删除等处理中都必须符合国家相关法律法规、准则、组织内部规定等，并应促进信息系统有效实现既定业务目标。

3. 提高组织信息系统的可靠性、稳定性、安全性，数据处理的完整性和准确性。

### 二、信息系统审计的特点

信息系统审计除了具备传统审计的权威性、客观性、公正性等特点之外，还具备一些独有的特点，如：信息系统审计可以突破物理区域限制，开展远程非现场审计；信息系统审计要求审计人员具备较高的信息化知识和技能；信息系统审计的内容更加广泛；信息系统工作难以量化，审计评价时需要定性与定量相结合等。

## 第三节　信息系统审计内容

### 一、信息系统审计内容概述

信息系统审计对象，包括操作系统、主机、网络、数据库、应用软件、数据、管理制度等。信息系统审计内容主要包括对组织层面信息技术控制、信息技术一般性控制及业务流程层面相关应用控制的检查和评价。

### 二、对组织层面信息技术控制的审计

组织层面信息技术控制审计的内容包括：

（一）控制环境

内部审计人员应当关注组织的信息技术战略规划与业务布局的契合度、信息技术治理制度体系建设、信息技术部门的组织架构、信息技术治理的相关职权与责任分配、信息技术的人力资源管理、对用户的教育和培训等方面。

（二）风险评估

内部审计人员应当关注组织在风险评估总体架构中关于信息技术风险管理流程，信息资产的分类及信息资产所有者的职责，以及对信息系统的风险识别方法、风险评价标准、风险应对措施。

（三）控制活动

内部审计人员应当关注信息系统管理的方法和程序，主要包括职责分工控制、授权控制、审核批准控制、系统保护控制、应急处置控制、绩效考评控制等。

（四）信息与沟通

内部审计人员应当关注组织决策层的信息沟通模式，信息系统对财务、业务流程的支持度，信息技术政策、信息安全制度传达与沟通等方面。

（五）内部监督

内部审计人员应当关注组织的监控管理报告系统、监控反馈、跟踪处理程序以及对信息技术内部控制自我评估机制等方面。

## 三、对信息系统一般性控制的审计

信息系统一般性控制是确保组织信息系统正常运行的制度和工作程序，目标是保护数据与应用程序的安全，并确保异常中断情况下计算机信息系统能持续运行。信息系统一般性控制包括硬件控制、软件控制、访问控制、职责分离等关键控制。审计人员应当采用适当的方法、合理的技术手段对信息系统建设的合规合法、信息系统的安全管理、访问控制、基础架构、数据保护以及灾难恢复等方面开展审计。信息系统一般性控制审计应当重点考虑下列控制活动：

### （一）系统开发和采购审计

内部审计人员应当关注组织的应用系统及相关系统基础架构的开发和采购的授权审批，系统开发所制定的系统目标以及预期功能是否合理，是否能够满足组织目标；系统开发的方法，开发环境、测试环境、生产环境的分离情况，系统的测试、审核、验收、移植到生产环境等环节的具体活动。

对应用系统的开发与实施过程所采用的方法和流程进行评价，以确保其满足组织目标。评估拟定的系统开发或采购方案，确保其符合组织战略目标;评估项目管理过程，确保组织在满足

成本效益原则的基础上实现风险管理框架下的组织业务目标，确保项目按计划开展，并有相应文档充分支持;评估相关信息系统的控制机制，确保其符合组织的相关制度规定;评估系统的开发、采购和测试、维护，对系统实施定期检查，确保其持续满足组织目标。

（二）系统运行审计

内部审计人员应当关注组织的信息技术资产管理、系统容量管理、系统物理环境控制、网络环境资源配置、系统和数据备份及恢复管理、问题管理和系统的日常运行管理等内容。一般控制措施包括但不限于保证数据安全、保护计算机应用程序正常运行、防止系统被非法侵入、保证在错误操作或意外中断情况下的持续运行等。

评估组织在信息系统运行日常操作以及信息系统基础设施管理的有效性及效率性，确保其支持组织的目标；评估信息系统服务相关实务，确保内部和外部服务提供商的服务等级是明确并可控的;评估运行管理，保证信息系统支持功能有效满足业务需求;评估数据管理，确保数据库的完整性和最优化;评估性能的发挥及监控工具与技术应用;评估问题和事件管理，确保所有事件、问题和错误被及时记录。

（三）系统变更审计

内部审计人员应当关注组织的应用系统及相关系统基础架构的变更、参数设置变更的授权与审批，变更测试及移植到生产环境系统中的流程控制等。评估变更、配置和发布管理，确保变更被详细记录。

（四）信息安全审计

内部审计人员应当关注组织的信息安全管理制度，物理访问及针对网络、操作系统、数据库、应用系统的身份认证和逻辑访问管理机制，系统设置的职责分离控制等。

内部审计人员对逻辑、环境与信息技术基础设施的安全性进行评价，确保其能支持组织保护信息资产的需要，防止信息资产在未经授权的情况下被使用、披露、修改、损坏或丢失。评估逻辑访问控制的设计、实施和监控，确保信息资产的机密性、完整性、有效性和授权使用合规性;评估网络框架和信息传输的安全;评估环境控制的设计、实施和监控，确保信息资产充分安全。

## 四、对信息系统应用控制的审计

信息系统应用控制是指在业务流程层面为了合理保证应用系统准确、完整、及时完成业务数据的生成、记录、处理、报告等功能而设计、执行的信息技术控制。对业务流程层面应用控制的审计应当考虑下列与数据输入、数据处理以及数据输出环节相关的控制活动：

（一）授权与批准

审计应用程序的访问控制，必须关注是否有被授权的使用人才可以访问系统数据或执行授权范围内的程序功能，输入控制是否保证每笔被处理的事务能够被正确完整地录入与编辑，是否只有合法且经授权的信息才能被正确输入。

（二）系统配置控制

审计配置控制主要关注应用系统基础参数的设置与调整。包括参数的正确性、审批与授权、调整日志等。

（三）异常情况报告和差错报告

审计信息系统在出现不能正常运行、计算结果错误等异常情况时，系统能否自动提醒、处理，接收、保存差错输出报告。

（四）接口/转换控制

审计应对接口的数据流向、数据传输能力、数据转换准确性等进行测试和检查，接口/转换能否保证数据流通的正确性以及数据传输能力是否满足系统功能需求。

（五）一致性核对

审计系统间传输时，需重点检查传输报告分发是否建立了相应的人工控制环节，包括但不限于安全打印、接收签名、加密、只读等，以防范非法篡改造成不一致。

（六）职责分离

审计系统数据的录入、修改与审核的职责分离，关注对数据进行加密和敏感性分级处理的规则以及加密方式是否满足工作需求。

（七）系统计算

审计信息系统对数据计算的准确性及计算效率。

（八）其他

**五、信息系统专项审计**

信息系统审计除上述常规的审计内容外，内部审计人员还可以根据组织面临的特殊风险或者需求，设计专项审计，具体包括但不限于下列领域：

（一）信息系统开发实施项目的专项审计。

（二）信息系统安全专项审计。

（三）信息技术投资专项审计。

（四）业务连续性的专项审计。

（五）法律、法规、行业规范要求的内部控制合规性专项审计。

（六）其他专项审计。

## 第四节　信息系统审计程序

信息系统审计程序一般包括审计准备、审计实施、审计报告和后续审计四个阶段。

## 一、审计准备

### （一）审前准备

内部审计人员在实施信息系统审计前，需要根据信息系统审计目标，开展审前调查，收集法规、制度依据以及其他有关资料。审前调查主要了解组织信息系统的治理管理体制、总体架构、规划和建设、应用管理情况等。具体如下：

1. 治理、管理体制。主要了解信息系统管理机构设置、管理职责、工作流程等。

2. 系统总体架构

（1）系统分布。包括系统数量、规模和分布，绘制信息系统分布图。

（2）信息系统主要类型。

（3）各信息系统的基本情况和系统之间的关联关系。

（4）信息系统应用覆盖面及应用程度。

3. 规划和建设情况

（1）规划：信息系统发展规划以及规划、年度计划落实情况。

（2）建设：信息系统建设程序、投入、管理，了解已完成系统和在建系统。

（3）使用：信息系统应用管理制度、使用率、应用中存在的主要问题、困难和矛盾。

（二）编制审计工作方案

根据审前准备情况，编制信息系统审计工作方案，方案内容包括但不限于被审计组织信息系统的基本情况。包括信息系统项目建设及应用情况、审计目的、审计依据、审计对象与范围、审计内容重点及方法、审计步骤与时间安排、审计组与人员分工等。在审计组组成环节，审计部门可以借助外部专家的力量，在审计组中应当有具备信息技术经验和知识的专兼职审计专家，便于补充提高审计组的胜任能力。

## 二、审计实施

审计实施是内部审计人员依据审计计划实施现场审计的过程。内部审计人员应结合审前准备了解的内容，按照被审计组织的信息化环境、业务流程、内控制度等方面的风险，明确具体项目审计目标、细化审计内容，突出审计重点。实施阶段主要应完成以下工作:

（一）了解评估被审计组织的信息系统内部控制

1. 收集被审计组织信息系统的内部控制管理制度及流程，对被审计组织相关人员进行访谈，了解组织的信息系统决策及管理政策、方法、控制活动主要内容包括但不限于：

（1）信息系统内部控制环境。

（2）风险管理。

（3）控制活动。

（4）信息与沟通。

（5）内部监督。

2. 开展控制测试

内部审计人员开展控制测试评价信息系统的内部控制要素，以确定组织能接受的控制风险。验证控制措施的执行是否符合管理政策和程序，为审计提供合理的保证。信息系统控制测试主要包括控制环境测试和功能测试：

（1）组织管理的控制测试。

（2）系统建设管理的控制测试。

（3）系统资源管理的控制测试。

（4）系统环境管理的控制测试。

（5）系统运行管理的控制测试。

（6）系统网络和通信管理的控制测试。

（7）系统数据库管理的控制测试。

（8）系统输入、处理、输出的控制测试。

（9）其他。

3. 初步评估信息系统内部控制

根据对组织信息系统的控制测试情况，选择组织信息系统的重点业务流程，对固有风险和控制风险进行初步评估，对信息系统控制有效性作出评价。

**（二）开展实质性测试**

内部审计人员应根据控制测试结果确定实质性测试的性质、时间和范围。组织层面评价内容包括组织架构、权责分配、发展战略、人力资源、培训与考核等。

对组织信息系统开展风险评估时，结合相关规范中有关风险评估的要求，重点关注内部和外部风险信息的搜集、利用风险识别机制按照风险评估的程序、方法，评估风险等级并检查应对策略的有效性。

对信息与沟通审计时，应结合组织信息与沟通的相关管理制度，对信息收集、处理和传递的及时性，反舞弊机制的健全性，财务报告的真实性，信息系统的安全性，以及利用信息系统实施内部控制的有效性等进行审查和评价。

对内部监督审计时应结合组织内部监督制度，对内部监督机制的有效性进行认定和评价。重点关注内部审计机构等监督机构是否在内部控制设计和运行中有效发挥监督作用，内部控制缺陷认定是否客观，整改方案措施是否得当，并有效整改。

内部控制检查评价方法主要包括：个别访谈法、调查问卷法、比较分析法、标杆法、穿行测试法、抽样法、实地查验法、重新执行法、专题讨论会法等。内部控制检查评价应综合运用上述方法，充分利用信息系统，实施在线检查、监控。

## 三、审计报告

信息系统审计报告阶段包括整理加工审计工作底稿、编写审计报告、做出审计结论。内部审计人员应运用专业判断,综合分析所收集到的相关证据,以经过核实的审计证据为依据，形成审计意见和结论、编制审计底稿、出具审计报告。

### 四、后续审计

后续审计主要通过监督组织整改的情况，督促被审计组织改进信息系统治理，完善相关的规章制度、流程等,以持续提高信息系统治理、管理水平。对审计中发现的重大问题和控制缺陷，整改效果不明显的信息系统项目开展后续审计。

## 第五节　信息系统审计方法与工具

### 一、信息系统主要审计方法

信息系统审计方法是为了完成信息系统审计任务所采取的手段。在信息系统审计工作中，要完成每一项审计工作，都应选择合适的审计方法。信息系统审计方法主要包括访谈法、调查法、检查法、观察法、测试和平行模拟法、程序代码检查、编码比较法、风险评估法等。

#### （一）访谈法

访谈法是指通过面对面或在线视频、音频等方式交谈来了解被审计对象的信息。依据不同问题的性质、目的或对象，采用不同的访谈形式。

（二）调查法

调查法是在制定调研计划的基础上,通过书面或口头回答问题的方式收集研究对象的相关资料,并做出分析综合,得到某一结论的研究方法。

（三）检查法

检查法是指内部审计人员对组织内部或外部生成的记录和文件(包括但不限于纸质、电子或其他介质形式存在的资料)进行检查，或对资产进行实物检查。

信息系统审计人员审阅可行性研究报告、系统分析说明书、现状分析报告、输入输出和代码调查表等文档，检查上述文档以及相应的信息系统建设、应用、管理、运行是否符合国家法律法规、行业标准以及组织内部规章制度等。

（四）观察法

内部审计人员运用观察法，观察被审计组织员工的职责履行情况以及业务操作程序等以识别员工的逻辑访问权限是否合规，软硬件物理控制是否有效，盘点信息资产是否安全。

（五）数据测试的黑、白盒法与平行模拟法

数据测试法：从计算机输入开始，跟踪某项业务直至计算机输出，以检验计算机应用程序、控制程序和系统可靠性。

黑盒法：当内部审计人员重点关注程序是否达到所需求的功能时，可采用黑盒法来设计测试数据。黑盒法设计出的测试

数据除了可以检查程序功能上的错误和缺陷外，还可以审计系统用户界面、接口、效率、初始化和终止错误。

白盒法：当内部审计人员主要关注在程序中是否存在错误的执行路线时可以采用白盒法。白盒法是从程序内部的逻辑结构出发选取测试数据的方法，它的原理是通过审计程序中的所有执行路线来发现程序中的错误和缺陷。

平行模拟法：针对某应用程序，审计人员用一个独立的程序去模拟该程序的部分功能，对输入数据同时进行并行处理，其结果和该应用程序处理的结果进行比较以验证其功能正确性的方法。

具体应用是先将测试数据输入信息系统和测试程序，经程序处理后输出结果，然后将输出结果与测试程序的结果相比较，从而确定系统的控制及应用程序在逻辑上是否正确。

内部审计人员在设计测试数据时，应充分考虑信息系统中可能发生的每一种错误包括但不限于：

1. 数据类型错误。

2. 顺序紊乱的编码。

3. 数据超越了限制的条件。

4. 数据比较出错。

5. 无效的账户编码及关键字。

6. 不合理的逻辑条件判断。

7. 内部数据文件不匹配。

8. 计量单位用错。

### （六）程序代码检查法、编码比较法

程序代码检查法是指对被审计程序的指令逐条审计,以验证程序的合法性、完整性和程序逻辑的正确性。

程序编码比较法：比较两个及以上独立保管的被审计程序版本，以确定被审计程序是否经过修改，并评估程序的改动所带来的后果。

### （七）风险评估法

风险评估常用技术。分级技术：根据审计对象的技术复杂性、现有控制程序的水平、可能造成的财务损失等各种因素的风险值累计为总风险值，根据分值大小进行排列分为高、中、低级风险。经验判断法：内部审计人员根据专业经验、业务知识、管理层的指导、业务目标、环境因素等进行判断，以决定风险大小。

## 二、信息系统审计的工具

### （一）数据分析工具

数据分析工具主要有文件查找工具、数据检索工具、数据结构转换工具、指针检测工具、数据处理工具(包括但不限于排序、合并、复制、创建、修改、删除、重组)、文件打印工具、数据比较工具等。

（二）数据库审计工具

数据库审计工具是指跟踪数据和数据库结构变化的工具。包括本地数据库审计、安全信息和事件管理及日志管理、数据库活动监控等。

（三）源代码安全审计工具

源代码安全审计是依据公共漏洞字典表、开放式 Web 应用程序安全项目以及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对各种程序语言编写的源代码进行安全审计。可提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、提出修改建议等一系列服务。

（四）日志安全审计工具

日志安全审计目的是收集系统日志，通过从各种网络设备、服务器、用户计算机、数据库、应用系统和网络安全设备中收集日志，进行统一管理和分析。日志审计系统功能包括信息采集、信息分析、信息存储、信息展示等功能。

（五）网络安全审计工具

网络安全审计是指按照一定的安全策略，利用记录、系统活动和用户活动等信息，检查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。也是检查评估系统安全风险并采取相应措施的一个过程。网络安全审

计从审计级别上可分为三种类型:系统级审计、应用级审计和用户级审计。

（六）专用审计工具箱

包括病毒查杀软件、坏磁盘恢复软件、数据反删除软件、磁盘反格式化软件、静态安全分析软件、动态安全分析软件、访问控制分析软件、漏洞扫描及渗透测试等专用工具软件。

## 第六节　信息系统审计组织方式

信息系统审计可以作为独立的审计项目组织实施，也可以作为综合性审计项目的组成部分实施。

当信息系统审计作为综合性审计项目的一部分时，信息系统审计人员应当及时与其他内部审计人员沟通信息系统审计中的发现，并考虑依据审计结果调整其他审计的范围、时间及性质。

信息系统审计组织方式包括但不限于：

1. 组织内部审计机构独立承担。

2. 与本组织信息系统相关部门联合开展。

3. 委托外部专门机构开展，但应做好委托项目的质量控制和保密措施。

审计目标及任务确定以后,审计部门应根据工作量大小、工作的强度与难度等，配备审计活动所需要的审计人员,组成信息

系统审计项目组。应选派技术能力、信息系统审计经验丰富的专业人员担任项目负责人及骨干人员。

# 第二章　组织层面信息管理控制审计

## 第一节　信息系统治理审计

### 一、业务概述

信息系统治理是组织治理的重要组成部分，专注于信息技术体系及其绩效和风险管理的治理规则。信息系统治理应当确保信息系统战略与组织战略的一致性、信息系统目标与业务目标一致、信息系统资源的统一管理和优化，风险的有效控制、信息技术业务活动符合法律法规规定和行业规范要求，以促进组织价值最大化。

信息系统治理是指组织中信息系统管理的治理架构、流程活动方式和运行关系，是治理主体以组织章程、监管职责、利益相关方期望、业务压力和业务要求为驱动力,建立评估、指导、监督的治理过程。

信息系统治理审计是指对信息系统治理中的体系、制度、方案、评估、指导与监督等过程进行审查和评价。

### 二、审计目标和内容

信息系统治理审计目标是评价信息系统治理是否满足组织战略需求、使其与业务目标保持一致、信息系统资源得以统一管理和优化，风险得到有效控制、信息技术业务活动符合法律法规和行业规范要求，促进组织价值最大化。

信息系统治理审计的主要内容包括：信息系统的战略规划、信息系统治理的组织架构设置、治理的职责权限分工、治理资源的合理分配、信息系统的考核及监督机制。

## 三、常见问题和风险

（一）信息系统治理与组织治理脱节。

（二）职责分工不清，未建立制衡机制。

（三）内部控制监督机制失效。

（四）信息与沟通机制失效。

（五）信息系统资源配置不合理。

（六）信息系统审计机构缺乏独立性。

（七）信息系统用户的信息技术教育和培训不足等问题。

## 四、审计的主要方法和程序

1. 访谈组织管理层中关于信息系统的主管人员，收集组织章程、收集信息系统管理的组织机构设置图，了解组织的战略布局、组织主营业务构成，从而评价信息系统架构与组织架构的一致性，信息系统战略与组织战略和业务需求的一致性。

2. 访谈管理人员，评估决策对组织信息系统风险及应对措施，评估决策及管理层对信息系统治理的支持程度。应当关注组织的风险评估的总体架构中信息技术风险管理的框架、流程和执行情况，信息资产的分类以及信息资产所有者的职责等方面。

3. 检查信息系统架构，包括但不限于：基础设施架构、应用架构、数据架构，评估治理架构和机制对设计与实施、服务与支持、监控与评估的闭环管理的有效性。

4. 查阅组织相关内部控制手册、权限指引，评估信息系统治理职权与责任分配以及制衡机制的合理性。

5. 查阅组织文件、会议纪要等流转处理记录，评估信息系统相关问题信息沟通机制的及时性、有效性。

6. 查阅组织内控审计报告、信息系统审计报告，评估内部监督机构设置、职责、权限、独立性及监督机制作用发挥情况。

## 第二节　信息系统与业务目标一致性审计

### 一、业务概述

信息系统与业务目标一致性审计是根据组织发展战略和业务发展规划，将信息系统目标和内容的整体规划与组织业务目标进行比对评价，保证信息系统战略规划围绕组织的战略意图展开，将战略意图转化成目标和任务，并且评估达成目标和完

成任务所需要的信息系统能力需求，根据信息系统能力的需求进行信息系统战略规划。

## 二、审计目标和内容

审计目标：通过比较组织信息系统战略规划与业务目标一致性，保障信息系统战略规划制定及实施过程得到合理的控制、监督并持续改进，保持与业务目标的一致性。

审计内容：内部审计机构通过与信息系统决策层、管理层访谈，查阅组织章程、中长期战略规划、发展计划、年度计划、管理流程等文件对下列内容进行审计：

（一）信息系统决策和管理层对信息系统战略规划过程的重视和参与程度。

（二）审计信息系统战略规划文件规范。

（三）审计信息系统目标相关内容的可操作性。

（四）审计对目标进行更新和沟通的需求。

（五）审计监督和评价需求。

（六）审计战略规划流程或框架是否完善。

（七）审计信息系统目标与其管理控制流程符合度。

## 三、常见问题和风险

（一）缺少信息系统战略规划目标。

（二）信息系统目标与组织战略规划不一致或更新不及时。

（三）信息系统目标与组织信息系统能力不符、缺乏实用性。

（四）信息系统目标与其他管理控制流程不符、缺乏操作性。

（五）信息系统目标缺少保障措施。

**四、审计的主要方法和程序**

（一）访谈组织管理人员，了解信息系统目标和业务目标是否一致。

（二）检查信息系统的建设方案、规划内容、实施内容与组织各主要业务的需要是否相符。

（三）审阅信息系统的可行研究报告设定目标，评估组织信息系统的能力是否能够支持信息系统设定的目标。

（四）对比分析信息系统建设与应用的内容与组织的主营业务目标是否一致，是否能够有效支撑主要业务目标。

## 第三节　信息系统投资与绩效审计

**一、业务概述**

信息系统投资及绩效审计，是指对信息系统投资过程、价值、回报、投入信息系统资源对实现业务目标、战略的影响能力的评价。

**二、审计目标和内容**

审计目标：通过对信息系统投资及绩效的评价，向管理层提供信息系统投资立项、决策、实施、监督、考核过程的合规性、合理性、合法性、经济性以及对业务目标影响的评估，以促进组织持续改善信息系统投资过程管理、提升信息系统投资价值。

审计内容：

1. 信息系统投资决策、监控、考核机制的健全性。

2. 信息系统投资审批流程。

3. 信息系统投资的预算、执行、节点报告、验收管理程序。

4. 信息系统投资项目的项目评估和绩效评价。

## 三、常见问题和风险

1. 信息系统投资立项与信息系统战略规划、业务目标不符。

2. 信息系统投资项目未经信息系统决策部门批准。

3. 信息系统投资项目流程控制不足。

4. 信息系统投资项目缺少后评估和绩效评价。

## 四、审计的主要方法和程序

1. 访谈高层管理人员，了解信息系统投资战略规划和年度计划，评估信息系统投资项目与战略规划和投资计划的一致性。

2. 检查信息系统投资管理制度，审核投资决策、监督、考核机制的执行情况。

3. 检查信息系统项目管理文件，年度投资计划文件等，审核信息系统项目授权审批情况。

4. 获取信息系统项目流程文件、管理文档等相关资料，审核信息系统投资预算、支付、进度报告、验收管理等关键流程的合规性、合法性、准确性。

5. 获取信息系统项目管理文件，绩效考核记录，审核是否对信息系统项目进行了项目评估和绩效考核。

## 第四节　信息系统组织与制度审计

### 一、业务概述

组织应设置信息系统管理机构，规定相应的职责和权限，建立相关制度，规范业务流程运转机制。

信息系统组织机构一般包括:

（一）信息系统决策与规划机构。

（二）信息系统执行与实施机构。

（三）信息系统风险管理机构。

（四）信息系统监督机构。

### 二、审计目标和内容

审计目标：通过对信息系统决策与规划、执行与实施、风险管理、监督机构的评价,向管理层提供信息系统组织工作得到控制、监督、持续优化的合理保证。

审计内容：

（一）信息系统决策与规划机构

1. 制定的信息系统战略目标和信息系统的应用是否符合业务目标的要求，是否有效保证信息技术战略方针目标、绩效、自我评价等体系的持续有效性等。

2. 信息系统治理是否纳入决策层、管理层的议事日程,并定期讨论、定期出具信息系统治理工作的报告。

（二）信息系统执行与实施机构

1. 信息系统组织架构与相关职责是否符合组织信息系统现状,是否得到及时更新等。

2. 是否明确了信息系统部门和岗位职责。

3. 是否存在职责不明确或不相容职责分离控制未能落实的情况，是否采取了有效的控制措施防止岗位职责冲突。

（三）信息系统风险管理机构

1. 是否建立信息系统风险管理机构，并明确职能，是否设置信息系统风险管理岗位，是否建立向风险管理委员会报告工作的机制。

2. 是否制定了风险管理的策略制度及流程、实施持续信息系统风险评估、监控信息安全威胁和不合规事件的发生，并跟踪整改意见的落实等。

（四）信息系统监督机构

1. 是否明确信息系统监督职能，在信息系统监督部门设立信息系统监督岗位。

2. 是否建立了信息系统审计制度，是否按照组织的要求开展信息系统审计。

## 三、常见问题和风险

1. 未建立信息系统治理组织架构、信息系统的战略规划、未统一管理。

2. 信息系统决策层与管理层职责权限不清。

3. 信息系统组织架构、职责、权限分工、流程机制缺少必要的制度规范。

4. 重大信息系统决策未通过信息系统决策层审批。

5. 信息系统决策和管理层未发挥应有作用。

## 四、审计的主要方法和程序

内部审计人员通过访谈决策层、管理层、相关机构，查阅相关治理工作报告，对信息系统组织架构进行评价。

1. 访谈相关人员,了解决策层的相关工作机制，检查相关文件、资料,确认决策层在信息系统治理中的作用等，取得相关文件，检查信息系统管理层成员的构成及工作机制的建立情况。

2. 审核信息系统治理采用的报告路线,核对信息系统治理方面的问题是否向组织最高管理层报告，获取信息系统工作年度报告，了解信息系统工作开展情况，检查信息系统工作报告

的收发记录，检查管理层对信息系统工作报告的审阅记录，取得并检查决策层及管理层的会议纪要等资料，确认管理层在信息系统治理中的作用。

3. 获取、审核信息系统组织架构图、信息系统部门工作职责资料，审核信息系统组织架构是否建立，信息系统部门的职责划分情况，是否采取了有效的控制措施防止岗位职责冲突。

4. 访谈决策层和管理层相关人员、了解风险管理机构职能的报告路线，访谈信息系统风险管理相关人员，获取信息系统风险管理职责等相关文件，获取信息系统风险管理相关记录，检查风险管理工作开展情况。

5. 访谈决策层、监督层及管理层相关人员，了解信息系统监督职能的确定及报告路线；访谈信息系统监督机构相关人员，获取信息系统监督管理相关记录，检查信息系统监督工作的开展情况。

6. 检查人力资源管理制度、信息系统人才选拔、培训、储备等关键岗位职责、绩效考核等制度，评价人力资源管理对信息系统架构的支持程度。

7. 检查主要业务流程如采购管理、资产管理、财务管理等制度，评价相关制度对信息系统架构的支持程度。

## 第五节　信息系统风险管理审计

### 一、业务概述

信息系统风险是指潜在影响业务的信息系统相关事件构成，包括不确定的频率以及重要性、符合业务目的和目标的挑战以及追求机会的不确定性。信息系统风险管理是组织在实现目标过程中，将不确定产生的与信息系统有关的影响，控制在可接受范围内的过程。

### 二、审计目标和内容

审计目标：根据组织战略目标、风险管理策略及相应的固有风险，评价组织如何实施信息系统风险管理，将与信息系统有关的风险因素控制在实现组织目标可接受的范围内。

审计内容：包括但不限于：系统风险的制度和流程符合性、有效性；风险管理的全面性、合理性、适用性；风险管理职责及人员分工的合理性；风险管理的监控、评估及应对等。

### 三、常见问题和风险

1. 信息系统风险管理机制未建立或不完善，导致组织风险缺乏管理。

2. 组织未开展风险识别和评估，未收集和建立信息系统风险清单，导致风险应对缺乏针对性和适用性。

3. 信息系统风险管理与组织的业务流程不匹配导致组织资源配置不合理，与管理层风险偏好发生偏离。

## 四、审计的主要方法和程序

1. 访谈决策层及信息系统风险管理部门及相关人员，了解组织信息系统风险管理机制建立健全的情况；了解风险管理工作的开展及人员配备等情况。

2. 获取信息系统风险管理相关资料，了解管理层风险偏好及风险容忍程度、风险管理目标、风险管理策略和原则、风险管理制度及流程、监控、评估及应对等。

3. 获取组织信息系统风险管理清单，选取组织的重点业务流程与风险清单对比，检查风险评估计划、风险评估实施记录、风险评估报告、风险处置计划，评价组织风险识别、评估的准确性、适当性、完整性。

**风险清单评估实例**

**信息系统战略规划风险**

| 风险定义描述 | 发生的条件 | 发生的可能性 |
| --- | --- | --- |
| 信息系统开发缺乏战略规划或规划不合理，造成信息系统缺乏可开展性、形成信息孤岛或重复建设，导致公司经营管理效率低下 | 1. 系统开发没有经过规划<br>2. 规划没有经过充分调研<br>3. 规划没有经过充分论证 | 低 |

**信息系统需求分析管理风险**

| 风险定义描述 | 发生的条件 | 发生的可能性 |
| --- | --- | --- |
| 系统需求分析不当，不符合业务处理和控制的需要；或需求文档的表述不能全面、准确地表达业务需求；或在技术上、经济上及合规上不可行，导致系统开发失败或应用价值下降，甚至引发法律纠纷或受到处罚 | 1. 系统需求不是由业务使用部门提出的<br>2. 系统需求没有经过充分论证<br>3. 需求文档文字表述不全面、不准确，没有准确表达业务需求<br>4. 对需求实现在技术、经济及合规上的可行性没有进行充分论证 | 中 |

4. 获取组织信息系统的测试及运行数据，选取组织的重点业务领域及重点工作环节，获取对应的数据，根据数据的内在联系，利用平行模拟法，查找异常点及可能存在舞弊的动机及机会，从而发现问题和风险。

## 第六节　信息系统项目管理审计

### 一、年度信息化项目计划

#### （一）业务概述

信息化项目：是指支撑组织战略实施，提高组织管理、决策的效率、效果，以计算机、网络、通信等技术为手段建设和服务的项目，包括咨询服务、软件产品采购、软件研发、系统实施、硬件设备采购、系统集成、系统运行维护等。

项目年度计划：是指信息化项目年度计划的编制、上报、汇总、审批、发布等。项目计划编制一般应包括但不限于以下事项：项目建设背景、必要性、项目的目标、范围和主要内容、初步业务需求分析、实施周期、投资估算以及系统所需要软硬件环境等内容。

信息化项目年度计划应遵循组织相关内部控制制度以及投资、计划和信息化规章制度进行上报和审批。为了确保有效地满足业务需求，在立项前应进行需求分析。分析过程包括：定

义需求、考虑替代资源，初步确定“开发”、“购买”、“外包”等方案。

（二）审计目标和内容

审计目标：合理地保证年度信息化项目计划与组织的发展战略、年度计划一致，并得到正式的审批。

审计内容：对信息化项目年度计划的编制、上报、汇总、审批、发布等环节进行审计。审计项目建设背景、必要性、项目的目标、范围和主要内容、初步业务需求分析、实施周期、投资估算以及系统所需要软硬件环境等内容。

（三）常见的问题和风险

1. 年度信息化项目计划与中长期规划不一致，可能导致信息系统缺乏可扩展性、形成信息孤岛或重复建设。

2. 在制定年度计划时，没有对项目进行必要的可行性分析，可能导致年度信息化项目计划与组织战略、管理等规划偏离。

3. 年度信息化项目计划没有得到组织管理层的正式审批，可能导致项目计划不能实施。

（四）审计的主要方法和程序

1. 审阅规章制度，访谈管理层，合理确定年度信息化项目计划的制定和审批管理的设计有效性。

获取并审阅年度信息化项目计划制定和审批的规章制度；访谈相关管理层，了解组织制定和审批年度信息化项目计划的流程和方法，评估合理性。

2. 审阅年度信息化项目计划相关文档和资料，合理确定年度信息化项目计划的制定和审批管理的执行有效性。获取并审阅组织的中长期规划或信息化建设规划、年度信息化项目计划、年度信息化项目计划审批文件等，确认年度信息化项目计划的制定和组织中长期规划的一致性。

## 二、信息系统项目立项管理

### （一）业务概述

项目立项管理：依据年度计划和有关规定，对信息化项目的可行性研究报告上报、论证、检查、办理批复和项目备案管理的过程。

### （二）审计目标和内容

审计目标：合理地保证项目的立项流程遵循了组织的规章制度，并得到了正式的审批。

审计内容：检查信息系统立项与年度计划的一致性，检查项目的可行性研究报告，重点关注需求提报、上报、技术经济论证、办理批复和项目备案管理的过程。

### （三）常见问题和风险

1. 信息化建设背景、必要性尽职调查不到位，导致系统建设与规划、计划的目标偏离等风险。

2. 系统需求分析不当，不符合业务处理和控制的需要，导致开发建设失败或应用价值不高等风险。

3. 在技术上、经济上不可行，导致系统开发失败或应用价值不符合立项目标的风险。

4. 可行性研究报告或者需求说明书未经业务需求主管单位负责人签字确认，需求及方案的合理性缺乏保障，后期由于需求的不断变更会导致项目成本增加或延期完成的风险。

5. 项目立项未批复即开始实施，导致项目合规风险。

**（四）审计的主要方法和程序**

1. 收集整理立项资料

按照信息化分类或分级管理的规定，收集项目立项上报、审批和批复全流程涉及的文件，包括但不限于可行性研究报告、年度信息化投资计划、评审资料、批复等纸质文件或电子资料等。

2. 审阅、对比分析立项主要资料

（1）分析项目建设背景：属于新建或新购项目，检查是否依据组织发展战略、规划、计划、文件、纪要及上级组织的批文、批件、业务部门提出的需求；属于完善提升类项目，检查是否详细陈述了项目前期实施和应用的总体情况，包括基础条

件、总体目标、实施范围和内容、完成的工作、取得的经验、应用效果和存在的问题。通过上述分析，检查项目的立项是否符合信息化发展的战略、项目建设规划和年度计划，检查重复建设或信息化建设出现孤岛的风险和问题。

（2）抽查审批流程文件，从分析比对立项报告中对国内外同类信息化项目建设和应用的现状，以及本组织业务发展对信息化的需求，检查信息化立项的必要性，避免技术上的落后造成开发失败或应用价值不高等问题。

（3）检查业务需求说明、技术方案，查看业务需求描述是否清晰明确，是否包括业务功能需要、技术方向、性能指标、成本、可靠性、兼容性、可审计性、有效性、可持续性、经济性、可用性、安全性和合规性等方面。

3. 检查信息化项目立项审批流程

（1）根据组织的信息化项目规章制度，收集组织现有信息化项目内控管理体系资料。

（2）依据组织的信息化项目内部控制管理体系，检查信息化项目投资立项上报审批流程；检查信息化项目立项报批流程是否按信息化内部控制和规章制度及细则执行，立项报告、投资计划、立项材料等资料是否齐全。

（3）检查立项报告，项目立项投资计划，项目背景资料文件及相关审批文件的领导签字、日期签署是否完整，时间逻辑是否一致。

通过上述内容的审计，检查项目的上报、审批流程的合规性，以及无计划立项、拆分项目躲避立项审批程序等问题和风险。

## 三、项目预算及执行

### （一）业务概述

信息化项目预算应依照组织的信息化计划及其预算申请批准程序报批。信息化项目预算编制，一般包括但不限于下列内容：软件配置费、硬件配置费、网络建设费、技术服务费、培训管理费、配套实施管理费、其他费用及不可预见费用。

### （二）审计目标和内容

审计目标：信息化系统的预算编制及执行审计检查预算的合理性、预算执行的真实、合法性，以规范资金应用，控制项目成本，确保较小的成本、费用支出取得较好的投资效益。

审计内容：审计预算目标的科学性，编制程序的合规性，预算内容的完整性、准确性，相关费用支出、资金支付的真实性，合规性。

### （三）常见问题和风险

1. 预算编制程序不规范，横向、纵向信息沟通不畅，导致预算目标缺乏科学性和可行性，可能会导致项目实际成本超预算的风险和预算虚高的风险。

2. 预算编制与信息系统项目内容偏离，存在不合理支出，导致项目实际成本与上报审批的预算计划差异较大。

3. 预算执行情况报告文件不全面，对预算使用情况无法真实反映，资金管理不透明。

4. 资金支付审批过程存在补签、无授权代签、漏签等现象，未能按照预算付款的进度和要求执行，存在提前支付或拖欠付款的现象，出现信用、法律风险。

**（四）审计的主要方法和程序**

项目预算及执行的测试程序一般包括：

1. 检查预算的编制及审批流程

（1）对比分析：将费用预算编制的费用事项、用途、工作数量、人工用量与业务需求进行核实，检查多报或漏报工作内容问题，同时采取抽样方法，选择重要事项或金额较大事项，对照相应的定额、标准和工作量进行重新测算，核实其费用预算的真实、准确性。

（2）检查信息化项目内部审批流程是否规范，包括：预算文件及审批流程文件的完整性、一致性、合规性。

2. 查阅信息化项目批复及审批过程文件，重点关注审批过程中项目预算的不同意见，检查是否存在违规审批，造成项目预算超计划的问题。

3. 预算执行情况审计

对项目建设期间费用支出及盈余收入使用情况与预算计划的差异进行比对。主要包括对信息化项目的预算计划、预算执行分析报告、各项收支情况统计、费用支付安排、项目管理手册、项目进度月报或季报和项目变更资料，重点检查超预算或无预算增加的其他费用。

（1）查阅项目预算计划、预算执行分析报告。

（2）抽查预算执行分析报告，并与相关支持文件和记录对比、核实。

（3）对预算出入较大的项目主要原因进行分析并做出结论。

4. 检查资金支付

资金支付审计程序主要针对项目建设中合同付款进度条款和其他费用支出程序的监督，包括信息化项目的主要费用支出构成，各项合同的付款进度控制，费用支出审批控制。

（1）了解被审计单位内部对合同付款的相关制度和规范。

（2）检查资金支付文件的审批程序是否齐全，其中审批人签字是否完整，审批时间逻辑顺序是否正确。

（3）抽取部分样本，检查资金支付凭证中实际支付金额与完成项目进度是否匹配，如有差异，深入分析差异原因。

## 四、项目招投标管理

### （一）业务概述

信息系统项目的招投标在遵守国家、地方及组织相关的法律、法规、规章、制度的基础上，应当采用公开招标方式的，其招标具体限额按所属组织实际情况确定；规定可以不公开招标的，遵守其相关规定。

### （二）审计目标和内容

审计目标：信息系统招投标审计是对组织的信息化项目招投标程序和形式的合法合规性、组织制定的信息系统招投标标准的合理性、招投标范围的完整性、组织招投标管理的规范性和一贯性开展审计，达到规范管理，杜绝漏洞，提升组织价值的目的。

审计内容：招标管理情况、投标管理情况、评标管理情况、中标及合同签订情况。

### （三）常见问题和风险

1. 应招标未招标，应公开招标未公开招标，甚至发生信息系统的招投标舞弊风险。

2. 信息系统项目招投标程序和标准没有专业部门参与，不符合相关法律、法规、组织内部规章制度要求，或以不合理的

条件限制、排斥潜在投标人或者投标人相互串通投标的舞弊风险和违法违规风险。

3. 招投标工作组织不当，招标方案、形式和文件表述不当、投标文件主要条款不满足招标文件、投标保证金不到位、未按时投标等导致的招投标失败风险。

4. 评标人员构成不满足招投标需求，或缺乏信息系统专业的胜任能力，未执行回避原则等；评审标准和方法不合理，不符合信息系统项目要求，评审程序执行不当导致无法实现项目目标，甚至造成损失或引起法律纠纷风险。

5. 未按评标结果选择供应商，不能保证信息系统项目在规定时间内保质保量按时间节点完成信息系统实施的风险。

（四）审计的主要方法和程序

1. 检查招标项目的招标范围是否与组织的规定相符，招标方式是否一贯执行了国家法律法规和组织规定。

2. 取得信息系统项目立项、招标公告、招标文件和补充招标文件、会议记录、投标文件、招标投标情况书面报告等文件资料，对比信息系统投资计划、可行性研究报告，需求分析等资料，检查组织是否存在化整为零、规避公开招投标的行为。

3. 查阅尽职调查的相关文件、资格检查公告结果、预审结果通知书、招标文件，检查信息系统中标人是否达到招标人所

要求的资质等级、资质是否真实、是否存在挂靠获取资质、是否存在转包分包问题。

4. 查阅开标资料，重点检查开标过程的规范性及组织在出现流标、废标时的处理程序。

5. 获取评标委员会名单，检查评标委员会人数组成和人员是否满足法定和组织要求；查阅评标资料，评价招标文件确定的评标标准和方法是否合理，检查评标委员会是否存在评标打分不合理的情况；组织是否按规定根据评标结果签订合同。

6. 检查信息系统项目投标资料，判断不同投标人的投标文件是否雷同、是否存在股权关系、投标报价是否呈规律性差异等，发现招投标过程中围标、串标等违法中标的现象。

7. 检查中标通知书发放和合同的签订是否符合国家和组织的相关规定，检查签订合同与中标人是否一致，合同内容是否与招标文件相符。

## 五、采购与合同管理

### （一）业务概述

信息系统采购是指由组织投资建设购买服务或需要运行维护的各类信息系统，包括执行信息处理的计算机、软件和外围设备等货物和服务。采购需求应与现有系统功能协调一致，避免重复建设。

### （二）审计目标和内容

审计目标：通过对信息系统项目采购合同审计，评价采购是否符合信息系统建设的需要。合理保证采购行为的合法、真实、准确、经济。

审计内容：组织信息系统采购及合同审计是对信息系统采购行为及合同的合法、真实、准确、经济等方面的内容进行监督。

（三）常见问题和风险

1. 信息系统建设未编制采购计划或采购计划未经适当审批导致的信息系统重复建设或效率低下。

2. 因采购方式或供应商选择不合理，组织明显缺乏议价能力，导致质次价高、技术参数不达标、服务交付不及时等采购风险。

3. 未建立供应商动态考评机制，导致选择的信息系统供应商技术水平与项目要求不匹配。对合同相对方的履约能力给出不当评价，导致信息系统合同相对人不能按约履行合同义务，影响组织信息系统的开发与应用的风险。

4. 采购尽职调查不充分，导致外购采购没有对比选择，在功能、性能、易用性方面无法满足需求，导致与无权代理人、无处分权人签订信息系统采购合同，组织利益受损。

5. 合同签订未经审核、审批，合同条款和内容不完整存在严重疏漏或缺陷，合同规定的权利义务内容不明确，合同存在法律风险。

6. 法律规定对于应当报经国家有关主管部门或组织上级部门检查或备案的信息系统合同文本，未履行相应报批报备程序，导致合同无效的风险。

7. 在合同执行过程中发生重大变动时，未及时与对方沟通变更合同，导致开发的信息系统不适用于组织的需要。

（四）审计的主要方法和程序

1. 明确组织内信息系统采购的关键控制点，询问信息系统相关采购人员执行的信息系统采购流程，查阅项目采购前期报批文件，判断项目采购是否符合信息系统技术要求，采购方式是否合法。

2. 获取供应商资质、业绩、提供服务等相关文件资料，确定供应商是否具备提供相应服务的实力、信用，能否按信息系统建设要求，保质保量地提供信息系统相关服务，关注实施组织与采购合同相关人是否一致，是否存在转包和违规分包行为。

3. 重点关注合同采购条款文本，检查是否存在关键条款不清晰，数据质量考核无标准，信息资产权属不清；检查合同价格的组成要素，将合同价格与同行业、同类型信息系统指标进行比对，判断采购价格是否合理。

