国家信息安全水平考试

知识体系大纲

（信息系统审计专项）

NISP 专项证书管理中心

2020 年 12 月 30 日

目 录

一、概述

信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。我国信息安全保障体系建设，需要完善信息安全立法，做好信息安全顶层设计，强化信息基础设施建设，特别地，需要加强信息安全人才培养与管理。在信息系统安全保障工作中，人是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一，近年来，我国网络安全人才培养取得一定进展，但专业人才缺口仍然较大。

为培养更多优秀的实践型网络安全人才，中国信息安全测评中心推出了国家信息安全水平考试（National Information Security Test Program，简称 NISP）。NISP 考试采用理论与实践相结合的教学模式，是评定考生掌握信息安全知识、技能和本领的全国性信息安全水平考试体系。NISP 水平考试分通用证书和专项证书，通用证书分为一级和二级，分别定位于不同层次的目标群体。专项证书面向特定技术领域的人才培养。

NISP 一级主要面向各行业信息系统使用人员及高校非信息安全专业学生，普及信息安全知识，增强信息安全意识，提高安全防范技能，为今后工作中能安全的使用信息系统。

NISP 二级主要面向从事信息安全相关行业人员及高校信息安全相关专业学生，构建信息安全知识框架，帮助学员形成信息安全保障的总体概念，为国家信息安全保障工作的顺利实施打下坚实的理论基础。

NISP 三级（专项）主要面向有志于从事信息安全相关行业的从业人员，在理解信息安全基础知识基础上，掌握信息系统安全运营知识、渗透测试、信息系统审计、数据隐私保护、工业控制系统安全等特定信息安全领域的知识和技能，为国家培养跨领域的信息安全专项人才。

1.1 适用范围

本大纲从我国国情和企事业单位信息系统审计人才的需求出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，兼顾知识体系的全面性、实用性和实践性。