4. 根据信息系统演示结果，审核供应商提供的服务是否满足信息采购需求，是否能按合同要求提供合格的信息资产或服务。

## 六、项目实施管理审计

### （一）业务概述

信息系统项目实施是指对信息系统项目的开发、测试、验收、正式上线等重要环节的质量、进度、安全、变更、风险实施控制和监管的过程。参与项目建设的所有人员应做好风险的识别和分析。涉及重大风险问题的应及时分析风险因素，形成风险应对方案。

### （二）审计目标和内容

审计目标：开展信息系统项目实施管理审计，关注信息系统项目实施（含初步设计、详细设计）的合理性、合规性，满足技术发展的技术前瞻性要求；以提高项目进度的可控性、提升项目质量管理，完善项目验收管理。

审计内容：包括但不限于：信息系统建设程序履行情况、信息系统的资金筹措和使用情况、项目概算执行及调整报批情况、质量监督情况、成本核算和财务管理情况、信息系统实施组织架构、人员胜任能力等内容。

### （三）常见问题和风险

1. 项目未建立相应的组织机构或组织机构不健全，项目人员配备不充足、关键岗位人员能力不胜任，未执行不相容岗位相分离，造成职责不清或缺失，导致的项目效率低下的风险。

2. 信息系统项目初步设计和详细设计未进行技术检查，业务需求不能满足组织要求，应用架构、数据架构、部署架构、业务架构、功能模块及子模块、标准化设置、系统设置等与实际不符，未设置相应的风险防控方案造成无法实现项目目标的风险。

3. 项目建设单位未对信息系统的建设进度与质量进行控制或对进度控制不当；未对项目质量开展定期检查，导致信息系统项目进度得不到保证、质量不合格、工期延误的风险。

4. 未制定信息系统变更程序或变更程序不合理，未严格执行变更程序，导致变更频繁，产生法律纠纷或费用超支、工期延误的风险。

5. 缺乏完整可行的数据迁移方案或方案实施不当，导致系统的业务处理错误；实施单位未进行知识转移，导致组织无法充分使用系统功能；系统生产环境未与开发环境、测试环境在物理上或逻辑上采取适当的隔离措施，导致生产环境运行不稳定或业务功能失效的风险。

6. 缺乏信息系统项目竣工验收机制或机制设计不当，验收手续不齐备或验收审核工作不严谨，缺乏验收标准，导致未达标项目通过验收，影响组织正常活动的验收风险。

7. 项目成本未及时、准确进行核算，或核算不正确而导致的核算风险；未及时出具项目结算报告，导致项目验收延期风险；未及时完整移交项目资料而导致的项目资料遗失风险。

8. 信息系统验收后未明确信息系统运维保障机制的建立与移交，导致信息系统运行和维护风险。

（四）审计的主要方法和程序

1. 获取信息系统项目总体情况资料，主要应当包括项目建设运作和管理模式，资产的交付，财务核算体系和方法，项目进度确认及进度款项拨付，评估项目过程管理总体情况。

2. 获取信息系统项目相应的组织机构图及职责权限，检查项目组成员组成及相应资质，岗位不相容职务分离是否符合组织管理要求。

3. 获取信息系统初步设计及详细设计、项目实施控制计划、项目进度控制计划、项目质量控制报告。检查项目建设单位是否按计划对项目进度与建设质量实施了控制。重点关注项目进度或设计受到资源约束或外部环境变化时，是否及时对进度计划进行调整。检查计划变更的原因、报价、进度是否合规、合

理，是否按规定程序通过相关部门审批，变更事项是否符合合同规定和变更的实际情况。

4. 对照合同、技术附件等资料中规定的信息系统中相应的项目验收规范，获取测试项目运行效果验收记录，检查验收程序是否符合组织规定，是否符合信息系统项目的设计需求，运行数据是否能满足组织需要。

5. 检查是否制定或选择系统出现安全、进度等事故时的技术处理方案，处理方案是否严格执行相应的技术规范与质量标准，事故处理技术方案是否切实可行、经济合理。

6. 检查信息系统项目建设资金的筹措与使用情况，关注系统建设资金来源是否真实合法，筹集资金的方式是否合规。

7. 检查项目成本的归集与分配是否恰当、准确，是否与批准的初步设计预算相符，检查项目各类投资是否真实、合法。检查交付资产是否真实、完整，资产交接手续是否完备，资产归属或管理责任是否划清，资产验收交接是否真实、合规。

## 七、项目绩效与后评估

### （一）业务概述

投资绩效考核内容包括：信息系统年度投资增量绩效考核、已验收投产项目的绩效考核、投资管理与控制绩效考核。项目后评价：为实现信息系统项目全过程闭环管理，所有信息系统投资项目一般在投产竣工验收后一定时期内开展后评价工作。

后评价内容包括：信息系统决策及建设管理后评价、实施结果后评价、经济效益后评价、影响后评价、可持续性后评价等。

（二）审计目标和内容

审计目标：通过开展绩效考核、后评估审计，了解信息系统持续对组织支撑作用是否达到预期及不足，便于及时开展相应的后续服务。

审计内容：包括但不限于组织信息系统项目绩效的考评机制，组织对信息系统运行后评价的评价标准、指标、体系。

（三）常见问题和风险

1. 缺乏科学有效的绩效考核机制，项目评价和考核不及时、不准确，导致的项目评价结果不当，无法持续支持改进管理水平的风险。

2. 没有严格执行项目后评估制度，导致无法及时发现项目执行偏差、无法实现信息系统预期目标的风险。

（四）审计的主要方法和程序

1. 获取组织内部的绩效考核制度、标准、评价结果，检查组织是否对信息系统的建设给予高度重视，信息系统绩效考评是否及时、准确，达到提升组织管理的作用。

2. 获取组织对信息系统开展的后评估资料、后评估流程，检查组织在项目出现执行偏差时的应急措施，在出现偏差时组织的处理程序是否得当。

# 第三章　信息系统一般控制审计

## 第一节　应用系统开发、测试与上线审计

### 一、应用系统开发审计

#### （一）业务概述

组织的信息系统开发根据方式不同，通常包括自主开发、外委开发、或者二者兼有的开发方式。组织在进行信息系统开发时，应当根据自身技术力量、资金状况、发展目标等实际情况，选择适合自身的开发方式和合作伙伴。

应用系统开发工作包括需求分析、架构设计、软件实现、系统测试、用户测试、系统试运行、系统验收、系统上线、数据迁移和产品维护等内容。

#### （二）审计目标和内容

审计目标：通过规范开发程序，提高信息系统开发的可控性、安全性、可靠性和经济性，揭示信息系统开发环节存在的风险及问题，提出完善信息系统开发控制的审计意见和建议，实现组织目标。

审计内容：开发组织机构设置、资源配置情况。开发过程中与业务部门的沟通情况。系统开发全过程的需求分析、架构设计、软件实现、系统测试、用户测试、系统试运行、系统验

收、系统上线和数据迁移、产品维护等内容的质量、安全管理情况。

（三）常见问题和风险

组织自主开发方式下的应用系统主要存在以下常见问题及风险：

1. 组织未成立专门的开发建设项目组，可能导致信息系统开发建设责任制未落实的风险。

2. 信息系统开发工作缺乏必要支持。组织内部无专业技术人员或是缺乏必要的财务支持，导致开发失败的风险。

3. 信息系统开发过程没有业务部门人员参与，未定期与业务部门共同审核信息系统的开发建设情况，未及时发现系统不能满足业务的需要，可能导致与业务需求不相符的风险。

4. 组织未制定合理的项目生命周期管理方案和符合质量管理标准的质量控制体系，不能有效控制开发质量；开发过程中未进行必要的安全控制，未对源代码进行有效管理和严格审查可能导致的风险。

5. 项目需求说明书阐述业务范围及内容不清晰，未能结合需求制定出最优化的技术设计方案的风险。开发环境、测试环境和生产环境未分离，网络未有效隔离，设备未独立于生产系统，开发人员直接接触生产系统，直接使用未经批准并脱敏的生产数据，导致泄密或造成生产系统受损的风险。

6. 在开发过程中未根据用户提出的业务需求，制定信息系统变更程序相关制度或变更程序不合理，导致与承建方或第三方产生合同法律纠纷或费用超支、工期延误的风险。

7. 信息系统开发工作完成后，未及时进行交付导致系统无法发挥作用的风险，未加强信息系统项目开发设计、源代码、技术使用、运行维护说明书、用户手册等文档管理和文档版本控制导致的开发效率低、不经济的风险。

8. 数据继承和迁移：组织在对信息系统升级变更时，未对历史数据的继承和迁移给予足够的重视。未对数据结构进行合理规划，未对数据进行兼容性分析，导致因兼容性不够而造成的历史数据无法使用和继承的风险。

除常见风险外，外委开发项目还应关注下列风险与问题：

1. 组织的信息管理部门对外委项目开发未进行有效的管理与控制，导致信息系统开发计划与实际运行不符，信息系统项目无法按时完工的风险。

2. 组织未及时与外部受托单位沟通项目开发阶段的计划执行情况，导致实施内容与建设目标偏离，造成开发工作无法满足组织需求的开发风险。

3. 组织未对外包开发的技术人员加强管理，离职的开发人员未签订保密协议而造成泄密的风险。未对外包开发的开发方进行充分调研分析，不能保证系统可靠性的风险。

（四）审计的主要方法和程序

自主开发项目的主要审计方法和程序

1. 调阅项目相关的制度、流程、指引和开发建设文档，查看是否有专门的项目组织机构，是否分配相应职责。

2. 查看项目开发进度报告是否包括计划的重大变更、关键人员或供应商的变更以及主要费用支出情况，检查组织是否建立了质量检测和风险评估机制等。

3. 检查组织的信息系统需求和技术架构评估文档，查看系统需求与业务目标是否保持一致；检查需求详细说明书，项目进度及详细的软件开发计划。

4. 询问系统开发小组负责人，了解组织是否建立了系统开发质量控制体系以及质量控制检查和监督记录。

5. 检查系统开发环境、测试环境和运行环境是否分离，网络是否有效隔离，设备是否独立于生产系统，开发人员是否不得接触生产系统，开发过程中是否使用了生产数据,使用的生产数据是否得到管理层的批准并经过脱敏或相关限制。

6. 检查系统开发过程中，是否进行了安全控制，是否对源代码进行了有效管理和严格检查，系统所有入口是否都经过安全规则的控制，并在系统开发文档中全部注明。

7. 检查是否制定了组织信息系统开发文档管理规范、制度，查看项目开发设计、源代码、技术使用和运行维护说明书、用

户使用手册，风险评估报告等项目文档管理是否符合规范，是否进行了文档的版本控制；检查组织是否有系统开发过程的检查记录，是否对系统完整性、恶意代码和后门程序进行了防范。

除常用检查程序外，外委开发项目还应采取以下审计方法和程序：

1. 检查外委项目的系统开发中组织信息管理部门与外部受托方的协调与沟通的记录，检查组织根据信息系统要求及时调整开发进度与考核的书面资料，是否存在系统开发偏离开发目标的问题，是否存在项目开发计划与进度不匹配的问题。

2. 检查外委项目关键技术人员的管理制度及保密协议，是否存在开发人员频繁调整影响开发进度，是否存在离职未签订保密协议造成泄密的情况。

3. 获取项目组关于业务需求变更的处理资料，检查是否根据项目需求及时变更项目开发程序，且该变更是否经过适当的授权与审批。

## 二、应用系统测试审计

### （一）业务概述

系统测试是指在规定条件下操作信息系统，以发现程序错误，衡量系统质量，评估其是否能满足设计要求的过程。通过测试避免开发风险。测试结论一般分为同意通过测试、需复议和不同意通过测试三种情况。

系统测试主要包括功能测试、界面测试、可靠性测试、易用性测试和性能测试。功能测试主要针对功能可用性、功能实现程度（功能流程和业务流程、数据处理和业务数据处理）等方面，一般包括系统单元测试、集成测试、性能测试、安全测试、用户测试等内容。

（二）审计目标和内容

审计目标：组织通过对测试方案和测试标准、测试步骤、测试用例和所需的系统设置要求过程开展审计，达到对信息系统项目的功能性、效益性和经济性进行评价。

审计内容：包括但不限于各阶段的测试计划与方案、各部分的测试报告，测试数据及对测试结果存在偏差的更正记录等。

（三）常见问题和风险

1. 测试计划、标准、步骤、用例和所需的系统设置要求不清晰、不明确，特别是缺少最终用户测试，导致无法实现需求功能的风险。

2. 测试过程中存在BUG, 在执行测试时未发现或发现后未与开发方沟通导致的BUG，未及时修正或对已修正的BUG未进行返测的风险。

3. 在系统测试完成后，未提交测试报告；未及时为用户测试准备数据，测试数据脱离生产环境的实际数据或与系统所实现的设计要求不符的风险。

4. 测试人员未依据安全技术标准进行安全测试，发生数据安全事故。

5. 系统安装部署手册、功能测试报告、集成测试报告、性能测试报告、用户培训教材等测试文档不全或出现缺失的风险。

6. 系统实施结果未经充分测试即投入使用，程序功能上的缺陷或系统配置上的错误未能及时发现，导致系统运行不稳定或业务功能失效的风险。

（四）审计的主要方法和程序

1. 获取信息系统的测试计划及标准、各阶段的测试报告，特别是最终用户的测试报告，现场演示系统运行效果，以检查测试结果满足功能需求的真实性和有效性。

2. 获取测试中发现问题的解决方案，检查测试发现的问题是否已得到解决；系统变更测试的环境是否与生产环境严格分离，检查是否对变更人员、日期、目的、内容、影响等进行审核，是否按照组织设立的审批流程对系统变更进行审核。

3. 组织在进行新旧系统切换时，是否开展业务数据兼容性测试，是否制订了详细的数据迁移计划；检查业务系统上线前，是否进行过数据迁移测试和数据有效性、兼容性验证。调阅信息系统升级文档，是否进行过更新；检查是否制订了相关制度、标准和流程，以保证信息系统开发、测试、维护过程中数据的完整性、保密性和可用性。

信息系统测试过程管理风险

| 风险定义描述 | 发生的条件 | 发生的可能性 |
| --- | --- | --- |
| 系统实施结果未经充分测试即投入使用，程序功能上的缺陷或系统配置上的错误未能及时发现，导致系统运行的不稳定或业务功能失效 | 1. 没有制定测试计划<br>2. 测试没有业务人员参与<br>3. 没有进行有关模块的联动测试<br>4. 没有进行测试验收 | 中 |

## 三、应用系统上线验收审计

### （一）业务概述

系统上线包括应用注册、生产资源申请及运行监控、系统及数据初始化、信息安全评估、技术架构符合性评估等。信息系统初始化工作，包括系统的权限设置、数据准备、流程配置以及提交用户手册、系统维护手册、应急处理办法，对运行人员、业务管理人员和业务操作人员进行培训，开发人员与运行维护人员职责移交等。

### （二）审计目标和内容

审计目标：组织通过对系统上线验收资料、验收程序、验收方式的审计，达到规范和完善组织对信息系统的上线验收工作，保证项目按时上线、发挥应有作用。

审计内容：包括但不限于验收资料，验收报告、检查工作报告、技术报告和用户报告、系统上线批复、用户操作手册、系统维护手册及相应的适用规章制度的建立和落实。

### （三）常见问题和风险

1. 未根据项目目标妥善进行验收或验收不规范，损害组织利益的验收风险。

2. 系统上线后，由于组织对信息系统的数据缺乏规范化管理的基础，或是没有足够的容量规划，导致项目运行低效。

3. 系统上线后，未对运行人员、业务管理人员、业务操作人员进行必要的培训，开发人员与运行维护人员未进行职责移交而引发的责任划分不清，导致运行低效或无效的风险。

**（四）审计的主要方法和程序**

1. 获取项目可行性研究报告、总体（基础）设计、经批准的项目变更文件及合同等。审计上述资料与项目验收资料的一致性。

2. 获取验收资料交接清单，包括项目启动时间，上线、单轨运行时间，项目实施、培训情况、相关资产、项目应用效益及效果。检查信息系统是否已完成项目规定的任务，对项目技术特点、应用及管理成果是否达到预期目标进行评价。

3. 检查文档资料管理，确认与该信息系统有关的各类文档资料已经正式归档保管，已纳入生产系统文档资料管理范围。

4. 获取项目培训相关文档，检查组织是否对系统用户开展全面培训，用户使用手册、维护手册、应急处理及培训教材，判断组织是否具备相应的上线能力。

5. 获取信息系统上线运行前的信息主管部门或信息主管部门委托的相关测评机构开展的信息安全评估报表，检查报告结论是否符合上线运行要求。

6. 与系统使用人员访谈，了解在投产时，运行人员是否已熟悉运行操作，维护人员是否接管维护职责，从而判断是否存在操作风险。

7. 与相关人员访谈，了解上线的完整过程，判断上线环境是否在启用时已经验证有效、测试环境中的业务数据是否按规定进行了清理。

## 第二节　信息系统运维与服务管理审计

### 一、业务概述

信息系统运维与服务管理是指组织的信息部门采用相关的方法、手段、技术、制度、流程和文档等,对信息系统的运行环境(软件环境、网络环境等)、信息系统的运维进行的综合管理。组织应从信息系统运维和服务的日常管理、信息系统及其物理环境的监控和故障管理、日志管理、日常事件和问题管理、信息系统的容量管理和变更管理等方面开展工作。

#### （一）审计目标和内容

审计目标：通过对人员管理、职责分离、值班巡检与操作规范等方面的检查，评价组织信息系统的运维与服务的合理性、安全性和规范性。

审计内容：审计运维与服务机构人员的配置和职责分离情况，信息运维制度和规范的建立健全情况，系统运行报告、监控和记录的完善情况，出现问题时的应对措施。

（二）常见问题和风险

1. 未对重要业务岗位或系统的运维管理岗位实施职责分离。

2. 未制定详尽的日常信息系统运行操作规范说明，操作任务和步骤不明确、不清晰。

3. 未定期生成信息系统运行报告并对其进行分析，特别是重要信息系统，或管理层未审阅有关报告。

4. 运维过程中出现问题，无有效应急处理预案，导致系统运行效率低的风险。

（三）审计的主要方法和程序

1. 人员及职责审计

（1）访谈信息系统部门负责人及信息系统风险审计负责人，调取组织岗位职责及人员名单，验证相关不相容岗位是否实现了分离，是否存在岗位分离但人员兼岗的现象。

（2）抽取部分应用系统，并从中取得操作系统用户清单、数据库用户清单、应用系统用户清单以及开发测试系统的相应清单，验证是否存在事实上的兼岗现象，是否存在开发人员在生产系统中存在账户的现象。

2. 值班巡检

（1）访谈信息系统部门负责人，了解组织是否根据信息系统规模和水平建立信息系统运行值班和巡检制度。

（2）查阅组织的信息系统巡检记录，验证巡检内容、巡检频率是否与巡检制度相符，发现问题是否完整记录并上报。

3. 操作规范

访谈信息系统部门负责人，询问是否针对重要信息系统制定操作规范，并实地查看对比值班人员职责，验证其履职情况。

4. 运行报告

（1）访谈信息系统部门负责人，是否针对日常运维与服务和重要信息系统，定期生成运行报告并提交管理层审阅。

（2）审计针对运行报告中的问题，有无有效的应急处理预案，是否存在未及时解决运行问题的情况。

## 二、日志管理审计

### （一）业务概述

日志管理是指组织为满足法律和行业监管的合规要求，对日常的交易记录采取必要的程序和技术加以保存，确保存档数据信息的完整性，满足安全保存和可恢复的要求。

### （二）审计目标和内容

审计目标：通过对日志管理的审计，合理地保证组织负责运营的信息系统所涉及的用户活动以及信息安全事件日志被记录，并按照规定的期限进行保留，以支持将来的调查和访问控制检查，确保对存在的问题及时采取措施纠正和防范。

审计内容：日志管理制度与策略体系的建立健全规范情况，用于日志信息及其存储介质安全防护的相关程序、技术和措施。

### （三）常见问题和风险

1. 未建立健全规范的日志管理制度与策略体系，或采取必要的技术工具，对组织所负责的信息系统日志进行留存并符合监管要求。

2. 未对存储的日志信息及其存储介质采取妥善的物理和逻辑安全防护措施。

3. 未定期对日志信息进行分析，可能导致未对存在的管理与技术漏洞采取纠正和防范措施。

### （四）审计的主要方法和程序

1. 日志管理制度与策略

（1）查阅组织日志管理规范与策略，检查日志存储内容、留存时间、访问控制策略等内容是否完整。

（2）对日志信息进行抽样检查，检查内容是否与规范要求相符以及日志留存时间是否符合规范要求。其中，存储的内容应至少包括：用户ID、登录和退出的日期、时间和关键事件等细节，终端用户的身份和位置、成功和被拒绝的对系统和数据及其他资源的访问记录、系统配置的变化、特权的使用、系统工具和应用的使用、访问的文件和访问类型、网络地址和协议、访问控制系统引发的报警、防护系统的激活和停用。

2. 日志信息的保护审计

（1）访谈系统运维负责人，询问是否存在对信息系统的日常运维操作及用户登录操作日志信息的管理，是否有防止非法访问和篡改的保护措施。

（2）查验日志存储信息是否存在日志信息被编辑或删除、日志保存介质耗尽、或者不能记录事件以及自身覆盖重写的情况。

（3）检查保存日志存储介质周围的物理环境是否存在安全隐患，并采取必要的物理防护措施，如防火、防磁等。

3. 日志检查审计

（1）访谈系统运维负责人，询问是否定期对系统管理员和系统操作者的活动日志进行了评审。

（2）抽样调阅系统日志信息，查验日志内容是否包括但不限于以下信息：事件发生的时间、关于事件（例如处理的文件）或故障（发生的差错和采取的纠正措施）的信息、涉及的账号和管理员或操作员、涉及的过程，并调阅日志检查记录，核实相关日志是否被定期评审。

（3）调阅系统错误日志，是否完整地记录处理信息、应用系统以及通信系统的问题，并明确记录故障处理的相关措施。主要包括:评审故障日志，了解是否已解决故障；评审纠正措施，评估方法的合理性。

## 三、系统监控与故障管理审计

### （一）业务概述

系统监控，是指组织为确保信息系统的运行安全，针对其所处的基础物理环境、系统性能（如网络、主机等）及其运行状况，明确并建立测评体系和监控机制，通过人工与自动化监控系统相结合的方式加强安全检查，从而及时发现问题并采取适当的措施进行处置。

### （二）审计目标和内容

审计目标：通过对信息系统基础物理环境、系统性能、系统运行等三方面监控的检查，确保组织建立了系统监控的相关管理制度规范与测评体系，并部署了相应的自动化监控系统与

工具；确保组织针对信息系统基础环境（如温湿度、消防、防水、空调、电力）建立了监控机制。

审计内容：测评体系和监控机制的建立情况，通过人工与自动化监控系统相结合的方式加强安全检查的应用情况，发现问题并及时采取适当的措施进行处置的情况。

（三）常见问题和风险

1. 未建立完善的系统监控与测评体系，测评指标无法完整地反映组织对信息系统基础物理环境、系统性能、系统运行的监控要求。

2. 未有效部署监控系统，或监控系统没有按照既定的监控指标对基础物理环境、系统性能、系统运行实施监控，监测内容不完整。

3. 监控过程中出现的问题不能及时预警或无法得到及时处置。

（四）审计的主要方法和程序

1. 系统监控与测评的制度规范体系建立

（1）访谈组织信息技术负责人，了解是否就信息系统自身及其所处的基础物理环境建立监控相关制度规范、运行和维护测评体系，以及是否有专门部门和人员负责系统测评考核工作。

（2）查阅相关文档，检查监控相关制度规范是否覆盖基础物理环境、系统性能和系统运行等三方面；查验是否建立了针对系统运行的测评体系，测评指标和内容是否覆盖基本要求。

（3）通过访谈及文档查阅，验证针对测评指标不达标的方面是否进行了及时处置。

2. 基础物理环境监控

（1）查阅组织基础物理环境监控相关制度，检查制度内容是否明确规定了基础环境监测相关内容。

（2）查阅组织日常巡检登记簿，验证是否按照相关制度严格进行监控、登记簿登记是否完整。

（3）查阅组织的故障记录，并对比日常巡查登记簿，验证是否能够及时发现基础环境中出现的问题。

3. 系统性能监控

（1）查阅组织系统性能监控相关制度，检查制度内容是否明确规定了系统性能监测相关内容。

（2）调阅组织日常巡检登记簿，验证是否按照相关制度进行监控、登记簿登记是否完整。

（3）实地查看监控系统，验证其监测内容是否完善，监控指标能否完整反映线路质量、通信设备的处理能力和网络服务质量的参数，如误码率、主机的CPU、内存、端口的使用率、吞吐量、传输和时延、响应时间等指标。

（4）查验监控系统是否能够及时监测性能异常并产生、发送警告，且与当前系统的实际情况进行验证。

（5）参照事件管理处置流程，验证组织在监测到系统性能异常后能否及时处置。

（6）通过查询组织系统故障记录验证监控的有效性。

4. 系统运行监控

（1）查阅组织应用系统监控相关制度，检查制度内容是否明确规定了应用系统监测相关内容。

（2）调阅组织日常巡检登记簿，验证组织是否按照相关制度严格进行监控、登记簿登记是否完整。

（3）实地查看监控系统，验证其监测内容是否完善，监控指标能否完整反映系统运行状态、并发用户数量、异常交易等。

（4）实地查看验证数据中心网管工作站、系统性能监视屏、系统资源监视屏、会话连接监视屏、应用错误监视屏是否有专人负责监控。

（5）通过查询组织系统故障记录验证监控的有效性，检查在监测到应用中断等异常时是否可以及时产生告警。

（6）参照事件管理处置流程，验证组织在监测到应用异常后能否及时处置。

## 四、变更管理审计

### （一）业务概述

变更管理，是指组织通过对信息系统服务组件的变更实施管理和评审，从而确保变更的有效性，满足业务需求，以及降低变更对服务质量的影响。

**（二）审计目标和内容**

审计目标：通过对变更管理制度、变更流程、配置文档的审计，及时识别、控制风险，确保达到信息系统安全策略要求的安全水平。

审计内容：变更管理制度的规范完整、重要变更评估方法和结果、重要变更的应急方案和措施。

**（三）常见问题和风险**

1. 未建立健全变更管理制度规范，未对变更进行明确分类并据此制定严格的变更流程。

2. 未针对生产系统的重要变更进行影响评估。

3. 变更前未制定应急回退计划。

4. 由于系统更新升级不及时影响目标实现。

**（四）审计的主要方法和程序**

1. 变更管理制度与流程

（1）访谈组织信息技术负责人，了解是否就信息系统的变更制定相应的制度规范和变更流程。

（2）查阅变更管理制度，检查其内容是否对变更进行明确分类（一般变更、重大变更和紧急变更），并据此规范变更的管理流程、角色和职责。

（3）抽样调阅变更文档，查看是否包括以下部分：变更的标识和记录；变更的策划和测试；变更影响的评估，包括安全影响；对变更的授权批准程序；向变更设计人员传递变更细节；反馈程序，包括从不成功变更、未预料事件中退出及恢复的程序和职责；验证是否包括变更后的测试及评估报告。

2. 变更评估与审批审计

（1）抽取组织部分变更记录，查验变更记录中是否有影响评估的内容，以及评估内容至少包括技术可行性、业务影响、风险等级等方面;查看评估报告是否经过管理层审阅。

（2）查验变更记录中的变更授权过程记录是否清楚，是否符合该机构变更管理规定中有关授权级别的规定;跟踪变更流程，验证是否能严格按照授权进行变更，是否存在超授权、无授权变更的情况。

（3）查阅变更记录，验证变更前是否制定了应急回退计划，因特殊情况无法回退的，是否说明了原因。

3. 变更执行审计

（1）查阅变更记录，验证相关变更是否定期安排进行。验证除紧急变更外，常规变更时间安排是否合理。

（2）查阅变更记录，验证组织是否尽量采用常规变更、减少紧急变更。

（3）查阅变更记录，验证变更手续是否完备，特殊情况无法书面申请的，是否在变更后及时补办了相关手续。

（4）紧急变更审计，查阅变更记录，验证紧急变更后是否经过相关负责人的补签并对紧急变更进行合理性评估。

## 五、事件与问题管理审计

### （一）业务概述

事件管理是指组织为防范任何可察觉和可识别的、对信息系统基础设施管理或者信息系统服务造成影响的现象而采取的管理机制，对信息系统运行事故及时响应，逐级上报，记录、分析和跟踪事故进展，直到对事故进行彻底的改正并完成根本原因分析。

问题管理是指组织为从根本上消除问题，定期组织人员对事件进行评估、分析，对有共源性的事件进行升级，通过建立问题管理台账机制，全面地追踪、分析和解决信息系统问题，分析问题发生的根源。

### （二）审计目标和内容

审计目标：通过对组织的事件与问题管理两方面的检查，督促组织建立正常的信息安全事件报告、应答和分类机制，通

过建立事件、问题管理台账机制，全面地追踪、分析和解决信息系统问题。

审计内容：检查信息安全事件、问题的管理机制，信息安全事件、问题的响应、评估、上报、处置情况。

（三）常见问题和风险

1. 事件未进行分类分级，导致事件处理不分大小、轻重的风险。

2. 事件的响应、处置、上报流程不明确的风险。

3. 未对事件进行有效的分类、评估、分析从而上升至问题管理流程，并采取措施从根本上消除问题。

（四）审计的主要方法和程序

1. 事件管理

（1）查阅组织事件管理相关制度，了解事件的分类标准、事件记录的内容项、报告流程和反馈机制。

（2）查看历史事件处置记录，验证：是否如实、完整地记录所有重要细节（如冲突类型、发生的故障、屏幕上的信息、异常行为等）；及时依照既定事件处理流程向相关联系人报告；是否采取了合适的反馈机制，以确保在信息安全事件处理完成后，能够将处理结果通知事件报告方及相关方。

（3）查看历史事件处置记录，验证相关规定和流程是否包括：事件原因的分析和确认；遏制事件再次发生的策略；向监管部门报告发生的行为。

（4）调阅组织历史事件处置记录，验证是否收集、保护审计踪迹和类似的证据。

2. 问题管理审计

（1）调阅组织相关文档，验证是否制定了完善的问题管理制度和事件管理升级为问题管理的标准。

（2）调阅组织事件管理登记表及详细记录，验证是否能够按照相关规定及时将事件管理升级为问题管理流程。

（3）调阅组织问题管理记录，验证是否建立问题管理台账，台账是否记录了问题处理的全过程，包括：对信息事件进行分析、评估；抽验组织是否及时将事件升级为问题管理查证事件管理记录，验证升级为问题管理流程并经过处置的信息事件是否再次发生，从而证明问题解决的有效性。

## 六、容量管理审计

### （一）业务概述

容量管理，是指组织通过对容量的监控、需求的识别、预先的规划和准备，确保及时提供足够的容量，保证资源可用性，最终确保业务系统的可用性和效率。

### （二）审计目标和内容

审计目标：通过对系统容量管理的检查，判断组织是否通过对应用系统的分析，监控并掌握系统容量需求，预测未来所需资源，以此制定容量规划，并在尽量减少对业务影响的前提下，通过规范的容量变更流程合理扩充系统容量。

审计内容：系统容量的监控、分析、调整、应急处置情况。

（三）常见问题和风险

1. 未对系统进行有效监控，从而掌握系统资源需求情况。

2. 未对组织的容量进行科学分析，从而影响容量规划制定的准确性和合理性。

3. 容量变更前未制定变更计划、应急措施或对其进行测试，影响业务运行。

（四）审计的主要方法和程序

1. 容量规划

（1）调阅组织项目需求文档，验证需求分析阶段是否考虑了容量需求。

（2）验证组织是否使用了分析、模拟和趋势预测等模型来确定系统的容量需求以及确定最佳的容量方案的过程，并验证模拟过程是否考虑到了各种不同的情形。

2. 容量监测

（1）查阅组织有关系统监控的管理规定，验证有关规定是否完备，能否覆盖组织重要信息系统及其主机性能、数据库、应用运行情况等方面。

（2）验证组织是否采取恰当的监控手段，调阅监控记录的审阅记录，验证相关监控记录能否及时得到审阅、分析，在容量超阈值的情况下能否及时报警。

（3）调阅组织容量监控记录，验证是否对容量报警及时进行了分析、处置。

3. 容量变更

（1）查阅组织系统监控报表，抽取部分性能监控超过阈值报警的情况。

（2）抽查报警事件的处理记录，验证是否对事件进行了及时、合理处置，是否根据情况制定了容量升级规划，若制定了容量升级规划，验证该规划是否对扩充容量进行了计算、是否制定了较为完备的升级预案和应急措施。

（3）通过查阅容量变更记录及了解变更相关人员，以确定容量变更之前是否已通知了所有系统相关人员。

（4）抽查容量扩充后的测试报告，验证容量扩充后是否进行了全面、严格的测试。

## 第三节　信息安全管理审计

信息安全，是指保护组织信息资产的机密性、完整性和可用性，信息内容符合国家法律、法规及监管要求。

信息安全管理审计，是指通过调查取证以发现组织中是否对信息安全治理、信息安全管理及信息安全技术等方面存在充分的控制，评价这些控制的有效性和适宜性。

### 一、安全管理审计

#### （一）业务概述

安全管理，是指组织通过制定总体信息安全管理方针，明确工作的总体目标、范围、原则和安全框架等内容；通过建立制度规范、操作规程、安全策略，确保安全管理工作的合规性，支持组织业务安全运营；通过风险评估、持续检查和独立审计等促进手段，实现信息安全管理体系的持续改进与完善。

#### （二）审计目标和内容

1. 评价信息安全制度规范是否符合所在地国家有关法律法规、技术标准及主管部门安全要求，是否得到切实、有效执行。

2. 检查是否根据资产敏感性、重要程度等因素，建立和实施相应的保护措施。

3. 检查组织是否持续对信息安全风险进行评估，及时发现并制定整改计划，将整改责任落实到位。

#### （三）常见问题和风险

1. 信息安全体系建设不全面，信息安全没有落实到具体的制度和流程中，无法有效落实各项信息安全管控要求。

2. 未建立信息安全战略规划，无法明确信息安全的总体目标和建设方向，不利于信息安全工作的长远发展。

3. 未对组织信息资产进行有效识别与管理，资产更新不及时，不利于对信息资产的识别、评估与保护。

4. 未建立有效的信息安全风险评估方法，不能对已识别出的风险制定有效的处置方案，导致信息安全风险发现与处置不及时。

5. 未持续开展信息安全检查与审计工作，无法通过自身或独立第三方对安全体系的控制有效性进行科学评价，不能有效推进安全体系的持续完善。

（四）审计的主要方法和程序

1. 规范制度制定与执行

（1）调阅组织信息安全管理规定，了解是否对重要信息系统安全管理岗位制定并明确规章制度、工作职责及信息安全事件报告制度、处理流程和违规处罚，判断其合理性。

（2）调阅组织信息安全体系建设方案、信息安全战略规划等文件，检查信息安全管理体系文件是否围绕着安全目标、安全规划、风险评估、体系设计、体系建设、检查考核等，提出了开展安全体系建设的方法与步骤。

（3）评估安全管理制度和流程是否涵盖了安全组织与人员、安全岗位与职责、信息资产管理、物理安全、网络安全、主机安全、应用安全、数据安全、终端安全、新技术安全等方面。

（4）访谈信息安全管理负责人员，了解信息安全制度的执行、修订、颁布实施及重大事件的上报、违规惩处情况。

（5）调阅安全风险评估、安全检查及内外部审计资料，查看安全风险评估、安全检查及内外部审计是否对评估、检查及审计发现的安全问题进行了整改落实，后续的整改落实情况是否符合安全管控的要求。

2. 合规遵守

（1）调阅信息安全制度，检查制度是否遵循国家有关信息技术管理的法律法规要求，以及技术性比较强的信息系统安全制度是否低于国家相关标准规定，且与主管部门相关办法、要求相冲突。

（2）访谈信息安全管理负责人，了解组织是否在境外设立分支机构，以及境外分支机构信息安全制度是否符合所在地区监管机构的要求。

3. 信息资产管理

（1）调阅并检查信息资产分类管理制度是否建立、健全，内容是否对信息类别和访问人员的范围、级别做出明确规定。

（2）查阅资产管理制度，查验是否根据信息资产安全级别制订不同的安全防范措施并采取不同的技术防范手段。

4. 信息安全风险评估

（1）检查信息安全风险评估的范围与频度，风险可接受水平设定的科学性，以及是否针对评估出来的风险制定风险处置计划。

（2）调阅信息安全风险评估报告，判断风险评估方法的科学性与适宜性，并检查是否得到了所在部门管理层的确认。

（3）检查是否按照计划进行了有效的控制，使风险在计划时间内降到可接受范围内。

5. 信息安全检查与持续改进

（1）调阅信息安全管理检查和审计相关计划及报告，了解检查、审计的频度与范围。

（2）对检查、审计报告的不符合项抽样进行审核，评估其整改效果，是否持续对信息安全管理体系进行更新与完善。

## 二、物理安全审计

### （一）业务概述

物理安全管理，是指组织为确保机房及办公场所的物理安全，特别是机房，从其规划建设到日常维护，采取一整套有效的，包括制度规范和物理工具的管理措施，确保物理环境的安全和组织的业务连续运行。

（二）审计目标和内容

通过对组织物理设施，特别是机房所处物理环境的安全检查，判断组织是否采取有效的物理安全控制措施，保障机房等物理环境的安全，防范非法访问，确保机房等重要物理设施持续、可靠地提供服务。

（三）常见问题和风险

1. 组织机房和办公场所所处的物理环境不符合安全需求，存在安全风险。

2. 组织机房和重要办公场所等未采取有效的物理安全防护措施，防范非法物理访问，存在资产丢失或遭受破坏的风险。

3. 未针对机房等重要物理设施建立完善的安全管理制度和操作规范流程，并缺失必要的资源保障或安全控制措施，存在发生电力中断、火灾、水灾等安全隐患。

（四）审计的主要方法和程序

1. 物理位置安全

（1）访谈物理安全负责人，询问机房和办公场地的环境条件是否满足信息系统业务和安全管理需求，具有基本的防震、防风和防雨等能力，并查验机房和办公场地所处周边环境是否存在强电场、强磁场、易燃、易爆等安全隐患。

（2）访谈物理安全负责人，询问机房等级并查验设计/验收文档是否符合安全标准。

（3）访谈机房维护人员，询问是否存在因机房和办公场地环境条件引发的安全事件或安全隐患，是否及时采取了补救措施。

2. 防盗窃和防破坏

（1）检查主要设备和部件是否存放于机房内，并对其进行加固和设置明显、不易去除的标记。

（2）检查通信线缆铺设在隐蔽处并可架空铺设在地板下或置于管道中，强弱电需隔离铺设并进行统一标识。

（3）检查是否对磁带、光盘等介质进行分类标识，并存储在介质库或档案室的金属防火、防磁柜中保管。

（4）检查是否对机房和重要物理设施设置监控报警系统，外围是否设置光、电等技术设施和防盗报警系统，防范对其进行非法访问、盗窃和破坏。

3. 机房安全管理

（1）通过座谈和调阅相关资料，了解是否制定并明确机房安全策略、操作规程、人员职责，并查验是否对机房基于业务和安全管理需要进行功能分区并判断划分的合理性。

（2）访谈相关人员了解其职责履行、教育培训、安全意识和制度执行情况，判断相关安全工作落实情况。

4. 机房物理安全防护与电力供应

（1）查阅机房建设设计/验收文档，了解机房的建设级别，了解物理安全设计规范要求。

（2）访谈物理安全负责人，并查验机房是否配备恒温、恒湿，防范、防止雷电、火灾、水灾和电磁与静电的设施。

（3）访谈电力供应保障部门，询问是否设置UPS过电压防护设备及采用双路供电，提供备用和冗余电力供应系统，确保短期电力供应保障。

## 三、网络与通讯安全审计

### （一）业务概述

网络与通讯的安全管理，是指组织为确保和加强自身网络通信安全的管理，从结构规划、传输使用、安全防护与监控等方面加以管理，确保网络的安全稳定和通讯畅通，避免因网络通信故障影响业务正常开展，防范因此在操作、法律和声誉等方面产生的风险并给组织造成损失。

### （二）审计目标和内容

通过对结构安全、传输安全、接入与访问控制、网络入侵防范、恶意代码防范以及安全审计等方面的检查，判断组织是否采取有效的控制措施，确保组织的网络与传输安全。

### （三）常见问题和风险

1. 网络安全架构设计不合理，网络安全域划分不完善，未采取有效的访问控制措施和边界安全控制措施。

2. 主机与设备的网络接入没有得到有效的识别与控制，存在网络非法接入或外联现象。

3. 未根据业务与场景的需要而采取有效的传输安全控制措施，存在传输数据泄露的风险。

4. 网络入侵与恶意代码防护不到位，容易造成内外部攻击者入侵风险和恶意代码传播风险。

5. 未部署有效的网络安全审计工具或日志管理机制不健全，导致无法实现对网络安全事件进行留痕和溯源的风险。

**（四）审计的主要方法和程序**

1. 结构安全

（1）访谈网络管理员，询问网段划分情况以及划分的原则及重要网段的保护措施有哪些，判断是否采取有效的隔离手段。

（2）访谈网络管理员，询问是否在关键网络节点部署核心网络设备及冗余设备，查阅网络拓扑图，查验设备部署合理性和一致性，判断是否具备业务安全处理能力。

（3）访谈网络管理员，询问信息系统中的边界和主要网络设备的性能以及业务高峰流量情况，网络带宽及控制情况和带宽分配的原则，并登录查看网络设备，查验负载情况及性能，判断是否可以满足业务高峰需要。

2. 传输安全

（1）访谈网络管理员，了解广域网和局域网重要传输链路采用的通信协议，以及是否采用加密技术和设备对其进行加密传输，从而判断重要应用服务是否采用不可靠连接的传输协议。

（2）查阅网络拓扑图，检查组织是否有至少两条的主干链路接入和备份线路，以及关键传输链路是否有冗余，并访谈网络管理员对其进行验证。

（3）通过执行安全工具扫描和渗透测试，验证网络之间传输数据的安全性。

3. 接入安全与访问控制

（1）查阅网络接入管理相关制度规范，了解是否针对网络接入采取制定管理控制措施及访问控制策略，并登录相关网络控制设备查验是否配置并开启相应的功能。

（2）访谈网络管理员，了解现有的网络访问控制措施、访问控制策略设计原则及更新频率，以及是否对非授权设备的非法内联和外联进行监测并采取相应的管控措施，查验安全控制措施的有效性。

（3）询问网络管理员是否配置了路由器远程拨号登录，拨号网络是否在拓扑图中标识。

（4）检查交换机、路由器的口令是否启用了加密功能，重要的路由表更新是否启用加密。

4. 网络入侵防范

（1）访谈网络安全管理员，询问是否在网络边界及重要系统或存储设备区域部署防火墙和入侵检测与防范系统，查阅组织网络拓扑结构图，验证其一致性。

（2）登录上述设备，查看是否配置并启用相应的安全策略，并测试其是否具有相应的安全防护能力，并验证：

①防火墙是否可对数据流实现端口级防护，对应用层实现应用协议的命令及控制，对会话超时、网络最大流量和网络连接数进行控制。

②入侵检测与防范设备是否具备对常见网络攻击监视的能力，以及当检测到网络攻击后是否可启动自动防护功能，记录攻击信息并在发生入侵事件时提供报警。

（3）上述设备的日志信息是否完整并具有防篡改的能力，以及是否提供报警功能并检查历史报警信息。

（4）通过执行安全工具扫描和渗透测试，可以验证网络入侵预警与防范机制是否有效。

5. 网络恶意代码防范

（1）查阅并了解组织是否制定恶意代码防范制度及更新策略。

（2）访谈安全管理员，了解组织目前所采用防恶意代码产品，询问网络恶意代码防范措施内容及恶意代码库的更新策略。

（3）查看在网络边界及核心业务网段处是否部署恶意代码防护产品（如防病毒网关），并查验防护产品是否开启实时更新功能及恶意代码库是否为最新版本。

6. 网络安全审计（注：这里的“安全审计”是指通过系统日志的形式对操作记录进行留痕，并通过软件工具对日志进行管理，可常态化地对系统运行状态及操作者的行为进行溯源分析和合法性分析，下同。）

（1）访谈负责网络审计的相关人员，询问对边界和网络设备是否实现集中安全审计，以及审计内容、审计记录和对审计记录的处理方式有哪些。

（2）检查边界和网络设备，查看审计策略是否对网络设备运行状况、网络流量、用户行为等进行全面的监测、记录，以及事件审计策略内容是否包括事件日期时间、用户、事件类型、事件成功情况等审计关键信息。

（3）检查边界和主要网络设备，查看时钟是否保持一致。

（4）查验边界和网络设备的日志是否被集中保管，并采取安全措施防范恶意删除、修改或覆盖，验证安全审计的保护情况与要求是否一致。

## 四、主机安全审计

### （一）业务概述

主机安全管理，是指组织为确保主机及其存储信息的安全，采取包括主机访问控制、用户身份鉴别、入侵及恶意代码防范等保护措施以及主机资源监控和安全审计等手段，确保主机资源的可用性并实现对主机重要操作等用户行为的安全监控和审计，同时满足对日志管理的合规要求。

### （二）审计目标和内容

检查组织为确保主机安全，是否制定合理的访问控制策略，并采用身份鉴别手段，对主机操作者身份进行识别和确认的过程，确保合法用户对主机及其资源的合法访问与使用；检查是否采取必要的措施，确保主机操作系统和数据管理系统所在的存储空间在重新分配给其他用户前所存储的信息得到完全清除，以及是否实施主机资源监控、入侵及恶意代码防范和主机安全审计等控制措施确保主机安全。

### （三）常见问题和风险

1. 未制定完善的访问控制策略或采取有效的访问控制措施对主机及其资源访问进行控制，容易造成访问权限过大、职责交叉等风险。

2. 主机用户的身份鉴别控制措施和策略不完善，致使出现主机用户身份识别有误、共享（重复）登录账号、身份验证信息泄露、主机密码设置过于简单，未采用多种身份鉴别技术等风险。

3. 未对主机实施有效的入侵检测与恶意代码防范措施，或主机恶意代码版本更新不及时，致使遭受恶意攻击。

4. 未对主机资源进行有效监控，导致主机资源不可用或无法有效支撑业务发展。

5. 未部署有效的主机安全审计工具或日志管理机制不健全，导致无法实现对主机的违规操作进行有效识别和记录。

**（四）审计的主要方法和程序**

1. 主机访问控制

（1）查阅组织访问控制策略规范，检查其制定原则是否遵循“权限分离”和“最小授权”原则，并基于角色制定和分配访问控制权限。

（2）登录信息系统，查验是否启用访问控制功能并基于制定的控制策略和用户角色进行权限分配和资源访问控制。

（3）检查是否对操作系统和数据库的特权用户实现权限分离，限制默认账户访问权限，修改系统默认账户名称及默认密码。

（4）检查是否对重要信息资源设置敏感标记并对其依据安全策略严格控制用户对其访问。

2. 身份鉴别

（1）查看组织是否制定账号与密码管理策略，检查是否涉及口令复杂度、长度、更换周期、账户锁定并登录服务器进行验证。

（2）访谈系统管理员对操作系统和数据库系统采取的用户身份鉴别方式，并验证是否采用多种身份鉴别技术，以及抽样检查是否存在重复、共享或过期账户。

（3）检查远程连接时采用的安全协议及加密传输方式是否可防止鉴别信息在传输过程中被窃听。

（4）通过执行配置检查，验证口令设置的安全性，包括口令复杂度、长度、更换周期等。

3. 剩余信息保护

（1）访谈系统管理员，询问操作系统用户（数据库管理员用户）的鉴别信息存储空间在被释放或重新分配给其他用户前是否得到完全清除；系统内的文件、目录所在的存储空间或数据库记录等资源所在的存储空间在分配前存储信息是否得到完全清除。

（2）查看主要操作系统和主要数据系统维护操作手册是否明确用户鉴别信息存储空间，被释放或再分配给其他用户前的处理方法和过程；文件、目录和数据记录所在的存储空间，被释放或再分配给其他用户前的处理方法和过程。

4. 主机入侵与恶意代码防范

（1）检查是否针对重要服务器部署入侵检测设备，查验是否对入侵行为可及时监测、记录和报警，检查入侵记录是否完整。

（2）检查服务器和操作系统是否安装恶意代码软件并支持统一管理，查验其版本和代码库是否与服务商提供的最新版本相一致，以及与网络恶意代码库不相一致。

5. 主机资源监控

（1）访谈系统管理员对重要服务器的访问终端采用的管理手段有哪些，并验证是否对终端接入方式、网络地址范围等条件做限制。

（2）检查是否根据安全策略设置登录终端操作超时锁定。

（3）检查是否限制单个用户对系统资源的最大或最小使用限度，以及同一时间会话数量。

（4）检查是否对主机资源的使用进行监视并设置阈值，从而在低于阈值时报警，以确保重要服务器提供既定的服务标准。

## 五、应用安全审计

### （一）业务概述

应用安全管理，是指组织为确保应用安全，从应用系统的生命周期以及服务端和客户端等三方面的安全管理为出发点，采取安全管理措施，在确保应用系统安全建设及管理贯穿整个

应用系统开发生命周期的同时，保证服务端和客户端具有必要的安全控制手段。

### （二）审计目标和内容

通过对应用系统客户端、服务端及应用系统自身全生命周期的安全审计，确保客户端业务逻辑模块、安全模块、交互功能、接口功能以及服务端认证鉴权、业务逻辑，及其所涉及的通信功能的安全；此外，还从应用系统开发生命周期角度，检查、评价应用软件在需求、设计、开发、测试、部署、运营及废弃各阶段的安全控制措施。

### （三）常见问题和风险

1. 应用系统在设计、编码和测试阶段未考虑安全控制措施，未使用国密安全算法或算法过于简单，可能无法保证应用系统中数据传输、操作和存储的安全性。

2. 未执行源代码安全检查或安全检查不到位，无法及时发现代码中存在的非法后门和安全漏洞，一旦受到恶意攻击，将威胁应用系统的安全性，甚至导致客户端敏感信息泄露。

3. 应用系统操作日志记录不全面，无法有效利用日志分析应用系统存在的安全风险和隐患，不利于应用系统的日常维护和安全管控。

4. 应用系统安全需求评审不到位，可能导致无法在设计和编码阶段融入安全需求，不利于应用系统的安全需求的落实。

（四）审计的主要方法和程序

1. 应用系统客户端安全

（1）源代码安全。获取客户端源代码，检查客户端源代码是否进行了混淆处理，是否具有完整性校验能力，是否对签名信息进行安全校验；检查客户端源代码是否删除应用中的冗余或注释代码。

（2）运行环境安全。安装应用客户端软件，观察应用系统是否可以正常运行，是否具有异常处理安全机制；通过执行客户端软件反汇编、客户端指令篡改、客户端密码暴力破解等技术手段，验证客户端运行环境的安全性；检查客户端软件是否具有版本检测机制，提供版本更新功能。

（3）算法安全。检测客户端软件是否采用了国家管理部门认可的加解密算法。例如SM2、SM3、SM4算法等。

（4）组件安全。检测客户端软件是否对组件权限进行限制，避免第三方应用随意调用组件内容。

（5）日志安全。检测客户端软件是否对日志数据进行了加密保护；必要时，是否删除了与应用系统运行逻辑相关的日志数据。

（6）存储数据安全。检测客户端软件是否对本地存储的数据进行加密保护，对本地存储数据进行完整性校验。

（7）权限安全。检测客户端软件是否删除了多余的权限配置，避免冗余权限的滥用，对权限申请模块进行完整性校验。

（8）通讯安全。检测客户端软件与服务器进行通信时是否采用安全通信协议，例如SSL/TLS、IPSec等；客户端是否对通信数字证书进行了安全性校验；检测是否对通信数据进行了加密保护，是否对通信数据进行了完整性校验。

2. 应用系统服务端安全

（1）身份认证安全。检查服务器是否应对用户任何请求等操作进行认证授权；检查服务器是否具有登录异常处理机制；通过执行渗透测试，检查服务器是否能对SQL注入、XSS跨站、上传漏洞、缓冲区溢出等安全问题引起的认证绕过进行防范。

（2）口令及密码安全。检查服务器与客户端进行身份认证时是否采用静态密码、动态口令、USBkey等认证方式；服务器与客户端应具有双因子或多因子认证机制；服务器是否对口令复杂度进行安全提示，服务器是否具有口令找回功能。

（3）会话安全。检查服务器是否对会话信息进行安全加密；检查服务器是否对会话信息添加时间戳，进行完整性校验。

（4）提示信息安全。检查服务器是否对客户端错误请求引起的提示信息进行处理。

（5）检查服务器与移动应用、与其他服务器进行通信时是否对通信数据进行加密保护；检查服务器与移动应用及服务器与其他服务器进行通信时，是否对通信数据进行完整性校验。

3. 应用系统生命周期安全

（1）检查应用系统开发的需求阶段是否能将安全评价要求纳入到软件评审过程中；是否能建立内部安全需求库，持续完善应用安全评价要求；是否能将相关行业安全规范纳入到安全评价要求中。

（2）检查应用系统设计阶段是否能对应用进行威胁建模，全面发现其威胁点；是否针对每一个威胁点，研究相应的应对措施，并应用到应用的设计过程。

（3）检查应用系统开发阶段是否能建立完备的安全编码规范体系；对于通用开发技术，是否能建立专用的模块库；在开发过程中是否能建立完善的代码审核机制。

（4）检查应用系统测试阶段是否能建立完善的测试方法（包括白盒测试和黑盒测试）；是否能在软件测试项增加安全测试的要求和进行了安全测试。

（5）检查应用系统交付阶段交付的应用是否具备适当的抵御恶意攻击的能力，交付的渠道是否安全可靠，是否具备对应用软件进行安全评估的能力，是否具备一定防范相关交付风险的能力。

（6）检查应用系统交付运营是否能建立快速响应平台，对发现的安全漏洞应有快速修复的能力；是否对提供的应用进行安全监控，发现安全风险并为用户提供安全更新。

## 六、数据安全审计

### （一）业务概述

数据安全管理，是指组织为确保自身数据资产的安全性，以数据全生命周期为线索，从人员、流程和技术三方面，采取安全管控措施，确保组织的数据安全。

### （二）审计目标和内容

通过制度层面以及数据全生命周期管理、完整性和保密性等方面的检查，确保组织对数据均进行安全控制，同时采取必要的技术工具，防范数据完整性遭受破坏、数据泄露并确保数据的可用性，了解组织是否在必要的情况下，为重要系统建立灾备系统。

### （三）常见问题和风险

1. 未建立数据全生命周期的安全管理制度，无法有效对数据安全的各项工作进行管控，不利于数据全生命周期的安全要求落实。

2. 未对重要和敏感数据进行分类分级，无法针对不同类别数据进行不同的安全控制措施，可能导致安全管控过重或安全管控缺失。

3. 在数据采集、处理、存储、传输、分发、备份、恢复、清理和销毁等阶段，未充分采取有效的技术工具，一旦数据遭到非法访问与使用，可能导致数据泄露和完整性遭到破坏等风险。

4. 未对组织重要和敏感数据实施有效的备份和恢复策略，或建立本地（异地）灾备系统，一旦发生网络安全事件或重大灾害，无法及时对重要数据进行恢复，数据的完整性和可用性得不到保证，将给系统稳定运行带来较大安全隐患。

**（四）审计的主要方法和程序**

1. 数据安全管理

（1）查阅组织的数据管理制度，确认其涵盖数据采集、处理、存储、传输、分发、备份、恢复、清理和销毁等阶段，是否分类分级管理，并据此制定相应的管理审批流程。

（2）调阅数据管理制度，查看是否有数据安全管理方面的管控措施以及用户敏感信息的保护措施，并检查其是否符合国家相关法律法规的要求。

（3）检查组织岗位职责相关文档，了解各岗位在数据的采集、处理、存储、传输、分发、备份、恢复、清理和销毁过程中的职责和权限划分，并判断各岗位之间职责分离的遵循程度，确认其划分的合理性。

（4）对数据安全管理负责人员进行访谈，了解各个工作岗位的人员情况，确认人员的相关资质是否符合数据安全管理的要求，以及是否签署相关的安全保密协定及遵守情况。

（5）对数据安全管理负责人员进行访谈和现场验证，了解组织是否部署了数据库防火墙、数据库审计系统、数据防泄漏系统、数据脱敏系统、终端用户行为分析系统等多层次的数据管控工具。

2. 数据完整性检查

（1）访谈安全管理人员和技术开发人员，了解组织为保证重要操作和应用系统数据、系统管理数据、鉴别信息和用户数据在传输、处理和存储过程中的完整性所采取的技术措施，并查验完整性是否受到影响以及恢复措施的有效性。

（2）访谈管理人员（系统管理员、网络管理员、安全员、数据库管理员），询问是否为所负责的重要系统通信提供专用通信协议或安全通信协议服务以及详细信息并验证是否正在使用。

3. 数据保密性检查

（1）查阅并判断组织数据保密相关管理制度、使用规范与技术标准是否符合国家标准。

（2）访谈信息安全管理人员或技术开发人员，了解网络设备鉴别信息、敏感系统管理数据和敏感的用户数据在存储、处

理和传输过程中所采取加密机制（如密码算法、密钥和加密设备）的有效性和合规性，特别关注利用公共网络传输业务数据时的加密处理办法及重要数据是否全部得到了保护。

（3）访谈安全员，询问在使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息。

（4）检查操作系统、网络设备、数据库管理系统、应用系统的设计/验收文档，查看其是否有关于应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述。

（5）通过使用数据获取工具，有效检验数据防泄漏效果。

（6）通过执行渗透测试，有效验证重要数据或敏感信息的保护能力。

4. 数据备份与恢复检查

（1）查阅组织是否制定数据备份和恢复策略文档，了解数据备份和恢复测试的对象、频率和方式以及数据保管的期限要求并判断其合理性。

（2）查看备份和恢复策略文档记录、恢复测试报告和测试记录，验证是否严格按照备份和恢复策略执行。

（3）查验数据备份环境，检查其是否符合防水、防盗、防尘、防磁等物理安全条件，并检查重要数据备份介质是否场外存放。

（4）访谈网络管理员，询问是否建立异地灾备，以及信息系统中的网络设备、操作系统、数据库管理系统是否提供自动备份机制并对重要信息进行本地和异地备份功能，以及是否提供重要设备和线路的硬件冗余。

（5）检查设计/验收文档，查看其是否有关于重要业务系统的本地和异地系统级热备份的描述，以及是否有关于在灾难发生时的业务自动切换和恢复功能的描述。

## 七、访问控制审计

### （一）业务概述

访问控制管理，是指组织为防止信息资源遭受未经授权的访问，确保其在合法的范围内使用，所采取的物理和逻辑的控制手段，并借助有效的用户身份识别和访问控制策略，对身份和权限进行管理，特别当组织存在用户远程接入时，重点对其进行安全管理。

### （二）审计目标和内容

该项的审计目的旨在通过对组织物理访问控制、逻辑访问控制以及账号权限的检查，判断组织是否对组织及信息系统所处区域实施物理安全防护，避免未授权的访问、损坏或干扰，

以及是否根据组织既有的访问控制策略，针对单个用户或组用户对组织资源的访问控制规则和权力进行逻辑控制；此外，通过对远程接入管理的检查，检查远程工作活动是否安全、受控，从而确保远程工作场地的安全，防止设备和信息被盗、未授权泄露信息、远程访问滥用。

（三）常见问题和风险

1. 对机房、办公环境等重要场所物理访问控制执行不严格，可能导致恶意人员非法进入重要场所，进而破坏重要场所中设备，导致系统中断、数据泄露或其他安全事件。

2. 未根据组织业务及安全管理需要，制定或定期更新访问控制策略并对其进行评审，可能存在重要数据被非法访问，导致敏感信息泄露。

3. 设备或系统上的账号及权限更新不及时，可能被恶意人员利用其控制缺陷，执行非法操作，威胁系统安全性。

4. 未建立远程接入安全管控机制或机制执行不到位，可能导致系统被远程非法接入，进而导致系统被破坏或重要数据泄露。

（四）审计的主要方法和程序

1. 物理访问控制

（1）查阅组织是否制定包括机房在内的物理关键设施或敏感区域出入的规章制度及访问控制策略，验证其是否包括对访问控制权限的定义、授权过程和策略更新等内容。

（2）通过抽查访问控制登记簿、观察敏感物理设施出入口是否安排专人值守及调阅访问权限修改记录等方式，验证物理访问控制策略实施的有效性及是否受控。

（3）选取部分离职人员名单，验证其是否依然存在于系统的已授权人员名单内。

（4）验证是否有门禁系统，不同区域间是否通过门禁分割，门禁是否有记录，对门禁卡的授权、发放和注销是否有明确规定。

2. 逻辑访问控制

（1）检查组织是否制定信息系统访问控制策略。

（2）调阅访问控制策略，验证该控制策略是否包括：各个业务系统的安全要求、数据的分类与授权策略、不同系统和网络的访问控制策略与数据分类策略的一致性、访问控制角色的分离、访问要求的正式授权要求、访问控制的周期性评审、访问权力取消等内容。

（3）验证组织访问控制策略是否区分必须强制执行的规则和有条件执行的规则。

（4）选取部分离职人员名单，验证其是否依然存在于系统的已授权人员名单内；选取部分转岗人员名单，验证其访问权限是否根据当前业务需要得到及时更新。

3. 账号及权限管理

（1）抽查组织重要应用系统，调阅用户清单和实际员工名单，核实用户ID是否唯一，用户所拥有的权力是否与其业务目的相适应，是否有用户授权的书面文件，离职或职位变更用户的访问权限是否得到删除或变更是否立即在信息系统中对权限进行调整，确保用户ID不会被共享。

（2）通过访谈了解每个系统所必须赋予的特权用户，检查是否存在分配特权用户的授权过程及其记录并验证组织应用程序是否必须要特权用户才能运行。

（3）验证组织是否制定有内部口令管理规定，包括口令的强度、初始口令的发放、口令的保管及口令变更。

（4）通过访谈，检查用户访问权限是否定期根据业务需要而评审，或因为岗位的变化而变更。

（5）针对特权用户的访问权限，通过访谈了解其变更频率、用户授权的评审和变更是否有日志记录。

4. 远程接入的访问控制

（1）检查组织是否制定针对远程接入的规章制度和访问控制策略。

（2）抽查部分远程接入是否留存接入日志，并检查是否符合既定的安全要求和控制策略。

（3）抽查部分访问控制申请，检查是否符合业务需要并经过授权。

（4）访谈部分远程接入用户并检查接入设备和网络入口，了解远程访问人员的家人、朋友是否有可能未授权访问信息资源，以及访问过程中是否有防病毒软件和防火墙保护。

（5）检查当远程工作活动停止时是否及时撤销授权，以及是否对客户端连接服务进行访问时间段限制。

## 八、安全防护审计

### （一）业务概述

安全防护，是指组织为确保主机、终端、网络通讯设备以及应用系统和数据的安全，所采取的补丁及漏洞管理、存储介质安全防护和密码终端与技术等安全防护手段。

### （二）审计目标和内容

通过从制度规范和技术工具层面，重点检查组织是否制定完善的制度管理规范，以及对主机、终端和网络设备采取补丁及漏洞管理，对普通和移动存储介质进行有效识别和管理，对日常通信和业务处理使用密码技术和产品，从而防范漏洞和恶意代码对业务及数据造成危害，存储介质上的信息遭受损失或

泄露，确保信息在传输、交换和存储过程中机密性、完整性、可用性和抗抵赖性。

（三）常见问题和风险

1. 安全补丁和漏洞更新不及时，一旦被恶意人员利用，可能直接威胁系统安全性，甚至导致敏感信息外泄或系统中断。

2. 主机、网络设备或系统的补丁及漏洞升级前，未制定有效的测试规范和流程，或系统重要数据未执行备份。一旦系统更新失败，可能对系统可用性和业务稳定性产生较大影响。

3. 未建立存储介质的安全管理制度，无法有效落实介质的登记、存放、使用、流转、维护、盘点、检查与销毁等环节的各项安全要求。

4. 密码技术和产品应用不符合国家安全规范，密码算法过于简单，一旦密码被暴力破解，可能导致数据在传输和存储等过程的完整性和机密性遭到破坏。

（四）审计的主要方法和程序

1. 补丁及漏洞管理

（1）查阅组织是否制定补丁与漏洞管理的制度规范、策略与流程。

（2）访谈操作系统管理员了解并查验是否对系统进行升级与维护以及具体操作流程、频率是否与既定的规范和策略相符。

（3）抽查历史补丁操作记录，检查文档是否齐备，更新流程是否包含事前的系统及业务影响性分析、安全测试及对重要文件的备份。

2. 存储介质安全防护

（1）查阅组织是否制定有关存储介质的安全管理制度，内容覆盖介质的登记、保管/存放、使用、流转、维护、盘点、检查与销毁等内容。

（2）查阅组织是否针对存储介质建立相应的资产清单，内容主要覆盖介质所有部门、当前使用者或位置信息、介质重要性以及存储信息的重要性。

（3）检查组织是否根据介质存储信息的安全级别对存储介质进行分类和标识，并对存储介质进行存储加密。

（4）检查对存储介质的物理传输或流转过程中的人员交付、打包进行控制和登记记录。

（5）调阅存储介质记录与清单对存储介质进行盘点，判断其一致性。

（6）对送修或销毁的介质记录进行检查，判断其是否符合相应的管理规范并检查审批流程是否完整。

（7）对于固定存储介质，检查其保存的物理环境是否按照制造厂商要求的存放条件进行存放，对各类介质的访问进行严格控制和保护，实现专人管理。

（8）调阅数据存储介质销毁清单，明确是否有至少两人在场，检查是否有相应文档记录证明。

3. 密码应用与管理

（1）查阅组织是否建立密码使用的管理制度。

（2）通过访谈，了解组织当前是否使用密码技术和产品，并了解当前密码产品的使用情况，从而判断组织是否使用符合国家密码管理规定的密码技术和产品以及符合组织相应的管理制度。

（3）查阅组织所使用的密码技术和产品相关资质与证明材料，判断是否合规。

## 九、终端安全

### （一）业务概述

移动终端安全管理，是指以移动存储介质为载体的固定终端和移动终端的安全管理，组织为确保上述终端的安全，一方面从其选取、采购、申领、发放等过程制定一整套完善的安全管理制度，另一方面通过常规的安全防护工具和技术，在对固定终端进行安全管理的基础之上，针对便携式终端采取特殊的管理手段。

### （二）审计目标和内容

通过对制度规范以及固定终端和移动终端安全的检查，检查组织是否制定相应的管理制度，从而对各类设备的选取、采

购、申领、发放和运维等流程进行管理，以及对两种终端采取安全保护措施。

（三）常见问题和风险

1. 未建立终端设备安全管理制度，可能无法有效落实对信息系统各类软、硬件设备的选取、采购、申领、发放等过程的规范化管理。

2. 对移动存储介质的安全防护措施部署不充分或执行不到位，可能会导致存储的重要数据或敏感信息遭到泄露。

（四）审计的主要方法和程序

1. 终端设备管理

（1）查阅组织是否针对终端设备制定安全管理制度，从而实现对信息系统各类软、硬件设备的选取、采购、申领、发放等过程进行规范化管理。

（2）检查组织是否对终端设备的维修和服务制定相应的管理制度、审批流程及维修过程的监督。

（3）查阅组织是否对信息设备带离机房或办公地点制定相应的管理制度和审批流程。

2. 基本终端安全防护

（1）检查组织是否基于组织业务安全需要和基本信息安全管理规范制定终端安全的管理规范，内容包括基本的系统安全配置、账户策略配置、日志与审核策略配置、浏览器安全配置，

并对终端采用恶意代码防范、个人防火墙和系统漏洞补丁升级等安全管理措施和工具。

（2）检查组织是否对终端采取安全防护措施和安全配置对其进行终端安全性检测，阻止防护措施不符合规范的终端接入组织网络。

（3）检查组织是否依据业务需要和安全策略对终端的应用程序和防护软件进行管理。

（4）检查组织是否对终端用户操作行为事件、配置信息更改事件进行审计，并支持审计数据的集中管理，防止审计数据未经授权的篡改和删除。

3. 移动终端安全防护

（1）检查移动存储介质是否能在宿主机硬件支撑下独立于宿主机操作系统，不与宿主机上的系统软件与应用软件通信。

（2）移动终端安全应用模式中产生和接收的信息是否存储在移动存储介质中的特定加密存储区域，存储过程不受宿主机干扰。

（3）检查便携式终端安全防护中所使用的自定制系统是否具有漏洞补丁更新、恶意代码特征库升级、系统安全核心配置等功能，支持自定制操作系统安全加固及数据加密存储等功能。

## 十、安全体系运行与事件管理审计

### （一）业务概述

安全体系运行与事件管理，是指组织以安全管理中心的形式，将制度流程、技术工具和人员统一集中管理应对日常网络安全事件，并通过建立具备安全态势感知和预警的能力，对网络安全事件采取积极、主动的防御措施。

### （二）审计目标和内容

通过检查组织是否对信息安全体系运行进行集中管理，是否对安全事件、恶意代码、安全日志、安全知识等安全相关事项进行集中管理；是否优化安全事件、安全监控、访问控制、防恶意代码、安全审计等方面的日常安全工作。

### （三）常见问题和风险

1. 信息安全未实现集中管理，不利于从全局视角审视信息安全的整体建设与工作成效，不利于信息安全整体规划与后续持续改进。

2. 信息安全管理体系运行不到位，无法有效落实信息安全各项管控要求，不利于信息安全管理的体系化、规范化建设和发展。

3. 未将信息安全管理要求纳入部门工作绩效，不利于推动信息安全管理体系的全面执行。

### （四）审计的主要方法和程序

1. 信息安全运行管理

（1）访谈信息安全负责人，询问是否已经建立安全管理中心并部署技术平台，对信息系统和安全设施的安全事件、恶意代码、补丁升级、设备状态、安全日志、用户终端行为等安全相关事项进行集中管理；了解是否配备有专门的管理人员利用安全管理中心进行对安全管理事件进行分析、处置、预警及报告工作。

（2）访谈信息安全负责人，询问是否已经建立信息安全管理流程，对安全事件、安全监控、防病毒、补丁管理、账号口令、备份恢复、远程接入、安全审计、物理访问、系统退役等日常安全工作进行优化以提高管理效率；调阅信息安全管理相关流程文档，分析流程设计的完备性与适宜性；选择一个或几个安全管理流程进行穿行测试，了解安全流程的执行情况。

（3）访谈信息安全运行管理员工，并调阅安全运行管理的工作计划、管理流程、分析报告、事件处置报告等工作记录，了解安全日志、安全情报和网络信息的收集过程、分析方法及安全知识库的形成过程，判断是否可以通过安全数据的分析，实现对组织安全态势的感知、预测与预警。

（4）分析信息安全管理相关流程的指标体系，判断其岗位职责的对应程度；抽样调查信息安全流程指标是否得到及时有效的测量；抽样调查信息安全流程运行绩效数据是否被纳入员工绩效考核体系。

# 第四章　信息系统应用控制审计

应用控制是信息系统为适应各种数据处理的特殊控制要求，保证数据处理的可靠性而建立的内部控制。因此，应用控制的目标是保证信息系统输入、处理和输出数据和记录的完整性和准确性。

应用控制涉及到各种类型的业务，每种业务及其数据处理有其特殊流程的要求，这就决定了具体的应用控制的设计需结合具体的业务，但一般都包括了业务流程控制、数据应用控制，以及信息共享和业务协同控制三方面的内容。

## 第一节　核心业务流程控制审计

### 一、业务流程设计审计

#### （一）业务概述

业务流程设计，是指组织对其业务流程进行规划与设计，并确保所设计的流程能满足其业务活动需要;而且根据业务需求对业务流程进行了整合、还原或再造，避免重复操作；同时确保关键环节、关键节点和关键岗位落实了授权审批、访问控制及不相容职责分离等必要的安全控制措施。

#### （二）审计目标和内容

从有效性和合规性两方面，检查组织是否对业务流程进行梳理、合理规划和设计，从而防范业务流程的操作风险，为实现职责分离提供保证并在业务流程中得以体现，以及系统流程与实际业务需求相吻合，在满足业务处理要求的同时，符合合规监管要求。

（三）常见问题和风险

1. 核心业务系统的业务流程设计没有满足组织的需求。

2. 组织信息系统业务流程缺乏或规划不合理，导致重复建设或组织的经营管理效率低下。

（四）审计的主要方法和程序

1. 审阅用户需求文档和系统各业务流程的设计文档，检查系统流程的设计是否与组织实际业务需求相吻合。

2. 访谈安全主管和业务部门主管，了解用户权限授权审批管理制度及流程、业务处理关键流程和关键岗位职责要求。

3. 检查岗位职责是否符合“职责分离”原则从而建立不相容的职责分离矩阵，并从关键系统中导出权限数据与职责矩阵对照，查验用户权限设置的一致性。

4. 调阅用户权限申请表，核查用户权限审批制度是否按照相应的制度规范严格执行，权限申请是否基于用户工作岗位和职责并得到业务部门和信息系统部门主管审批。

5. 运行系统权限报表或执行相关数据库语句从权限表中直接取出权限数据，基于关键系统权限和导出的权限数据，检查用户权限设置的合理性。

## 二、业务流程处理审计

### （一）业务概述

业务流程处理，是指组织系统为确保业务处理的正确性和控制的有效性，在各流程节点的操作上落实组织对业务活动审批及处理的过程要求，并设置相同业务处理自动批量操作，对重要业务流程处理实施有效性控制和完整性校验，同时确保系统接口处理正确、控制有效。

### （二）审计目标和内容

从有效性和完整性两方面，检查组织的主要业务流程可通过信息系统实现。

### （三）常见问题和风险

1. 未统筹兼顾业务风险和信息科技风险，从而在业务信息系统的流程处理控制中未做风险控制的考虑。

2. 业务流程中关键环节的相关控制点没有得到有效执行。

3. 业务系统的接口不符合相关规范的要求，存在接口标准不统一、安全控制不到位的风险。

4. 业务处理流程过程中的接口访问权限没有得到有效管理，存在数据泄露及被滥用的风险。

（四）审计的主要方法和程序

1. 调阅系统业务流程设计文档，检查是否为业务流程风险提供合理人工或自动化控制措施。

2. 现场观察业务流程关键环节的系统操作，检查相关控制点执行的有效性。

3. 调阅系统接口规划文档，结合被审计单位具体业务分析接口规划是否符合法律法规要求，接口规划是否涵盖数据采集、转换、传输、系统容错处理和访问权限等方面的内容。

4. 综合采用接口规划文档审阅，接口程序测试以及接口数据分析等手段，检查接口数据处理是否能确保数据的完整性；查阅系统接口处理日志，分析接口容错机制的有效性。

5. 调阅接口权限分配文件，获得权限实际配置数据，检查接口用户的系统访问权限是否经过严格授权和审批，其所具有的权限是否与其工作职责相匹配。

## 三、业务流程功能审计

### （一）业务概述

业务流程功能，是指组织为满足业务的需要，通过应用系统的功能设计实现业务流程中的要求，比如利息计算、成本核算等。

### （二）审计目标和内容

从有效性和合规性两方面，检查组织的业务流程细化后各功能点是否完备有效，各功能模块是否实现业务流程的子目标，各功能点之间的连续性，对业务处理衔接的通畅性，以及业务流程中各功能的实现过程是否符合国家及行业基本监管规范要求。

（三）常见问题和风险

1. 信息系统业务流程功能对系统的性能和容量有一定要求时，因缺乏有效、及时的监控，导致信息系统运行效率低下，甚至出现安全事故使信息系统不能正常运行，从而无法满足业务需求。

2. 当发生信息系统的业务控制缺失，人工控制或补偿控制失效所进行的补丁安装或版本升级，容易促使发生部署问题或版本错误；

3. 未经试运行就部署上线，促使发生重大变更风险。

（四）审计的主要方法和程序

1. 梳理被审计单位的关键业务需求，评估被审计单位关键业务需求对信息系统的依赖程度，评价是否存在信息系统应实现而未实现的功能。

2. 访谈系统关键用户，设计用户满意度调查问卷，评估分析系统业务功能的完备性。

3. 调阅问题管理、故障管理流程管理制度，问题处理、故障处理记录单，评价系统用户服务的及时性。

4. 调查系统常见问题和故障发生的频率和性质，分析反映出的系统功能薄弱环节。

## 第二节　应用系统输入控制审计

### 一、数据录入和导入控制审计

#### （一）业务概述

数据录入和导入控制，是指为确保信息系统的数据录入、导入等数据采集功能符合国家、行业或者组织规范标准，数据采集者的身份与权限合理有效所采取的一系列控制措施。

#### （二）审计目标和内容

从合规性、安全性、完整性和准确性方面，检查：

1. 系统的数据录入、导入接口是否符合国家、行业或组织自身规范，是否制定数据录入、导入的制度规范；是否在系统中建立用户账号和权限管理机制，并根据设定的权限使用数据录入、导入功能，以及监督操作的规范性。

2. 系统是否存在未经许可的数据录入、导入接口，以及是否能阻止非授权用户的数据录入和导入操作，同时具备日志记录功能。

3. 系统是否具备数据准确性检查功能。

（三）常见问题和风险

1. 数据录入、导入的系统账号与权限管理机制不存在或不健全。

2. 系统功能不完善，无法记录用户的数据录入、导入操作，或日志功能未开启，造成记录信息缺失。

3. 系统的数据录入、导入接口不符合国家、行业或组织规范标准，或存在未经许可的数据录入、导入接口。

4. 数据录入、导入结果不准确、不完整，或错误的数据被录入、导入到系统中。

5. 导入的数据文件格式不符合要求或数据类型不符合规范标准。

（四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据录入和导入的岗位及其职责与权限；检查系统的访问控制列表，了解系统对数据录入和导入功能权限的设定与规定是否相符；对比国家、行业或者单位规范，检查组织设置的数据录入、导入接口是否符合国家、行业或者单位规范。

2. 设定不同权限的测试用户，对系统进行穿行测试，检查系统是否严格限定只有满足权限要求的用户使用数据录入和导入功能；检查系统日志是否按照规定记录了用户的数据录入和导入的操作；

3. 检查系统是否提供了输入值约束功能，以保证输入数据的准确性。

## 二、数据修改和删除控制审计

### （一）业务概述

数据修改和删除控制，是指对系统中的数据修改和删除功能通过授权管理、限制操作等手段，确保其符合国家、行业或组织的相关安全规范，同时，确保数据修改或删除功能符合组织自身的业务管理需要。

### （二）审计目标和内容

该项的审计目标是从合规性、安全性和完整准确性角度，分别检查：

1. 系统的数据修改、删除是否符合国家、行业或组织自身规范，是否制定数据修改、删除的制度规范；是否在系统中建立用户账号和权限管理机制，并在用户使用系统时，根据设定的权限使用数据修改、删除功能，以及监督操作的规范性。

2. 系统是否存在未经许可的数据修改、删除功能，以及是否能阻止非授权用户的数据修改、删除操作，同时具备日志记录功能。

3. 系统是否具备数据准确性检查功能。

### （三）常见问题和风险

1. 数据修改、删除的系统账号与权限管理机制不存在或不健全，缺乏有效的约束机制。

2. 系统功能不完善，无法记录用户的数据修改、删除操作，或日志功能未开启，造成记录信息缺失。

3. 系统的数据修改、删除功能不符合国家、行业或组织规范标准，或存在未经许可的数据修改、删除功能。

4. 数据修改、删除结果不完整、不准确，或错误的数据被修改、删除，造成数据不一致。

（四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据修改和删除的岗位及其职责与权限；检查系统的访问控制列表，了解系统对数据修改和删除功能权限的设定与规定是否相符；对比国家、行业或者单位规范，检查被审计单位设置的数据修改和删除功能是否符合国家、行业或者单位规范。

2. 设定不同权限的测试用户，对系统进行穿行测试，检查系统是否严格限定只有满足权限要求的用户使用数据修改和删除功能；检查系统日志是否按照规定记录了用户的数据修改和删除的操作；检查系统是否存在未经许可的数据修改和删除功能。

3. 设定不同权限的测试用户，对系统进行穿行测试，检查系统是否能够保证数据修改和删除的准确性，是否所有需要修

改或删除的数据都能被正确地修改或删除；抽取一部分已处理过的业务进行核对，以证实数据修改或删除的完整有效性。

## 三、数据校验控制审计

### （一）业务概述

数据校验控制，是对系统的数据录入、导入接口等数据采集功能进行校验控制，确保其符合国家、行业或组织自身的规定，并且确保系统中校验控制措施的有效性。

### （二）审计目标和内容

从合规性和有效性方面，检查：

1. 信息系统的数据录入、导入接口是否设置了数据校验控制，数据校验控制是否符合国家、行业或者单位规范。

2. 信息系统数据录入、导入接口的数据校验功能是否能够满足数据校验的要求，数据校验控制是否有效。

### （三）常见问题和风险

1. 信息系统功能不完善，数据录入、导入接口未设置数据校验控制，或设置的数据校验控制失效。

2. 信息系统的数据校验功能不符合国家、行业或组织自身的规范标准。

### （四）审计的主要方法和程序

1. 审阅信息系统开发文档，检查信息系统是否设置了数据录入、导入接口的数据校验功能。

2. 对比国家、行业或者单位规范，检查组织设置的数据校验控制是否符合国家、行业或者单位规范。

3. 访谈开发人员，了解数据录入、导入接口的数据校验控制的需求定义及算法实现，判断其有效性和完备性。

## 四、数据入库控制审计

### （一）业务概述

数据入库控制，是指录入、导入接口等采集的数据、缓冲区数据与进入数据库的最终数据保持一致的相关控制。

### （二）审计目标和内容

从合规性和有效性方面，检查：

1. 组织是否制定数据管理规范，规定数据入库的工作流程和岗位职责，以及数据入库工作是否严格按照规范和制度执行。

2. 信息系统功能是否存在数据入库控制，系统的数据入库控制是否有效。

### （三）常见问题和风险

1. 未制定数据管理规范、数据入库的工作流程和岗位职责，或虽然制定但没严格按照制度执行。

2. 组织信息系统的数据入库控制功能缺失。

3. 数据入库不完整，采集数据、缓冲区数据的最终数据库数据出现不一致情况。

### （四）审计的主要方法和程序

1. 审阅信息系统开发文档、组织结构文件、岗位职责与流程和用户授权文档，检查信息系统是否设置了数据入库控制功能，了解数据入库的岗位及其职责与权限。

2. 访谈管理人员，了解被审计单位是否存在数据入库工作的制度规范的认知和执行。

3. 访谈数据库管理员和应用系统开发人员，了解数据入库控制的需求定义及算法实现，判断其有效性和完备性。

4. 检查系统的访问控制列表，了解系统对数据入库功能权限的设定与规定是否相符。

5. 设定不同权限的测试用户，对系统进行穿行测试，检查系统中的数据入库控制是否有效。

## 五、数据共享与交换控制审计

### （一）业务概述

数据共享与交换控制，是指不同信息系统之间的信息共享与交换需要符合国家、行业及组织的相关质量与安全要求，要确保用户或系统的数据共享与交换的系统账号与权限控制合理，数据共享与交换方法和渠道安全可控。

### （二）审计目标和内容

从合规性、安全性和完整准确性这三方面，检查：

1. 组织是否在信息系统中建立用户账号与权限管理机制，制定控制数据共享与交换的制度规范；用户在使用系统时，是否按照制度规范操作。

2. 系统能否发现并阻止非授权用户使用数据共享功能；是否有日志记录；对传输的信息是否加密；对于敏感数据的共享与交换操作，是否除了信息系统记录日志以外，还有数据控制责任人的监督和确认。

3. 系统是否能够保证共享与交换数据的完整性和准确性。

（三）常见问题和风险

1. 数据共享与交换功能的系统账号与权限管理机制不存在或不健全，未根据用户需要约束其使用数据共享与交换功能，或虽然建立了权限控制但未建立相关约束用户数据共享与交换操作的制度规范。

2. 系统功能不完善，造成无法记录用户数据共享与交换操作，或虽有日志功能但未正式使用，造成数据共享与交换操作的相关信息缺失，导致无据可查。

3. 未建立数据共享与交换的加密传输机制，或共享与交换后无法确认数据是否被指定用户使用从而无法确认是否被非法用户获取，最终无法保障数据的安全性。

4. 敏感数据的共享与交换失控，相关人员的许可和监督缺失。

5. 共享与交换的数据不完整或不准确。

### （四）审计的主要方法和程序

1. 审阅组织结构文件、岗位职责与流程和用户授权文档，确认涉及数据共享与交换的岗位及其职责与权限；观察关键岗位员工操作，考察其是否按照数据共享与交换的相关制度规定完成操作；检查系统的访问控制列表，了解系统对数据共享与交换功能权限的设定与规定是否相符。

2. 设定不同权限的测试用户，对系统进行穿行测试，测试系统是否严格限定只有满足权限要求的用户才能使用数据共享与交换功能；检查系统日志是否按照规定记录了用户对数据信息进行共享与交换的操作；检查信息系统是否对传输的信息加密以保证共享与交换数据的传输安全；抽取敏感数据的共享与交换记录进行分析核对，确定是否存在数据控制责任人的监督和确认。

3. 设定不同权限的测试用户，对系统进行穿行测试，测试系统数据的共享与交换结果是否完整准确。

## 六、备份与恢复数据接收控制审计

### （一）业务概述

备份与恢复数据接收控制，是指对备份与恢复中的数据接收进行身份与权限控制,确保接收数据与输出数据保持一致。

### （二）审计目标和内容

从合规性、安全性和准确性方面，检查：

1. 组织是否在信息系统中建立了用户身份与权限体系，是否制定了控制数据备份与恢复数据接收的制度规范；用户在使用系统时，是否按照制度规范操作。

2. 系统能否发现并阻止非授权用户使用数据备份与恢复数据接收功能；是否有日志记录；接收数据备份时对数据备份包的有效性是否进行了测试。

3. 系统是否能够保证用户通过数据备份与恢复数据接收功能接收的数据的完整、准确、可用。

（三）常见问题和风险

1. 数据备份与恢复数据接收的系统账号与权限管理机制不存在或不健全，未根据用户需要约束其使用数据备份与恢复数据接收功能，或虽然建立了权限控制但未建立相关约束用户数据备份与恢复数据接收操作的制度规范。

2. 系统功能不完善，造成无法记录用户数据备份与恢复数据接收操作，或虽有日志功能但未正式使用，造成数据备份与恢复数据接收操作的相关信息缺失，导致无据可查。

3. 备份与恢复接收数据的安全性无法得到保障，备份数据未进行恢复测试，无法确认数据包是否安全、完整、可用。

（四）审计的主要方法和程序

1. 审阅组织结构文件、岗位职责与流程和用户授权文档，确认涉及数据备份与恢复数据接收的岗位及其职责与权限；观察关键岗位员工操作，考察其是否按照数据备份与恢复数据接收的相关制度规定完成操作；检查系统的访问控制列表，了解系统对数据备份与恢复数据接收功能权限的设定与规定是否相符。

2. 设定不同权限的测试用户，对系统进行穿行测试，测试系统是否严格限定只有满足权限要求的用户才能使用数据备份与恢复数据接收功能；检查系统日志是否按照规定记录了用户对数据信息进行备份与恢复数据接收的操作；抽取部分日志进行分析，判断是否符合相关规定；检查接收备份数据时是否对备份数据包进行恢复测试以保证备份数据的安全性。

3. 设定满足权限的测试用户，测试系统提供的数据备份包是否可恢复，数据是否完整、准确、可用。

## 第三节　应用系统处理控制审计

### 一、数据转换控制审计

#### （一）业务概述

数据转换控制，是指对系统采集外部数据和转换过程中的各项操作进行安全控制，使其符合国家、行业或组织的数据转换标准、格式规范及安全保护等方面的要求。

（二）审计目标和内容

从合规性和完整准确性两方面，检查：

1. 信息系统的数据转换功能是否符合国家、行业或者单位的数据转换标准和格式规范。

2. 数据转换是否按照预定的业务逻辑进行，数据转换后结果是否完整、是否准确，异常值是否已进行了处理。

（三）常见问题和风险

1. 数据转换的身份与权限控制不存在或不健全，未根据用户需要约束其使用数据转换功能，或虽然建立了权限控制但未建立相关约束用户数据转换操作的制度规范。

2. 系统功能不完善，造成无法记录用户数据转换操作，或虽有日志功能但未正式使用，造成数据转换操作的相关信息缺失，导致无据可查。

3. 系统的数据转换功能不符合国家、行业、组织规范，或存在未经许可的数据转换接口。

4. 数据转换结果不准确、不完整，或错误的数据被转换进入信息系统。

5. 转换的数据文件格式不符合规范要求。

（四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据转换的岗位及其职责与权限；审阅信息系统的开发文档，

了解被审计单位信息系统的数据转换功能的需求、设计实现情况，判断是否符合国家、行业或者单位规范。

2. 设定不同权限的测试用户，对系统进行穿行测试，检查系统是否严格限定只有满足权限要求的用户使用数据转换功能；检查系统日志是否按照规定记录了用户的数据转换操作；设定模拟转换数据，检查转换后的数据的完整准确性；抽取一部分已处理过的业务进行核对，以证实数据转换的完整准确性。