本大纲明确 NISP 信息系统审计专项能力（NISP-A）应当掌握的知识要点，是 NISP-A 课程教材编制、讲师授课、学员学习以及考试命题的重要依据。

1.2 大纲框架结构

NISP 课程使用组件模块化的结构，包括知识域和知识子域两个层次。

知识域：是属于同一技术领域的知识内容构成的相对独立的知识集合；

知识子域：是构成知识域的基本模块，对知识域进一步分解细化形成的完整的知识组件。每个知识子域由一至多个具体知识要点构成。

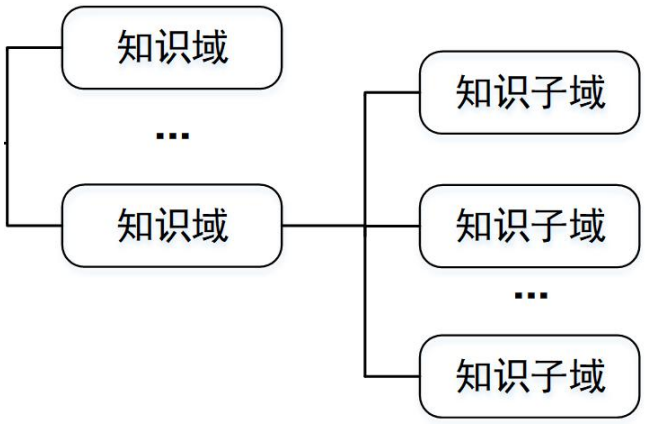

图 1：知识体系组件模块结构

本大纲规定了知识子域中每一个知识要点的内容和深度要求，分为“了解”、“理解”和“掌握”三类。

了解：是最低深度要求，学员需要正确认识该知识要点的基本概念和原理；

理解：是中等深度要求，学员需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进一步的判断和推理；

掌握：是最高深度要求，学员需要正确认识该知识点的概念、原理，并在深入理解的基础上灵活运用。

1.3 知识体系构成及考试

NISP 信息系统审计专项知识体系包括综合理论、专项基础和专项能力三个模块。

综合理论模块为所有 NISP 专项课程通用，采用 NISP 二级课程体系。

专项基础模块划分为八个知识域，是信息系统审计专项能力的基础，在培训时可根据学员基础水平安排适当课程。该模块中的知识在理论考试中均可能作为考点。

专项能力模块包括十个知识域，在理论考试和实操考试中会将此模块中的知识点作为考点。

图 2 NISP-A （信息系统审计专项）知识体系结构

NISP 信息系统审计专项考试题型为单项选择题，共 100 道考题，每题分值为 1 分，总分共 100 分，得到 70 分以上（含 70 分）为通过。

二、专项基础模块

2.1 知识域：网络与网络安全设备

2.1.1 知识子域：网络与网络设备

了解网络拓扑、网络结构等计算机网络基础知识；

了解路由器、交换机等网络设备的工作原理及作用；

了解 IP 地址规划、Vlan 等网络设计规划相关概念。

2.1.2 知识子域：防火墙

了解防火墙产品的基本概念、工作原理及应用场景；

了解包过滤、代理、NAT、状态检测等防火墙应用技术；

了解防火墙部署的方式及防火墙应用中的优缺点。

2.1.3 知识子域：边界安全设备

了解网闸的工作原理及应用场景；

了解 IPS、UTM 等边界安全防护设备的工作原理及应用场景；

了解防病毒网关、上网行为管理等防护设备的工作原理及应用场景。

2.1.4 知识子域：入侵检测与网络审计

了解入侵检测系统的基本概念、工作原理及应用场景；

了解入侵检测系统的数据采集、入侵检测实现原理；

了解入侵检测产品的类型、部署方式及优缺点；

了解网络审计、数据库审计等审计类产品的工作原理、部署方式及应用场景。

2.1.5 知识子域：虚拟专网（VPN）

了解虚拟专网（VPN）的概念，作用及应用场景；

了解 VPN 实现的技术原理及隧道模式、传输模式的区别；

了解 IPSec、SSL 两种不同 VPN 协议的区别。

2.2 知识域：Window 系统安全基础

2.2.1 知识子域：windows 终端安全

了解 windows 终端安全安装的基本要求；

了解 Windows 终端安全配置等相关要求。

2.2.2 知识子域：windows server 安全设置

了解 windows server 安全安装的基本概念要求；

掌握 windows Server 安全策略设置；

掌握 windows 系统常用命令的使用。

2.2.3 知识子域：windows 系统服务配置

掌握 Windows server 上各类服务的部署及安全设置；

了解 Windows Server 上 VPN、远程终端等远程管理服务的部署及安全设置。

2.3 知识域：Linux 系统服务及安全管理

2.3.1 知识子域：Linux 系统终端安全

了解 Linux 系统终端安装过程；

掌握 Linux 系统常用命令的使用；

了解 Linux 系统的日常使用及安全策略设置。

2.3.2 知识子域：Linux 系统服务安全部署

了解 Linux 系统服务器安装过程；

掌握 Linux 系统上 FTP、DNS、Openssh 等常用应用的安全部署。

2.4 知识域：Web 应用安全基础

2.4.1 知识子域：Web 浏览器安全

了解 Web 应用体系的结构及相关问题；

理解 Web 客户端（浏览器）常用的安全机制及安全风险；

理解浏览器端面临的网页挂马、网络钓鱼等攻击的技术原理并掌握浏览器安全设置方法。

了解 XML、HMTL 等 Web 应用中常用开发语言。

2.4.2 知识子域：HTTP 协议

理解 HTTP 协议的请求、响应工作机制；

了解 URL、请求方法（Post、get 等）、响应状态码等基本概念；

了解 cookie、session 等机制及存在的安全风险。

2.5 知识域：数据库安全

2.5.1 知识子域：数据库安全基础

了解 SQL 的基本概念并掌握 Select、update、delete 等常用的 SQL 命令的使用；

了解数据库用户、权限管理机制及安全策略；

了解存储过程、视图等数据库机制对安全的作用；

掌握数据库漏洞扫描软件的使用；

理解针对数据库的攻击方法并掌握如何构建安全的数据库防御体系。

2.5.2 知识子域：数据库安全配置及管理

掌握 SQL server 安全配置、安全管理的方法与工具；

掌握 Mysql 安全配置、安全管理的方法与工具；