## 二、数据整理控制审计

### （一）业务概述

数据整理控制，是指采集数据的分类入库、数据库中相关数据的清洗、数据库间和数据表间的数据抽取与合并、数据库或者数据表的生成与报废等功能的控制要符合系统需求和设计要求。

### （二）审计目标和内容

从合规性和完整准确性两方面，检查：

1. 数据整理功能是否符合系统需求和设计需求。

2. 数据整理的结果是否完整，是否准确。

### （三）常见问题和风险

1. 数据整理的身份与权限控制不存在或不健全，未根据用户需要约束其使用数据整理功能，或虽然建立了权限控制但未建立相关约束用户数据整理操作的制度规范。

2. 系统功能不完善，造成无法记录用户数据整理操作，或虽有日志功能但未正式使用，造成数据整理操作的相关信息缺失，导致无据可查。

3. 系统的数据整理功能与信息系统设计不符，不符合系统需求和设计需求。

4. 数据整理结果不准确，不符合业务逻辑或数据整理结果不完整，缺失实际业务数据。

### （四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据整理的岗位及其职责与权限；审阅信息系统的开发文档，了解被审计单位信息系统的数据整理功能的需求、设计实现情况；对系统进行穿行测试，检查系统是否严格限定只有满足权限要求的用户使用数据整理功能。

2. 设定不同权限的测试用户，对系统进行穿行测试，完成数据整理流程，检查结果是否符合业务逻辑、是否符合预定的数据整理逻辑；抽取一部分已处理过的真实业务进行核对，以证实数据整理的完整性、准确性。

## 三、数据计算控制审计

### （一）业务概述

数据计算控制，是指系统中经济业务活动的计量、计费、核算、分析以及数据平衡等计算功能的控制要符合国家、行业或组织的相关规定与规范。

**（二）审计目标和内容**

从合规性和有效性两方面，检查：

1. 信息系统的数据计算控制是否符合国家、行业或者单位相关规定和规范。

2. 数据计算控制是否能够按照预计条件完成数据计算过程中的正确控制。

**（三）常见问题和风险**

1. 信息系统的数据计算控制不符合国家、行业、组织规范。

2. 信息系统存在未经许可的数据计算功能。

3. 存在数据计算控制失效的情况。

**（四）审计的主要方法和程序**

1. 审阅组织的信息系统开发文档，了解业务系统的数据计算需求与设计情况；访谈管理人员，了解关键的数据计算流程；确定信息系统中关键的数据计算控制点和控制逻辑；对比国家、行业或者单位规范，检查关键数据计算控制点和控制逻辑是否符合国家、行业或者单位规范。

2. 设定不同权限的测试用户，对系统进行穿行测试，检查系统中的关键数据计算控制点和控制逻辑的有效性；检查系统

是否存在未经许可的数据计算功能；抽取一部分已处理过的真实业务进行核对，以证实数据计算控制的有效性。

## 四、数据汇总控制审计

### （一）业务概述

数据汇总控制，是指检查系统中经济业务活动的财务科目汇总、报表汇总和相关业务汇总等功能实现的控制要符合国家、行业或者组织的相关规定和规范。

### （二）审计目标和内容

从合规性和准确性两方面，检查：

1. 信息系统的数据汇总功能的汇总逻辑、计算方法、计算过程、计算口径等是否符合国家、行业或者单位的相关规定和规范。

2. 信息系统的数据在通过正确的汇总过程后，是否正确，是否能够真实反映实际的业务情况。

### （三）常见问题和风险

1. 系统的数据汇总功能不符合国家、行业或组织的规范。

2. 系统功能不完善，造成无法记录用户数据汇总操作，或虽有日志功能但未正常使用，造成数据汇总操作的相关信息缺失，导致无据可查。

3. 数据汇总结果不准确。

### （四）审计的主要方法和程序

1. 审阅信息系统的开发文档，了解组织信息系统的数据汇总功能的需求、设计实现情况；对比国家、行业或者单位规范，检查系统设置的数据汇总功能是否符合国家、行业或者单位规范；访谈管理人员，了解组织数据汇总的工作流程。

2. 设定不同权限的测试用户，对系统进行穿行测试，检查系统是否严格限定只有满足权限要求的用户使用数据汇总功能；检查系统日志是否按照规定记录了用户的数据汇总操作；抽取部分日志进行分析，判断是否符合相关规定；设定模拟汇总数据，检查汇总后的数据的准确性；抽取一部分已处理过的业务进行核对，以证实数据汇总的准确性。

## 第四节　应用系统输出控制审计

### 一、数据外设输出控制审计

#### （一）业务概述

数据外设输出控制，是指计算机显示、打印和介质拷贝等数据输出功能的身份与权限控制要符合标准规范及组织自身业务的相关要求。

#### （二）审计目标和内容

从合规性和安全性两方面，检查：

1. 组织是否在信息系统中建立了用户身份与权限体系，是否制定了控制数据外设输出的制度规范；用户在使用系统时，是否按照制度规范操作。

2. 系统能否发现并阻止非授权用户使用数据信息的计算机显示、打印、介质拷贝等外设输出功能；是否有日志记录；对于敏感数据的查看、打印和介质存储操作，是否有日志记录，并有数据控制责任人的监督、签字。

（三）常见问题和风险

1. 数据外设输出的身份与权限控制不存在或不健全，未根据用户需要约束其使用数据信息的计算机显示、打印、介质拷贝等外设输出功能，或虽然建立了权限控制但未建立相关约束用户数据外设输出操作的制度规范。

2. 系统功能不完善，造成无法记录用户数据外设输出操作，或虽有日志功能但未正式使用，造成数据外设输出操作的相关信息缺失，导致无据可查。

3. 敏感数据的外设输出失控，缺失相关人员的许可与监督。

（四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据外设输出的岗位及其职责与权限；访谈关键岗位员工，是否按照数据外设输出的相关制度规定完成操作；检查系统的

访问控制列表，了解系统对数据信息的计算机显示、打印、介质拷贝等外设输出功能权限的设定与规定是否相符。

2. 设定不同权限的测试用户，对系统进行穿行测试，是否严格限定只有满足权限要求的用户使用数据信息的计算机显示、打印、介质拷贝等外设输出功能；检查系统日志是否按照规定记录了用户对数据信息进行计算机显示、打印、介质拷贝等外设输出的操作；抽取敏感数据的外设输出记录进行分析核对，确定是否存在数据控制责任人的监督、签字。

## 二、数据检索输出控制审计

### （一）业务概述

数据检索输出控制，是指利用单项检索、组合检索等检索工具对系统中部分数据或者全部数据的检索输出功能的身份与权限控制要符合标准规范及组织自身业务的相关要求。

### （二）审计目标和内容

从合规性、安全性和准确性三方面，检查：

1. 组织是否在信息系统中建立了用户身份与权限体系，是否制定了控制数据检索输出的制度规范；用户在使用系统时，是否按照制度规范操作。

2. 系统能否发现并阻止非授权用户使用数据检索输出功能；是否有日志记录；对于敏感的数据的检索操作，是否有日志记录，并有数据控制责任人的监督、签字。

3. 系统是否能够保证用户通过数据检索功能获取并输出的数据的准确性。

（三）常见问题和风险

1. 数据检索的身份与权限控制不存在或不健全，未根据用户需要约束其使用数据检索功能，或虽然建立了权限控制但未建立相关约束用户数据检索操作的制度规范。

2. 系统功能不完善，造成无法记录用户数据检索输出操作，或虽有日志功能但未正式使用，造成数据检索输出操作的相关信息缺失，导致无据可查。

3. 敏感数据的检索输出失控，缺失相关人员的许可与监督。

4. 检索输出结果不准确。

（四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据检索输出的岗位及其职责与权限，检查系统的访问控制列表，了解系统对数据检索输出功能权限的设定与规定是否相符。

2. 设定不同权限的测试用户，对系统进行穿行测试，测试系统是否严格限定只有满足权限要求的用户才能使用数据检索输出功能；对数据信息进行检索输出的操作是否有日志记录；抽取敏感数据的检索输出记录进行分析核对，确定是否存在数据控制责任人的监督、签字。

3. 测试系统提供的数据检索输出的数据结果是否完整准确。

## 三、数据共享输出控制审计

### （一）业务概述

数据共享输出控制，是指系统内部相关子系统之间、系统与外部系统之间通过信息交换或信息共享方式数据输出功能的身份与权限控制要符合标准规范及组织自身业务的相关要求。

### （二）审计目标和内容

从合规性、安全性和准确性三方面，检查：

1. 组织是否在信息系统中建立了用户身份与权限体系，是否制定了控制数据共享输出的制度规范；用户在使用系统时，是否按照制度规范操作；系统是否严格限定只有满足权限要求的用户才能使用数据共享输出功能。

2. 系统能否发现并阻止非授权用户使用数据共享输出功能；是否有日志记录；对传输的信息是否加密；对于敏感的数据的共享操作，是否除了信息系统记录日志以外，还有数据控制责任人的监督、签字。

3. 系统是否能够保证用户通过数据共享输出功能输出的数据的准确性。

### （三）常见问题和风险

1. 数据共享输出的身份与权限控制不存在或不健全，未根据用户需要约束其使用数据共享输出功能，或虽然建立了权限控制但未建立相关约束用户数据共享输出的制度规范。

2. 系统功能不完善，造成无法记录用户数据共享输出操作，或虽有日志功能但未正式使用，造成数据共享输出操作的相关信息缺失，导致无据可查。

3. 因未建立加密传输机制，或共享后无法确认是否被指定用户使用无法确认是否存在非法用户获取共享数据，从而共享数据的安全性无法得到保障。

4. 敏感数据的共享输出失控，相关人员的许可与监督缺失。

5. 共享输出结果不完整或不准确。

（四）审计的主要方法和程序

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据共享输出的岗位及其职责与权限；检查系统的访问控制列表，了解系统对数据共享输出功能权限的设定与规定是否相符。

2. 设定不同权限的测试用户，对系统进行穿行测试，测试系统是否严格限定只有满足权限要求的用户才能使用数据共享输出功能；检查系统日志是否按照规定记录了用户对数据信息进行共享输出的操作；检查信息系统是否对传输的信息是否加

密以保证共享数据的传输安全；抽取敏感数据的共享输出记录进行分析核对，确定是否存在数据控制责任人的监督、签字。

3. 测试系统提供的数据共享输出的数据结果是否完整准确。

## 四、备份与恢复输出控制审计

### （一）业务概述

备份与恢复输出控制，是指生产系统向备份系统、备份系统向恢复系统数据输出的身份与权限控制要确保合理、有效，并符合标准规范及组织自身业务的相关要求。

### （二）审计目标和内容

从合规性、安全性和准确性三方面，检查：

1. 组织是否在信息系统中建立了用户身份与权限体系，是否制定了控制数据备份与恢复输出的制度规范；用户在使用系统时，是否按照制度规范操作。

2. 系统能否发现并阻止非授权用户使用数据备份与恢复输出功能；是否有日志记录；对数据备份包的有效性是否进行了测试。

3. 系统是否能够保证用户通过数据备份与恢复输出功能输出的数据的完整、准确、可用。

### （三）常见问题和风险

1. 数据备份和恢复的身份与权限控制不存在或不健全，未根据用户需要约束其使用数据备份和恢复功能，或虽然建立了权限控制但未建立相关约束用户数据备份和恢复的制度规范。

2. 系统功能不完善，造成无法记录用户数据备份和恢复操作，或虽有日志功能但未正式使用，造成数据备份和恢复操作的相关信息缺失，导致无据可查。

3. 因未建立加密传输机制，或共享后无法确认是否被指定用户使用无法确认是否存在非法用户获取共享数据，从而共享数据的安全性得不到保障。

4. 因备份数据未进行恢复测试，无法确认备份数据是否安全、完整、可用从而导致数据备份和恢复的安全无法得到保障。

**（四）审计的主要方法和程序**

1. 审阅组织制度流程、岗位职责和用户授权文档，确认涉及数据备份与恢复输出的岗位及其职责与权限；检查系统的访问控制列表，了解系统对数据备份与恢复输出功能权限的设定与规定是否相符。

2. 设定不同权限的测试用户，对系统进行穿行测试，测试系统是否严格限定只有满足权限要求的用户才能使用数据备份与恢复输出功能；检查系统日志是否按照规定记录了用户对数据信息进行备份与恢复输出的操作；检查是否对备份数据包进行恢复测试以保证备份数据的安全性。

3. 设定满足权限的测试用户，测试系统提供的数据备份包是否可恢复，数据是否完整、准确、可用。

## 第五节　信息共享与业务协同审计

### 一、信息资源目录体系测评审计

#### （一）业务概述

信息资源目录体系，是指组织以其统一的电子网络为基础，通过构建覆盖多级信息资源目录体系技术总体架构，采用元数据对共享信息资源特征进行描述形成统一规范的目录内容，最终提供信息资源的发现定位服务，支持大范围内跨部门、跨地区的普遍信息共享。

#### （二）审计目标和内容

检查组织的信息资源目录体系是否符合国家或行业的相关规范，是否较好地满足各类业务和管理需要。

#### （三）常见问题和风险

1. 信息规划、部署过程中未设置信息资源目录体系。

2. 目录体系设计缺乏整体性，未覆盖组织的主要信息系统。

3. 目录体系的要素设计不全。

4. 由于信息化建设缺乏长远和统筹规划，造成不同系统间形成彼此隔离的信息孤岛问题。

#### （四）审计的主要方法和程序

1. 就组织目录体系的建立，检查在其信息系统构建过程中，是否进行了相应的规划以及实施，要求利用目录技术和元数据技术，以及其他网络技术，构造统一的信息资源目录管理系统。

2. 就信息资源目录体系的规范性，检查其是否符合国家及行业规范标准的要求，是否符合本单位信息系统规划的要求。

3. 信息资源目录体系技术构架是否包括信息库系统和目录服务系统；信息库系统是否包括了应用目录信息库、专业目录信息库、共享目录信息库、共享信息库、交换目录信息库、交换信息库；目录服务系统是否包括了目录编制系统、目录注册系统、应用目录系统、共享目录系统、交换目录系统、交换桥接系统。

## 二、信息资源交换体系测评审计

### （一）业务概述

信息资源交换体系，是指按照统一的标准和规范，为支持跨部门、地域间、层级间信息共享以及协同而建设的信息服务体系。

### （二）审计目标和内容

检查信息资源交换体系是否符合国家或行业的相关规范，是否较好地满足信息交换的需要。

### （三）常见问题和风险

1. 信息化规划、部署过程中未设置信息资源交换体系。

2. 交换体系设计与目录体系缺乏一致性，未能充分运用和体现目录体系的构建结果。

3. 交换体系设计缺乏整体性，未能覆盖组织的主要业务信息系统。

4. 交换体系的要素设计不全。

### （四）审计的主要方法和程序

1. 检查在其信息系统构建过程中，是否进行了相应的规划，是否建立信息资源交换体系。

2. 就信息资源交换体系的规范性，检查交换体系的技术架构是否与目录体系一致；对于组织的信息资源交换体系，检查其是否符合国家及行业规范标准的要求，是否符合本单位信息系统规划的要求。

3. 评价信息资源交换体系的实施效果，交换体系技术构架是否包括信息资源的业务应用、信息共享、信息交换三部分内容及相应实现方式；信息共享技术架构、信息交换技术构架是否包括了信息库系统和共享服务系统。

## 三、元数据和主数据测评审计

### （一）业务概述

元数据是关于数据的数据，其用于描述信息数据集的内容、质量、表示方式、管理方式以及数据集的其他特征，是实现数据集共享的核心内容之一。

### （二）审计目标和内容

检查组织系统中的元数据和主数据是否符合国家、行业或者组织的相关规范，是否较好地满足信息系统建设、应用和共享的需要。

### （三）常见问题和风险

接受审计的组织未开展元数据标准化工作，系统间的数据无法共享和交换。

### （四）审计的主要方法和程序

1. 检查组织在其信息系统构建过程中，是否按照国家及行业相关规范对元数据进行了规划，是否包含必选的元数据实体和元数据元素。

2. 检查组织各部门提供的元数据是否符合标准要求；是否按照标准建立核心元数据库，进行管理和发布。

3. 检查组织是否按标准要求扩展核心元数据，并形成元数据扩展文档。

## 四、数据元素和数据库表测评审计

### （一）业务概述

数据元素是数据的基本单位；数据库表则是数据元素的集合，其包含结构化数据和非结构化数据。因此，在组织的信息系统中，只有数据元素和数据库表遵循统一的规划进行规划、设计、运行，才能实现信息的交换和共享。

（二）审计目标和内容

检查数据元素和数据库表是否符合行业或组织的相关规范，是否较好地满足信息系统建设、应用和共享的需要。

（三）常见问题和风险

1. 数据元素和数据库表的规划与交换体系、目录体系缺乏一致性，未能充分运用和体现目录体系、交换体系的构建结果。

2. 各信息系统的数据元素和数据库表规划不统一，不具备共享和交换基础。

3. 数据元素和数据库表的要素设计缺乏全面性。

（四）审计的主要方法和程序

1. 确认组织在其信息系统构建过程中，是否按统一标准对数据元素和数据库表进行了规划，并遵循规划实施。

2. 就数据元素和数据库表的一致性，检查组织对数据元素和数据库表的规划，是否符合目录体系和交换体系的要求；及其各系统中数据元素的编码规划、表示方法是否一致。

3. 就数据元素和数据库表的规范性，检查数据元素的标识符、数据元素的名称、数据元素的说明、数据元素的表示、数据元素的英文名称、数据元素的短名、数据元素的注释等要素是否齐全，是否符合国家统一规范；数据库表中是否包含了资源名称、资源摘要、资源负责方、资源分类、资源标识符和数据项说明 6 个必选的实体和元素。

## 五、内部数据和外部数据测评审计

### （一）业务概述

内部数据是组织信息系统运行时产生的包括预算管理、会计核算和相关业务的数据，主要反映组织运行和管理情况。外部数据则是组织为履行其职能或实现经济业务活动而从其他单位获取的数据。该测评指标是基于信息共享和交换的需要而设计，更多地从内外部数据获取方式、相互间是否可印证等方面来确认数据的质量。

### （二）审计目标和内容

从完整性、真实性和正确性三方面：

1. 检查获取的内部数据是否涵盖了被审计单位预算管理、会计核算和相关业务的主要方面；获取的外部数据，是否包括了被审计单位履行职能或者实现经济业务活动需要的主要数据。

2. 在信息系统业务流程控制审计，数据输入、处理和输出控制审计中，通过相应的审计程序和方法，已可基本确认被审计单位内部数据的真实性。在内部数据和外部数据测评中，是通过内部、外部数据的相互印证，以进一步确定数据的真实性。

3. 通过内、外部数据的比对，确认数据之间不存在重大不相符或歧义现象。

### （三）常见问题和风险

1. 外部数据的获取渠道和方式存在问题，与内部数据出现重大分歧和不一致。

2. 通过外部数据验证，发现内部数据的完整性、正确性和真实性存在问题。

3. 通过内部数据的验证，发现外部数据的可信度和准确度较低。

### （四）审计的主要方法和程序

1. 就内、外部数据的完整性，检查组织的内部数据是否涵盖了被审计单位预算管理、会计核算和相关业务的主要方面；组织履行职能或者实现经济业务活动是否需要外部数据，是否以恰当的技术手段获取。

2. 就内、外部数据的真实性，检查内部数据是否经过了业务流程控制审计，数据输入、处理和输出控制审计等程序，是否能确认数据的真实性；外部数据的提供部门是否值得信赖；外部数据获取的技术方法是否恰当。

3. 就内、外部数据的正确性，检查内、外部数据是否相互可验证；抽查内、外部数据，相互验证结果如何；内、外部数据之间是否有重大不一致。

## 六、信息资源标准化测评审计

### （一）业务概述

信息资源标准化是组织实现信息共享和交换的前提。组织各下属单位、各部门的信息系统只有按统一的标准建设和运行，才能实现共享与交换。因此，该指标用于测评被审单位信息资源的标准化程度。

### （二）审计目标和内容

检查信息系统是否建立了满足信息共享和业务协同的信息资源标准和规范，是否执行了国家或者行业的标准化要求，是否为推进经济业务活动的共享协同提供了有效支撑。

### （三）常见问题和风险

1. 组织未开展信息资源标准化工作，各信息系统之间的数据无法实现共享和交换。

2. 被审计单位信息资源标准化工作缺乏规范性或科学性，导致信息系统之间数据共享和交换效率低下，甚至出现错误。

### （四）审计的主要方法和程序

1. 就信息资源标准化建设，检查组织是否建立了信息资源标准化规范；被审计单位在信息化工作中，是否按照相关标准化规范建设信息系统。

2. 就信息资源标准化的规范性，检查是否执行了国家或者行业的标准化要求。

3. 检查信息资源标准化的效果，计算相关应用比重。

## 七、公共基础信息建设测评审计

（一）业务概述

公共基础信息建设，是指组织履行职能或者实现经济业务活动，需要利用人口、法人、空间地理等公共基础信息。

（二）审计目标和内容

从真实性、完整性、合规性和连续性四方面，检查：

1. 公共基础信息建设项目确实存在，项目的立项申请或者备案确实发生，不存在虚假项目或者以备案名义变相审批的情况。

2. 所获取的公共基础信息是否涵盖了组织利用该信息履行职能或者实现经济业务活动需要的主要数据，是否满足组织履行职能或实现经济业务活动的特定时间段需要。

3. 公共基础信息的获取，是否来源于该信息产生或发布的合法、权威部门，是否履行了获取该信息的相关手续；获取的公共基础信息中是否含有信息产生、发布部门的敏感数据；公共基础信息的存储是否遵循了国家信息安全相关制度、标准及规范。

4. 是否建立了与信息产生或发布部门的定期获取共享信息的制度。

（三）常见问题和风险

1. 立项申请项目不符合国家和行业的相关规定与规划。

2. 公共基础信息建设获取的信息不够完整，对组织履行职能或者实现经济业务活动的支撑不够完整。

3. 项目主管部门对立项申请项目的审批或审核不符合国家相关规定和规划。

（四）审计的主要方法和程序

1. 就公共基础信息建设的真实性，检查组织的公共基础信息建设是否存在；若建设项目确实存在，项目的立项申请或者备案确实发生；若公共基础信息建设项目属于续建项目，该项目确实具有续建的必要性。

2. 就公共基础信息建设的完整性，检查获取的公共基础信息是否涵盖了组织利用该信息履行职能或者实现经济业务活动需要的主要数据；获取的公共基础信息是否满足组织履行职能或实现经济业务活动的特定需要。

3. 就公共基础信息建设的合规性，检查公共基础信息的获取是否来源于该信息产生或发布的合法、权威部门，是否履行了获取该信息的相关手续；获取的公共基础信息中是否含有信息产生、发布部门的敏感数据；公共基础信息的存储是否遵循了国家信息安全相关制度、标准及规范。

4. 就公共基础信息建设的连续性，检查组织是否建立了与信息产生或发布部门的定期获取共享信息的制度；所获取公共基础信息的实际行动是否与信息产生或发布部门定期进行。

## 八、其他共享信息建设测评审计

### （一）业务概述

组织履行职能或者实现经济业务活动，按照国家或者行业确定、或者与其他部门协定需要向其他部门提供其所需的共享信息。需要按照国家、行业或者协定的共享信息标准规范组织建设，建立共享信息的管理制度和机制，具有较为完备的信息系统实现功能，支持其他部门的信息共享与业务协同。

### （二）审计目标和内容

从真实性、完整性、合规性和连续性四方面，检查：

1. 其他共享信息建设项目确实存在，项目的立项申请或者备案确实发生，不存在虚假项目或者以备案名义变相审批的情况。

2. 提供的其他共享信息是否涵盖了其他共享信息履行职能或者实现经济业务活动需要的主要数据，是否满足其他部门履行职能或实现经济业务活动的特定需要。

3. 产生和发布是否履行了提供该信息的相关手续；提供的其他共享信息中是否含有敏感数据；存储是否遵循了国家信息安全相关制度、标准及规范。

4. 组织是否建立了与信息需求部门的定期提供共享信息的制度；提供其他共享信息的实际活动是否与信息需求部门定期进行。

（三）常见问题和风险

1. 立项申请项目不符合国家和行业的相关规定与规划。

2. 其他共享信息建设提供的信息不够完整，对信息需求单位履行职能或者实现经济业务活动的支撑不够完整。

3. 项目主管部门对立项申请项目的审批或审核不符合国家相关规定和规划。

（四）审计的主要方法和程序

1. 检查组织的其他共享信息建设是否存在；若建设项目确实存在，项目的立项申请或者备案确实发生；若其他共享信息建设项目属于续建项目，该项目确实具有续建的必要性。

2. 检查提供的其他共享信息是否涵盖了其他部门利用该信息履行职能或者实现经济业务活动需要的主要数据；提供的其他共享信息是否满足其他部门的履行职能或实现经济业务活动的特定需要。

3. 检查是否履行了提供该信息的相关手续；获取的其他共享信息中是否含有敏感数据，存储是否遵循了国家信息安全相关制度、标准及规范。

4. 检查组织是否建立了与信息需求部门的定期提供共享信息的制度；提供其他共享信息的实际行动是否与信息需求部门定期进行。

# 第五章　信息系统专项审计

## 第一节　信息科技外包审计

信息科技外包是指组织将原来由自身负责处理的某些业务活动委托给服务提供商进行持续处理的行为，包括系统研发类外包、咨询服务类外包、系统运行维护类外包及业务外包中的相关信息科技活动等内容。

服务提供商包括独立的第三方、组织母公司或其所属集团设立在中国境内外的子公司、关联公司或附属机构。非驻场外包是一种特殊形式的外包，与驻场外包一样也会导致各类风险，但具体管控环节和方式不同。

本节将从信息科技外包战略规划、信息科技外包治理、信息科技外包商管理审计、信息科技外包项目管理审计、信息科技外包人员管理审计、信息科技外包安全管理等方面对信息科技外包审计的方法与步骤进行描述。

### 一、信息科技外包战略规划审计

#### （一）业务概述

信息科技外包战略是指企业对信息科技外包的目标和策略的组合，企业信息科技外包的远景、使命、命题等的全局规划和方针及定位。

#### （二）审计目标和内容

通过对信息科技外包战略规划的审计，判断组织在外包战略规划方面：

1. 是否建立了信息科技外包战略，所建立的外包战略是否具有全局性、长远性及可操作性的特点。

2. 是否明确了外包管理基本原则，是否能确保风险、成本和效益的平衡，并考虑了减少对供应商过分依赖和掌握核心技术的相关因素。

3. 是否定期修正外包战略；外包战略是否定期由高级管理层审阅，外包战略是否被各相关部门知悉。

**（三）常见问题和风险**

1. 未建立信息科技外包战略或战略制定不合理，不利于确定信息科技外包管控重点，无法从外包核心能力丧失、关键技术自主可控、外包成本效益分析等方面指明外包发展目标和方向。

2. 信息科技外包战略未有效执行，过度依赖外包商，间接导致企业自主发展能力丧失，一旦供应商异常退出，企业无法独立运维和实现功能升级，将会影响系统的安全和稳定。

**（四）审计的主要方法和程序**

1. 信息科技外包战略的制定

（1）访谈科技信息部各个部室的负责人对于组织信息科技外包战略的理解。

（2）获取相关会议纪要，审阅组织对于信息科技外包管理战略的定义和变化。

2. 信息科技外包战略合理性

（1）获取组织整体发展战略，审阅信息科技外包管理战略与整体发展战略是否一致。

（2）审阅组织整体发展战略或信息科技外包管理战略中是否有适用年限的定义。

（3）审阅信息科技外包战略中是否进行了同行对比，是否有公开的定义。

3. 信息科技外包战略内容

（1）建立选择和实施战略的方针，确定指导外包行为的总则。

（2）建立外包战略长期目标和短期目标—盈利能力、财力资源、产品、研究与创新、组织结构与活动等。

（3）决定用以实现外包目标的战略，明确外包管理原则，确保风险、成本和效益的平衡，掌握核心技术的发展趋势。

（4）加强自身能力建设，降低对外包商的依赖。

## 二、信息科技外包治理审计

### （一）业务概述

信息科技外包治理是指组织中的信息科技外包的决策机制和管理方式和管理制度等内容。

（二）审计目标和内容

通过对信息科技外包治理的审计，判断组织在外包治理方面：

1. 是否建立信息科技外包组织、明确组织职责、岗位职责；是否建立信息科技外包管理体系，明确管理流程和管理方法。

2. 是否建立了正式的信息科技外包管理制度，并评价外包制度和流程的可操作性。

3. 是否建立了针对信息科技外包各个环节的风险评估要求，是否建立了外包商尽职调查、外包集中度评估和外包应急预案制订等规定，并得到了有效执行。

（三）常见问题和风险

1. 未建立信息科技外包制度体系文件或外包管理制度覆盖不全面，可能导致外包管控要求无法落实或外包精细化管控不足。

2. 外包组织架构不健全或职责冲突，无法有效履行外包管控职责，不利于信息科技外包的规范化管理。

3. 未定期开展信息科技外包管理的风险评估，无法有效对外包战略、外包供应商管理、外包人员管理、外包安全管理等各项管控措施的执行情况进行验证，不利于外包管理体系的持续改进。

（四）审计的主要方法和程序

1. 信息科技外包制度

（1）访谈了解已经制定颁布的信息科技外包管理相关制度。

（2）获取已经制定颁布的信息科技外包管理相关制度并审阅其内容是否包括分类分级管理、供应商管理、人员管理、应急管理等方面，并检查制度的执行情况。

2. 信息科技外包组织架构

（1）访谈了解信息科技外包组织架构。

（2）获取并审阅信息科技外包相关制度，是否包含信息科技外包管理架构和具体的管理角色以及职责分工。

（3）访谈了解各部门职能，验证其与设计职能是否一致。

（4）针对项目协调人，从所有项目中抽取审计样本，获取审计样本的项目牵头部门和负责人，审阅其与组织架构是否一致。

（5）明确信息科技外包风险主管部门的主要职责包括对外包风险进行识别、评估、处置、监控和报告。

（6）访谈了解信息科技外包管理架构管理层审阅流程。

（7）获取相应管理层对信息科技外包管理架构的审阅记录或会议纪要，并检查其中是否包含管理层审阅证据的内容。

（8）获取相应管理层对信息科技外包管理架构的审阅记录或会议纪要，并检查后续行动的监控及状态记录，以及最终处理状态。

3. 信息科技外包风险管理

与相关人员访谈，验证是否建立信息科技外包风险管理制度与流程，并获取相应制度进行验证；验证是否建立了年度信息科技外包商风险管理工作计划，并验证计划的执行力，获取相关工作成果。

## 三、信息科技外包商管理审计

### （一）业务概述

信息科技外包商管理是指对为组织提供信息科技服务的外包商进行准入、外包采购需求管理、外包商选择与尽职调查、外包合同签订等方面的管理工作。

### （二）审计目标和内容

通过对信息科技外包商管理的审计，判断组织在外包商管理方面：

1. 获取了充分的信息科技外包商准入信息，包括但不限于：内部控制与管理能力信息、持续经营能力信息、技术与服务能力信息等。

2. 开展了信息科技外包采购需求管理。外包项目的需求应符合信息系统规划框架，对未纳入采购计划或项目推迟的项目需求进行原因分析,并及时反馈给需求方。

3. 通过招标方式来选择信息科技外包商，并对外包商进行了尽职调查;与外包商签订了适宜的信息科技外包合同与服务水平协议（SLA）。

4. 组织的外包项目验收小组应对阶段性验收和最终验收的结果进行记录与归档，形成验收报告，记录实际项目情况与服务水平协议的一致性与差异性。

5. 组织应对外包商进行阶段性的考核工作，对外包商的异常情况进行及时纠正,根据考核结果对外包商建立奖惩机制。

（三）常见问题和风险

1. 未建立外包商准入标准或准入不严格，导致不合格外包商参与项目实施，导致外包交付延期或质量下降。

2. 未执行外包商尽职调查或尽职调查流于形式，对服务能力、资质、经验、市场评价等调查不彻底，导致外包项目失败或意外中断。

3. 企业或组织为追求短期目标，如成本、进度、技术等因素，将某些业务活动集中委托给少数服务商，可能导致企业或组织在商务谈判、合同、服务质量环节的把控力度下降。

4. 外包合同对知识产权定义不清晰，知识产权保护意识不强等引起的知识产权纠纷的风险。

5. 外包服务商因经营不善、与外包商的合同纠纷中断外包服务，导致组织生产和运营风险、服务中断的风险。

6. 未建立外包商服务评价机制或评价指标不够细致，导致外包商评价流于形式，无法实现对外包商工作的准确评价，不利于外包商的规范化管理和外包质量和风险的控制。

**（四）审计的主要方法和程序**

1. 信息科技外包商准入管理

（1）与相关人员访谈，验证是否对外包商准入信息进行定期收集。

（2）查看外包商准入信息收集文档。

（3）获取外包商准入信息指标，验证是否对外包商进行准入管理。

（4）获取已获得准入资格的外包商名单，验证在正常情况下的项目准入是否优先选择了满足准入条件的外包商。

2. 信息科技外包采购需求管理

（1）审阅年度集中采购项目清单。

（2）检查年度集中采购项目是否划分了优先级，以及优先级制定的依据。

（3）获取未按照信息系统规划制定的项目清单。

（4）检查其审批流程和根源分析证据。

（5）抽取部分未批准项目作为测试样本，审阅将未通过审批情况反馈给需求部门的证据。

3. 信息科技外包商选择与尽职调查

（1）选取部分项目作为测试样本。

（2）获取该项目外包商的背景调查报告，验证是否对外包商进行了充分的背景调查。

（3）获取样本项目的项目建议书、工作说明书，审阅其是否包含信息科技外包商技术资质、项目工作方法以及初步技术解决方案。

（4）获取评标文件，审阅其选定最终外包商后是否经过管理层的审批。

4. 信息科技外包合同与服务水平协议（SLA）

（1）获取合同变更的制度与流程。

（2）审阅其审批流程是否与正式流程的审批力度保持一致。

（3）选取部分项目作为测试样本。

（4）获取合同变更项目的相应流程文档。

5. 信息科技外包合同验收

（1）选取部分项目作为测试样本。

（2）与组织相关负责人访谈，了解是否制定了明确的信息科技外包服务商交付产品或提供服务的验收差异矫正措施报告。

（3）获取验收差异矫正报告，并验证其是否有效执行。

6. 信息科技外包商评价

（1）访谈相关岗位人员，了解外包商评价机制和评价情

况。

（2）访谈外包服务人员，特别是外包方项目经理，了解对方对考核结果的知晓情况。

（3）审查评价较差的外包商整改情况。

（4）审计评价结果的应用及效果。

## 四、信息科技外包项目管理审计

### （一）业务概述

信息科技外包项目管理是指对信息科技外包项目运用项目管理的方法和技术工具进行管理。

### （二）审计目标和内容

通过对信息科技外包项目管理的审计，判断组织在外包项目管理方面：

1. 开展了信息科技外包项目计划管理，在项目计划阶段对项目进行基本分工，明确各生命周期阶段的里程碑与交付品，确定各阶段的时间计划。

2. 在信息科技外包项目预算管理方面，组织建立了外包项目财务预算管理策略，制定管理制度，对外包服务的预算进行有序管理。

3. 实施了对信息科技外包项目的监控，确保外包商定期提交项目进度报告及成本与绩效报告；比较外包项目的实际完成情况及时间进度、投入人力情况、资源实际可用度、知识转移

情况等。

4. 开展了对信息科技外包项目的后评价，应至少从以下方面对外包项目进行绩评价：过程质量、交付质量、知识管理、客户满意度等。

（三）常见问题和风险

1. 由于信息科技外包项目计划制定不充分，导致外包交付延期或交付质量不满足预期要求。

2. 由于外包项目的需求不明确、项目进度、项目质量、奖惩机制不完善，导致外包项目实施效率低下，项目质量不高。

3. 信息科技外包项目实施过程中，由于缺乏有效的监控机制，或者检查评估措施不完善，导致项目交付延期或项目交付质量下降。

4. 由于组织的信息科技外包项目集中度过高，导致过度依赖于某个或某些外包商，从而削弱和丧失了自主开发运维和自主创新的能力。

5. 未建立外包项目后评价机制，无法准确对外包商交付成果进行评价，无法将外包评价结果作为外包商再次准入的重要参考依据。

（四）审计的主要方法和程序

1. 信息科技外包项目计划管理

（1）获取项目初级分工结构图，验证是否按照生命周期各

阶段对交付品进行规定。

（2）获取项目初级分工结构图，验证其是否包含上述内容。

（3）获取项目计划，验证项目计划中是否对资源进行了分配。

（4）选取部分项目作为测试样本。

2. 信息科技外包项目预算管理

（1）与相关负责人进行访谈，了解财务预算管理政策及执行情况。

（2）获取财务预算管理制度，检查预算管理制度是否合理，是否有针对外包服务的预算规则等方面。

（3）与相关人员访谈并获取会议纪要等文档，验证科技部门是否根据信息科技外包规划开展预算评估。

3. 信息科技外包项目监控

（1）获取外包商提供的项目进度报告，审查外包商是否对项目进度进行监控。

（2）获取外包项目过程文档，审查项目质量、进度、预算、风险的监控情况。

（3）获取项目质量评估报告，审查质量评估情况、整改情况。

（4）检查不符率和持续改进情况。

4. 信息科技外包项目后评价

（1）与相关负责人访谈了解组织是否针对不同类型信息科技外包项目建立了项目绩效评价指标体系。

（2）与相关负责人访谈了解建立项目绩效评价指标体系的过程，并获取相关文档，验证是否获得了组织管理层审批，并记入外包商合同中。

（3）与相关负责人访谈了解组织是否依据项目绩效评价指标体系定期及项目结束后对项目绩效进行评价，并获取相关文档。

（4）与相关负责人访谈了解组织在进行下一阶段项目或全新项目信息科技外包商选择时是否把前一阶段绩效评价结果纳入考量因素中，并获取相关文档。

（5）与相关负责人访谈了解组织是否在项目结束后，定期抽查分析项目立项目的是否实现，并根据分析结果判断外包商资质，以及更新项目绩效评价指标体系中相关参数，并获取相关文档。

（6）与相关负责人访谈了解组织的外包是否过于集中于一个或几个外包商，是否能防范行业垄断和机构集中度风险；是否可以通过引入适当的竞争在降低采购成本的同时提高服务质量，合理管控服务提供商的数量从而降低风险及管理成本。

## 五、信息科技外包人员管理审计

### （一）业务概述

信息科技外包人员管理是指对信息科技外包服务人员进行行政、服务方面的管理。

### （二）审计目标和内容

通过对信息科技外包人员管理的审计，判断组织在外包人员管理方面：

1. 开展了信息科技外包人员入场前管理，对外包人员进行入场前的教育与培训，使其知悉组织的外包安全管理要求。

2. 对驻场人员提出了日常管理的基本要求，建立了正式的外包人员违反外包人员管理的惩戒机制。

3. 对驻场人员离场提出相关管理要求，及时收回退出人员的门禁卡并清查办公物品，对退出人员使用的电子设备中保存的与组织业务有关系的文件或数据进行清除。

4. 对驻场人员进行考核管理，必要时应对外包人员的绩效水平与服务成果进行定期考核，确保外包人员有能力提供持续的外包服务。

### （三）常见问题和风险

1. 未实施重要外包项目的外包人员背景调查，可能无法有效识别外包人员的历史违规、数据泄露等历史风险。

2. 未开展外包人员安全教育，可能导致外包人员不经意泄露银行敏感信息，导致银行声誉风险。

3. 外包人员考勤及考核不严格，导致外包效率较低或外包质量不满足预期目标。

（四）审计的主要方法和程序

1. 信息科技外包人员入场前管理

（1）抽样获取并验证外包商进场前是否填写了外包人员驻场情况。

（2）与驻场人员访谈，验证是否对初次进入项目的外包人员建立试用期机制、入场前培训情况。

（3）检查驻场人员保密协议、个人简历、专业资质、背景调查情况。

2. 驻场人员日常管理

（1）与驻场人员访谈，验证驻场人员是否遵守了相关外包安全管理制度，是否开展过外包安全相关意识宣贯和技能培训。

（2）抽样并查看驻场外包人员的个人电脑，验证是否存在非法的网络外联，是否私自更改设定 IP 地址，是否安装了其他不允许安装的软件。

3. 驻场人员离场管理

（1）与相关人员访谈，了解外包人员退出程序和执行情况。

（2）与外包人员访谈，了解已经离职人员情况，检查是否属于人员流失。

4. 驻场人员考核管理

（1）与驻场人员访谈，检查驻场人员对考勤、考核制度的了解情况。

（2）检查考勤与考核记录。

（3）检查考核结果的公正性及考核效果。

（4）检查外包人员奖惩情况。

## 六、信息科技外包安全管理审计

### （一）业务概述

信息科技外包安全管理是指对信息科技外包相关的访问控制、信息资产、操作安全、数据安全、应急预案、应急处置等安全管理工作。

### （二）审计目标和内容

通过对信息科技外包安全管理的审计，判断组织在外包安全管理方面：

1. 组织的信息安全管理覆盖了外包项目和外包人员管理，包括访问控制、信息资产管理、操作安全、数据安全等领域。

2. 组织开展了信息科技外包应急管理，建立了外包项目范围的业务连续性管理规范，定期对外包商进行业务连续性管理安全检查。

3. 在外包项目开展前，应对外包项目的业务连续性进行风险分析，包括灾难、区域性灾难、金融领域关联性风险等。

4. 应定期对外包项目的灾难恢复计划进行测试和演练。

（三）常见问题和风险

1. 外包人员权限管控不严格，导致外包过程中出现操作失误或敏感信息泄露。

2. 如果不将外包风险纳入全面风险管理体系，没有建立外包风险检查与绩效机制，会使外包风险游离于组织风险管理体系之外。

3. 未建立外包应急预案，无法有效对外包应急场景进行识别与演练，不利于外包商异常中断的快速处置。

（四）审计的主要方法和程序

1. 信息科技外包应急管理

（1）检查外包应急预案。

（2）检查应急预案演练情况。

（3）检查外包合同中是否明确紧急情况下外包服务商的责任和应急要求。

（4）检查关键外包人员对应急的理解程度。

2. 信息科技外包安全管理

（1）检查外包服务使用部门，对外包安全的履职情况，包括签订保密协议、授权访问资产等。

（2）访谈外包人员，判断其对外包人员管理要求和义务的理解和执行情况。

（3）检查违反外包安全规定的处罚情况。

## 第二节　灾备与业务连续性审计

灾备与业务连续性是组织通过预防和恢复控制的结合，将意外事故的影响降低到最低水平，并将损失恢复到可接受程度的整个过程。其主要目标是防止业务活动中断，保护关键业务流程不会受信息系统失效或自然灾害的影响，并确保其及时恢复。

业务连续性管理应包括识别和降低风险、有效的业务及风险评估、限制有害事故的影响范围以及确保业务及时恢复等步骤。典型的信息业务连续性管理应包括应急管理、灾难备份和业务连续性计划三个方面的内容，灾难备份（以下简称灾备）是指为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业支持能力和运行管理能力进行备份的过程；业务连续性计划是机构通过制定计划，通过预防和恢复控制的结合，将意外事故的影响降低到最低水平，并将损失恢复到可接受程度的整个过程。

本节只涉及灾难备份与业务连续性的审计，有关应急管理的审计可参考第三章第四节中的内容。

### 一、灾难备份管理审计

#### （一）业务概述

灾难备份管理，是指组织为了更好应对灾难发生确保业务连续性而从组织与人员，制度与策略、工具与技术等三方面所建立的灾难备份管理体系。

### (二)审计目标和内容

该项审计的目标旨在通过对灾难管理涉及的人员与组织、制度与策略，以及工具与技术的检查，以判断：

1. 组织是否根据其经营规模和业务发展的具体情况建立相应的负责灾难备份、恢复的组织架构，明确灾备组织中各类小组及人员的职责。

2. 组织是否根据其经营规模和业务发展的具体情况建立完备、正式的灾备系统规划，制定适宜的灾难备份与灾难恢复策略。其中，灾难恢复策略的制定应根据系统风险分析和业务影响性分析的结果进行灾难恢复等级划分，并根据成本风险平衡的原则确定每项关键业务功能的灾难恢复策略。

3. 组织是否依据灾难恢复策略制定恢复预案，重点检查预案的完整性、兼容性、指导性和及时性，并确保恢复预案得到定期的评审与周期性的演练。

### (三)常见问题和风险

1. 组织未根据国家、行业的合规监管要求以及自身的经营规模和业务需求，建立健全灾难恢复管理体系，如未建立跨部门的灾难恢复组织、未明确组织中各类小组及人员职责、未制