掌握 Oracle 安全配置、安全管理的方法与工具。

2.6 知识域：Web 服务软件安全

2.6.1 知识子域：IIS 服务配置及安全管理

掌握 IIS 服务网站配置的方法；

掌握 IIS 安全配置及安全管理的方法；

掌握 IIS 中 Https 的配置方法；

掌握 IIS 日志安全配置及管理相关要求。

2.6.2 知识子域：Web 服务配置及安全管理

掌握基于 Apache 配置 Web 网站的方法及安全管理要求；

掌握基于 Tomcat 配置 Web 网站及安全管理要求；

了解 Nginx、weblogic 等其他 Linux 系统常用 Web 服务软件的配置和管理要求。

2.7 知识域：信息安全法律及标准

2.7.1 知识子域：网络安全法

了解网络安全法出台相关背景；

理解网络安全法中相关条款的要求；

理解网络安全法配套的其他法律法规相关要求。

2.7.2 知识子域：等级保护

了解等级保护发展及相关政策法规；

掌握等级保护定级方法及流程；

掌握等级保护相关要求及测评方法。

2.7.3 知识子域：关键信息基础设施保护条例

了解关键信息基础设施保护条例出台背景及相关政策；

理解关键信息基础设施划分范围；

理解关键信息基础设施相关部门的管理职责；

理解关键信息基础设施保护条例相关要求。

2.7.4 知识子域：个人信息保护法

了解个人信息保护法出台的背景及想政策；

理解个人信息保护相关规则和要求。

2.8 知识域：信息系统审计工具

2.8.1 知识子域：信息系统审计工具

了解 kali Linux 等渗透测试集成工具包；

掌握 Kali Linux 在虚拟机及实体计算机上安装及配置。、

了解系统漏洞扫描、数据库漏洞扫描、Web 漏洞扫描等漏洞扫描软件的作用及使用。

2.8.1 知识子域：文档及数据编辑工具

了解 WPS 文字、Word 等文字编辑软件的使用技巧；

了解 WPS 幻灯片、Powerpoint 等汇报幻灯片的编写及使用技巧；

了解 WPS 表格、Excel 等表格及统计软件使用技巧。

2.8.2 知识子域：python 语言基础

掌握 Python 语言环境的部署；

了解 Python 脚本在渗透测试中的应用。

三、专项能力模块

3.1 知识域：信息系统审计基础

3.1.1 知识子域：审计与信息系统审计

了解审计的基本概念，审计主体、客体、依据等概念；

了解我国审计的三种组织形式的差异、特点；

理解审计模式的变迁；

了解信息系统审计的概念、发展；

理解信息系统审计的重要性。

3.1.2 知识子域：信息系统审计实施基础

了解信息系统审计的目标、基本类型、范围等概念；

了解信息系统审计一般控制、应用控制和系统数据三类审计内容；

了解信息系统中进行审计的审阅法、面谈法、现场观察法、调查问卷法、函证法的概念。

3.1.3 知识子域：信息系统审计依据和规范

了解信息系统审计依据的概念；

了解 ISACA 审计准则体系及我国信息系统审计相关法律、法规政策；

了解审计职业道德规范；

了解审计专业能力和职业审慎的概念；

了解审计质量控制的概念及方法。

3.1.4 知识子域：信息系统审计测试

了解审计测试的概念、审计测试程序的作用；

理解符合性测试和实质性测试方法的差异；

了解黑箱法、白箱法审计测试方式的区别；

了解审计抽样的概念，统计抽样和非统计抽样的区别及优缺点；

了解审计抽样的风险及受控再处理法的概念。

3.2 知识域：信息系统审计流程

3.2.1 知识子域：信息系统审计前期阶段

理解前期调研的工作内容；

理解审计团队组建工作内容；

理解信息系统审计风险管理工作内容；

掌握审计计划制定的方法。

3.2.2 知识子域：信息系统审计实施阶段

了解审计过程方法；

掌握审计证据收集的工作内容；

掌握审计工作底稿的内容及编写。

3.2.3 知识子域：信息系统审计完成阶段

掌握信息系统审计报告编写方法；

理解提交审计报告及后续工作。

3.3 知识域：风险管理与 IT 治理审计

3.3.1 知识子域：风险管理

了解风险管理的概念及常见风险管理模型；

了解风险管理的过程；

了解风险评估的实施流程；

了解自评估、检查评估两种风险评估方式；

了解定性、定量及半定量等风险评估方法；

了解控制自我评估(CSA)的概念。

3.3.2 知识子域：IT 治理基础

了解 IT 治理的基本概念及与企业治理、IT 管理的关系；

了解 Cobit 等 IT 治理的标准与框架；

了解企业架构的概念及扎克曼模型（Zachman）、SABSA（舍伍德的商业应用安全架构）等企业安全架构的构成。

3.3.3 知识子域：IT 治理方法与审计

了解 IT 治理的方法；

了解 IT 治理组织结构、职责分离控制等概念；

了解 IT 治理审计的概念与审计的内容。

3.4 知识域：信息安全管理审计

3.4.1 知识子域：信息安全管理基础

理解信息安全属性的概念及 CIA 三元组（保密性、完整性、可用性）；

理解信息安全管理的作用。

3.4.2 知识子域：信息安全管理体系建设

了解信息安全管理体系实施成功的基本要素；

了解信息安全管理过程方法；

了解信息安全管理体系建设过程。

3.4.3 知识子域：信息安全管理审计

了解信息安全管理控制措施内部结构；

了解信息安全管理体系中信息安全方针、信息安全组织、人力资源安全、资产管理、访问控制、加密、物理和环境安全、操作安全、通信安全、系统的获取、开发及维护、供应商关系、信息安全事件管理、业务连续性管理中的信息安全、符合性等 14 个控制类别的审计。