定健全的灾难恢复管理制度与操作规范、未部署灾难备份和恢复系统，进而导致灾难发生时无法及时、有序地进行处置和恢复。

2. 在制定灾难恢复策略前，未进行系统风险分析和业务影响性分析，无法确定重要信息系统的恢复时间目标、恢复点目标和恢复优先级策略。

3. 灾难恢复预案未经正式的审批与发布，导致预案程序未得到有效的认同。发生灾难事件时，无法通过预案协调各部门进行有效的配合、应对、处置与恢复。

4. 灾难恢复预案未开展定期演练，无法有效验证灾难恢复流程的合理性和适用性，一旦发生灾难事件，无法按照灾难恢复预案所规定的处置流程进行快速处置和恢复。

**(四)审计的主要方法和程序**

1. 调阅相关文件和资料，了解组织是否建立灾备恢复机构，明确机构内各类小组（灾备领导小组、灾备规划小组、灾备运行小组）和人员职责，并判断人员构成及其职责设置的合理性，其中，组织机构人员组成应包括管理、业务、技术和后勤方面的人员；检查是否指定同职责的备份人员。

2. 灾备总体规划与系统工作范围定义

（1）通过访谈或现场查阅方式，了解是否建立灾难备份、恢复机制及其总体控制目标；是否明确定义为减少灾难造成的

损失以及确保信息系统所支持的关键业务在灾难后迅速恢复和继续运行的总体安排和计划。

（2）访谈信息系统主管人员并审阅相关资料，检查灾备系统工作范围定义的完整性，即灾备系统规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和重新运行，主系统灾后重建和回退工作，突发事件的响应等。

3. 审阅灾难恢复策略制定过程相关文档：

（1）检查其是否包括覆盖所有关键业务的信息系统风险分析文档，以及是否根据风险分析结果确定风险防范和风险接受的程度，并以此作为灾备系统开发的重要依据，且经过管理层的正式审批。

（2）检查其是否包括：经营管理层正式审批的所有关键业务系统的业务影响性分析，明确相关信息的保密性、完整性和可用性要求；中断影响评估，包括评估的方法（定性或定量），业务功能中断可能给组织带来的损失及由此带来的风险。

（3）检查是否明确定义了关键业务功能及恢复的优先顺序，且该顺序的制定过程中由业务部门发起，并经高级管理层的审批；RTO/RPO 时间定义是否符合企业业务连续性的要求。

（4）检查每项关键业务的灾难恢复策略是否基于经过全面分析灾难恢复资源成本与风险可能造成损失之间的平衡基础之上；灾难恢复策略内容是否完整地包括了灾难恢复资源的获取

方式和灾难恢复能力等级。

（5）检查灾难恢复、备份策略中是否与所涉及的电信、电力、设备及技术支持供应商之间签署服务水平协议（SLA），确保灾难发生时可以得到及时的服务。

4. 外部资源的获取

访谈信息系统主管人员，询问是否存在委托外部机构的灾备系统建设，若存在，检查外部机构的资质及是否与其签署服务水平协议（SLA），查看并评判安全保密措施要求的适当性。

5. 灾难恢复预案制定及演练

（1）审阅灾难恢复预案制定过程产生的文档记录，确认其是否经过起草、评审、测试、完善、审核和批准的全过程，判断其过程的完整性和合规性。

（2）查阅灾难恢复预案，检查其内容是否涵盖灾难恢复的整个过程，以及所需的尽可能全面、及时的数据和资料，明确定义灾难恢复的各流程及其工作内容、工作步骤、涉及人员及其职责，判断预案的完整性、可读性、明确性和易用性；访谈负责应急系统管理和灾备系统管理的主管人员，了解灾难恢复预案与其他应急体系的结合程度，确保其兼容性。

（3）检查灾难恢复预案是否记录了涉及的关键岗位的详细通讯方式以及灾难发生时可用的备份联系方式；根据灾难恢复预案中的记录，确认关键岗位通讯方式的有效性；访谈灾难恢

复预案中涉及的人员，确认所有人都已得到该通讯记录，并在异地进行了备份存储，且可以及时取得。

（4）访谈灾难恢复预案的管理人员并调阅相关管理制度，了解预案的保存和分发的流程，并检查流程是否合规，并落实专人负责，统一多份拷贝，异地保存，且分发给所有参与灾难恢复工作的人员；定期修订更新，旧版本仅留存一套备查，其余统一销毁。

（5）访谈灾备系统相关人员，了解组织是否将灾备系统观念或相关知识纳入安全意识培训体系并持续开展教育；访谈灾备相关的技术支持人员，确认组织持续提供关于灾备、应急、专业技术、业务系统方面的培训；检查已经实施的灾难恢复演练计划所形成的报告，根据演练的类型（桌面演练、模拟演练、真实演练、混合演练）和结果，确认其演练过程的有效性，及每年存在至少一次的、有最终用户参与的完整演练。

6. 评估、维护与更新

（1）访谈组织及业务和信息系统相关负责人，了解组织是否随着自身业务发展，定期进行系统风险分析和业务影响性分析，并根据其结果对灾难恢复、备份策略进行补充和修订；审阅相关制度和会议记录，明确灾备策略评估、维护、更新经过了管理层及所有业务部门的参与和审批。

（2）审阅相关制度和会议记录，明确灾难恢复预案的评估

和修订经过管理层及相关部门的参与和审批。所有的修订都应经过起草、评审、测试、完善、审核和批准等程序；检查灾难恢复预案的维护和变更记录及审核文档，确保业务流程的变化、信息系统的变更、人员的变更都在灾难恢复预案中及时反映；审阅测试、演练和执行的效果评估结果，以及预案相应的修订记录，确保灾难恢复预案进行了相应的修订；审阅针对灾难恢复预案进行的评审或内部信息系统审计的相关报告，确认灾难恢复预案进行了相应的修订。

## 二、业务连续性计划审计

### (一)业务概述

组织建立实施业务连续性计划的责任架构和日常管理制度，可提高自身的风险防范能力，降低突发灾难的破坏并降低不良影响。

信息系统业务连续性管理主要包括：制定、管理、执行的组织架构及实施工作人员管理；制定完备的信息业务连续性计划并对其进行测试、更新；对相关业务人员的培训；对信息业务连续性计划的审计以及管理工作的合规管理。

### (二)审计目标和内容

该项的审计目标旨在：

1.检查组织的高管层是否为满足组织自身业务连续性管理的要求，履行管理职责，组建由高级管理层和业务连续性管理

相关部门负责人组成的业务连续性管理机构，明确其职责，配置足够资源以及经过充分培训的员工，并对其工作开展进行审查、监督和评价。

2. 检查业务连续性管理组织是否履行其职责，制定并开展业务连续性计划，协调业务条线部门，汇总、确定重要业务的恢复目标和恢复策略。

3. 检查组织是否在统一的业务连续性计划框架下制定信息业务连续性计划,从而明确总体目标及风险底线，确保计划涵盖所有业务部门的重要应用系统及不同网络与信息安全事件，充分体现计划的完整性、合理性和合规性。

4. 检查组织是否针对信息业务连续性计划进行业务影响分析，并以此为基础明确业务运行恢复的优先顺序，制定合理的业务恢复策略，确保恢复策略的可操作性、规范性。

5. 检查组织是否将外部信息技术服务商纳入到信息业务连续性恢复框架内，并对关键服务供应商、外包商在突发状况发生时的应对能力进行评估；制定组织在使用海外机构支持的情况下应对法律和合规问题的方案。

(三) 常见问题和风险

1. 未建立由组织高层领导的、跨部门的业务连续性管理机构并将业务连续性管理纳入企业文化建设中，未明确业务连续性管理组织和人员的职责，造成业务连续性管理缺失，无法有

效履行管理职责。

2. 未制定业务连续性计划，或业务连续性计划未覆盖组织重要业务和系统，导致业务连续性计划无法有效执行。

3. 未针对业务连续性计划制定演练计划及定期开展演练，不利于检验业务连续性计划的合理性和适用性，不利于业务连续性计划的持续改进。

**(四)审计的主要方法和程序**

1. 业务连续性管理的组织

（1）（组织的高级管理层）访谈组织管理层，了解其是否知悉自己在组织内部业务连续性管理中的定位与职责；是否参与相关政策的审批并对组织的审批提供了资源支持；是否通过相关管理层会议推进业务连续性计划的建立、实施及更新，以符合业务发展的需要。

（2）（业务连续性管理委员会）调阅组织业务连续性管理相关规章制度、文件以及人员名单，检查其是否设定了跨部门的业务连续性管理委员会并明确了其职责；与委员会的负责人进行座谈，询问委员会推动协调本单位业务连续性计划实施情况，对相关规章制度规范、计划制定与实施、计划持续改进等情况进行证实。

（3）（业务连续性主管部门或岗位）调阅组织业务连续性管理相关规章制度、文件，检查是否对业务连续性主管部门或

岗位的职责做出明确规定，分析其职责界定是否合理、完整；调阅业务连续性主管部门的有关业务连续性的相关工作计划、实施方案、评估报告、会议纪要、工作记录等，检查其是否主导开展业务连续性管理工作。

（4）（业务连续性计划执行部门和保障部门）访谈业务条线部门及信息技术部门负责人，了解业务条线部门是否实施了风险评估、业务影响分析，确定重要业务恢复目标和恢复策略，负责业务条线重要业务应急响应与恢复等工作；了解信息科技部门是否负责了信息技术应急响应与恢复工作；访谈保障部门，了解其是否为本单位的业务连续性计划提供了人力、物力、财力以及安全保障和法律咨询服务。

2. 业务连续性计划的实施

（1）（计划的完备性）调阅企业的总体业务连续性计划，检查其是否包括信息系统业务连续性计划，如果包括，则判断其内容、要点是否具备以上相关基本要求；调阅信息业务连续性计划业务影响分析报告，检查其分析是否全面、合理，符合要求；调阅突发事件应急管理预案和灾难恢复策略，检查其制定是否合理、完善;与信息业务连续性计划负责人、相关工作人员进行座谈。询问是否制定不同事件的信息业务连续性计划，是否定期对信息业务连续性计划进行测试，测试周期多长，是否对信息业务连续性计划定期进行审查并更新，目前的预案文

档为第几版，了解其对信息业务连续性计划的掌握程度；与信息业务连续性计划负责人、相关工作人员进行座谈，询问是否具备应急设备并能正常工作，信息业务连续性计划执行所需资金是否做过预算并能够落实。

（2）(业务影响分析)调阅业务影响分析报告，确定其是否对本机构所有部门和功能进行了分析，确定其对业务优先级的制定是否合适，是否明确了本机构关键业务系统所允许的最大非正常停止时间、数据丢失数量以及日志损失，是否明确定义了时间恢复目标；调阅机构风险评估报告，验证其是否包括了信息服务、技术、人员、设施以及服务提供商可能出现问题的场景；调阅相关记录，验证业务影响分析和风险评估报告是否经过了高级管理层和董事会的审核。

（3）（业务连续性计划的编制）调阅企业信息业务连续性计划编制、维护相关规章制度以及人员名单，检查其建立健全情况；与信息业务连续性计划编制、维护相关人员进行座谈，询问业务连续性计划编制、维护情况，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

（4）（业务连续性计划的执行）调阅企业与信息业务连续性计划执行相关的规章制度、文件以及人员名单，检查其是否制定了业务连续性计划执行组织及明确其职责，检查其建立健全情况；调阅信息业务连续性计划组织相关会议纪要等资料，

检查其工作开展情况；与业务连续性计划执行组织相关人员进行座谈，包括信息业务连续性计划执行领导小组、专家小组、执行小组、支持保障小组等人员，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

（5）（业务连续性计划的保障）调阅组织的所有业务连续性计划，核实其是否至少包括以下内容：关键岗位人员缺失的处理方式；关键建筑、设施不可用的处理方式；设备故障的处理方式（硬件、统信或者操作设备）；软件或数据不可用或被破坏的处理方式；外包商或服务提供商不可用的处理方式；外部设施不可用的处理方式（电力、统信等）；关键文档或记录不可用的处理方式。

（6）（业务连续性计划的测试）调阅信息业务连续性计划测试记录和更新记录，检查与相关支持部门的联系方式和记录，测试联系渠道是否保持畅通；检查业务流程、信息系统、人员变更是否在信息业务连续性计划中及时反映和修订；调阅信息业务连续性计划测试、更新记录，检查其在测试、演练和灾难发生后实际执行时，其过程是否均有详细的记录，是否对测试、演练和执行的效果进行评估，是否对信息业务连续性计划进行相应的修订；调阅信息业务连续性计划测试记录，检查对该计划是否定期测试、评审和修订；检查计划的修订和年度测试结果是否经过董事会和高级管理层、信息系统风险管理部门、内

审部门、信息管理委员会的审核签字。

## 第三节　关键信息基础设施安全审计

关键信息基础设施作为国家的重要资产，在《网络安全法》中被重点提及并要求实行重点保护。由国家互联网信息办公室发布的《关键信息基础设施安全保护条例（征求意见稿）》，划定了关键信息基础设施的保护范围，明确了各相关部门的安全保护职责，规定了安全保护的基本制度。

关键信息基础设施的安全保护，首先在于如何准确识别关键信息基础设施的具体范畴及其面临的风险；其次，应制定完善的关键信息基础设施安全保护制度体系并建立保护工作的组织架构，明确责任主体；再次，提高态势感知和风险应对能力并健全应急管理体系，提升应急响应和恢复能力。

本节将从关键信息基础设施的管理体系建设、风险识别与报告、安全防护、安全检测与评估、安全监测与应急处置等方面对关键信息基础设施安全审计的方法与步骤进行描述。

### 一、关键信息基础设施管理体系建设审计

#### （一）业务概述

关键信息基础设施，是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会

影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施管理体系建设，是指组织为确保关键信息基础设施安全而建立的一套完整、有效的，包括制度与流程、组织与人员以及技术和工具等三方面内容的整体。

**（二）审计目标和内容**

关键信息基础设施管理体系建设的审计目标，旨在审查组织一般信息安全管理的基础之上，是否对关键信息基础设施安全管理予以重点关注，建立健全完善的制度体系与组织和人员管理体系，并对其提供必要的资金和人员保障。

**（三）常见问题和风险**

1. 组织未在其内部设置专职的关键信息基础设施安全管理机构及其安全管理负责人。

2. 组织在进行整体信息安全规划时，未对关键信息基础设施规划予以重点关注，并接受组织高层分管信息安全工作领导及机构（如信息安全管理委员会）的指导和监督。

3. 组织未在制度层面建立健全关键信息基础设施的管理制度和流程要求，并以书面形式获得组织管理层对于关键信息基础设施建设的资金和人员保障承诺。

**（四）审计的主要方法和程序**

1. 通过对关键信息基础设施相关安全管理制度与规划方案

的收集：

（1）检查组织是否对关键信息基础设施发展规划予以单独制定并分为总体规划和专项规划。

（2）收集关键信息基础设施相关的安全管理制度、规范、标准和策略等组织文档，检查组织文档是否依照制度管理规范要求进行制定、审批、下发及修订。

（3）检查制度与规范中是否明确关键信息基础设施专职管理机构的职责及其岗位安全职责，判断是否遵循“职责分离”和“最小授权”原则，以及明确对其安全建设和运维管理提供资金和人员保障，同时了解人员占比与人员构成情况。

（4）检查组织是否为确保关键信息基础设施的人员安全，制定包括第三方供应商在内的人员管理制度，确保对关键岗位人员实施录用前的背景审查、学历和资历确认、签署保密协议以及在离职和转岗时访问权限的回收。

2. 访谈信息安全主管部门及关键基础设施管理负责人，了解规划方案的具体落实及优化情况，判断一致性。

3. 访谈关键信息基础设施部门负责人及关键岗位负责人，了解其对所承担职责的知晓情况。

4. 访谈组织财务管理及信息安全管理负责人，了解组织针对关键信息基础设施安全建设与管理的当年度及过往年度预算额、安全建设投资额等资金支持和投入情况，以及总体占比情

况。

5. 访谈人力资源管理负责人，了解人才储备机制、现有人才储备规模情况及人员资质情况。

## 二、关键信息基础设施及其风险识别与报告

### （一）业务概述

关键信息基础设施识别，是指通过识别组织所属行业及关键业务从而确定支撑关键业务的信息系统或工业控制系统，再根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。关键信息基础设施包括网站类、平台类和生产业务类。

### （二）审计目标和内容

该项的审计目标旨在审查组织是否围绕关键业务和行业特点，识别支持关键业务的关键信息系统并制定和上报资产清单，同时围绕已识别的关键信息基础设施及其所处的环境，识别与基础设施相关的风险。

### （三）常见问题和风险

1. 未依照组织所属的行业监管要求和经营业务准确识别关键信息基础设施所产生的风险，无法针对风险建立有效的防护措施。

2. 未建立关键信息基础设施的风险指标及定期执行风险评估，不利于潜在风险的发现及对问题的整改及优化。

（四）审计的主要方法和程序

1. 访谈组织各业务管理部门负责人，了解是否对其关键业务进行梳理并形成关键业务链及存在的业务风险明确其安全防护优先级。

2. 访谈关键业务管理负责人是否将已识别的关键业务及风险点与支撑的信息资产相映射，从而建立与关键业务链相关的网络和系统关键信息基础设施资产目录，若有需要，还应上报监管部门。

3. 访谈关键信息基础设施负责人，了解是否基于资产的威胁性和脆弱性对已识别的关键信息基础设施建立风险评估指标，定期或在关键信息基础设施新建、停运、外部环境发生重大变化时重新开展风险评估并及时进行上报，同时更新相应的安全策略。

4. 查阅风险评估报告及安全策略更新记录。

## 三、关键信息基础设施安全防护审计

（一）业务概述

关键信息基础设施保护从安全保护意识上分为三种思维方式：动态、全链条式保护思维，核心工作重点保护思维和主体的全面责任思维。采取措施，监测、防御、处置风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏。

（二）审计目标和内容

该项的审计目标在于审查组织是否为保障关键信息基础设施的安全，依据《网络安全法》中的相关要求采取相关防护措施。

（三）常见问题和风险

1. 在新建或改建、扩建关键信息基础设施时，未充分考虑网络安全因素，无法实现关键信息基础设施安全的同步规划、同步建设、同步使用。

2. 未对所运营的关键信息基础设施开展等级保护工作并定期进行等保测评，无法有效验证现有控制措施与等保合规要求的符合度，存在合规风险。

3. 重要数据和个人信息安全管理措施不严格，无法确保其境内存储和跨境传输的安全，存在重要数据泄露或被滥用的风险。

4. 未在安全产品和服务采购前，进行严格的安全审查，导致产品和服务不满足国家相关规定，存在合规风险。

（四）审计的主要方法和程序

1. 访谈关键信息基础设施负责人，了解组织是否在基础设施建设的规划或改建之初，将其对网络安全需求融入其中；在建设（开发）阶段，是否基于既定义的安全要求，设计并建设安全体系，满足系统内各类信息安全组件及信息安全服务的安全需求规划并符合其等级要求；在运维阶段是否对安全设施同

步实施配置管理并部署安全管理设备，并根据承载业务的重要性和数据的敏感程度，对关键信息基础设施实施分区分域管理，制定安全策略，避免重要网络、系统和资产遭受未经授权的访问，防止重要数据泄露或者被窃取、篡改。防止未经授权的访问，防止重要数据泄露或者被窃取、篡改。

2. 调阅组织的数据管理制度与规范，检查是否对关键信息基础设施所涉及的重要数据和个人信息在资产清单中予以标识；是否制定重要数据和个人信息出境的安全评估制度与规范，并访谈和检查重要数据和个人信息存放物理位置是否满足境内存储要求，若存在境外存储现象，检查出境前的安全评估记录和审批流程是否合规。

3. 访谈关键信息基础设施管理负责人及数据存储岗位负责人，检查是否制定容灾备份策略对重要系统和数据采取冗余措施或容灾备份；是否对已识别的重要数据和个人信息基于备份策略执行数据备份，并验证容灾备份和恢复策略的有效性。

4. 访谈关键信息基础设施管理负责人及各岗位负责人，了解组织是否采取审计措施，监测、记录系统运行、操作、故障维护等行为并留存相关日志，并检查日志留存期限是否不低于 6 个月。

5. 访谈关键信息基础设施负责人及采购管理，询问是否制定针对服务商及其产品和服务进行安全检查和评估的规范标准，

查阅检查与评估记录及安全产品测试报告。

6. 访谈人力资源管理负责人，了解组织是否建立针对关键信息基础设施安全管理的教育和培训制度，定期开展安全教育培训和技能考核，查阅培训记录，检查培训对象是否重点包括关键信息基础设施负责人、关键岗位负责人。

7. 访谈关键信息基础设施负责人，询问是否对关键基础信息设施等保定级、备案、测评及整改，并查看相关文档。

## 四、关键信息基础设施的安全检测与评估

### (一) 业务概述

安全检测与评估，是指组织基于既定检测与评估制度、标准与流程，对关键信息基础设施的网络与信息安全开展常规性检查，如日常安全规范和操作流程的遵守情况，重要数据和个人信息的保护情况等，并评估当前安全措施的有效性，分析潜在安全风险及可能引起的安全事件。

### (二) 审计目标和内容

该项的审计目标在于通过查阅组织既定的安全检测与评估制度、标准与流程，检查组织是否建立完善的检测与评估体系，定期开展检测与评估工作，对发现的问题及时上报或主动采取措施应对安全隐患或问题。

### (三) 常见问题和风险

1. 尚未建立关键信息基础设施的安全检测与评估体系，或

体系不健全，检测与评估的内容不完整，安全检测与测评指标不明确，导致无法及时发现潜在的风险与隐患。

2. 对存在的安全问题未及时发现或整改不到位，留有安全隐患，不利于关键信息基础设施的有效改进。

(四)审计的主要方法和程序

1. 调阅组织的关键信息基础设施安全检测与评估制度规范、标准与流程，检查组织是否建立了完善的安全检测与评估体系，了解具体执行者、频率、流程、内容（包括但不限于网络安全制度落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、技术防护情况、风险评估情况、应急演练情况、网络安全等级保护工作落实情况等）。

2. 访谈关键信息基础设施管理负责人，了解在新建或改建、扩建关键信息基础设施时，是否对其进行安全检测评估，并在发现安全问题后是否采取整改措施。

3. 访谈关键信息基础设施负责人，了解是否对关键信息基础设施的安全性和可能存在的风险进行监测和评估，了解检测评估结果和整改情况的上报情况。

4. 访谈关键信息基础设施负责人，了解是否对其存储的重要数据和个人信息予以重点关注，特别在进行个人信息收集时是否明示或在使用时超出用户授权范围等其他违规行为，违反相关法律法规的情况并投诉和举报机制与渠道。

5. 调阅历史安全监测与评估报告，审查其内容是否与制度规范相符，重大问题是否及时汇报与处理，以及是否及时采取应对措施进行整改。

## 五、关键信息基础设施的安全监测与应急处置审计

### (一) 业务概述

安全监测，是指组织以明确的制度规范与流程，借助技术工具对关键信息基础设施的网络和信息安全采取监控、预警，动态、及时识别关键信息基础设施的安全风险并采取措施恢复由于网络安全事件而受损的功能或服务。

应急处置，是指组织为应对突发网络安全事件造成关键信息基础设施的性能下降、服务不可用、信息泄露等问题而制定的一整套应急处置方案，并据此定期开展应急演练工作，验证应急处置方案的有效性和应急处置机构与人员的配合度与熟练性。

### (二) 审计目标和内容

该项的审计目标旨在检查组织是否制定并实施网络安全监测预警机制，对即将发生或正在发生的网络安全事件或威胁，动态识别关键信息基础设施的安全风险，提前或及时发出安全警示并及时采取措施恢复由于网络安全事件而受损的功能或服务。

检查组织是否将网络安全应急管理工作纳入整体应急管理

工作框架之内，制定应急预案并据此开展应急演练工作。

(三)常见问题和风险

1. 尚未建立针对关键信息基础设施的网络安全监测机制，或监测体系不完善，缺乏应急团队和专家团队，现有应急监测系统无法对网络安全事件实现动态识别与预警。

2. 尚未建立完善的关键信息基础设施网络安全应急预案，或预案场景无法覆盖到相关设施，导致应急预案无法有效执行或预案适用性较差。

(四)审计的主要方法和程序

1. 访谈关键信息基础设施部门负责人，询问是否针对关键信息基础设施建立动态识别安全风险与事件的监测体系并部署监测设施。

2. 访谈关键信息基础设施负责人和运维人员，了解其对网络安全管理制度、安全事件的分类、分级管理要求以及上报流程的知晓情况。

3. 检查安全监测的制度规范，检查是否包括安全监测的指标及安全威胁和事件的信息通报与信息共享等内容和相关操作流程。

4. 查看安全态势监测记录，验证监测设施是否具备发现和预警的能力，并检查安全事件是否得到及时上报与处置。

5. 访谈关键信息基础设施部门负责人，询问是否根据行业

和地方的特殊要求，针对关键信息基础设施制定网络安全事件应急预案与恢复计划并建立相应的应急支撑、恢复和专家团队，同时开展定期的应急演练。

6. 查阅应急预案与应急演练计划，检查应急预案内容是否包括启动条件、应急处理流程、系统恢复流程、事件报告流程、事后教育和培训等内容，以及应急演练计划是否将全面恢复和重构信息系统到已知状态作为其的一部分。

7. 查看应急处置历史记录，检查其内容是否至少包括：事件描述、原因和影响分析、处置方式，应急上报及处理情况，判断是否符合组织规范要求。

8. 查看应急演练记录，检查是否按照应急预案的规范和流程进行处置。

## 第四节　云安全审计

云计算作为一种新兴的计算资源利用方式逐渐被各行业所接受和部署。采用了云计算技术的信息系统，称为云计算平台（系统）。 云计算平台由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）是三种基本的云计算服务模式。在不同的服务模式中，云服务商和云服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任

的边界。

由于云服务平台建设的复杂性以及传统信息系统安全和云计算自身技术特点所引发的新的信息安全和风险，与传统信息系统安全审计相比,对于云服务平台的安全审计有其自身的特点。本节将从云服务规划与需求分析、供应商选择与合同签署、云服务平台开发测试与交付、云计算平台的安全管理、云计算平台的迁移与部署、云计算平台的安全运维、云计算服务关闭与数据迁移等方面对云安全审计的方法与步骤进行描述。

## 一、云服务规划与需求分析审计

### （一）业务概述

在规划与需求分析阶段,组织应根据自身的经营战略与规划，通过对组织资产、云服务平台功能性、非功能性和安全性等四个方面的需求分析，以及云服务的效益评估,综合评判部署云计算服务平台的合理性及其建设模式，并最终形成决策报告。

### （二）审计目标和内容

1. 云服务综合评估

该控制项旨在检查组织在部署云计算服务平台前，是否综合评估采用云计算服务后获得的效益（经济效益和社会效益）、可能面临的信息安全风险、可以采取的安全措施后做出决策，从而判断组织是否可在其可承受、容忍的风险范围内,或在当安全风险引发信息安全事件时有适当的控制或补救措施而采用云

计算服务。

2. 决策建议与审批

该控制项旨在检查组织在部署云服务平台时，是否在基于服务综合评估的基础之上，对其进行综合分析形成采用云计算服务的决策报告,并经本单位最高领导批准，从而成为指导采用云计算服务的重要依据。

（三）常见问题和风险

1. 云平台规划与建设时未充分考虑部署模式、服务模式对于经济效益、功能性需求、现有资源利用、现有流程的影响，导致项目建设与预期差距较大，经济效益较差。

2. 云平台规划与建设时未充分考虑数据安全和整体安全防护，导致云平台安全管控能力不足，容易造成数据泄露或安全风险。

3. 云平台建设缺乏严格的审批程度，导致需求模糊、边界不清晰、性能不满足预期要求，严重影响云平台的交付和使用。

（四）审计的主要方法和程序

1. 云服务综合评估

（1）查阅组织项目建设的相关制度规范，了解涉及科技项目建设的评价指标和流程。

（2）检查组织是否对业务进行识别并进行优先级划分，并访谈关键业务部门负责人，了解关键业务特点、资源需求、时

延、连续性以及安全保护的要求。

（3）访谈信息科技建设负责人，了解组织在规划建设云服务平台项目时是否基于部署模式（公有云、私有云和混合云）、服务模式（IaaS、PaaS、SaaS）对经济效益、功能性需求、非功能性需求、安全需求、现有资源利用/需求情况、现有信息系统管理流程是否受到影响等方面进行综合评估，以及评估、审批的流程，参与人员，并调阅项目建设的立项文档，从而判断效益评估的合理性、科学性以及合规性，其中，效益评估应至少包括建设成本、运维成本、人力成本、创新性以及对业务性能和质量带来的优势。

（4）检查组织与数据管理相关的规章制度，了解组织是否明确数据类型，并查看数据存放的位置，从而判断云平台数据是否涉及敏感信息以及数据存储的合规性。

（5）访谈云服务平台负责人，了解现有的云部署模式和服务模式，并询问其对在该模式下的安全风险和平台运营者所应承担的安全责任知晓情况及其采取的常规安全防护措施、平台可移植和互操作性，从而判断现有云服务平台对业务的安全风险承受能力。

（6）检查组织是否对其资产进行识别和归属分析，从而明确其部署的软件所有权/使用权，数据资产的归属权。

2. 决策建议与审批

（1）查阅云计算服务平台建设项目的决策报告，检查是否包括：背景描述，描述拟采用云计算服务的信息和业务；效益分析，从场地、人员、设备、软件、运行管理、维护升级、能耗等方面，对采用本地应用与云计算服务所需费用进行综合分析；云计算服务模式、部署模式选择，从而明确客户与云服务商的安全措施、实施边界和管理边界；数据和业务部署到云计算环境后可能遇到的功能需求分析，不同模式下的资源需求分析，数据的备份与数据的传输方式和网络带宽要求等；拟部署到云服务平台中数据或系统的可用性、可靠性、恢复能力、事务响应时间、吞吐率等指标；基于对拟部署到云计算平台的信息和业务的安全能力要求；将业务系统迁移到云计算平台后,为确保业务连续性进行的部署方案;退出云计算服务或变更云服务商的初步方案；对客户相关人员进行安全意识、技术和管理培训的方案；本单位负责采用云计算服务的领导、工作机构及其责任；采购和使用云计算服务过程中应该考虑的其他重要事项。

（2）检查决策报告是否经过业务部门及管理层或专家团队的评审，以及审批流程是否完整；若存在改进建议是否及时完善从而有效控制风险。

## 二、供应商选择与合同签署审计

### （一）业务概述

在服务商选择与合同部署阶段，客户应根据上阶段所提的需求和决策报告，从服务能力、服务风险和服务费用等三个方面评估云服务商的服务能力，选择并与其协商和签署服务合同(包括服务水平协议、安全需求、保密要求等内容)，从而完成云服务平台的开发、建设、测试以及数据和业务向云计算平台的迁移与部署。

### （二）审计目标和内容

1. 云服务安全风险评估

该控制项旨在重点检查组织是否从数据安全与存储合规角度，结合自身对部署云服务平台后可能产生风险的容忍度和处置能力进行评估，并作为云服务商选择和评估的参考依据。

2. 服务安全能力评估

该控制项旨在检查组织在选择第三方云服务平台时，是否对其基本的服务安全能力进行评估。

3. 云安全控制措施责任的识别

该控制项旨在检查组织是否基于所选择的云服务部署模式，明确与服务提供方的责任。

4. 云服务合同及保密协议签署

该控制项旨在检查组织在选择第三方云服务商时，是否与其签署服务合同，并检查其内容是否包含明确的服务水平协议、安全需求、保密要求等关键内容，从而保障组织的权益。

（三）常见问题和风险

1. 组织没有对云环境下其数据所有权的保障能力进行风险评估的风险。

2. 组织没有根据采用的服务模式（IaaS、PaaS、SaaS），明确云服务提供商与自身所承担安全责任的风险，以及没有能力采取相应的控制措施所产生的风险。

3. 组织所选择的云服务商自身安全风险管控体系不完善，自身的安全评估不足，导致存在较大风险隐患。

4. 云服务商第三方机构审计不到位，无法对云服务商的风险进行识别与监督。

5. 云服务商安全与应急响应机制不健全，导致发生安全事件无法及时进行处置。

（四）审计的主要方法和程序

1. 云服务安全风险评估

（1）检查云服务平台存储的生产经营数据是否属于国家规定的重要数据范畴，从而判断组织是否存在可能的数据管辖风险。（数据管辖风险）

（2）检查组织是否对其数据所有权的保障能力进行风险评估。（数据所有权保障风险）

（3）检查组织所部署的云服务平台是否提供或具有有效的机制、标准或工具来验证所删除的数据可否完全删除，以防止

其退出云计算服务后组织数据仍然可能完整保存或残留在云计算平台上。（数据残留风险评估）

（4）评估是否存在单一云服务供应商的风险。（供应商锁定的风险评估）

2. 服务安全能力评估

（1）对云服务平台所处的机房物理与环境保护能力进行检查或评估，确保云服务商机房位于中国境内并符合国家标准规范，机房是否采取监控措施以确保最低限度的人员物理接触。（物理安全，数据境内存储）

（2）检查云服务商或组织自身是否建立风险评估体系和监控目标清单，从而确保在威胁环境发生变化时，对云计算平台定期进行风险评估,确保云计算平台的安全风险处于可接受水平，并监控目标清单,对目标进行持续安全监控，在发生异常和非授权情况时发出警报。（风险管理，安全监控）

（3）检查云服务商是否接受云租户以外的第三方运行监管，并定期开展云安全审计，并向组织或社会定期公布安全审计报告。（第三方安全监管，云安全审计）

（4）检查云服务商是否建立针对云计算平台设施和软件维护所使用有效控制维护机制并具备相关能力，包括制度、工具、技术、人员及能力。（云安全监控）

（5）检查云服务商是否提供通用的安全控制措施，以及针

对组织特定的应用需要及服务模式，提供专用的安全控制措施，并制定每个应用或服务的安全计划。（通用安全控制措施，专用安全控制措施）

（6）检查云服务商是否提供开放接口或开放性安全服务，允许组织接入第三方安全产品或在云平台选择第三方安全服务，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。（第三方安全产品接入）

（7）检查云服务商的云服务平台是否通过安全测试及国家等级保护认证，以及其供应商通过安全测评，从而对其安全措施的有效性进行验证和评估，并检查相关资质证书和安全检测报告，必要时须向组织提交供应商清单。（安全测试评估，等保安全测评，产品及服务安全检查）

（8）检查云服务商是否为云计算平台制定应急响应计划并具备容灾恢复能力，建立必要的备份与恢复设施和机制应急响应与灾备。（应急管理与应急处置）

（9）检查云服务商的对外沟通渠道与方式，从而确保其具备在发生供应链安全事件信息、威胁信息、重大或紧急变更时能及时传递给组织。（应急沟通）

3. 云安全控制措施责任的识别

检查在公有云环境下，组织是否根据采用的服务模式（IaaS、PaaS、SaaS），明确云服务提供商与自身所承担的安全责任，

以及是否有能力采取相应的控制措施，如通用安全控制措施、专用安全控制措施和混合安全措施。（安全控制措施）

4. 云服务合同及保密协议签署

检查组织与云服务商是否签署服务合同，以及合同内容中是否包括：双方的安全责任和义务；客户方就云计算服务的安全功能要求、强度要求、保障要求、保密要求；云服务商应遵从的安全技术和管理标准；服务级别协议（SLA）及具体的参数，并对涉及术语、指标、管理范围、职责划分、访问授权、隐私保护、行为准则进行确定；约定提供给云服务商的数据、设备等资源，以及云计算平台上客户业务运行过程中收集、产生、存储的数据和文档等都属客户所有，云服务商应保证客户对这些资源的访问、利用、支配等；约定利用云服务商平台或与云服务商合作开发创造出成果（软件、信息和计算成果）的所有权、使用权等归属问题；约定云服务商不得依据其他国家的法律和司法要求将客户数据及相关信息提供给他国政府及组织；未经客户授权，不得访问、修改、披露、利用、转让、销毁客户数据；在服务合同终止时，应将数据、文档等归还给客户，并按要求彻底清除数据。如果客户有明确的留存要求，应按要求留存客户数据；采取有效管理和技术措施确保客户数据和业务系统的保密性、完整性和可用性。提供客户有效的安全监管、服务质量下降及应急处置的沟通渠道；约定当发生安全事件并造成损失时

对客户的经济赔偿；不以持有客户数据相要挟,配合做好客户数据和业务的迁移或退出；发生纠纷时,在双方约定期限内仍应保证客户数据安全；合同终止的条件及合同终止后云服务商应履行的责任和义务；若云计算平台中的业务系统与客户其他业务系统之间需要数据交互,约定交互方式和接口;云计算服务的计费方式、标准,客户的支付方式等；安全审计的支持与报告。

检查组织是否对可访问客户信息或掌握客户业务运行信息的云服务商签订保密协议，以及对能够接触客户信息或掌握客户业务运行信息的云服务商内部员工与其签订保密协议,并作为合同附件，保密协议应至少包括：合规要求、敏感信息披露、发现与报告、保密协议的有效期。

## 三、云服务平台开发测试与交付审计

### （一）业务概述

组织部署云服务平台可根据自身的能力，可选择自建、二次开发或完全采购。因此，对该生命周期的检查，重点在于检查组织是否建立完善的开发、测试和验收的管理流程，从而确保在云服务平台交付后得以稳定运行。

若组织直接从云服务商处采购的云服务不涉及二次开发，则该项审计内容可不予考虑。

### （二）审计目标和内容

1. 云平台开发规划

该控制项旨在检查组织进行云服务平台开发建设时，是否将开发测试安全与平台安全规划纳入到整体规划建设方案当中，并提前制定平台开发的质量管理、变更管理、测试与验收以及开发全过程安全监控等相关规范文档。

2. 开发安全风险管理

该控制项旨在检查组织进行云服务平台开发建设时，是否实施平台开发安全风险管理，并将其集成到系统开发各生命周期活动中。

3. 安全测试与培训

该控制项旨在检查组织在进行云服务平台开发建设时是否制定相关的平台测试计划和规程，并对其进行安全测试和平台交付前的安全培训。

### （三）常见问题和风险

1. 云服务平台规划与设计未同步考虑安全功能需求，导致安全整体保护能力不足。

2. 云上应用的相关安全需求、安全架构和安全设计规范缺失，不利于落实各项安全要求，安全与功能建设未实现同步管理。

3. 组织的云计算服务平台由外部服务商进行开发建设时，未定义针对其安全措施有效性的持续监控计划，可能导致持续监控失效的风险。

4. 云服务平台的安全测试与培训不到位，未发现潜在的安全漏洞，一旦漏洞被利用，可能造成云平台重要数据泄露。

（四）审计的主要方法和程序

1. 平台开发规划

（1）检查组织是否制定云服务平台设计规范、安全架构以及涉及开发过程的安全策略与规程等相关文档,其应定义各项安全功能、 机制和服务如何协同工作，以提供完整一致的保护能力，并查看其是否定义各阶段的信息安全角色及相应责任人。

（2）检查组织在进行云计算服务系统开发时，是否制定安全策略与规程等相关文档，以及是否定义了系统生命周期,（如规划阶段、设计阶段、实施阶段、运维阶段、废止阶段等），并提出各阶段信息系统和服务的安全需求、安全架构和安全设计规范，并检查系统规划文档、系统设计说明书。

（3）检查系统开发安全策略与规程等相关文档，是否定义了在系统生命周期中使用的系统工程方法、软件开发方法、测试技术和质量控制过程，检查开发测试文档、变更文档。

（4）检查组织云计算服务平台由外部服务商进行开发建设时，是否定义了针对其安全措施有效性的持续监控计划，并检查持续监控计划的详细程度。

（5）检查系统开发安全策略与规程等相关文档,是否对开发的环境和预期运行环境、验收准则及强制配置要求等进行了

描述，并检查云计算平台信息系统、组件或服务开发清单中的相应管理文档。

2. 开发安全风险管理

（1）检查系统开发安全策略与规程等相关文档，查看其是否有将信息安全风险管理过程集成到系统开发各生命周期活动中的要求，并访谈相关安全负责人，了解风险管理的落实情况。

（2）访谈相关安全负责人，询问组织是否对开发商说明的系统功能、端口、协议和服务进行必要的风险评估,并基于该评估结果禁用不必要或高风险的功能、端口、协议或服务。

3. 安全测试与培训

（1）检查组织或云服务平台开发商是否制定测试计划与测试规程等文档，查看其是否定义了在单元、集成、系统以及回归测试或评估时应执行的深度和覆盖面，并检查云计算服务系统的测试报告及代码安全审查。

（2）检查是否对云服务平台部署前进行渗透测试和安全评估，了解其存在的脆弱性和威胁，并检查测试和评估报告是否出自独立第三方。

（3）检查系统开发安全策略与规程等相关文档，查看其是否定义了开发商需提供的有助于正确使用所交付系统或产品中的安全功能、措施和机制的培训，是否要求开发商提供所定义的培训，并检查相关培训记录。

## 四、云计算平台的安全管理审计

### （一）业务概述

是指云计算平台的安全合规管理，信息安全等级保护检查测评及其他安全规范遵循工作。

### （二）审计目标和内容

1. 合规识别与制度制定

该控制项旨在检查组织是否准确识别与云计算相关的安全合规要求，如数据安全、数据存储等内容，同时制定云服务平台安全管理的规章制度及安全监督指标。

2. 云服务安全管理角色及责任

该控制项旨在检查组织在其内部是否识别并定义云服务管理的角色及其安全职责，特别关注是否涉及与客户、云服务提供商共同确定的涉及云计算服务的安全职责，同时检查职责设置的合理性。

3. 信息安全等级保护落实检查

该控制项旨在检查组织部署的云服务平台是否依据等保要求定级备案，并定期开展等保的落实检查工作。

4. 资源保障

该控制项旨在检查组织是否为云服务平台的开发部署和后期运行从制度层面提供保证机制并检查工作的落实情况。

### （三）常见问题和风险

1. 云服务平台安全管理策略与制度不健全，无法有效发挥安全监督作用。

2. 云服务安全管理角色及责任定义不清晰，无法有效落实云平台安全管控要求。

3. 未定期开展信息安全等级保护检查，无法及时发现现有控制措施与等保的差距，同时存在合规风险。

**（四）审计的主要方法和程序**

1. 合规识别与制度制定

（1）检查组织是否制定了云服务平台安全管理的规章制度，查看其内容是否至少包括云服务平台的安全制度与策略、安全组织与人员的相关规程、评审和更新信息安全规章制度的频率。

（2）访谈系统安全负责人、外部服务提供商、开发商或客户等内外部相关人员，询问传达信息安全规章制度的情况，信息安全规章制度的评审和更新的情况，并检查是否按要求进行了信息安全规章制度的评审和更新。

（3）检查组织是否收集和整理相关的法律、法规、政策和标准要求,并形成合规文件清单。

2. 云服务安全管理角色及责任

（1）调阅安全组织与人员策略与规程等相关文档,查看是否明确岗位信息安全职责要求,定义需进行分离的关键职责从而满足关键职责分离要求。

（2）访谈系统管理员、账号管理员或安全管理员等相关人员,询问通过访问控制措施进行职责分离落实的情况。

（3）检查岗位信息安全职责的相关文档，查看其是否有与客户和云服务提供商共同确定涉及云计算服务的安全职责。

（4）检查组织是否对已确立的责任，包括组织自身、客户和云服务提供商进行监管与检查，从而确保安全责任的落实。

3. 信息安全等级保护落实检查

（1）检查组织是否基于已部署的云服务平台上存储数据和运行的重要性及受到侵害的程度对其进行等保定级。

（2）检查组织是否基于云服务平台的等保级别定期开展等保落实检查工作，并调阅相关检查文档。

4. 资源保障

（1）查阅组织的云服务管理制度文档，检查是否有为云服务平台开发部署和后期运行提供资源保障的承诺描述。

（2）检查工作计划、预算管理过程文档，查看是否有为保护信息系统和服务提供所需资源( 如有关资金、场地、人力等) 的项目。

（3）访谈信息安全负责人或系统安全负责人等相关人员，询问为保护信息系统和服务所需资源的落实情况。

## 五、云计算平台的迁移与部署审计

### （一）业务概述

是指组织根据自身的安全需求和云计算服务的安全能力要求，制定云计算服务迁移与部署计划并加以实施，确保数据和业务可以安全地向云计算平台进行迁移与部署。

### （二）审计目标和内容

1. 迁移计划

该控制项旨在检查组织在进行云服务平台迁移、部署前是否制定完善的迁移方案并对迁移过程可能产生的风险进行分析并制定应对方案，从而为后期执行迁移部署提供保证。

2. 平台迁移测试与部署

该控制项旨在检查组织是否依据已制定的迁移方案进行部署前的测试，并在部署完成后进行云服务平台的运行测试，从而保证云服务平台满足既定的各项服务指标。

### （三）常见问题和风险

1. 未制定迁移部署方案或未严格执行迁移部署方案，导致迁移失败或迁移过程中业务中断和数据丢失。

2. 未开展针对迁移部署过程的风险分析，无法根据识别出的风险制定应对方案和回退策略。

3. 云服务平台部署后，未依据既定的验收标准对平台的功能、性能和安全性进行测试，平台功能未满足预期要求并存在安全隐患。

### （四）审计的主要方法和程序

1. 迁移计划

（1）检查组织是否制定迁移部署方案（一次性迁移、阶段性迁移）和实施进度计划表，明确参与人员及职责，并查阅方案是否经过审批。

（2）是否制定迁移部署的培训计划并对参与人员进行相关培训。

（3）是否开展针对迁移部署过程的风险分析，如数据丢失、业务中断、部署过程中组织客户数据和资源权限的泄露等，并根据识别出的风险制定应对方案和回退策略。

2. 平台迁移测试与部署

（1）检查组织是否根据事前制定的平台迁移测试计划，组织技术力量或委托第三方对云服务平台的迁移（包括数据和系统）进行部署前的测试，查看测试评估报告和整改建议并检查具体整改措施的执行情况。