3.5 知识域：业务连续性审计

3.5.1 知识子域：业务连续性管理

了解业务连续性、业务连续性管理的概念；

理解业务连续性管理对组织机构的重要性；

了解业务连续性管理生命周期六个阶段的工作内容；

了解业务连续性政策；

3.5.2 知识子域：灾难备份与恢复

了解灾难备份与恢复基本概念；

了解灾难备份相关技术；

理解灾难恢复策略与灾难恢复规划管理过程。

3.5.3 知识子域：业务连续性审计

了解业务连续性及灾难恢复审计的内容；

理解业务连续性及灾难恢复审计的程序。

3.6 知识域：信息系统购置与建设审计

3.6.1 知识子域：项目管理

了解项目管理基本概念；

了解项目管理内容；

了解项目管理组织结构。

了解信息系统验收流程；

了解系统上线方式；

了解系统验收内容。

3.6.2 知识子域：系统安全工程能力成熟度模型

了解能力成熟度模型的概念；

了解系统安全工程能力成熟度模型（SSE-CMM）的体系结构；

了解 SSE-CMM 中域维及风险过程、工程过程、保证过程中 11 个 PA 的构成；

了解 SSE-CMM 中 1~5 级成熟度级别的差异。

3.6.3 知识子域：信息资产保护

了解信息资产管理 (硬件、软件、数据等)审计；

了解信息系统用户身份鉴别、访问控制安全性；

了解密码技术及 PKI 体系应用。

3.6.4 知识子域：新技术应用审计

了解云计算、虚拟化的安全风险；

了解工业控制系统安全风险；

了解大数据应用安全风险；

了解物联网安全风险。

3.7 知识域：物理风险与网络通信安全审计

3.7.1 知识子域：物理环境风险审计

了解物理环境安全风险；

了解物理环境安全审计要求。

3.7.2 知识子域：基础网络架构

了解网络拓扑结构、网络边界等概念；

了解网络规划的概念及规划基本方法。

3.7.3 知识子域：网络安全设备

了解防火墙、网闸等边界安全设备；

了解入侵检测等旁路型安全设备；

了解 VPN 等接入管理设备；

了解安全管理平台等安全管理设备。

3.7.4 知识子域：网络通信安全审计

了解网络通信安全审计内容；

理解网络通信安全审计流程；

3.8 知识域：计算环境安全审计

3.8.1 知识子域：操作系统安全审计

了解操作系统安全审计内容；

了解 Windows 系统日志、安全策略设置等审计内容；

了解 Linux 系统日志、安全配置等审计内容；

3.8.2 知识子域：Web 及电子邮件应用安全审计

了解 Web 系统体系结构；

了解典型的 Web 应用安全问题；

了解 Web 应用安全配置；

了解 Web 日志安全审计；

了解电子邮件应用安全风险及控制。

3.8.3 知识子域：数据库安全审计

了解数据库安全与安全机制；

了解数据库访问控制技术、备份与回复等技术措施；

了解数据库审计方法与内容；

掌握 Mysql 数据库安全策略设置、日志管理及审计方法；

掌握 Sql Server 数据库安全策略设置、日志管理及审计方法；

掌握 Oracle 数据库安全策略设置、日志管理及审计方法。

3.9 知识域：业务系统开发审计

3.9.1 知识子域：软件安全开发生命周期

了解瀑布模型等软件开发生命周期模型；

了解软件安全开发生命周期（SDL）模型；

理解系统开发审计。

3.9.2 知识子域：业务系统安全测试与代码审计

了解软件安全测试的基本概念及测试方法；

了解模糊测试原理及应用；

了解渗透测试原理及应用；

了解代码审计方法。

3.9.3 知识子域：业务应用风险审计

了解互联网应用安全风险控制；

了解电子金融安全风险控制；

了解大数据应用安全风险控制；

3.10 知识域：信息系统运营管理审计

3.10.1 知识子域：信息系统运营管理

了解 IT 服务管理概念及管理框架；

了解服务台、变更管理、配置管理、事件管理、问题管理等流程。

3.10.2 知识子域：日志审计

了解日志及日志管理等概念；

理解日志审计的方法。

3.10.3 知识子域：安全事件处置及应急响应

了解信息安全事件分类分级相关概念；

了解国际及我国信息安全应急响应组织；

了解应急响应组织架构；

了解应急响应预案编写、演练等相关工作；

了解计算机犯罪及取证相关概念。