（2）检查组织是否采取技术手段，确保迁移前后数据的完整性与保密性，并调阅数据完整性测试报告。

（3）检查组织在云服务平台部署后，是否依据既定的验收标准和监控指标对平台的功能、性能和安全性进行监控与测试，在满足要求后投入运行，并调阅运行验收测试报告。

## 六、云计算平台的安全运维审计

### （一）业务概述

云平台投入运行后，虽然客户将部分控制和管理任务转移给云服务商,但最终安全责任还是由客户自身承担。因此需要对自身的云计算服务运维进行良好的安全管理。

### （二）审计目标和内容

1. 网络与通信安全

该控制项旨在从两种视角，针对网络与通信安全，检查组织或云服务商是否采取有效的措施，保证云服务平台的安全，包括实施物理和虚拟网络及主机的安全区域划分、安全隔离、安全防护，并采取管理和技术措施确保网络与通信的安全性和可用性。

2. 身份鉴别

该控制项旨在检查组织或云服务提供者是否在云计算环境中，针对云用户、租户和管理员采取多种身份鉴别手段，并确保在系统整个生命周期内用户标识的唯一性，以及对主机、虚拟机监视器和管理平台采用证书技术，确保证书的可信度和系统的抗抵赖性，检查整个身份鉴别机制的相关配置是否受到统一控制。

3. 访问控制

该控制项旨在检查组织或云服务商是否针对物理资源、虚拟资源、网络与通信和用户与管理员制定相应的访问控制策略并据此执行。

4. 恶意代码与入侵防范

该控制项旨在检查组织或云服务商的云服务平台是否具有从基础设施层到资源抽象层的区域边界和恶意代码防护功能，并部署相应的产品；是否制定恶意代码库的升级策略并主动进行更新，并对恶意代码进行自动检测、防范和响应。

5. 应用与数据安全

该控制项旨在检查云服务商或组织是否采取措施对云服务平台涉及的重要数据进行有效识别和分类，并从平台数据静态存储、动态传输与数据调用等三方面，检查是否采取措施确保数据的机密性和完整性，以及为确保已识别出的重要数据的可用性采取备份与恢复措施，同时检查云服务平台对外接口的安全性。

6. 安全监控与审计

该控制项旨在检查组织或云服务商是否对云服务平台制定安全监测的制度规范与策略，明确安全监控指标和监控对象，至少应包括资源类、安全事件和操作行为，并就云服务平台的运营管理开展安全审计。（建立日志留痕记录）

（三）常见问题和风险

1. 云计算服务系统安全区域划分不合理，导致安全要求覆盖不全面，存在安全风险隐患。

2. 云计算服务系统未部署流量检测和清洗设备，无法对异

常流量的监控和统计分析，受异常流量影响，导致网络不可用。

3. 云计算服务系统身份鉴别机制不严格，导致身份认证机制被绕过，造成重要数据或敏感信息的泄露。

4. 云计算服务系统审计功能未开启或审计日志未定期查看，无法及时发现存在的违规操作或风险隐患。

**（四）审计的主要方法和程序**

1. 网络与通信安全

（1）查阅网络拓扑图，并访谈安全管理人员，了解组织或云服务提供商是否对云计算服务系统根据业务安全需要对平台资源层、服务层和应用层进行安全区域的划分，并在安全边界进行隔离防护，同时，云租户之间及租户内部也应根据安全业务需要、等级保护原则和业务生命周期进一步划分安全区域，制定各区域的安全策略并部署隔离防护设施，从而实现网络隔离和虚拟机之间的隔离。（区域边界划分、网络安全隔离与防护、虚拟安全域划分）

（2）检查虚拟机监视器、云管理平台，查看同一宿主机内虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控，并查看不同宿主机的虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控。（流量监管）

（3）检查网络架构、配置策略和云管理平台，查看是否实现管理流量和业务流量的分离，以及云平台管理流量与云租户

业务流量的分离。（流量分离）

（4）检查云服务提供商或组织是否对云计算系统各组成部分之间、虚拟机之间、云计算系统内部通信网络，通过通信完整性校验、密码技术和 VPN 技术确保网络和通信的完整性与安全性。（网络安全性）

（5）检查云服务提供商或组织是否部署流量检测和清洗设备，实现对异常流量的监控和统计分析，防止因异常流量造成的网络不可用。（网络可用性）

（6）查阅网络拓扑图，检查服务商或组织对网络是否采用冗余技术，对关键链路、主要物理网络设备、虚拟网络设备、网络核心和汇聚层等部署冗余设备，并根据租户、主机和应用的业务重要程度，划分对应的网络带宽优先级，从而确保网络的可用性。（网络可用性）

2. 身份鉴别

（1）检查组织是否制定身份认证和账号策略，包括用户身份与终端绑定、完整性验证检查、账号锁定、账号时效、禁止重复登录等策略,并采取两种及两种以上组合机制对用户身份进行验证，对系统管理员和安全管理员是否采用单点登录的集中用户验证机制。（单点登录、集中用户认证）

（2）检查用户的验证信息是否加密存储，限制登录口令最小长度和更换周期。

（3）检查云管理平台，在进行远程管理时，是否对管理终端和云平台边界设备之间建立双向身份验证机制（如证书、共享密钥等），并限制访问重要物理资源及虚拟资源、安全管理中心的远程登录地址。（远程登录身份认证）

（4）检查网络策略控制器和网络设备（或设备代理）之间是否建立双向身份验证机制，并验证网络设备防护能力是否符合要求。（设备间的身份鉴别）

3. 访问控制

（1）检查服务商或组织是否基于系统业务类型、重要性或信息的重要程度，根据安全域的划分，制定访问控制策略，并检查不同安全等级网络区域边界访问控制机制部署情况及访问控制规则，从而判断针对边界访问控制机制或边界访问控制设备、不同虚拟机间访问控制、虚拟机迁移是否得到有效控制。（网络访问控制，虚拟资源访问控制）

（2）检查服务商或组织是否对特权用户、系统管理员、用户和云租户依据“最小授权”原则和“职责分离”原则进行访问控制权限的设置。

（3）检查服务商或组织是否对包括用户、访问协议实现对云服务平台的网络设备访问进行控制。

（4）检查服务商或组织是否制定并部署针对虚拟机和多租户的访问控制策略，并允许租户在自身虚拟机上部署各自的访

问控制策略，或通过在虚拟机监视器上集中部署访问控制策略。（虚拟化和多租户访问控制）

4. 恶意代码与入侵防范

（1）检查云服务提供商或组织内部是否制定恶意代码和入侵防范系统特征库的更新策略，并检查恶意代码版本和入侵防范系统特征库是否与其服务提供商的最新版本相一致。

（2）检查恶意代码防护系统是否采取集中管理、统一部署的方式，可自动对恶意代码感染及其在虚拟机之间的蔓延进行检测和告警，并在监测到破坏后进行修复，同时为确保虚拟机安全系统建立恶意代码传播路径的追踪和安全隔离。（恶意代码防范）

（3）检查恶意代码保护和入侵防范的对象，在基础设施层到资源抽象层是否针对包括宿主机和虚拟主机以及虚拟机监视器和云管理平台。

（4）检查云服务提供商或组织内部是否在（高风险）区域边界和关键网络节点处部署恶意代码防护系统，从而实现对终端、web 应用、邮件系统、数据库、中间件、网络虚拟化软件、虚拟机监视器或云管理平台恶意代码检测与清除，特别是虚拟服务器之间数据交换和云终端接入通信。

（5）检查云服务提供商或组织内部是否在区域边界、关键业务系统采取相关技术措施，根据风险大小，在其附近部署入

侵检测与防范系统，从而实现对用户行为、恶意流量、恶意攻击、恶意扫描及异常流量和未知威胁的识别、监控、防护，同时对上述活动进行数据收集、存储和分析。（入侵防范）

（6）检查部署的入侵检测与防范系统日志，审计日志记录内容是否与审计信息相关及是否受到安全保护和定期备份，防止非预期的修改、删除和覆盖，并检查云服务提供商或组织是否对日志进行关联分析并进行关联响应。

5. 应用与数据安全

（1）检查组织是否制定针对云服务平台对外接口的安全策略，并检查接口设计文档或开放性服务技术文档，查看是否符合开放性及安全性要求。

（2）检查组织是否对云服务平台对外接口进行渗透测试或代码审计并调阅测试或审计报告，从而验证是否存在安全漏洞或安全隐患。

（3）检查云服务商或组织是否针对系统管理数据（如镜像文件、快照）、鉴别信息和重要业务数据，在存储、传输过程（包括云计算系统内部和虚拟机之间的通信）中，使用具有完整性校验和加密的技术与工具进行完整性校验，从而防止在存储和传输过程中遭到破坏、恶意篡改和泄露，并对不一致的数据进行恢复。（镜像与快照保护）

（4）检查是否采用完整性校验算法和工具防止被恶意篡

改。

（5）检查云服务商或组织是否使用统一的调用接口，对存储和使用环节的数据进行完整性检查。

（6）检查云服务商或组织对上层提供接口、操作云服务控制平台、向云主机或云存储系统及数据库传输数据是否采用加密技术，包括加密协议、算法。

（7）检查云服务商或组织是否针对云服务系统涉及的本地数据、在线数据、重要业务信息及软件系统，根据重要程度和数据敏感性，制定分类分级策略及相应的备份恢复策略，对不同等级的数据进行备份与恢复。

（8）检查是否制定并实施针对虚拟资源数据级、系统级和应用级的冗余备份。

6. 安全监控与安全审计

（1）访谈系统安全负责人，询问制定哪些相关策略从而对安全措施有效性进行持续监控，并检查云平台对安全措施有效性进行持续监控，监控应至少包括漏洞与补丁监控、宿主机监控、网络监控、用户/租户/管理员的操作行为监控、网络安全事件监控和系统行为监控。（安全监控）

（2）检查审计策略与规程等相关文档，查看是否可对上述监控对象进行审计，并定义可（连续）审计事件，是否制定并维护该审计事件清单，及是否定义了需连续审计事件的审计频

率。（连续性审计）

（3）检查审计范围是否包括重要用户行为、系统安全事件、数据库行为、虚拟机的迁移、虚拟资源申请、虚拟资源调度、虚拟资源分配、虚拟资源异常使用和重要命令进行安全审计，以及是否可以实现集中审计或第三方审计。

（4）检查审计策略与规程等相关文档，查看是否对审计记录内容提出要求，应至少包含:事件类型、事件发生的时间和地点、事件来源、事件结果以及与事件相关的用户或主体的身份等相关信息，并检查日志的存储安全和存储周期是否符合审计策略与规程。

（5）检查审计策略与规程等相关文档，查看是否建立了与其他组织针对安全审计的协调机制。（外部审计协调）

（6）检查组织是否根据不同的审计对象部署审计产品，并登录查看审计功能是否开启并基于审计策略进行配置，查看审计记录是否包含所规定的审计内容。

（7）检查审计记录存储容量配置信息，查看是否按照要求配置了相应的存储容量。

（8）检查审计策略与规程等相关文档，查看是否定义了当审计过程失败时接收报警信息的人员（角色）清单。

（9）检查审计系统配置信息，查看是否有系统审计过程失败的报警机制，并访谈云服务商定义的人员或角色，询问接收

到审计失败告警信息的情况和处理机制与流程。

（10）检查审计策略与规程、系统设计说明书等相关文档，查看是否提供审计处理和审计报告生成的机制，以及是否支持实时或准实时的审查、分析和报告，并对安全事件的事后调查。

（11）检查审计策略与规程等相关文档，查看是否定义了在线保存审计记录的时间段，是否要求支持安全事件的事后调查，是否要求符合法律法规及客户的信息留存的要求，并检查记录留存的时间配置信息，查看是否与定义的时间段一致。

## 七、服务关闭与数据迁移审计

### （一）业务概述

是指组织在云服务关闭与数据迁移前应当制定关闭当前云服务平台或向其他云服务平台迁移时相关流程，从而确保组织完整退出当前云服务阶段，同时确保原云服务商的相关责任和义务得到履行。

### （二）审计目标和内容

1. 关闭和迁移规划

该控制项旨在检查组织是否就云服务平台关闭及其所涉及的平台数据迁移制定相应的规划方案和应急预案，从而确保数据迁移的妥善执行以及服务的连续性、可用性。

2. 数据迁移及完整性和保密性保障

该控制项旨在检查组织在云服务平台关闭时所进行的平台

数据迁移操作是否有效确保组织数据的完整性和保密性。

（三）常见问题和风险

1. 原有云平台上存储的数据完全未返回组织或执行彻底清除程序，导致残留数据泄露。

2. 未制定云平台数据迁移和资料移交清单，导致迁移数据不完整或资料不全面，影响迁移效果，也不利于迁移资料的规范化管理。

（四）审计的主要方法和程序

1. 关闭和迁移规划

（1）检查组织是否制定云服务平台关闭及其数据迁移的规划、方案、流程，从而确保平台数据和业务的可用性、连续性，如是否制定回退方案和应急预案等。

（2）检查组织是否对回退方案或应急预案进行测试并调阅测试报告。

2. 数据迁移及完整性和保密性保障

（1）检查组织是否制定平台数据迁移和资料移交清单，包括客户移交给云服务商的数据和资料，以及客户业务系统在云计算平台上运行期间产生、收集的数据以及相关文档资料，如数据文件、程序代码、说明书、技术资料、运行日志等。

（2）检查组织是否为确保迁移数据的完整性和保密性而采取相应的措施。

（3）调阅组织平台数据迁移的历史记录和迁移数据完整性、有效性测试报告。

（4）调阅原有云服务合同，了解组织对于原云服务商平台数据存储的时限要求和删除要求，并查阅相关数据删除与介质销毁的历史记录，判断是否符合组织数据与介质销毁的服务要求。

## 第五节　数据安全审计

伴随互联网、云计算、移动互联网等新技术的迅猛发展，无处不在的移动设备、无线传感器等设备以及数以亿计的互联网用户和企业产生的消费数据及经营数据使得各类信息呈现爆炸式增长。同时，数据的高度集中，共享开放和交叉使用以及数据流动的趋势也在不断加剧。组织由于数据管理、安全隔离、访问控制及数据加密等措施不充分而面临的网络入侵和信息泄露风险越来越大。

一旦数据的机密性、完善性和可用性受到损害，将不能支撑组织业务的健康运行；随着网络安全法的实施，国家对重要业务数据和个人敏感信息保护的力度也在加强，数据安全的违规成本已越来越高。因此，数据安全是数字经济时代生产力要素的必要属性，持续性开展数据安全审计已成为信息系统审计的重要内容。

本节所涉及的数据包括了日常数据和大数据（按结构化程度和数据规模）、个人信息和重要数据（按数据对象类型）的相关内容。本节将从数据安全治理、数据安全管理、数据生命周期安全管理、个人信息安全管理、重要数据安全管理、数据平台与技术安全管理等方面对数据安全的审计方法和步骤进行描述。

## 一、数据安全治理审计

### （一）业务概述

数据是指对客观事件进行记录并可以鉴别的符号，是对客观事物的性质、状态以及相互关系等进行记载的物理符号或这些物理符号的组合。

数据安全风险涉及面较广，既体现在组织在治理层面的治理风险，还体现在数据在其生命周期和服务过程中的管理风险，以及伴随的个人信息和重要数据等敏感信息泄露和跨境流通风险。

### （二）审计目标和内容

1. 董事会的职责

该控制项旨在从组织的治理层面，检查组织是否将数据的安全治理工作纳入组织治理工作范畴，建立健全包括风险管理和数据安全审计监督在内的架构体系，从而完善数据的安全合规管理。

2. 战略规划与价值实现

该控制项旨在检查组织是否依据董事会所明确的数据安全治理目标制定相关的安全战略。

3. 数据安全合规管理

该控制项旨在检查组织是否基于数据安全战略规划，建立健全数据安全管理制度体系，满足合规监管要求。

4. 数据风险管理

该控制项旨在检查组织是否从数据、人员、产品与服务等方面，建立并完善数据安全风险管理体系，并将其纳入组织风险管理体系当中。

5. 数据安全审计监督

该控制项旨在检查组织是否将数据的安全审计工作纳入到组织的安全审计体系范畴内，建立并完善针对数据安全审计的专项工作。

（三）常见问题和风险

1. 未建立数据安全治理组织架构及职责，无法自上而下推动相关数据安全治理工作的有序开展。

2. 未建立组织级数据战略规划，无法有效覆盖网络安全法及等级保护等相关法规与标准的要求，无法指明数据整体的发展目标和规划，不利于数据长远发展。

3. 未制定数据安全相关管理制度及流程，导致数据安全管

控要求无法有效落实。

4. 数据安全风险评估执行不到位，未识别出重要的数据安全风险，不利于数据安全治理体系的持续优化。

**（四）审计的主要方法和程序**

1. 董事会的职责

（1）检查组织董事会和执行管理部门职责，是否将数据安全治理工作纳入到组织综合治理工作范畴当中，明确数据安全治理职责并对其安全治理予以承诺和支持，从战略、组织、架构和实施等多个环节提供保障。

（2）查阅组织数据治理的规章制度，明确数据安全治理需要达到的目标和定位，判断其治理目标是否与组织战略、业务战略、业务目标、业务需求相一致。

（3）检查组织是否建立跨部门的数据安全管理委员会和风险管理委员会，明确安全治理的角色和责任。

（4）检查组织是否建立基于满足业务战略的数据架构，并进行持续的评估、监督和改进。

（5）访谈组织信息科技治理负责人，了解组织是否已经或即将部署云服务平台，以及是否将基于云平台中的数据安全治理列入主要治理目标和任务当中。

2. 战略规划与价值实现

（1）访谈战略规划负责人或查阅组织经营战略规划，判断

数据战略规划是否满足经营战略需要。（经营战略一致性）

（2）查阅组织数据战略规划，判断其战略内容是否与组织数据治理目标相一致，检查内容上是否包括数据服务战略、数据平台与应用战略，且战略规划内容是否涉及数据安全，体现《网络安全法》和网络安全等级保护等制度对于数据安全的相关要求。

（3）访谈信息系统战略规划负责人，了解组织信息化及信息安全战略规划要求，判断数据安全战略是否与信息系统安全战略和需求相一致。（信息系统安全战略一致性）

（4）查阅数据安全战略规划，判断其从内容上是否体现组织对于个人信息（隐私）保护和重要数据保护治理方面的要求。

3. 数据安全合规管理

（1）查阅组织制定的与数据管理相关的制度与规范，从而判断其是否符合数据安全相关的政策、法律、法规等各项监管要求。

（2）检查组织的数据安全管理相关制度与规范，查看其内容是否涵盖国家和社会生产的重要数据的安全管理要求，个人信息的保护要求，数据跨境传输与共享的安全管理要求，以及密码使用要求。

4. 数据风险管理

访谈组织风险管理负责人，询问组织是否将数据风险管理

纳入组织风险管理体系当中，重点突出数据、人员、产品/服务三个方面，并建立数据安全内控体系；数据方面，以数据生命周期为出发点，识别全周期面临的威胁和自身脆弱性，分析数据服务安全风险和应对措施需求；人员方面，基于数据安全管理需要，基于员工日常数据操作行为，识别风险并建立风险量化机制和信息安全评价指标体系；产品/服务方面，以对个人信息和重要数据保护为目的，构建产品/服务提供商在组织、规范、设计、流程、监控等一系列的安全风险评价体系和控制机制。

5. 数据安全审计监督

（1）访谈组织审计负责人，询问组织是否将数据安全管理审计纳入到组织安全审计管理体系内。

（2）访谈组织审计负责人或信息安全审计负责人，了解组织是否建立负责数据安全监督与审计管理的职能机构及制度与规范，了解组织对数据服务及其用户操作行为审计的方法和内容。

（3）查阅组织有关数据安全审计的制度和规范，了解针对数据安全审计的方法、频率和周期，并查阅相关审计报告。

## 二、数据安全管理审计

### （一）业务概述

数据安全管理是指保护数据免受威胁的影响，确保业务的连续性，降低业务可能面临的风险，为业务部门提供有力保障。

（二）审计目标和内容

1. 数据安全组织管理

该控制项旨在检查组织为落实数据安全治理工作及其战略规划，是否从组织层面设置跨部门的数据安全管理机构及负责人，明确安全管理职责。

2. 人员与意识管理

该控制项旨在基于组织对数据安全管理的要求和需求，从人员安全管理、资源建设与技能培养、职责落实与考核等三方面进行检查，判断人员综合管理的落实情况。

3. 制度与规范管理

该控制项旨在从制度层面检查组织是否制定并完善数据安全管理的制度体系及其落实情况。

4. 元数据安全管理

该控制项旨在从元数据的安全管理角度，检查组织是否建立完善的元数据安全管理规范，并从技术层面予以安全保障。

5. 数据及平台（系统）管理

该控制项旨在从数据平台（系统）管理角度，检查组织是否对平台（系统）及其管理之下的数据制定相应的安全规范与标准，实现统一管理，并与组织经营战略中的安全需求相一致。

6. 服务接口安全管理

该控制项旨在从服务接口角度，检查组织是否完善接口安

全管理的制度和规范，并用技术手段保障接口间数据传输的安全性。

7. 数据供应链安全管理

该控制项旨在从供应链安全管理角度，检查组织在存在上下游数据交换的前提下，制定相关管理规范，满足合规监管要求。

8. 数据安全审计管理

该控制项旨在从审计角度，检查组织是否落实数据安全审计与监督的要求，对组织的数据服务开展安全审计，同时确保国家对于日志管理的安全合规要求。

（三）常见问题和风险

1. 数据安全组织架构及责任人缺失，导致数据安全管控要求无法落实。

2. 未定期开展数据安全意识宣贯，由于安全意识不足，导致数据不经意的泄露。

3. 元数据安全管控不到位，导致元数据血缘关系模糊、可追溯性不强，影响元数据与数据标准的结合。

4. 未部署数据管控平台，无法对数据标准、数据质量、元数据进行规范化管控和技术实现。

5. 数据服务接口与应用在其内部跨安全域间的接口调用未采用包括安全通道、加密传输等安全机制可能带来的风险。

6. 未建立数据供应链安全管理方针，无法落实上下游供应链间数据交换和使用的要求，不利于供应商之间的数据交换与共享。

**（四）审计的主要方法和程序**

1. 数据安全组织管理

（1）访谈组织人力管理部门或信息安全管理部门负责人，了解组织是否设置专门的数据安全管理机构和责任人及其相关的部门和岗位。

（2）访谈数据安全管理机构负责人，了解组织目前是否制定与数据安全相关的包括数据服务安全追责在内的规章制度，并定期对责任部门和安全岗位组织安全检查，形成检查报告；组织目前数据及其服务平台与应用的安全规划、安全建设、安全运营和系统维护工作整体情况；组织是否清楚地界定服务提供者、数据使用者（包括终端用户与设备）；是否设置专职的数据服务安全岗位，建立规范化的数据服务安全保护、评估及考核专职队伍。

2. 人员安全管理

（1）访谈人力资源管理和数据安全管理负责人，了解组织是否基于数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施，制定数据服务人力资源安全策略。

（2）访谈数据安全管理负责人，了解是否明确数据服务相

关重要岗位及其角色安全要求，建立重要岗位角色清单和授权机制。

（3）访谈人力资源管理负责人，是否就数据安全管理的关键岗位做好人力资源培养和储备工作。

（4）访谈人力资源管理负责人，是否在组织内部针对所有接触个人信息和重要数据等敏感信息的全职员工签署保密协议，知晓组织对于数据安全管理的规范制度与操作须知，并抽检保密协议和制度知晓的记录。

（5）访谈人力资源管理负责人，了解组织是否建立第三方人员安全管理制度，对接触个人信息、重要数据等数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查，并调阅相关管理制度、保密协议和历史审批与登记记录。

（6）检查组织是否建立数据安全教育培训机制，分别针对数据操作人、数据安全管理人员和第三方人员制定培训计划，并定期对全员，特别是关键岗位人员进行能力检查和考核，考核应纳入到个人与组织的绩效考核体系当中，查阅教育培训与考核的历史记录。

3. 制度与规范管理

（1）调阅并检查组织是否制定包括数据服务在内的数据安全管理制度和规范、数据分类分级规范和标准、数据安全人员

能力要求及向第三方提供或共享数据时的安全管理制度和标准，其中，制度在范围上应覆盖数据全生命周期。

（2）检查制度和标准是否得到定期评审和更新，并分发至机构数据服务部门和操作人员，抽样访谈数据操作和管理人员，了解其对制度规范的知晓情况并查阅制度规范的更新记录。

4. 元数据安全管理

（1）检查组织是否建立与数据服务相关的元数据及其管理规范、与数据服务安全架构相应的安全元数据管理规范和数据访问控制策略，从而明确元数据管理角色及其授权控制机制和查询限制。

（2）检查元数据的安全管理制度和规范是否包括：依据资产分类分级策略所建立的元数据安全属性的自动/手工分级机制；可依据元数据安全属性建立标记的策略及标记定义和管理机制。

（3）检查组织是否从技术手段上实现：对表字段、表与上下游表的血缘关系查询进行安全设置和查询限制。可对表访问操作权限进行限制。

（4）检查组织是否建立针对元数据操作的审计制度，并确保对元数据的操作具有可追溯性。

5. 数据及平台（系统）管理

（1）检查组织是否建立数据资产安全管理规范和数据资产

分类、分级方法、标准、操作指南、数据资产分类分级变更审批流程，并对其进行定期审核和更新。

（2）检查组织是否对数据资产实施登记制度，其应明确数据资产管理相关方及管理责任、数据资产管理范围和属性，并调阅数据资产登记目录清单。

（3）检查组织是否在技术上建立综合的数据管理平台或系统，实现对数据资产的统一管理，包括：是否制定数据系统平台资产安全管理规范，并明确安全管理的目标和原则；数据系统平台的规划和建设应与组织经营战略和平台（系统）全生命周期的安全需求相一致。可依据数据资产和数据主体安全分级要求建立相应的标记策略、访问控制、数据加解密、数据脱敏等安全机制和管控措施。

6. 服务接口安全管理

（1）检查组织是否制定与数据服务接口安全管理有关的控制策略和安全规范。

（2）检查组织的数据平台与应用在其内部跨安全域间的接口调用是否采用包括安全通道、加密传输等安全机制。

7. 数据供应链安全管理

（1）访谈组织数据管理部门负责人，了解组织目前是否存在数据供应链上下游间数据交换和使用的现象，若存在，则了解并查看：组织是否建立与数据供应链安全管理有关的规范和

安全方针，其应明确数据供应链安全目标、原则和范围，并对其进行查阅；组织是否识别并建立数据供应链上下游间数据交换和使用的合规要求及合规目录，从而确保其数据交换和使用的合规；建立数据供应链目录和相关数据源数据字典，明确数据供应链的责任部门和人员。

（2）查阅组织与上下游数据供应链服务商签署的合作协议，检查协议是否：明确数据供应链上下游责任和义务,并检查是否采用安全技术保障措施确保数据供应链上下游对数据交换、使用的安全、可靠与合规；明确数据供应链中数据的使用目的、供应方式、保密约定等内容。

（3）检查组织是否对数据供应链上下游的数据服务提供者和数据使用者的行为进行合规性审核和分析，并查阅相关记录和报告。

8. 数据安全审计管理

（1）访谈组织负责数据审计的负责人，询问组织是否明确对于数据安全审计的要求、审计范围、审计方式。

（2）访谈组织负责数据审计的负责人，询问对数据服务平台（系统）部署审计产品，登录安全审计产品并查看审计日志是否完整，其保存期限是否符合国家强制要求并具有防篡改的功能。

（3）查阅历史审计报告，了解审计对象是否包括与数据相

关的物理环境、网络传输、平台/系统、数据库及存储介质，以及基于数据平台/提供者，数据提供者，服务提供者和内部服务/数据使用者针对主要操作、敏感行为、敏感数据流通等安全事件。

## 三、数据生命周期安全管理审计

### （一）业务概述

数据生命周期管理是指在数据采集、传输、存储、处理、交换（共享、应用）、销毁等阶段下对流动的数据进行综合管理。

### （二）审计目标和内容

1. 数据收集

该控制项旨在针对数据收集过程，检查组织是否依据收集数据的敏感性对其进行数据标识，从而基于该标识进行后续数据操作处理的监控。

2. 数据传输

该控制项旨在针对数据传输过程，检查组织是否根据传输过程的安全性划分安全域，并根据安全域的级别采取相应的安全控制措施，防范数据遭受窃听或泄露，确保数据的完整性。

3. 数据存储与恢复

该控制项旨在针对数据存储，检查组织是否对所存储的数据采取安全措施，确保其安全性和完整性，同时，根据组织对

于数据可用性的要求，检查组织是否采取备份措施。

4. 数据处理与加工

该控制项旨在针对处理和加工过程，检查组织是否对可接触到数据的人员基于角色采取身份验证和访问控制，并对该过程采取加密和脱敏处置措施，防范数据非法访问或敏感信息遭到泄露。

5. 数据使用与安全审计

该控制项旨在针对数据使用过程，检查组织是否采取身份验证和访问控制措施，防止人员对于数据的非法访问，并采取加密和脱敏等技术手段，防止在使用环节造成信息泄露并对使用环节进行安全审计。

6. 数据共享与流动

该控制项旨在针对组织存在数据共享与流动，特别是跨境流动时，是否制定相应的规范制度和审批流程，满足国家合规监管要求。

7. 数据归档与销毁

该控制项旨在检查组织是否针对数据归档与销毁过程，并基于数据敏感程度制定完善的管理制度与规范流程，防范在该过程中出现数据泄露。

（三）常见问题和风险

1. 在数据生命周期管理期间，由于在人员、管理、技术三

个层面没有建立适用的数据安全管理体系，使得数据安全管理的效率与效果低下。

2. 未实现数据分类分级管理或分级方法不合理，导致未按照不同类别建立不同的安全控制措施，导致保护过重或保护不当。

3. 数据在收集、传输、存储和恢复、处理和加工、使用与审计、归档与销毁等过程中，由于缺乏有效的数据加密和访问控制，容易导致数据泄露风险。

4. 数据在共享与流动，特别是跨边界和跨境流动时，由于未制定相应的安全规范制度和审批流程，容易产生违规风险。

5. 数据销毁机制不健全或执行不严格，导致销毁过程中敏感数据的泄露。

（四）审计的主要方法和程序

1. 数据收集

（1）检查组织是否根据数据分级分类管理制度中定义的数据类型、安全等级对所收集的数据进行标识，特别是敏感数据，并根据数据标识和合规要求进行后续传输、存储等流程的跟踪和监控。

（2）对收集的数据进行抽查，检查是否对已收集的数据进行标记。

2. 数据传输

（1）访谈网络安全管理员，询问组织是否在数据传输过程中进行安全域的划分。

（2）访谈网络安全管理员，询问数据在跨域传输，特别是在非安全域传输时是否采用安全加密机制确保传输链路的安全可靠和对数据进行安全加密，查阅组织网络拓扑图并进行实质性查验。

（3）通过执行渗透，获取传输数据包，查验数据包的完整性和保密性措施是否有效。

3. 数据存储与恢复

（1）访谈数据安全管理员，询问组织为确保静态数据的安全性和完整性所采取的安全措施、加密手段与方式、完整性校验手段与方式有哪些。

（2）访谈组织核心业务部门负责人对于数据可用性的要求，并查阅组织业务连续性计划，了解组织业务对关键数据的可用性指标。

（3）访谈数据安全管理员，询问组织为确保静态数据的可用性，所采取的存储架构、技术手段和工具有哪些，以及是否部署实现集群异地灾备，判断数据存储和恢复是否满足业务需求。

（4）查阅数据完整性测试报告和异地数据恢复的测试报告。

4. 数据处理与加工

（1）访谈数据安全管理员，询问在对数据进行操作处理过程中是否采用安全的身份验证和加密措施，确保数据交换和处理过程中的安全、可靠。

（2）访谈数据安全管理员，询问在对数据进行操作处理过程中涉及敏感信息时，是否对其脱敏处理。

5. 数据使用与安全审计

（1）访谈数据安全管理员或系统管理员，询问在进行数据展示时，是否对敏感数据进行不可逆加密、区间随机、掩码替换等脱敏手段。

（2）访谈系统管理员，询问是否基于数据安全管理员或系统管理员，基于角色和“按需所知”原则做到对数据表列级的访问和操作权限控制。

（3）访谈数据安全管理员或系统管理员，询问用户在对数据进行操作和管理的过程中，是否基于制定的访问权限，建立统一的身份识别和权限管理系统，实现对各类业务系统、数据库等账号实现统一管理，并对数据的访问和使用进行安全审计。

6. 数据共享与流动

（1）访谈数据应用或管理部门的负责人，询问组织是否基于业务战略和信息安全战略制定数据共享和流动的安全评估和处理流程、审批制度、安全策略等规范制度，调阅制度并检查

其内容是否符合对于数据共享与跨境传输的合规要求。

（2）访谈数据应用或管理部门的负责人，询问并查阅组织在进行日常数据服务时：是否与第三方签订数据服务合同，审查合同是否约定数据接收方的数据处理目的、方式和采取的安全措施以及数据接收方应配合组织对数据出境活动进行调查等关键内容；合同是否约定在未获得数据发送方的授权前提下，数据接收方不得对数据进行公开披露及再转移；是否约定数据接收方使用、留存数据的合法周期及超出合法周期后数据接收方对数据所采取的处理措施；是否约定数据接收方应配合数据发送方履行的安全责任和义务。

（3）访谈数据应用或管理部门的负责人，询问组织日常数据共享与流动若涉及跨境传输，是否开展如下活动并调阅相关操作文档：在数据出境前应制定出境计划，满足合法性、正当性和必要性的要求；在数据跨境传输前开展安全风险评估，并周期性的开展安全评估，评估应包括安全自评估和主管部门评估；在开展数据共享或跨境传输前，是否对数据接受方的背景、资质进行安全审查和检查，并基于国家关于个人信息和重要数据出境安全评估相关条件进行安全评估；对数据出境的全过程进行记录并保留所有操作流程，操作日志应保存不少于2年；当发生数据出境安全事件时，是否制定安全事件的通报机制和手段；访谈数据应用或管理部门的负责人，询问组织是否制定

数据共享与流动的安全事件应急预案，并进行应急演练，审查应急预案是否包含应急处置、安全事件告知和上报等相关内容。

（4）当发生数据出境安全事件时，应按照国家有关规定及时向国家网信部门或行业主管部门上报数据出境安全事件，上报内容包括但不限于：安全事件发生的时间、数据类型、数量、范围、可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式。

7. 数据归档与销毁

（1）检查组织是否基于数据分类分级标准制定数据及存储介质销毁相关的管理制度和安全策略，明确销毁对象、流程、方式及审批、监督和评价机制。

（2）访谈组织目前本地和网络分布式存储数据的销毁方式与技术手段，并查阅历史销毁记录。

## 四、个人信息安全管理审计

### （一）业务概述

个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为。旨在遏制个人信息非

法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

（二）审计目标和内容

1. 通用管理

该控制项旨在检查组织是否针对个人信息，建立健全个人信息保护的管理体系和风险管理体系，并提供个人信息泄露或非法使用的申诉管理机制和举报渠道。

2. 个人信息的收集

该控制项旨在检查组织在个人信息收集环节，是否制定完善的安全策略和规范，满足《网络安全法》中关于个人信息保护的合规要求。

3. 个人信息的传输与存储

该控制项旨在检查组织在个人信息传输与存储环节，是否采取管理与技术手段，确保个人信息境内存储和离境前安全与风险评估的合规要求，以及个人敏感信息不被泄露。

4. 个人信息的处理

该控制项旨在检查组织在个人信息处理环节，是否采取技术手段防范个人信息主体被识别和还原。

5. 个人信息的使用

该控制项旨在检查组织是否在个人信息使用环节，采取访问控制措施防范对其非法访问，并在个人信息控制权发生转移

时对接收方进行安全评估，并获得其安全使用的承诺。

6. 个人信息的变更与销毁

该控制项旨在检查组织在个人信息变更和销毁环节，是否为个人信息主体提供合法变更的渠道，或在完成所收集个人信息使用目的后，规范个人信息的删除流程和途径。

### （三）常见问题和风险

1. 未建立个人信息保护组织或缺乏相关负责人，不利于个人信息保护工作的推广和执行，也无法有效落实个人信息保护的责任。

2. 未建立规范化的个人信息保护制度和流程，可能造成个人信息的收集、存储、使用、变更、销毁等操作不合法的情况。

3. 组织在使用个人信息时，没有开展安全影响评估，无法判断个人信息使用与保护的程度，容易造成侵权与违规风险。

4. 在收集个人信息时，没有注意最小化要求，或者在没有得到允许的情况下公开披露个人信息，容易造成侵权与违规风险。

5. 组织在处理个人敏感信息时，个人信息的传输、处理、存储、销毁未采用加密、访问控制等安全措施，容易造成泄露个人敏感信息的风险。

### （四）审计的主要方法和程序

1. 通用管理

（1）访谈组织数据管理部门，了解是否基于业务量和个人信息处理数量，设立专职的个人信息保护负责机构与负责人，并明确相关工作职责。

（2）访谈组织数据管理部门，了解组织是否制定关于个人信息和个人隐私保护的管理规范，其明确定义个人敏感信息的识别范围、类别，以及对个人信息进行匿名化处理的条件和定期评审更新机制。

（3）访谈组织数据管理部门或风险管理部门，询问是否建立针对个人信息安全影响的风险评估制度并定期开展个人信息安全影响评估，并查阅历史风险评估记录。

（4）访谈组织数据管理部门，询问是否制定个人信息安全事件应急预案并定期开展应急响应培训和应急演练，包括当发生个人信息泄露时通知个人信息主体的方式、方法与内容。

（5）访谈人力资源管理部门，询问从事或接触个人信息处理岗位的人员（包括第三方人员），在录用时是否进行背景审查并签署保密协议，在调离岗位或终止劳动合同时是否要求继续履行保密义务，并对上述人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

（6）访谈组织数据管理部门，是否建立个人信息泄露或非法使用的申诉管理机制和举报渠道，并对造成安全事件违反安全使用的人员制定处罚机制。

2. 个人信息的收集

（1）访谈个人信息收集岗位的负责人，了解在进行个人信息收集前，组织是否以明示的方式（如隐私政策）向个人信息主体说明收集、使用的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等，确保个人信息主体的知情权并得到其授权，同时抽查信息收集说明和信息主体的授权确认信息。

（2）抽查年满 14 周岁的未成年人个人信息收集记录，查看是否征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。

（3）访谈个人信息收集岗位的负责人，了解组织间接获得的个人信息，是否获得个人信息提供方就个人信息来源的书面确认，确保来源的合法性，包括个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等。

（4）访谈个人信息收集岗位的负责人，了解组织是否向个人信息主体提供撤回收集、使用其个人信息同意授权的途径和方法。

3. 个人信息的传输与存储

（1）分别访谈数据安全管理者及数据存储管理员，了解组织在传输和存储个人敏感信息时是否采用加密等安全措施，对

于个人生物识别信息，询问是否采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要。

（2）访谈数据存储管理员，询问组织所收集和产生的个人信息是否在中华人民共和国境内存储。

（3）分别访谈数据安全管理者及数据存储管理员，了解组织若涉及个人信息的跨境传输与存储业务，是否制定相应的审批流程，并在进行跨境传输与存储时，按照合规监管要求进行安全检查和安全评估，调阅并查看相关的审批、审查和评估历史文档。

4. 个人信息的处理

（1）访谈数据安全管理负责人，了解组织是否制定针对个人信息去标识化的规范与流程，由专人、专岗负责。

（2）访谈个人信息去标识化负责人，了解所使用的个人信息匿名化、去标识化和加密手段，并抽查去标识化后的个人信息是否可被识别、复原，或在不借助额外信息的情况下，无法识别个人信息主体。

（3）访谈个人信息去标识化负责人，了解对不满足隐私保护的数据项进行删除时应采用的抑制技术。

5. 个人信息的使用

（1）访谈数据安全负责人或个人信息安全负责人，了解组织是否在将其个人信息控制权向另一个控制者转移时，对其安

全管理环境进行风险评估，并以书面形式获得转移方的安全评估结果和使用承诺，查阅历史风险评估记录、接受方的安全评估结果和使用承诺书。

（2）访谈数据安全负责人或个人信息安全负责人，了解组织对内部个人信息使用者、管理者和操作者是否基于业务需要和角色对个人敏感信息的访问、修改等行为进行访问权限设置，并对涉及个人信息的重要操作应设置内部审批流程。

6. 个人信息的变更与销毁

（1）访谈个人信息安全负责人，了解组织是否在收集到有错误或不完整的个人信息主体修改请求时，提供更正或补充信息的方法或渠道，并对其进行验证。

（2）访谈个人信息安全负责人，了解组织是否制定个人信息销毁的规范与流程，向通过注册账户获得个人信息的个人信息主体提供注销账户的方法，并删除其个人信息或做匿名化处理。

## 五、重要数据安全管理审计

### （一）业务概述

重要数据，一方面是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南；另一方面是指企事业单位的战略规划、管理方法、商业模式、财务信息等经营信息和设计程序、产品配方、

制作工艺、技术诀窍等技术信息。

规范重要数据在收集、保存、使用、传输、共享等信息处理环节中的相关行为。旨在遏制数据非授权收集、滥用、泄漏等乱象，最大程度地保障重要数据的安全。

（二）审计目标和内容

1. 通用管理

该控制项旨在检查组织针对其重要数据是否建立健全完善的管理体系，包括制度体系、组织与人员体系、应急管理体系，并提供重要数据安全事件的申诉渠道。

2. 重要数据识别与分类分级

该控制项旨在检查组织是否就所属行业和经营业务制定重要数据识别及分类分级的制度规范、标准以及变更和审批流程，从而为后续重要数据操作和处理提供依据。

3. 跨境传输与存储前安全风险评估

该控制项旨在检查组织在其存在重要数据跨境传输与境外存储的背景下，是否建立完善的安全风险评估与审批流程，满足国家合规监管要求。

4. 应急管理

该控制项旨在检查组织依据建立的重要数据安全事件应急管理体系，制定并完善应急管理制度并定期开展应急演练，在满足合规要求的同时，确保安全事件发生时得到有效、迅速的遏

制，防范事件蔓延。

（三）常见问题和风险

1. 未建立重要数据保护工作机构或指定负责人，不利于重要数据的保护和管理，同时无法有效落实重要数据保护的责任。

2. 未实现重要数据分类分级管理，无法有效对重要数据建立针对性的保护措施，由于保护机制不到位，造成的重要数据泄露或非法访问。

3. 未建立规范化的重要数据保护制度和流程，可能造成重要数据的收集、存储、使用、变更、销毁等操作不合法的情况。

4. 组织在使用重要数据时，没有开展安全风险评估，无法判断重要数据的使用与保护的程度，容易造成侵权与违规风险。

5. 组织在处理重要数据时，数据的传输、处理、存储、销毁未采用加密、访问控制等安全措施，容易造成重要数据泄露的风险。

6. 未建立数据应急预案，无法有效制定数据丢失、数据泄露等重要场景的处置措施，不利于重要数据发生异常的处置和恢复。

（四）审计的主要方法和程序

1. 通用管理

（1）访谈组织负责数据安全管理的负责人，询问了解组织是否在其内部成立重要数据保护的工作机构、日常办事机构，

并指定专门的安全管理人员。

（2）访谈组织负责数据安全管理的负责人，询问了解组织目前是否建立关于重要数据保护的管理体系和相应的规章制度，并基于合规和监管要求，对组织日常经营活动所涉及的重要数据进行了识别，并明确定义了对重要数据进行匿名化处理的条件。

（3）访谈组织负责数据安全管理的负责人，询问了解组织是否建立针对重要数据安全事件的处置、应急响应和事后调查的流程与机制，记录事件的处置与调查全过程，及时发现并消除重要数据的违规使用和滥用等情况，同时查看有关处置方案和历史记录。

（4）访谈组织负责数据安全管理的负责人，询问了解组织是否建立申诉管理机制和渠道。

2. 重要数据识别与分类分级

（1）访谈组织数据安全管理的负责人，询问了解是否基于行业监管要求制定重要数据识别的管理制度与规范。

（2）访谈组织负责数据安全管理的负责人，询问了解组织是否制定针对重要数据的分类分级策略和管理制度与规范，查看是否对各类重要数据的保护期限和标记做出明确规定。

（3）访谈组织负责数据安全管理的负责人，询问了解组织是否制定重要数据保护范围和分类分级的变更与审批流程，并

查看历史变更和审批记录。

3. 跨境传输与存储前安全风险评估

（1）访谈组织负责数据安全管理的负责人，询问了解组织重要数据的存储位置及是否涉及跨境流动和存储。

（2）访谈组织负责数据安全管理的负责人，询问了解组织对涉及跨境传输与存储的重要数据是否进行安全检查与风险评估，并建立完善的审批流程，同时查看历史相关记录，判断记录的完整性与合规性。

4. 应急管理

（1）访谈负责数据安全管理的负责人，询问了解组织是否制定针对重要数据安全事件应急预案并定期开展应急响应培训和应急演练。

（2）调阅并查看应急预案，检查其内容是否明确安全事件的具体处置措施、上报和信息披露流程，并查看培训和演练的历史记录。

## 六、数据平台与技术安全管理审计

### （一）业务概述

数据平台是指为数据应用提供资源和服务的支撑集成环境，包括基础设施层、数据平台层和计算分析层。重点关注数据平台基础设施安全、网络与通信安全、应用安全及安全审计工具使用等内容。

### （二）审计目标和内容

1. 平台基础设施安全

该控制项旨在检查组织为确保数据平台基础设施安全，除对其所处的物理环境进行安全检查外，还应检查是否采取技术措施与工具，监控并防范平台受到恶意代码等非法攻击。

2. 网络与通信安全

该控制项旨在检查组织为确保数据平台的网络与通信安全，是否制定访问控制策略并在网络隔离设备上部署、实施，同时，检查为确保通信链路的安全是否采取相应的安全监控与链路加密手段。

3. 应用安全

该控制项旨在检查组织在应用层面针对应用接口、平台服务和平台资源是否采取相应的安全控制措施。

4. 安全审计

该控制项旨在检查组织针对数据平台的日常服务和运维是否开展安全审计，并验证安全审计是否具有自动分析和报警的功能。

### （三）常见问题和风险

1. 数据平台或系统安全保护措施部署不到位，导致数据泄露或非法访问。

2. 数据平台与其他平台交换数据未实施加密，导致数据外

泄。

3. 未部署独立的数据库审计系统，无法对数据违规操作行为进行跟踪分析，不利于数据的规范化管理。

**（四）审计的主要方法和程序**

1. 平台基础设施安全

（1）访谈负责数据平台或系统的负责人，询问是否对各类基础设施采用防病毒、边界防护、入侵防护、态势感知、威胁情报等手段保障其设备安全，并调阅查看最新网络拓扑图，检查符合性。

（2）访谈负责数据平台物理基础设施安全的负责人，了解对数据平台依赖的机房环境所采取的具体安全保障措施并进行实际走查和传感器监控数据的抽查。

（3）检查是否对平台系统和主机制定预警策略，并对漏洞爆发等威胁进行自动预警和漏洞修复。

（4）检查是否定期组织第三方机构对应用系统进行渗透测试，及时发现并修复应用层安全漏洞。

（5）检查组织是否根据识别出的数据关键业务，对其安全基线检查及后续加固。

2. 网络与通信安全

（1）访谈网络安全管理员，了解为确保数据平台所进行的网络安全规划和具体措施，检查是否至少在业务层面与管理层

面采用隔离措施和工具。

（2）访谈网络安全管理员，是否为采取的安全隔离措施制定访问控制策略，并登录隔离设备查看隔离策略的配置与运行情况。

（3）访谈网络安全管理员，是否在数据平台网络边界出口部署流量控制系统，对异常流量实现实时阻断。

（4）访谈网络安全管理员，了解针对数据平台的日常管理维护和开发测试的人员接入平台的方式，判断接入链路是否安全，操作行为是否受控并对其进行安全审计。

（5）访谈网络安全管理员，了解为确保客户端与数据库服务器间通信安全所采取的加密安全措施。

3. 应用安全

访谈应用系统安全管理员，询问为确保数据平台应用安全：应用接口是否采用身份认证、权限控制等安全措施；对数据平台服务用户是否采用安全认证方式并对密钥采取全生命周期的安全管理；访谈数据平台负责基础设施资源或应用管理员，询问是否对平台资源的分配和使用进行安全监控并实施最大限额管理，并在超过设定的资源配置阈值时，对用户使用行为进行限制；访谈数据平台应用安全管理员，询问组织在分布式环境下，是否对用户进行的数据资源访问以及对数据资源执行的操作批量授权管理，以及与原有平台认证体系的完全独立，确保

节点不会被冒充，保证集群中的服务的身份可靠性。

4. 安全审计

（1）检查是否对数据平台部署独立、实时的审计系统，从而确保对登录主机的用户操作行为、对流量层及包括服务器终端命令等内容进行安全审计，同时确保审计记录在数据库系统运行时的访问控制安全以及对被审计安全事件的自动分析和报警。（安全审计）

（2）验证数据平台的安全审计系统是否具有日志自动分析功能，并在遭受危害平台安全的操作时是否触发安全报警。

## 第六节　移动互联网安全审计

移动通讯及互联网技术的快速发展以及平台和商业模式的巨大转变，显著推动了移动互联网的发展并呈现出一种加速化和扩大化的特征，以移动互联技术为基础的新业务和创新技术也逐步成为日常工作和生活中不可或缺的组成部分。

移动互联网由移动终端、移动应用和无线网络三部分组成。移动互联网由于其边界的不确定性及设备的移动性等特点，与有线网络相比，不仅仅表现为安全风险更大，而且需要在易用性和安全性之间取得平衡。

本节将从制度与人员、移动无线网络物理与环境安全、网络与通信安全、安全区域边界管理、设备和计算安全、应用与

数据安全、安全审计等方面对移动互联网安全审计的方法与步骤进行描述。

## 一、制度与人员管理审计

### （一）业务概述

移动互联网的安全管理包括日常管理机制的建立以及对于人员的安全管理。

### （二）审计目标和内容

1. 制度管理

该控制项旨在检查组织是否将移动互联网安全管理纳入组织整体网络及信息安全管理体系当中，制定相关制度规范。

2. 岗位设置与人员配备

该控制项旨在检查组织是否根据移动互联网安全管理的需要，设立专职管理部门及各安全管理岗位，明确部门及安全岗位负责人的职责，配备相应的专职管理员、操作员和审计人员。

3. 安全意识教育与技能培训

该控制项旨在检查组织是否将移动互联网安全意识培训与教育纳入组织整体意识培训与教育规划当中。

### （三）常见问题和风险

1. 未建立移动互联网安全管理制度，无法有效落实移动互联网安全管控的各项要求。

2. 未明确移动互联网安全管理专职部门或岗位，无法有效落实移动互联网的安全管控责任，不利于移动互联网安全工作的落实。

**（四）审计的主要方法和程序**

1. 制度管理

（1）访谈信息安全管理负责人，询问是否将移动互联网安全管理纳入组织整体网络与信息安全管理范畴当中，并制定相应的管理规范。

（2）查看移动互联网安全管理制度，审查管理制度是否包括人员日常管理操作规程。

（3）访谈管理人员或移动终端操作人员，询问是否知晓基本的操作规程。

2. 岗位设置与人员配备

（1）访谈信息安全负责人，询问是否设置移动互联网安全管理专职部门及相关安全管理岗位，明确部门和各岗位职责，同时查看部门及岗位安全职责说明书。

（2）查阅移动互联网安全管理部门人员清单，检查是否与岗位规划和人员数量需求相一致。

3. 安全意识教育与技能培训

（1）访谈信息安全负责人，询问是否对各类人员进行移动互联网安全教育和岗位技能培训，告知相关的安全知识、安全

责任和惩戒措施等。

（2）访谈信息安全负责人，询问是否对移动终端管理服务端的专职管理员、操作员进行移动互联网安全教育和岗位技能培训，告知相关的安全知识、安全责任和惩戒措施等。

（3）调阅并查看安全意识教育与培训规划和历史记录，检查培训人员与培训内容是否与规划相符。

## 二、移动无线网络物理与环境安全审计

### （一）业务概述

是指移动无线无线接入网络与设备的安装应选择合理的物理位置，避免不合理的覆盖区域和电磁干扰。

### （二）审计目标和内容

该控制项旨在检查移动无线网络所处物理环境是否符合安全传输要求，防止对无线网络的传输信号产生影响。

### （三）常见问题和风险

1. 未建立移动无线网络电磁干扰设施，导致无线网络被电磁干扰，导致网络不可用。

2. 无线网络设备覆盖范围未满足业务需求，无法有效为业务发展提供助力和支撑，可能会影响业务的正常运营。

### （四）审计的主要方法和程序

访谈网络管理员，询问移动无线网络与设备所处的物理环境是否存在电磁干扰，测试所处物理环境或查验验收报告；访

谈网络管理员，询问移动无线网络与设备的覆盖范围与处理能力能否满足业务需求，并检查无线接入设备的物理位置与无线信号的覆盖范围是否在合理区域内。

## 三、网络与通信安全审计

### （一）业务概述

是指移动无线网络与通信的结构安全、通信的完整性的保密性、无线网络设备防护等内容。

### （二）审计目标和内容

1. 结构安全

该控制项旨在检查组织的移动无线接入设备在设计使用时，其处理能力和网络带宽能否满足业务高峰需要，且是否采用符合国家强制安全要求的产品。

2. 无线网络通信完整性与保密性

该控制项旨在检查组织是否对传输数据的无线通信网络采取加密技术，确保传输数据的完整性与保密性，并验证加密措施的合规及有效性。

3. 无线网络设备防护

该控制项旨在检查是否对接入组织的移动无线网络终端设备及接入网关进行安全管理，防范对所接入的无线网络构成安全威胁。

### （三）常见问题和风险

1. 无线接入网关的业务处理能力不满足业务需求，导致高峰期业务受阻或中断，影响业务的正常开展。

2. 无线网络通信加密机制不严格，造成无线网络传输过程中重要数据外泄。

3. 无法网络可信验证机制不健全，导致其他网络的非法接入，造成网络不可用或敏感信息的外泄。

（四）审计的主要方法和程序

1. 结构安全

（1）访谈网络管理员，询问无线接入网关的业务处理能力能否满足基本业务需求，并查看在业务高峰期接入网关的 CPU 和内存使用情况。

（2）访谈网络管理员，询问无线接入设备的网络带宽，并检查业务高峰时期内带宽使用峰值，判断是否满足业务需求。

（3）查看无线接入设备是否开启符合国密算法的接入认证功能。

2. 无线网络通信完整性与保密性

（1）访谈网络管理员，询问是否采用加密技术保证无线网络通信过程中数据的完整性，并查阅设计、验收文档或源代码，查看是否有采用加密技术保护无线通信完整性的描述。

（2）访谈网络管理员，询问是否采用加密技术保证无线网络通信过程中数据的保密性，并查阅设计、验收文档或源代码，

查看是否有采用国产加密技术保护无线通信保密性的描述，同时测试无线通信过程中重要数据是否进行了安全加密。

3. 无线网络设备防护

（1）访谈网络管理员，询问是否通过基于密码的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。（通信网络设备真实性验证）

（2）查阅组织是否针对无线接入设备和无线接入网关等设备制定补丁管理制度，访谈网络管理员，询问是否对上述设备采取补丁管理，定期对其补丁进行更新，并检查上述设备。

（3）访谈网络管理员，询问并检查无线接入设备和无线接入网关是否关闭了“SSID 广播、WEP 认证” 等存在风险的功能。

（4）访谈网络管理员，询问并检查无线接入设备是否分别使用了不同的鉴别密钥。

## 四、安全区域边界管理审计

### （一）业务概述

对移动计算节点安全区域的安全设置，制定和实施的访问控制策略，防止非授权访问数据信息。

### （二）审计目标和内容

1. 移动计算节点区域边界安全管理

该控制项旨在检查是否对移动计算节点安全区域进行安全设置，制定并实施访问控制策略，从而对进出该安全区域的数据信息进行控制，防止非授权访问。

2. 传统计算节点区域边界安全管理

该控制项旨在检查对传统计算节点安全区域进行安全设置，制定并实施访问控制策略，从而对进出该安全区域的数据信息进行控制，防止非授权访问。

3. 无线和有线网络间的边界安全管理

该控制项旨在检查有线网络与无线网络边界之间的访问和数据流是否通过无线接入网关设备。

**（三）常见问题和风险**

1. 移动网络的区域边界访问控制不严格，遭受非法入侵或网络攻击，引起网络异常或中断。

2. 进出网络的信息内容过滤不严格，导致注入攻击、网络入侵、恶意代码入侵的发生，影响网络的安全性和稳定性。

**（四）审计的主要方法和程序**

1. 移动计算节点区域边界安全管理

（1）针对移动网络的区域边界访问控制：访谈网络管理员，询问是否对接入系统的移动终端，采取基于 SIM 卡、证书等信息的强认证措施，并对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入；访谈网络管理员

询问是否能限制移动设备在不同工作场景下对 WIFI、3G、4G 等网络的访问能力。

（2）针对移动网络的边界入侵防范：访谈网络管理员，询问是否在区域边界采取相关技术措施，对无线接入点的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位，防止网络入侵、恶意代码入侵等攻击行为；检查是否对部署的边界防护设备进行定期升级和更新，并检测特征库是否为最新版本。

（3）针对移动网络的边界完整性保护：访谈网络管理员，询问是否对区域边界设置完整性保护机制，探测非法网络连接（内联和外联）和网络入侵行为；访谈网络管理员，询问并验证移动终端区域边界检测设备监控范围是否完整覆盖移动终端办公区，并具备无线路由器设备位置检测功能，且对非法无线路由器设备接入进行报警和阻断。

2. 传统计算节点区域边界安全管理

（1）针对传统网络的区域边界访问控制：访谈网络管理员，询问是否对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入；访谈网络管理员，询问是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；访谈网络管理员，询问是否知道网络最大流量数及网络连接数。

（2）针对传统网络的边界入侵防范：访谈网络管理员，询问是否在区域边界采取相关技术措施，对无线接入点的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位，防止网络入侵、恶意代码入侵等攻击行为；检查是否对部署的边界防护设备进行定期升级和更新，并检测特征库是否为最新版本。

（3）针对传统网络的边界完整性保护，访谈网络管理员，询问是否对区域边界设置完整性保护机制，探测非法网络连接（内联和外联）和网络入侵行为。

3. 无线和有线网络间的边界安全管理

访谈网络安全管理员，询问并检查是否在有线网络与无线网络边界之间部署无线接入网关设备。

4. 通过对移动网络边界进行安全工具扫描和渗透测试，验证其安全防护能力和防护效果满足网络保护要求。

## 五、设备和计算安全审计

### （一）业务概述

移动终端及其管理系统应该使用采取身份标识和身份鉴别等管理措施，确保移动终端的应用软件符合安全管理的要求并处于受控环境。

### （二）审计目标和内容

1. 设备身份鉴别

该控制项旨在检查组织是否对移动终端及其管理系统使用采取身份标识和身份鉴别等管理措施。

2. 终端应用管控

该控制项旨在检查组织是否对移动终端的应用采取安全管控措施，确保移动终端的应用软件安装符合安全管理要求并处于受控环境。

3. 终端入侵及恶意代码防范

该控制项旨在检查组织是否对移动终端采取恶意代码防护及漏洞管理措施，并确保漏洞补丁及恶意代码防范软件均处于最新状态。

### （三）常见问题和风险

1. 移动用户及登录终端身份鉴别机制不严格，导致身份验证机制被绕过，存在敏感信息泄露或交易被篡改的风险。

2. 移动终端默认配置修改不及时，导致端口或服务被利用，造成移动终端被越权或敏感信息泄露。

### （四）审计的主要方法和程序

1. 设备身份鉴别

（1）访谈系统管理员，询问是否制定移动用户及登录终端、移动终端管理系统登录的身份鉴别策略及主要主、客体的安全标记策略和规范，检查是否部署身份鉴别设施并基于身份及鉴别策略进行身份鉴别和操作控制。

（2）检查是否对移动用户及登录终端进行身份的唯一标识。

（3）访谈系统管理员，询问并测试移动终端、移动终端管理系统的登录口令复杂度及是否采用不少于两种的身份验证手段。

（4）访谈系统管理员，询问并测试移动终端是否启用了登录失败处理功能及移动终端的登录失败处理功能。

2. 终端应用管控

（1）访谈安全管理员，询问是否制定移动终端管理的全流程管理策略，明确必要的业务应用安装。

（2）检查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略。

（3）检查终端是否遵循最小安装的原则，仅安装需要的组件和业务应用程序。

（4）访谈安全管理员，询问移动终端管理客户端是否具有软件白名单功能，并测试使用白名单控制应用软件安装、运行。

（5）访谈安全管理员，询问移动终端管理客户端是否具有应用软件权限控制功能，并测试是否可以对移动终端中资源的访问进行限制。

（6）检查移动终端管理客户端所允许使用的签名证书。

（7）访谈安全管理员，询问移动终端管理客户端是否具有

接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

3. 终端入侵及恶意代码防范

（1）访谈安全管理员，询问是否制定终端补丁及恶意代码防护的管理制度、策略及系统和软件的安装配置基线。

（2）检查移动终端是否应关闭不需要的系统服务、默认共享和高危端口。

（3）检查移动终端操作系统版本，查看补丁是否得到了及时更新。

（4）检查移动终端是否安装恶意代码的防护软件并查看代码库是否为最新版本。

## 六、应用与数据安全审计

### （一）业务概述

应用在开发测试等方面的安全管理，数据在完整性、机密性、可用性三方面的安全管理。

### （二）审计目标和内容

1. 应用软件安全测评

该控制项旨在检查组织是否对移动终端应用软件的开发、测试和使用进行安全测评，防范漏洞及违规信息收集现象的存在。

2. 数据安全管理

该控制项旨在检查移动终端应用程序是否具有确保数据安全存储、完整性保护和残余信息清除等功能。

3. 数据备份

该控制项旨在检查组织是否采取安全措施对移动终端存储的重要信息进行及时安全备份并制定相关的备份管理制度规范与安全策略。

### （三）常见问题和风险

1. 对应用软件的开发、测试和使用阶段的安全措施部署及安全测评不到位，造成软件系统有较大的安全漏洞。

2. 采集、使用和保存的个人数据不符合国家及行业有关个人信息保护的要求，造成个人敏感泄露和非授权使用。

3. 未执行有效的备份与恢复程序，导致备份数据不可用。

### （四）审计的主要方法和程序

1. 应用软件安全测评

（1）访谈应用软件开发负责人，询问是否在移动应用软件开发结束后至发布前进行了安全检测并查阅测评报告。

（2）查阅测评报告并检查移动应用软件，检查移动应用软件所采集和保存的用户个人信息是否为业务必须，防范存在过度信息收集现象。

（3）查阅测评报告并检查移动应用软件，检查移动应用软件是否存在安全漏洞。

2. 数据安全管理

（1）访谈应用管理员，询问移动应用软件应采用哪种密码技术保证通信过程中数据的完整性，查阅移动应用软件设计、验收文档或源代码，查看是否有关于能检测数据通信和存储过程中完整性受到破坏的描述，并测试移动应用软件是否可对通信报文中进行完整性保护。

（2）检查移动应用软件，查看其鉴别信息和主要数据是否采用加密或其他有效措施实现本地存储保密性。

（3）测试移动应用软件，验证移动应用软件之间的重要数据是否能被互操作。

（4）查阅设计、验收文档或源代码，检查是否有关于系统在释放或再分配数据文件所在存储空间给其他用户前，如何将其进行完全清除的描述，并验证不同用户登录移动终端系统提供的剩余信息保护功能是否正确。（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）

3. 数据备份

访谈系统运维负责人，询问是否识别需要定期备份移动应用软件中的重要信息，包括但不限于业务信息、系统数据和软件系统；询问是否制定重要信息的备份策略，如：定时批量传送的备用位置、备份方式（如是否为完全数据备份）、频率和

介质存放方式等。

## 七、安全审计

### （一）业务概述

根据有关法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。

### （二）审计目标和内容

1. 移动互联网安全审计制度

该控制项旨在检查组织是否就移动互联网安全审计制定专项的审计规范、策略并据此部署和开展安全审计。

2. 移动互联网安全审计工具

该控制项旨在检查组织所部署的移动互联审计工具所具备的功能是否有效支撑日常安全审计工作。

### （三）常见问题和风险

1. 未定期开展移动互联网安全审计，无法及时发现存在的安全风险与隐患，不利于移动互联网管控措施的持续改进。

2. 未部署移动互联网安全审计工具，无法对移动互联网重要操作和异常行为进行持续监控。

### （四）审计的主要方法和程序

1. 移动互联网安全审计制度

（1）检查组织是否制定针对移动互联网（或无线网络）及

其终端安全的审计规范和审计策略，以及是否部署安全审计的工具或平台。

（2）查看安全审计规范，检查其内容：是否对审计对象（如行为审计、流量审计、日志审计、移动应用审计）、格式、访问、存储和安全报警事件进行明确要求，并对审计日志进行抽样检查，检查其日志管理要求是否符合制度规范要求；是否对审计记录的存储、管理和查询进行明确要求，防止非授权访问和破坏，并验证保存时间是否符合规范要求。（审计存储）

（3）查看审计策略，检查其内容：是否定义安全相关事件，明确安全事件的主体、客体、时间、类型和结果等内容；是否定义事件采集、记录、分析、存储、告警等各种安全相关事件的规则，如黑白名单定制和管控策略定制。

2. 移动互联网安全审计工具

检查并测试部署的审计工具是否可对移动互联网络的设备运行状况、网络流量、管理账户的登录及重要操作进行审计；是否具备对安全审计域正在发生的所有联网行为进行实时监督、响应和记录；是否具备日志收集（特别是移动终端）、关联分析及存储备份的功能；是否具有采用数据流跟踪、特征分析等方法检测移动应用（APP）的安全漏洞、编码隐患等功能，如APP 程序安全、应用数据安全、业务逻辑安全、系统环境安全、集成插件安全等。

## 第七节　工控系统安全审计

工业控制系统(ICS)是数据采集与监视控制系统(SCADA)、集散控制系统(DCS)和其他控制系统(例如可编程逻辑控制器PLC)的总称。工业控制系统主要由过程级、操作级以及各级之间和内部的通信网络构成。对于大规模的控制系统，也包括管理级。工控系统的脆弱性分布较广，但主要集中在系统安全管理的策略和程序、工控平台与工业网络等方面。

本节将从工控系统的安全策略与制度规范审计、机构与人员管理审计、安全建设与管理审计、平台及数据安全审计、边界与网络通信安全审计、安全管理中心及安全审计等方面对工控系统安全的审计方法和步骤进行描述。。

### 一、安全策略与制度规范审计

#### （一）业务概述

是指制定工控系统的安全战略与安全规划、编写安全管理制度与规范并予以发布与执行。

#### （二）审计目标和内容

1. 安全战略与规划

该控制项旨在检查组织是否将工控网络的信息安全纳入到组织信息安全管理体系当中，制定相应的安全战略与规划，从而判断与组织整体信息安全战略的一致性。

2. 安全管理制度与规范

该控制项旨在检查组织是否根据既定的工控安全战略和规划建立相应的安全管理制度体系，并检查相关制度与规范的完整性。

3. 制度发布与修订

该控制项旨在检查组织是否根据既定的制度管理规范，对工控安全制度规范的发布、评审和修订进行管理。

**（三）常见问题和风险**

1. 未建立工控系统安全战略规划，无法有效指导工控系统安全总体发展目标和思路，不利于工控系统安全管控工作的有序开展。

2. 未建立工控系统安全管理制度和流程，不利于有效落实安全管控各项要求。

**（四）审计的主要方法和程序**

1. 安全战略与规划

（1）调阅组织信息安全工作的总体方针和安全策略，了解组织安全工作的总体目标、范围、原则和安全框架等内容。

（2）调阅组织工业控制系统的安全规划和方针策略，了解其安全工作的目标、范围、原则，并审查与组织信息安全工作总体方针和安全战略的一致性。

2. 安全管理制度与策略

（1）检查组织是否建立完善的工控信息安全制度体系，其

应包括安全策略、管理制度、操作规程、记录表单等内容。

（2）调阅组织工业控制信息系统的安全管理制度，检查是否将工控系统安全防护及其信息报送纳入日常安全生产管理体系，并在内容上覆盖物理、网络、主机系统、数据、应用、建设和运维等层面。

（3）检查组织是否制定管理人员或操作人员执行的日常管理操作规程。

（4）检查组织的安全策略是否针对工业网络的特定领域、安全架构与设计、网络变更、业务连续性或灾难恢复、安全审计等内容。

3. 制度发布与修订

（1）访谈安全主管，询问是否由专门的部门或人员负责安全管理制度的制定、发布与定期评审。

（2）查阅组织有关制度制定和发布要求的管理文档，查看文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容。

（3）查阅组织已发布的工控安全管理制度，检查其是否定期接受修订并查看修订记录和版本号。

## 二、机构与人员管理审计

### （一）业务概述

是指工控安全管理组织的岗位设置、人员与资金保障、安

全检查与核查工作开展情况。

（二）审计目标和内容

1. 岗位设置

该控制项旨在检查在组织层面是否建立工控信息安全组织及负责人，明确相应安全职责。

2. 人员与资金保障

该控制项旨在从资金、人员配置与人员技能方面，检查组织是否为其工控安全提供相应的保障。

3. 安全检查与核查

该控制项旨在检查组织是否对其工控安全开展定期安全检查和核查工作，明确检查与核查内容，并对不符合项进行整改。

4. 人员安全

该控制项旨在检查组织是否对包括第三方人员在内的工控安全管理人员在招聘、录用和离职（转岗）各环节开展相应的安全检查并根据其安全职责分配对应的访问权限，从而确保人员安全。

（三）常见问题和风险

1. 安全管控职责落实不到位，无法有效执行工控系统信息安全管控要求，落实管控责任。

2. 人员与资金保障不足，导致工控系统安全管控机制和要求落实不到位，影响工控系统安全管控工作的有序推进。

（四）审计的主要方法和程序

1. 岗位设置

（1）访谈信息安全主管，了解组织是否成立专门的工控信息安全工作委员会（领导小组），或由信息安全工作委员会（领导小组）统一管理，其最高领导由单位主管领导委任或授权，并定期组织开展信息安全工作。

（2）查看工作委员会或领导小组的构成情况和相关职责描述，及其会议纪要或相关记录。

（3）访谈信息安全主管，确认是否由主管安全生产的领导作为工控系统安全防护的主要责任人，并查看其岗位职责说明书。

（4）访谈信息安全主管或人力资源主管，了解是否成立负责工控安全的部门及负责人，并查看部门职责和负责人岗位职责说明。

（5）访谈工控安全负责人，了解是否划分部门内部的安全管理岗位并定义其岗位职责，查看相关岗位职责说明书。

2. 人员与资金保障

（1）检查工控安全管理制度中是否有保障工控系统安全建设、运维、核查、等级保护测评及其他信息安全资金的内容。

（2）访谈信息安全主管关于工控系统安全建设、运维、核查、等级保护测评及其他信息安全资金预算及实际投入情况，

从而判断是否获得组织的资金保障。

（3）访谈工控信息安全负责人，了解各岗位人员配备情况，核查人员配备文档，查看并确认各岗位实际人员配备情况。

（4）调阅工控安全各岗位的技能需求，并查阅相关岗位人员学历、技能证书，从而确保技能需求与人员实际情况相符。

3. 检查与核查

（1）访谈信息安全主管，确认是否定期对组织工控系统的常规安全开展检查工作，检查内容至少应包括系统日常运行、系统漏洞和数据备份等情况，检查历史核查记录是否完整并对安全检查结果进行通报，对不符合项进行整改。

（2）访谈信息安全主管，确认是否定期开展全面安全核查，核查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，检查历史核查记录是否完整并对安全核查结果进行通报，对不符合项进行整改。

4. 人员安全

具体审计程序可参考“信息系统一般控制审计”中“信息安全审计-人员安全”审计项及审计程序。

## 三、安全建设与管理审计

### （一）业务概述

工控系统的项目建设需要将安全方案的规划与设计纳入其

中，需要对工控产品与服务的供应商采取有效的安全管理。

### （二）审计目标和内容

1. 安全方案规划与设计

该控制项旨在检查组织在开展工控系统项目建设时，是否将安全规划设计纳入到整体设计方案当中，并经过安全评估和主管单位的审批与备案。

2. 安全检查及服务商管理

该控制项旨在检查组织对工控系统的产品和服务采购是否进行安全检查和测试，并对供应商采取有效的安全管理。

3. 工程实施与验收

该控制项旨在检查组织在工控系统的安全建设过程中，是否对其进行包括进度、质量和过程文档等方面的严格管理，制定系统安全测试方案并履行执行和结果审批。

4. 工程交付

该控制项旨在检查组织对工控系统安全建设项目在交付收尾阶段是否按照既定的交付清单进行验收，并开展相应的技术培训以确保后期运维等工作的顺利开展。

### （三）常见问题和风险

1. 工控系统建设未有效落实安全需求与规划设计，导致安全与建设不同步，安全需求严重滞后。

2. 工控系统选取的密码产品，不满足国家安全要求，存在

合规风险。

3. 工控系统项目交付审批程序不严格，造成功能和性能不满足预期，未实现有效的知识转移及培训，验收程序存在较大管理漏洞。

（四）审计的主要方法和程序

1. 安全方案规划与设计

（1）检查组织在开展工控系统建设前是否经过安全需求及其合理性和正确性的论证和评审，形成配套的安全整体规划和设计方案经上级并经主管部门或本单位相关部门审批，检查安全规划和设计方案及其历史审批记录。

（2）检查工控系统的建设是否经过定级和备案，检查历史备案材料报告和备案记录。

2. 安全检查及服务商管理

（1）访谈建设负责人，询问工控系统使用的有关信息安全产品和服务是否符合国家安全规定并通过国家安全检查和安全测试，查阅相关产品的测试报告；询问工控系统是否采用密码产品，以及密码产品的采购和使用是否符合国家密码主管部门的要求；询问是否制定服务商安全管理、服务商评价和审核制度及服务商目录清单，审查供应商是否符合国家有关标准。

（2）检查是否具有与安全服务商签订的服务合同或安全责任合同书、服务协议，合同或协议应明确整个服务供应链各方

需履行的信息安全相关义务、后期的技术支持和服务承诺等内容、符合指标要求及其服务变更控制要求。

3. 工程实施与验收

（1）访谈建设负责人，询问工控系统的安全建设是否由专门部门或人员实施进度和质量控制。

（2）检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，并按照工程实施方面的管理制度进行各类控制，同时产生阶段性文档等。

（3）检查工控系统安全建设是否制定测试验收方案，查看是否明确说明参与测试的部门、人员、测试验收内容和现场操作过程等内容。

（4）检查上线前的验收测试报告，查看是否具有相关部门和人员对工控系统安全测试验收报告的审定意见。

4. 工程交付

（1）查阅工控安全建设设备采购合同，核查是否明确交付清单，其应明确交付的各类设备、软件、文档等，并查验交付验收记录。

（2）检查工程交付过程是否有系统交付的技术培训记录和运维文档，查看培训记录是否包括培训内容、培训时间和参与人员等。

## 四、平台及数据安全审计

（一）业务概述

是指工控系统平台及数据相关的物理环境安全、身份鉴别与访问控制、安全配置管理、恶意代码防护与数据安全保护。

（二）审计目标和内容

1. 物理与环境安全

该控制项旨在检查组织是否为确保工控网络和系统平台所处物理环境的安全而采取相应的安全控制措施。

2. 身份鉴别与访问控制

该控制项旨在检查是否对组织工控系统中用户、重要主机设备和工控设备的身份进行鉴别并根据安全控制原则制定访问控制策略，实施相应的访问控制。

3. 安全配置管理

该控制项旨在检查组织是否对重要主机和工控系统进行安全设置并对安全配置的基线进行定期安全备份和审核。

4. 恶意代码防护

该控制项旨在检查组织是否对工控网络环境下的主机、工控系统和终端部署恶意代码防护设备与入侵检测设备，并定期开展漏洞扫描和代码库的升级与更新工作，验证防护设备有效性。

5. 工控系统数据安全

该控制项旨在检查组织是否为确保工控网络和系统平台传

输、处理和存储的用户数据、系统管理数据、鉴别信息及重要控制数据安全性而从完整性、保密性及重用性等角度而采取的安全控制措施。

（三）常见问题和风险

1. 工控系统恶意代码防范措施不严格，导致恶意代码入侵系统，给系统安全性和稳定性产生较大影响。

2. 工控系统数据安全分类分级不严格，无法针对不同级别数据建立不同的安全措施，导致个别数据保护过当或保护不足。

（四）审计的主要方法和程序

1. 物理与环境安全

具体审计程序可参考“信息系统一般控制审计”中“信息安全审计-物理安全”审计项及审计程序。

2. 身份鉴别与访问控制

（1）查阅组织的安全控制策略，访谈主机、工控系统安全管理员，询问并检查是否对登录操作重要主机系统、工控设备的操作系统、数据库系统和通用程序的用户进行身份标识和鉴别；询问是否支持对重要主机和工控设备的身份标识和鉴别，并防止未经授权的更改；询问是否对用户和设备身份鉴别的信息在存储和传输时采用加密方式；询问是否根据设备的安全保障需求制定相应的访问控制策略，实现相应的访问控制方式，设置对访问客体的操作粒度，确保合法操作。

（2）查阅是否制定用户账号与口令的管理策略，检查是否采用单一登录和双重（多重）身份验证手段对登录用户进行身份有效性验证，并确保账号在系统整个生命周期的唯一性。

3. 安全配置管理

（1）访谈主机和工控系统安全管理员，询问了解是否制定安全配置基线并依据“最小化安全原则”，对重要主机和工控系统一安装只与自身业务相关的操作系统组件和应用组件。

（2）检查是否对安全基线及其相应的安全配置进行定期审核，并对关键配置进行定期备份，查看历史审核和备份记录。

4. 恶意代码防护

（1）检查是否对主机服务器、工控系统和终端安装防病毒软件并定期对其进行更新及在监测出恶意代码后及时报警，查验其版本和代码库是否与服务商提供的最新版本相一致以及报警记录。

（2）检查是否对主机服务器、工控系统部署漏洞扫描系统从而对其进行定期的漏洞扫描，查验历史漏洞扫描记录。

（3）检查是否对主机服务器、工控系统部署入侵检测，查验历史记录判断是否对监测出的入侵行为或异常业务操作异常分析和报警。

（4）访谈主机和工控系统安全管理员，询问是否对主机服务器、工控系统进行防恶意代码库和补丁漏洞升级与修补前进

行安全测试并制定回退计划，并查阅历史更新记录。

5. 工控系统数据安全

（1）访谈工控安全负责人，询问是否制定了工控网络中受保护数据的安全管理制度，明确数据分类和分级策略；询问是否为确保信息不被泄露，明确了需对存储空间及内存进行清除的客体资源对象，并查验是否对其部署了具有安全客体重用功能的系统软件或具有相应功能的信息技术产品。（客体安全重用）

（2）检查是否对工控环境下的现场设备数据完整性采取保护措施，并对点对点的通信过程采取会话认证。

（3）其他审计程序可参考“信息系统一般控制审计”中“信息安全审计-数据”审计项及审计程序。

## 五、边界与网络通信安全审计

### （一）业务概述

根据工控网络及业务安全需求进行层级和安全域的划分，并据此对其部署和实现边界访问控制。

### （二）审计目标和内容

1. 安全区域边界访问控制

该控制项旨在检查组织是否根据组织工控网络限制及业务安全需求，对其进行层级和安全域的划分，并据此对其部署和实现边界访问控制。

2. 安全区域边界防护

该控制项旨在检查组织是否根据已划分的工控网络层级和安全域，部署边界防护设备，实现边界防护。

3. 网络通信安全管理

该控制项旨在检查组织是否为确保工控网络（包括工控无线网络）及数据传输的完整性、保密性采取安全控制手段及其传输鉴别保护手段，防范传输数据遭到非法访问或修改，并对网络进行安全监控。

4. 无线网络防护

该控制项旨在检查组织在部署工控无线网络前是否进行安全风险分析并制定相应的管理制度，采取必要的安全防护措施确保工控无线网络安全。

**（三）常见问题和风险**

1. 工控系统安全区域边界访问控制不严格，遭受非法入侵或网络攻击，引起网络异常或中断。

2. 工控系统边界防护能力较弱，导致注入攻击、网络入侵、恶意代码入侵的发生，影响网络的安全性和稳定性。

**（四）审计的主要方法和程序**

1. 安全区域边界访问控制

（1）访谈工控系统安全负责人，询问是否对组织工控系统采取分层和安全域的管理方式，并对各层和各安全域之间基于

安全要求制定访问控制策略，部署相应访问控制设备。

（2）查阅工控网络拓扑图，验证部署的设备（如工业防火墙）位置是否能起到边界访问控制目的。

（3）访谈组织是否制定访问控制策略，并检查其是否设置于部署的访问控制设备上，实现区域边界访问控制，边界防护隔离，边界防护安全管道通信和消息来源、用户、设备身份鉴别及访问控制。（区域边界访问控制）

（4）检查组织是否基于访问控制策略实现对访问源地址、目的地址、源端口、目的端口、协议的检查，从而实现对安全区域间的数据包过滤、安全域之间的路由控制和层间的会话控制。（区域边界包过滤）

2. 安全区域边界防护

（1）检查组织是否制定恶意代码防范的规章制度和安全控制策略，其内容至少应包括恶意病毒库的升级与更新策略,针对恶意入侵行为的分类、报警、处置等防护规则和处置流程。

（2）检查组织是否部署探测器，实现对非法外联行为（如非授权设备私自连接到内网，或内部网络用户私自连接到外部其他网络）进行准确定位和有效阻断，并对探测设备进行有效性验证。（边界完整性防护）

（3）检查组织是否采用验证机制，对重要控制指令和现场数据在存储和传输过程中的完整性进行有效验证和适当的恢复、

修复等处置措施，并验证处置措施的有效性。

（4）检查组织是否在区域边界部署恶意代码检测和防范设备，实现如端口扫描等恶意代码入侵行为进行监视、报告和有效监测与清除。

（5）验证恶意代码防范设备的代码库是否及时升级和更新，以及设备间是否对攻击行为进行定位并提供相应的报警和自动处置，防止恶意代码传播。

3. 网络通信安全管理

（1）访谈工控网络安全管理员，询问是否对工控数据传输网络采取密码技术等完整性校验机制，保证传输过程中数据传输的完整性并对其进行完整性校验以及在遭到破坏时进行恢复；询问是否对工控数据传输网络采取密码技术和加密算法与加密设备，从而保证传输过程中数据传输的保密性，实现对会话初始化验证、报文或会话加密、传输保密性保护等安全要求；询问是否对工控数据传输网络采取密码技术，实现对数据来源的鉴别，从而实现对非法的数据访问和数据修改予以拒绝；询问是否对工控网络部署网络监控设备或软件，对网络数据、程序、操作和控制命令进行识别和监测，对恶意行为、攻击、异常流量进行识别、监测、记录、定位，以及对恶意流量进行阻断。

（2）验证加密算法和设备的合规性，以及传输加密的速度和加密有效性是否符合业务要求。

4. 无线网络防护

（1）访谈工控网络安全负责人，了解目前组织在工控网络是否部署无线网络并对其存在的威胁和潜在风险进行分析，查看风险评估报告；了解是否制定工控无线网络的安全管理制度、规范及安全控制策略。

（2）查看工控无线网络的管理制度及规范，检查是否明确其保护措施（如物理防护、电磁屏蔽），并查验保护措施的实际部署情况（如无线防火墙）。

## 六、安全管理中心及安全审计

### （一）业务概述

工控安全建立安全管理中心，实现对工控系统资源、安全运行的集中、统一管理，同时对工控系统涉及的主客体制定统一的安全策略。

### （二）审计目标和内容

1. 安全管理中心建设与管理

该控制项旨在检查组织是否为确保工控安全建立安全管理中心，实现对工控系统资源、安全运行的集中、统一管理，同时对工控系统涉及的主客体制定统一的安全策略，执行包括身份鉴别、系统与安全事件监控、安全管理与维护，以及自动化的安全监测与预警。

2. 安全审计管理与实施

该控制项旨在检查组织是否就工控涉及的主机和系统制定相应的安全审计规范、策略，并将其部署于安全管理中心，基于其具有的审计管理功能对工控平台主机系统和工控网络及其相关管理操作实施安全审计。

（三）常见问题和风险

1. 工控系统安全管理过于分散，无法实现有效集中管控，增加管理负担和管理成本。

2. 重要工控主机和系统未部署安全审计工具，无法对操作行为进行记录，不利于及时发现存在的违规操作，不利于工控系统的安全发展。

（四）审计的主要方法和程序

1. 安全管理中心建设与管理

（1）查阅组织工控安全管理战略规划及其相关安全管理制度与安全策略，了解组织对于工控安全管理的基本要求。

（2）访谈工控安全负责人，询问是否建立统一、集中的工控安全管理中心并了解其功能和实现方式。

（3）查阅安全管理中心建设的规划和验收报告，综合组织对于工控安全管理和基本要求以及当前工控安全管理中的功能，判断安全管理中心所具有的功能是否可以满足组织对于工控安全管理的要求。

（4）检查安全管理中心是否具备：对工控系统资源和运行

的配置、控制和管理的系统管理功能，并具有运行监控与告警、系统日志记录等功能，同时实现用户身份管理、系统运行异常处理、灾难备份与恢复和对系统管理操作进行安全审计的功能；对工控系统设备的可用性、安全性实施监控与告警，设备集中管理与维护，漏洞扫描与配置加固以及安全预警的安全管理功能。

（5）检查安全管理中心的管理制度与安全策略：是否对日志收集及其内容、格式、访问、存储进行要求，并验证安全日志数据采集的记录项是否符合制度规范要求，以及对日志的访问和保存是否采用校验机制并实现异地、冗余存放，保存周期不低于6个月；是否定义工控数据采集、内容监测、恶意（异常）行为判断标准、事件和行为处理标准以及事件监测、预警、处置、响应是否符合既定的标准与规范，验证安全管理中心是否可对安全事件进行监测报警和处置，并审查历史安全事件的处置记录是否符合既定的流程规范；检查安全管理中心的漏洞扫描与加固历史记录，验证关键漏洞是否已得到安全加固。

2. 安全审计管理与实施

（1）查阅并检查组织是否制定安全审计规范与审计策略。

（2）检查工控安全管理中心的安全审计策略配置是否运行有效。

（3）检查组织是否对重要工控主机和系统部署安全审计工

具，并部署在各关键主机和系统之上且在安全管理中心对所收集的日志实施集中、独立的安全审计。

（4）询问安全管理中心负责人，了解安全管理中心是否支持安全信息的分类管理与查询以及安全审计功能是否支持二次开发和报警与日志信息的关联分析，并调阅审计报告验证其功能。

## 第八节　物联网安全审计

物联网通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。对大型物联网来说，处理应用层一般是云计算平台和业务应用终端设备。物联网安全的风险着重体现在感知节点及其所处物理环境的安全，物联网及其异构传输网络的通信和结构安全（如是否采取安全加密机制、网络安全防护），用户/设备鉴别信息和感知节点数据采集信息的安全和服务中断等多种风险。

本节将从物联网的感知设备物理与环境安全、网络与通信安全、安全区域边界、设备和计算安全、应用与数据安全、安全审计等方面对物联网安全的审计方法和步骤进行描述。

### 一、感知设备物理与环境安全审计

#### （一）业务概述

是指感知层终端节点所处的物理环境对其安全产生的影响，

以及所采取的相关安全防护措施是否充分。

（二）审计目标和内容

1. 终端感知节点物理与环境安全

该控制项旨在检查感知层终端节点所处的物理环境是否对其安全产生影响，以及是否受到安全防护措施及其措施的有效性。

2. 感知层网关节点物理与环境安全

该控制项旨在检查感知层网关节点所处物理环境是否对其安全产生影响，以及是否受到安全防护措施并审查防护措施的有效性。

3. 感知设备访问控制

该控制项旨在检查感知层网的节点、网关设备及其网络资源采取访问控制措施，确保上层用户对上述资源的合法访问与使用。

4. 感知设备恶意代码与入侵防护

该控制项旨在检查组织是否对终端感知节点和感知网关节点部署恶意代码防护设备与入侵检测设备，并定期开展漏洞扫描和代码库的升级与更新工作，验证防护措施有效性。

（三）常见问题和风险

1. 终端感知节点物理环境安全管控不严格，导致意外断电、电磁干扰、发生火灾等情况，影响终端感知的正常运行。

2. 终端感知节点和感知网关节点未安装恶意代码防护设备，导致恶意代码入侵系统或恶意代码在网络传播，造成网络中断和感知状态中断。

**（四）审计的主要方法和程序**

1. 终端感知节点物理与环境安全

访谈物理安全负责人，询问终端感知节点的物理安全需求及环境现状（或实地查看），判断是否对其产生物理破坏；询问针对感知节点所处的物理环境，采取哪些防范措施以确保其物理环境安全（如非法物理访问、防雷、防电磁干扰等），并检查是否与实际情况相一致；询问感知节点是否可以准确反映其所处物理环境状态，并对其所获取的物理数据与实际环境数据进行验证，或者查阅物理环境的设计和验收文档；询问感知节点是否设置备用电源从而满足其最低电力供应需求，并验证电力供应系统是否可在规定时间内正常启动和供电；询问是否对感知节点进行物理加固并设置明显、不易去除的标志，且确保标识的唯一性。

2. 感知层网关节点物理与环境安全

（1）访谈物理安全负责人，询问感知层网关节点的物理安全需求（如防火、防静电等）及其为满足安全需求所采取的安全防护措施；询问感知层关键网关节点所在物理环境是否具有良好的信号收发能力，并检查是否对其所在物理环境部署反屏

蔽设施，验证所在物理环境的信号收发能力。

（2）查看感知层网关节点的实际物理环境，验证物理防护措施的有效性。

（3）检查感知层网关节点的主要部件是否接受安全固定，防止被移动或被搬走；是否有明显的不易除去的标记；是否设置短期备用电源从而满足其最低电力供应需求，并验证电力供应系统是否可在规定时间内正常启动和供电。

3. 感知设备访问控制

访谈网络管理员，询问针对物联网终端及感知节点设备，是否采取必要的技术手段防止其非法下载软件应用，且对合法用户的身份及其访问控制权限进行识别，确保对感知网资源和设备的合法访问与使用，并对技术手段的有效性进行验证；（感知设备/节点的访问控制）

4. 感知设备恶意代码与入侵防护

（1）访谈安全管理员，询问是否对终端感知节点和感知网关节点安装恶意代码防护设备，并定期对其进行更新且在监测出恶意代码后及时报警。

（2）检查是否定期对终端感知节点和感知网关节点进行漏洞扫描，防范被用于木马、病毒的攻击，使得终端节点被非法控制或处于不可用状态，从而获取未授权的访问实施攻击或成为网络渗透入口，并查验历史漏洞扫描记录。

## 二、网络与通信安全审计

### （一）业务概述

是指物联网的感知设备的身份认证、访问控制、无线接入的安全，以及通讯网络安全管理、数据安全传输等措施的实施。

### （二）审计目标和内容

1. 入网感知设备安全认证

该控制项旨在检查是否对接入物联网的感知设备进行认证，以确保感知设备及其数据收集、传输的安全可靠。

2. 感知设备访问控制

该控制项旨在检查是否对感知设备/节点及其传感网的接入网络采取必要的安全访问控制措施，防止对感知设备/节点及其感知网资源的非法访问与使用。

3. 无线网的安全接入

该控制项旨在检查组织是否存在通过无线网络接入的感知终端，并验证是否对其采取必要的安全工作措施确保无线网络的安全性。

4. 异构网的安全接入与保护

该控制项旨在检查组织是否存在异构网的物联网接入，并验证是否对其采取必要的安全工作措施确保异构网数据传输的完整性和保密性。

5. 网络数据传输保护

该控制项旨在重点检查是否为确保物联网传输数据的完整性、保密性和新鲜度采取控制措施，并对接入物联网的通信设备进行可信验证，防止非法接入。

6. 通信网络安全管理

该控制项旨在检查组织是否对物联网通信网络采取安全监控、应急等安全管理措施，防范因传输链路故障造成数据传输失效及服务不可用。

### （三）常见问题和风险

1. 入网感知设备安全认证机制不完善，导致安全认证机制被绕开或非法的物联网终端接入，对感知设备运行造成安全影响。

2. 网络数据传输保护机制不严格，导致感知层感知数据在传输过程中外泄或数据传输过程中被篡改。

### （四）审计的主要方法和程序

1. 入网感知设备安全认证

访谈网络管理员，询问是否对感知终端接入网络时采取设备认证机制以及所采取认证的具体措施；是否制定感知终端认证的策略文档，查看是否包括防止非法的物联网终端接入网络的机制描述；询问是否存在较大数量物联网终端设备接入网络的应用以及是否提供组认证的机制及其相关举措。

2. 感知设备访问控制

（1）访谈网络管理员，询问是否制定访问控制策略对传感网入网采取必要的访问控制措施，并了解访问控制措施的具体内容，查看相应的控制策略文档；询问是否对感知终端设备的网络接入制定相应访问控制策略并检查传感网入网访问控制设备，验证访问控制策略的配置情况；询问是否允许远程配置物联网感知终端和节点设备上的软件应用，以及是否制定相应的远程访问安全控制机制并采取安全防护措施，了解安全机制是否覆盖对资源访问相关的主体、客体及它们之间的操作。

3. 无线网的安全接入

访谈网络管理员，询问组织目前是否存在无线网接入的感知终端，或通过无线网进行采集信息的传输；询问并查阅是否对制定无线网安全管理制度及安全策略；询问是否定期根据无线网络脆弱性对其进行安全风险评估和安全检查。

4. 异构网的安全接入与保护

访谈网络管理员，询问组织目前的联网是否存在异构网络的接入需要及其各接入网的工作职能、重要性和所涉及信息的重要程度等因素；询问是否对各异构网的接入网网关进行子网或网段的划分，了解各安全划分子网/网段的功能，并查看接入网关的安全配置；询问并查阅是否对异构网的物联网接入制定相应安全管理制度及安全策略；询问是否对异构网接入时的数据转发采取安全措施（如加密及完整性校验）确保数据完整性

和保密性，了解保密性保护机制是否符合国家密码行政主管部门规定，验证安全措施的有效性并调阅测试报告；询问是否采用入侵检测等技术拒绝恶意设备的接入，保证合法设备不被恶意设备攻击而被拒绝接入，保证网络资源的可使用性。

5. 网络数据传输保护

访谈网络管理员，询问为确保包括感知层感知数据在内的数据传输的完整性和保密性所采取的加密算法和完整性机制，了解是否符合国家密码管理的相关规定并验证在发现完整性被破坏时进行恢复；询问为确保感知层感知数据的新鲜度所采取的控制措施；询问是否对连接到通信网络的设备进行可信检验，从而确保接入通信网络的设备真实可信，防止设备的非法接入。

6. 通信网络安全管理

（1）访谈网络管理员，询问终端感知设备进行数据传输的网络现状，如服务商数量（若存在外部网络运营服务商）、传输链路数量，从而判断是否存在单点故障；询问是否对感知终端的数据传输网络流量进行监控并制定流量应急管控方案，防范传输流量过大造成的网络拥塞；询问是否对连接感知终端与服务端的通信网络增加流量分析、态势感知等安全策略。

（2）访谈物联网管理负责人，询问是否制定通信网络的专项应急预案，并进行定期应急演练，查看历史记录并检查是否将外部网络运营商纳入到应急演练参与者当中。

## 三、安全区域边界审计

### （一）业务概述

是指为物联网建立安全区域边界，对安全区域边界进行访问控制，对进出边界的数据进行安全过滤，对进入物联网的设备采用准入控制等安全措施。

### （二）审计目标和内容

1. 安全区域边界访问控制

该控制项旨在检查组织是否对物联网进行安全区域的划分，并对其制定相应的访问控制策略及开展安全访问控制。

2. 区域边界过滤与控制

该控制项旨在检查组织是否基于已制定的访问控制策略，对进出区域边界的数据包和报文实施过滤机制。

3. 区域边界完整性保护和准入控制

该控制项旨在检查是否采取安全控制措施以确保区域边界的完整性并对其实施准入的控制措施。

### （三）常见问题和风险

1. 物联网安全区域边界访问控制不严格，遭受非法入侵或网络攻击，引起网络异常或中断。

2. 物联网区域边界完整性保护不足，容易导致非法外联和入侵行为，影响感知设备的正常使用。

### （四）审计的主要方法和程序

1. 安全区域边界访问控制

访谈网络管理员，询问是否对信息系统进行安全区域的划分，了解各区域的访问控制方式及是否制定相应的访问控制策略，从而对进出安全区域边界的数据信息进行控制，防止非授权访问；询问是否对物联网区域实施边界访问控制，制定针对数据、协议、流量和最大连接数等内容的访问控制策略。

2. 区域边界过滤与控制

访谈网络管理员，询问是否根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界；询问是否在安全区域边界设置协议过滤，从而对物联网通信内容进行过滤，并对通信报文进行合规检查，以及根据协议特性，设置相对应控制机制。（区域边界协议过滤与控制）

3. 区域边界完整性保护和准入控制

访谈网络安全管理员，询问是否制定物联网边界区域完整性保护的策略及相关安全措施；询问是否制定安全区域边界的准入控制机制对接入设备进行有效标识、识别，从而保证合法设备接入，拒绝恶意设备或非法接入；询问是否在区域边界设置探测器或探测软件，探测非法外联和入侵行为并及时报告，同时验证非法接入识别的有效性；询问是否在区域边界设置轻量级的双向认证机制，能够保证防止数据的违规传输；询问是

否可对感知设备的健康数据进行收集（如固件版本、标识、配置信息校验值等），从而对接入的感知设备进行健康性检查，拒绝非健康设备的接入。

## 四、设备和计算安全审计

### （一）业务概述

是指对物联网系统设备身份进行鉴别与访问控制，对设备数据进行安全管理，以及对其进行安全监测及恶意代码和漏洞防护。

### （二）审计目标和内容

1. 设备身份鉴别与访问控制

该控制项旨在检查是否分别对物联网系统的设备身份进行有效标识和鉴别，并确保其唯一性和鉴别信息的保密性与完整性；同时，检查是否制定相应的访问控制策略和访问操作权限。

2. 设备数据信息安全管理

该控制项旨在检查组织对物联网系统的设备信息及其收集、处理和存储的重要数据信息采取安全控制措施，确保数据安全，同时审核所采取的安全技术手段是否符合国家的安全规定。

3. 安全监测及恶意代码和漏洞防护

该控制项旨在检查组织是否采取安全控制手段，对应用端服务器进行安全监测，部署恶意代码防护工具，同时开展漏洞扫描和渗透测试。

（三）常见问题和风险

1. 终端感知节点（包括 RFID 标签）和感知层网关节点（包括 RFID 读写器）未建立统一的身份标识和鉴别机制，造成身份认证混乱或身份认证机制被破解，影响设备的正常运行。

2. 物理网设备对于生存信息、鉴别信息、隐私性数据和重要业务数据的保护力度不足，造成数据传输过程中被非法访问或泄露。

3. 关注设备数据信息安全风险，安全技术手段不符合国家安全规定的风险。

（四）审计的主要方法和程序

1. 设备身份鉴别与访问控制

访谈系统管理员，询问是否对终端感知节点（包括 RFID 标签）和感知层网关节点（包括 RFID 读写器）进行统一身份标识和鉴别管理，并确保在系统整个生存周期设备标识的唯一性；询问是否对设备的身份鉴别信息在传输与存储过程中采取必要的安全措施，确保其机密性和完整性，并对感知设备发送的数据进行鉴别，确保防范虚假信息的恶意注入，并核查加密算法是否符合国家规范；询问身份鉴别管理系统是否可对合法的连接设备（包括终端节点、路由节点、数据处理中心）进行有效鉴别，并可识别非法节点和伪造节点，过滤其发送的数据和重放合法节点的历史数据；询问是否针对感知设备和其他设备（感

知层网关、其他感知设备）间的通信，制定访问控制策略，确保权限检查通过后才允许设备间开始通信或对用户进行权限检查，只有经过授权的合法用户才能通过外部接口对感知设备进行更新配置、下载软件等。

2. 设备数据信息安全管理

（1）访谈系统管理员，是否对物理网设备的生存信息、鉴别信息、隐私性数据和重要业务数据在存储过程中采用密码等技术进行完整性校验，确保校验信息在其受到破坏时能够进行恢复、重传，以及使用符合国家密码行政主管部门规定的数字摘要算法、签名算法等；询问是否对物理网设备的生存信息、鉴别信息、隐私性数据和重要业务数据在存储过程中采用密码等技术进行加密，并检查加密算法是否符合国家规定。

（2）访谈数据库安全管理员，询问感知终端数据的存储模式，以及是否对网络服务端的数据管理系统做到系统加固、漏洞检测与修复、防黑客、抗 DDoS 攻击、安全审计、行为检测等服务器安全防护，以防发生由于主机被攻破导致的数据泄漏、数据篡改等安全问题。

3. 安全监测及恶意代码和漏洞防护

（1）访谈主机和工控系统安全管理员，询问并检查是否对工业主机服务器和工控系统：部署入侵检测系统并查验历史记录，判断系统是否可对监测出的入侵行为或异常业务操作进行

异常分析和报警；部署并进行防恶意代码库和补丁漏洞的升级与修补，并在此之前进行安全测试及制定回退计划，并查阅相关历史记录。

（2）访谈系统管理员，询问是否对应用端的服务器采取：设置安全基线，制定防篡改、防挂马安全规范，提出监测、防护与处置机制和要求；对应用服务器部署自动检测工具并定期开展漏洞扫描、渗透测试等检查工作；安装防病毒、通讯监视等软件。

## 五、应用与数据安全审计

### （一）业务概述

是指物联相关应用在身份鉴别与访问控制等方面的安全管理，相关数据在完整性、机密性、可用性等方面的安全管理。

### （二）审计目标和内容

1. 用户身份鉴别与访问控制

该控制项旨在检查组织是否采取有效的控制措施，对物联网系统的用户身份进行鉴别并确保鉴别信息的安全，同时检查是否根据用户身份制定访问控制策略确保操作合规可控。

2. 用户及业务数据信息安全管理

该控制项旨在检查组织是否对物联网系统用户数据和重要业务数据制定数据安全管理策略并采取安全控制措施，确保数据的保密性与可用性。

3. 抗数据重放

该控制项旨在检查组织是否采取安全控制手段，在确保数据新鲜性的同时，监测并防范历史数据被重放。

### （三）常见问题和风险

1. 物联网系统访问控制机制不严格，导致重要或敏感数据被非授权访问，造成重要或敏感数据的破坏或泄露。

2. 感知节点数据新鲜性保护措施不足，导致系统遭到重放攻击，认证凭据被非法篡改。

### （四）审计的主要方法和程序

1. 用户身份鉴别与访问控制

访谈系统管理员，询问是否对物联网系统的用户进行标识和鉴别，确保在系统整个生存周期用户标识的唯一性以及采用统一、集中且不少于两种组合机制进行身份鉴别，同时，可对假冒用户使用未授权的业务应用或者合法用户使用未定制的业务应用进行鉴别；询问是否对用户身份鉴别信息、口令、密钥在传输与存储过程中采取必要的安全措施，确保其机密性和完整性；询问是否针对物联网用户和管理员制定访问控制策略，明确访问控制规则、访问控制的颗粒度及操作权限；询问是否提供对远程登录用户的认证功能，以及认证的方式有哪些，并验证远程登录用户的认证功能。

2. 用户及业务数据信息安全管理

（1）访谈系统管理员，是否对存储和处理的用户数据及重要数据（指令控制数据、业务数据）采用密码等技术进行完整性校验机制和保密机制，发现完整性受破坏的数据并对重要数据进行恢复，同时确保数据的保密性。

（2）访谈网络管理员，询问是否对感知层重要业务数据进行本地备份，以及是否制定备份策略和数据重传策略，并检查感知层重要业务数据的本地备份和重传功能，其配置是否正确，查看其备份结果是否与备份策略一致，重传策略是否生效。（数据可用性）

3. 抗数据重放

（1）访谈安全管理员，询问针对感知节点数据新鲜性的保护措施有哪些。

（2）检查感知节点鉴别数据新鲜性的措施，并尝试将感知节点设备历史数据进行重放，验证其保护措施是否生效。

（3）访谈安全管理员，询问针对防范历史数据被非法修改的防护和检测措施有哪些。

（4）检查感知层是否配备检测感知节点历史数据被非法篡改的措施，并验证检测措施的有效性是否能够避免数据的修改重放攻击，以及在检测到被修改时是否能采取必要的恢复措施。

## 六、安全审计

### （一）业务概述

是指制定物联网相关安全审计规范和安全审计策略，部署安全审计平台和工具，开展安全审计工作。

### （二）审计目标和内容

1. 安全审计的管理

该控制项旨在检查组织是否就物联网安全制定专项的安全审计规范和安全审计策略并据此部署和开展安全审计工作。

2. 安全审计的实施

该控制项旨在检查组织是否根据既定的安全审计规范与策略开展安全审计，并检查安全审计的内容是否涵盖物联网通信安全、边界安全及系统安全，同时验证集中式安全管理中心是否对已定义的安全事件及时发现并报警。

### （三）常见问题和风险

1. 未制定物联网安全专项审计规范和策略，无法有效落实物联网安全审计要求，不利于物联网管控措施的持续改进。

2. 未针对分布在物联网上的系统部署安全审计工具，无法有效监控各系统的状态和异常，无法及时发现系统的攻击行为和非授权访问和破坏。

### （四）审计的主要方法和程序

1. 安全审计的管理

（1）检查组织是否制定物联网安全专项审计规范和审计策略，并部署安全审计工具或平台。

（2）查看物联网安全审计规范，检查其内容是否对审计日志的内容、格式、访问、存储和安全报警事件进行明确要求，并对审计日志进行抽样检查，检查其日志管理要求是否符合制度规范要求；检查其内容是否对物联网安全事件进行定义、分类，明确安全事件的主体、客体、时间、类型和结果等内容；检查其内容是否对审计记录的存储、管理和查询进行明确要求，防止非授权访问和破坏，并验证保存时间是否符合规范要求。

（3）访谈信息安全审计负责人，询问是否对分布在物联网系统的各个重要组件部署安全审计工具并实现集中管理，且具有：为集中安全管理工具或平台提供接口；可按时间段开启和关闭相应类型的安全审计功能；对审计记录的查询、分类、分析和存储保护的功能，并根据分析结果进行处理；对安全审计员进行身份鉴别，且只允许其通过特定的命令或操作界面进行安全审计操作的功能。

2. 安全审计的实施

（1）查看物联网安全审计规范，审查其内容是否对物联网通信网络提出审计要求，查阅审计记录，判断并验证是否对通信网络设置审计机制，并由安全管理中心集中管理，且对确认的违规行为进行报警。

（2）审查其内容是否对物联网区域边界安全提出审计要求，查阅审计记录，判断并验证是否对安全区域边界设置审计机制，

由安全管理中心集中管理，并对确认的违规行为及时报警。

（3）审查其内容是否对系统安全审计提出审计要求，查看系统安全审计工具，检查其是否具备对不能由系统独立处理的安全事件，提供由授权主体调用的接口，并验证其是否可由安全管理中心集中管理，且对确认的违规行为及时报警。

# 第六章　信息系统审计质量控制

## 第一节　信息系统审计质量控制

### 一、信息系统审计质量概述

为了确保信息系统审计的质量，组织应建立信息系统审计质量控制策略、程序、方法,明确内部审计人员职责，遵循国家法律法规、信息系统审计操作规范和组织内部审计工作规定；审计工作底稿、审计报告、审计决定等审计文书的格式、要素和内容应当符合组织内部审计规范的要求；组织信息系统管理和应用方面存在的重大问题得以充分揭示，并提出建议，以合理保证审计目标的实现。

信息系统审计项目质量控制主要包括对审计计划、审计实施、审计终结等阶段的全过程质量控制。

### 二、审计质量控制内容

#### （一）质量控制制度建设

信息系统审计的质量控制应当按照国家审计准则、中国内部审计准则、参照国内外信息系统审计标准和规范，建立起包含质量责任、职业道德、职业胜任能力、业务执行和质量监控等在内的质量控制制度，同时，应制定适用本组织的信息系统审计流程、标准和规范。

#### （二）审计全过程质量控制

1. 审计计划质量控制

计划立项和审前准备阶段需要对组织的信息系统进行初步调查，主要获取组织业务流程对信息化的依赖程度;与信息系统有关的管理机构及管理方式，根据掌握的信息系统基本情况，确定审计目标与重要性水平，在制定审计实施方案时，应充分考虑以下因素：

（1）组织高度依赖信息技术、信息系统的关键业务流程及相关的组织战略目标。

（2）信息技术管理的组织架构。

（3）信息系统框架和信息系统的长期发展规划及近期发展计划。

（4）信息系统及其支持的业务流程的变更情况。

（5）以前年度信息系统内外部审计等相关的审计发现及后续审计情况。

（6）其他影响信息系统审计的因素。

2. 审计实施质量控制

（1）控制测试质量控制

控制测试是为测试组织对控制程序的符合性而收集证据，验证控制的执行是否符合管理政策和规程要求。根据组织确定的内部控制缺陷标准及风险评估标准，对组织的内部控制实施控制测试。应当采用抽样执行的控制测试包括用户访问权限、

程序变更控制流程、文件流程、编程文档、例外跟踪、日志检查、软件许可审计等。根据控制测试的结果决定实质性测试的时间、范围和性质。

在实质性测试时,内部审计人员要对交易和事项的安全控制措施进行测试，对信息系统的安全性、可靠性和经济性进行评价。为保证评价的质量，内部审计人员要对交易或事项进行测试，在验证数据库可靠性时，应对交易日志中的查询进行抽样审查，以评价该查询操作的可靠性，在评价信息系统的效率性时，内部审计人员要评价提交作业到执行后结果返回用户所评价周转时间是否在可接受范围内。

在进行审计时要根据情况确定审计抽样的方法及测试的范围。采用随机、统计、判断等抽样方法，并合理确定样本量，根据抽样样本的实质性测试结果,评价信息系统控制是否达到控制目标。当抽样不能达到审计目标时还应采用替代程序。

（2）审计证据质量控制

明确审计取证的范围,审计证据要足以支持审计报告和审计结论中揭示的问题；为保障审计证据的充分性、相关性和可靠性,应规范审计取证的方法，除通用证据获取方法外，应根据信息系统取证的要求,侧重于利用数据工具、安全工具、测评工具、系统运行监测、系统监控检测等方法取证,以规范审计取证行为。应恰当处理和评价审计证据,要求证据的提供部门确认其

来源真实。评价审计证据时,应当考虑电子数据、纸质数据、结构化数据、非结构化数据之间的相互印证及证据来源的可靠程度。

3. 审计报告质量控制

（1）审计工作底稿复核

审计工作底稿是内部审计人员在审计过程中形成的审计工作记录和获取的资料。审计工作底稿是审计证据的载体,是联系审计证据和审计结论的桥梁。审计工作底稿的全部内容，是内部审计人员形成审计结论、发表审计意见的直接依据。审计工作底稿必须进行复核,以保证审计意见的正确性和审计工作底稿的规范性。

（2）审计报告编制、复核与交换意见

内部审计人员应对审计发现进行分析，使用职业判断，确定哪些审计发现应提交给哪个层级的管理人员。向管理层提交审计报告。审计报告具有如下特征：

①足够重要、值得向管理层报告。

②事实清楚、证据充分。

③描述客观、公正。

④与所审计的事实相关。

⑤有充分的说服力，促使组织采取纠正措施等。

除了对信息系统的安全性、可靠性、经济性发表意见外，还需要对信息系统所承载的业务信息的真实性、完整性、正确性发表意见。

在与高级管理层沟通审计结果前，内部审计人员应当首先与被审计组织的管理人员讨论审计发现的问题，在审计报告征求意见过程中，内部审计人员和被审计组织应当针对审计建议、预定实施日期等内容进行讨论，明确影响实施的各种因素。被审计组织管理层应当对审计报告中描述的审计发现制定整改计划,陈述将要采取的整改措施及整改时间等，促进双方达到一致性观点。当不能达成一致时，内部审计人员应当详细描述审计发现的重要性。确保报告中反映的情况是真实的，相关建议切实可行且符合成本效益，针对建议的实施日期与管理层进行讨论等。

（3）审计报告正式上报前需要考虑的质量问题

在出具正式审计报告之前，内部审计人员应考虑在此期间被审计组织及其信息系统活动是否会发生导致重大变化的事项(如机房搬迁、更新原有模块等)。针对这种情况，审计人员应当判断这些事项对审计结论和建议的影响，并采取增加审计程序、修改审计意见等措施，提醒报告使用者注意上述影响。

4. 归档质量的控制

内部审计机构应当制定保管、保留和发布审计文档的相关政策。各审计主体在实际工作中，应根据相关规范的要求管理审计文档。

5. 后续审计质量控制

实施后续审计，主要应考虑：

（1）审计意见和建议的重要性。

（2）整改措施的复杂性。

（3）落实整改措施所要的时间和成本。

（4）整改措施失败可能产生的影响。

后续审计的质量管理控制包括：

（1）制定跟踪程序以确认既定的整改措施是否已经落实。

（2）审计实施管理，合理确定跟踪检查的程度。

（3）合理确定跟踪时间。

（4）与适当层级的管理人员沟通跟踪结果。

通过上述信息系统审计全过程质量控制活动，达到规范审计行为，规避审计风险，提高审计质量的质量控制目标。

## 第二节　信息系统审计人员胜任能力

一、审计机构人员素质保障。基于信息系统审计的特殊性和复杂性，作为组织的审计机构，要求人才结构合理配置，包

含审计业务骨干、信息技术专家、信息系统管理专家，同时，应考虑建立信息系统审计兼职业务专家团队。

二、审计项目团队素质保障。制定信息系统审计项目计划时，根据审计项目的特点，充分评估审计人员的知识结构、年龄结构、实际操作能力，合理确定审计组长、主审人、审计成员等，审计组应包括审计业务人员、计算机专业人员、信息系统开发人员、网络管理、系统运维管理人员等，必要时信息系统项目审计可以对外聘请具有相应资质的外部信息系统审计机构或具备相应能力的技术专家参与或独立开展审计，以防范审计风险。

三、强化审计项目团队的培训。有针对性的培训是项目顺利实施，按质量实现审计目标的重要保证，包括对审计信息化知识和技术的培训、对相关制度规范的培训等。

四、内部审计机构与人员责任落实。在信息系统审计实施过程中，审计组长、主审、审计人员等应各司其职，确保审计过程中的质量。相关业务部门人员、质量复核人员、审计机构负责人应承担相应的质量控制责任，确保信息系统审计质量控制措施得到贯彻执行。

## 附录 1：相关术语

### ·信息系统

信息系统是由计算机硬件、网络和通讯设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的，通过对信息的收集、传输、加工、存储、更新和维护，以组织战略竞优、提高效益和效率为目的,支持组织高层决策、中层控制、基层运作的集成化的人机系统。

### ·信息系统审计

信息系统审计是指内部审计机构和内部审计人员对组织的信息系统建设的合法合规性及其相关信息技术内部控制的有效性、信息系统的安全性、业务流程合理有效性、信息系统运行的经济性所进行的检查与评价活动。

### ·联网审计

联网审计是指内部审计机构与被审计单位进行网络互连后，在对被审计单位财政财务管理相关信息系统进行测评和高效率的数据采集与分析的基础上，对被审计单位财政财务收支的真实、合法、效益进行实时、远程检查监督的行为。通过联网审计，内部审计人员可以非现场实时或定时地监督被审计单位的业务活动、内部控制和风险管理。

### ·大数据审计

大数据审计主要指运用大数据思维，归集不同行业和部门的数据，进行分析、挖掘，进而发现数据之间的内在联系，提高问题的洞察力，是提高审计质量、提高审计效率和实现审计全覆盖的关键所在。

**• 信息系统生命周期**

信息系统生命周期是指信息系统在使用过程中随着其生存环境的变化而变化，信息系统的生命周期可分为立项、开发、运维和消亡四个阶段。

**• 组织控制审计**

对组织层面建立并实施的信息系统相关控制开展的审计。

**• 一般控制审计**

为了保证信息系统安全、稳定地运行，对整个信息系统以及外部各种环境要素实施的、对所有的应用或控制模块具有普遍影响的控制审计。

**• 应用控制审计**

业务流程层面为合理保证应用系统准确、完整、及时地完成业务数据的生成、记录、处理、报告等功能、而设计、执行的控制审计。

**• 安全审计**

安全审计是指按照一定的安全策略，利用操作记录、系统活动和用户活动等日志信息，通过检查、审查和检验操作事件

的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。安全审计从审计级别上可分为三种类型：系统级审计、应用级审计和用户级审计。

**• 信息系统可靠性**

是指信息系统在遭受非人为因素破坏或误操作情况下仍然能正常运行的概率。威胁信息系统可靠性的因素包括自然灾害对硬件和环境的破坏、误操作对软件和硬件的破坏、以及设备故障、软件故障等。

**• 信息系统稳定性**

是指信息系统要素在外界影响下表现出的某种稳定状态。包括但不限于外界自然条件、城市基础设施、信息系统所依赖的各类资源等各种变化、干扰。

**• 信息系统安全性**

是指信息系统在遭受各种人为因素破坏的情况下仍然能正常运行的概率。威胁信息系统安全性的因素可能来自信息系统和组织外部和内部。外部包括但不限于黑客入侵、病毒攻击、线路侦听、木马、非法用户访问等，内部包括授权用户的越权访问、修改、删除等操作。

**• 数据处理的完整性和准确性**

是指信息系统中的数据不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性，能够如实地反映

组织实际生产经营活动。通过一系列技术手段可以确保数据的真实、准确，包括但不限于数字签名、时间戳、不可否认协议、不可修改存储装置等。

**• 软件配置费**

包括但不限于：购买操作系统、数据库、工具软件、应用软件等的费用。

**• 硬件配置费**

包括但不限于：购买服务器、计算机、打印机、扫描仪、接口等硬件设备的费用。

**• 网络建设费**

包括但不限于：购买交换机、路由器、光缆、配件及布线、集成等网络建设的费用。

**• 技术服务费**

包括但不限于：软件设计、开发、采集数据、建模、安装、调试、集成、实施、咨询等技术服务类的人工费用。

**• 培训管理费、所属单位配套实施管理费、其他费用**

一般包括但不限于：用户单位的项目实施人员、系统使用人员、系统维护人员的国内外技术培训所需费用；用于维持项目基本运行所必需的各项办公、日常用品等项目费用以及所属组织在项目实施中发生的相关管理费用。

**• 不可预见费**

指为保证项目正常进行，避免上述各项费用预算出现差异而列示的项目机动费用。

**• 咨询费用**

指系统建设与运行维护中支付给咨询单位或专家的费用。

**• 链路租赁费**

指支付给内、外部通信运营商的链路租赁费用。

**• 场地租赁费**

指数据中心、办公场地租赁费用。

**• 折旧及摊销费用**

指房屋、服务器等固定资产折旧以及无形资产摊销费用及其他专项费用。

## 附录 2：主要参考法规与标准

1. 第 2203 号内部审计具体准则——信息系统审计. 中国内部审计协会

2. 信息技术服务治理第 4 部分：审计导则（GB/T 34960. 4-2017）

3. 信息技术软件生存周期过程(GB/T8566-2007 或 GB/T8566-2007）

4. 中国内部审计准则. 中国内部审计协会（2013 年第 1 号公告）

5. 信息系统审计指南—计算机审计实务公告第 34 号. 中华人民共和国审计署（审计发【2012】11 号）

6. 国家电子政务信息系统审计实务指南. 中国审计学会计算机审计分会，2015 年 9 月

7. 审计署关于内部审计工作的规定. 中华人民共和国审计署（审计署令第 11 号）

8. 中央企业全面风险管理指引. 国务院国有资产监督管理委员会（国资发改革【2006】108 号）

9. 企业内部控制基本规范. 中华人民共和国财政部（财会【2008】7 号）

10. 企业内部控制审计指引. 中华人民共和国财政部（财会【2010】11 号）

11. 国家法律《中华人民共和国网络安全法》

12. 国家标准《信息安全技术—网络安全等级保护基本要求》

13. 国家标准《关键信息基础设施网络安全保护基本要求》（报批稿）

14. 国家标准《云计算服务安全指南》

15. 国家标准《云计算服务安全能力要求》

16. 国家标准《大数据服务安全能力要求》

17. 国际标准《ISO 27001 信息安全管理体系》

18. 国际标准《ISO 20000 IT 服务管理体系》

19. 国际标准《ISO 22301 业务连续性管理体系》

## 附录 3：参考文献

1.《管理信息系统》.上海国家会计学院 CFO 丛书　经济科学出版社　2011 年 7 月

2.《公司治理与内外部审计》．秦荣生　化学工业出版社　2013 年 6 月

3.《现代内部审计学》．秦荣生　立信会计出版社 2017 年 8 月

4.《信息系统审计研究报告》．中国审计学会计算机审计分会. 中国时代经济出版社　2015 年 11 月

5.《信息系统审计之道》．高林、俞文平、周平　清华大学出版社　2016 年 6 月

## 附录 4：信息系统审计文档示例

### • 信息系统审计计划示例

### 关于**（组织）信息化投入及管理情况的专项审计调查审计计划

#### 一、组织方式、工作分工及时间安排

此项审计调查由*统一组织实施，*月重点检查*公司；*月重点检查*公司；*月，*对检查结果进行归纳汇总和综合分析，撰写并提交综合检查报告。

#### 二、信息系统审计调查的主要工作分工

1. *主要负责了解信息化投入的总体情况和制度建设情况，信息系统的立项与计划、预算与执行。

2. *主要负责投资及费用管理及供应商的招投标、合同的签订。

3. *主要负责经营管理类系统的开发、测试、验收上线、运行与维护管理审计，*协助。

4. *主要负责生产运营类、基础建设类系统的运行管理，*协助，重点关注硬件的采购。

#### 三、具体工作要求

（一）审计组成员要严格按照《审计业务流程》、《审计项目质量考核办法》等规定以及审计实施方案的分工和要求开展工作。对审计发现的问题要注意落实相关责任。

（二）审计人员在审计期间要遵守审计局和被审计单位的有关规定，严格执行审计“八不准”等审计纪律，遵守劳动纪律，自觉维护审计人员的良好形象。

**·信息系统审计方案示例**

关于组织信息化投入及管理情况的专项审计调查方案

**一、专项审计调查的目的**

通过调查了解**年信息系统投入及管理运行情况，总结相关应用经验,评价其主要信息系统的安全性、可靠性、有效性、经济性，揭示信息系统管理中存在的问题并分析问题产生的原因，进一步促进*单位信息化建设严格、规范和高效。

**二、专项审计调查的主要依据**

（一）项目实施依据

1.*公司《内部审计工作规定》。

2.*公司《*年审计工作计划》。

（二）检查评价依据

1.《第 2203 号内部审计具体准则——信息系统审计》

2.《*信息化项目规章制度》（*〔2011〕60*号）

3.《*信息技术风险评估规章制度》（*〔2011〕3*号）

4.《*信息系统应用与运维规章制度》（*〔2011〕86*号）

5.《*信息系统供应商管理实施细则》（*）

6.其他信息化规章制度及相关的投资、内控、财务等其他规章制度见附件。

**三、专项审计调查的范围**

对*单位*至*年底各类信息化建设项目的投入及管理情况进行审计调查，重大问题延伸至审计日或追溯到以前年度。

**四、本次专项审计调查的重点内容**

（一）审前调查了解到的主要内容

通过对*单位信息化管理部的调研了解到，目前信息化建设项目按业务类型可划分为*类：如：**类、***类***类等；按管理层级可划分为**和**类。总部项目是指总部统一组织开发、推广或在组织试点的项目，主要由股份公司负担软件开发费用，股份公司及组织共同承担硬件设施和实施管理费用；组织项目指组织自行开发的项目，主要是组织对软件开发进行自主招投标，自行承担硬件及管理实施费用。本次审计的重点主要包括年后验收的新建项目及*年前验收、截止2013年底仍在运行的项目。

通过对*单位的审前调查了解到，*单位上报*年至*年共新建系统*个，其中资金来源为总部或组织投资的共*个，资金来源为科技开发费的共*个，资金来源为运维费用的共*个。经应用“投资项目抽样-基于项目定义”程序检查，总部或组织投资的*个项目中共有*个与*系统中项目核对无误，其余*个项目均未在*系统投资模块中反映；经应用“内部订单分类明细清单”程序检查，计入“科技开发费”的*个项目中有*个与*系统核对无误，有*个未在*系统中发现，另有疑似*个信息系统未上报；经应用“科目余额表”程序检查，计入“信息系统运行维护费”中的*个项目均与*系统核对无误。

此外，经审前调查了解，组织或将新建项目列入“修理费”、“其他费用”等费用类科目，或转资形成资产，计入“固定资产”、“无形资产”等资产类科目，审计组已对相关科目进行了远程检查。

（二）本次专项审计调查的关注重点

根据以上审前调查发现的结果，结合近几年信息化审计发现的问题，特提出以下重点内容。

1. 总体管理情况

一是重点了解组织建立的信息化管理制度、规范和规章制度，是否涵盖了信息化管理的全流程；内控制度中信息流程制定的完整性，执行的有效性；二是重点了解组织的信息化管理

体制机制，组织机构的设置，人员力量的配备等；三是依据审前调查的结果，核实组织在审计期间新建信息项目的数量及投入的总体情况。

2. 信息化投入情况

结合审前调查的结果，本次调查重点关注组织已在审前调查表中上报但未通过*系统*模块反映的 19 个新建项目、组织未在审前调查表中上报的各类自行组织开发项目，及部分合同金额较大的组织项目，对总部项目和已在审前调查表中上报的组织项目将采取审计抽样的方式进行内控测试，如发现疑点再进一步追踪并进行实质性检查。对上述项目，主要检查以下几个方面：

一是项目的可研和立项过程。重点检查未履行审批程序，自行开发的信息项目，按总部或组织管理要求履行内控审批流程的执行情况，可研报告中建设开发目的、功能、效用与其他项目的重叠性，是否存在重复开发。

二是项目的招投标和合同管理情况。重点检查供应商是否具备资质、招投标程序的规范性、询比价过程的合规性和招标结果的公平性；合同是否符合制度规定流程、授权签订，是否存在重大变更，合同规定的质量、安全、工期等事项是否履行到位。

三是项目实施与验收情况。重点检查项目的开发内容与可研报告的一致性，阶段性验收、试点运行和系统用户培训各过程的确认；组织是否对信息项目进行了竣工验收，各类文档资料是否完整、齐全。

四是项目投资执行、资金管理和成本核算情况。重点检查项目的投资执行过程与可研报告的一致性，是否存在截留、挤占、挪用项目经费的问题，侧重是否存在不同信息化建设项目之间相互挤占费用的情况，重点关注在运维费、科研费中列支的项目资金来源的合规性。投资成本的归集及核算是否规范、真实、准确。

3. 信息系统运行和安全管理情况

一是重点关注组织当前运维管理体制的科学性，对自行运维的组织，运维人员、技术力量的配置是否充足；对外包的组织，是否对承担系统运维的供应商进行了有效管理、有效约束，运维文档是否完整。

二是重点关注信息系统的安全性。对软硬件、系统数据采取的安全保护措施，系统权限的管理有效性，系统账号与权限的新增或变更是否履行了内控流程，离职或工作调动人员账号是否已按规定删除或者禁用。

此外，还要对系统运行的效率和效果进行调查了解，关注信息系统在组织经营管理方面发挥的实际作用，是否达到可研计划中的预期效益分析结果。

**五、专项审计调查方法**

一是查阅文档法。文档包括纸质文档、电子文档或者其他介质的记录。主要包括：组织的信息技术规划、内控手册，各类信息系统的项目开发合同及技术附件、可行性研究报告、开发各阶段的文档资料、系统评审或者验收记录、系统日志文件、系统运维记录等。

二是访谈法。访谈重点了解组织对信息系统的认识，评价系统用户对系统的应用能力，判断系统的实际效益。

三是实地观察法。观察信息环境下的业务活动、内部控制执行情况、设备存放的物理环境、计算机系统操作使用过程、数据备份与存储过程。

四是审计抽样法。对系统账号清单或员工离职清单进行抽样，检查用户权限的恰当性，或者离职用户的账号和密码是否按规定及时终止所有访问权。

五是穿行测试法。选取部分信息项目进行全流程穿行测试，包括立项审批流程、招投标流程、实施开发过程及运维管理情况等项目所有环节。

## •信息系统审计底稿示例

### *单位审计工作底稿

编　号:　　共 页 第 页

<table>
<tr><td colspan="3">被审计单位名称：*公司</td></tr>
<tr><td colspan="2">审计项目名称:组织信息化投入及管理情况</td><td>审计事项：信息系统立项及建设过程的合规性</td></tr>
<tr><td colspan="3">审计事项期间：*年 1 月至*年 12 月</td></tr>
<tr><td rowspan="2">审计事实描述</td><td colspan="2">系统建设配套的计算机购置问题<br><br>审计组抽查了*公司*项目投资计划管理信息系统（一期）等*套系统，购置便携电脑 *台，台式机*台，合计*台。其中列入相关部门管理的资产中便携式电脑*台，式机*台，列入信息中心管理的资产中便携式电脑*台，台式机*台，经审核相关会计簿和凭证，上述计算机资产都按要求进行了转资。（详见附件）<br><br>附件：</td></tr>
<tr><td>审计人员：　***</td><td>编制日期:201*年*月*日</td></tr>
<tr><td rowspan="2">复核意见</td><td colspan="2"></td></tr>
<tr><td>复核人员：**</td><td>复核日期：201*年*月*日</td></tr>
<tr><td rowspan="2">被审计<br>单位意见</td><td colspan="2"></td></tr>
<tr><td>签字:</td><td>盖章:</td></tr>
</table>

# *审计工作底稿

编　　号:　　共 页　第 页

<table>
<tr><td rowspan="2">审计结论及依据</td><td colspan="2">项目建设内容与立项内容不符<br>审计组对相关信息系统的可行性研究报告、立项批复、商务合同及合同技术附件进行核对，均未发现有购置便携式电脑和台式电脑的内容，因此上述*台电脑购置与信息系统建设的立项内容不符，但没有超出立项批复的计划金额。<br>不符合《*信息化规章制度》（*（2011）60*号）：“3.3.11 项目承建单位在开发实施中，不得擅自修改设计方案。若有重大技术方案或其他变更，由变更提出方提交书面变更申请，说明变更原因、内容、对整个项目的影响等，报信息部门审批”的规定。<br>审计建议：<br>一是在信息系统建设中要严格按照可研批复内容、设计方案实施。<br>二是在信息系统建设和应用中如确实需要配套购置便携式电脑和台式机，也应实事求是在设计方案中如实反映，并按固定资产购置的程序进行采购、核算和管理。</td></tr>
<tr><td>审计人员：　*</td><td>编制日期：201*年*月*日</td></tr>
<tr><td rowspan="2">复核意见</td><td colspan="2"></td></tr>
<tr><td>复核人员:*</td><td>复核日期:201*-11-201*年</td></tr>
</table>

• 信息系统审计报告示例

## 信息化投入及管理情况的专项审计调查报告

按照*年审计工作计划安排，*派出审计组一行*人，于*年*月*日至*日，对*公司*年至*年信息化投入及管理情况进行了审计调查……。审计调查结果如下：

一、信息化投入情况

（一）资金投入情况

……

（二）信息系统建设和使用情况

……

二、主要管理经验

（一）建立了相对完善、规范的信息化制度和标准体系。

……

（二）信息化建设符合生产管理实际需要，成效明显。

……

（三）持续完善经营管理平台和集中集成建设，强化服务共享及业务协同。

……

三、审计发现的主要问题

（一）信息系统建设管理问题

1. 部分信息系统可研目标与实际存在差异，且个别系统存在功能重叠现象，增大了投资成本。……

（二）信息系统应用管理问题

1. 服务器整合集中利用率不高。……

2. 各系统之间集成和数据共享度不高，信息孤岛仍未完全消除。……

（三）信息系统安全运行问题

1. 机房环境及配套设施存在安全隐患。……

2. 未建立独立的 ERP 角色变更流程。……

四、审计意见和建议

针对审计发现的上述问题，为严格规范管理和防控风险，提出以下审计处理意见和建议：

……

20**年*月*日