北京市电子政务与重要行业
信息安全服务（高级）工程师资格考试大纲
（试行）

一、考试说明

1. 考试科目

考试分为信息安全服务工程师资格考试和信息安全服务高级工程师资格考试两类。两类考试在考试的要求、题型、深浅和范围上有差别。

2．考试要求

2.1．信息安全服务工程师

2.1.1 掌握信息安全基本概念和发展规律；

2.1.2 了解我国信息安全保障工作方面存在的主要问题、总体要求、主要原则和主要任务；

2.1.3 了解国家和北京市网络与信息安全的组织领导情况；

2.1.4 理解和掌握国家和北京市涉及信息安全的政策法规和标准；

2.1.5 掌握信息安全管理咨询、信息安全风险评估、信息安全运维、信息安全工程建设、信息安全应急等信息安全服务的基本方法和实践技能；

2.1.6 掌握信息安全等级保护各个关键环节，理解和掌握 5 个安全等级的基本要求；

2.1.7 理解和掌握信息技术基础知识。

2.2．信息安全服务高级工程师

2.2.1 掌握信息安全的基本概念和发展规律；

2.2.2 了解我国信息安全保障工作方面存在的主要问题、总体要求、主要原则和主要任务；

2.2.3 了解国家和北京市网络与信息安全的组织领导情况；

2.2.4 理解和掌握国家和北京市涉及信息安全的政策法规和标准；

2.2.5 掌握信息安全管理咨询、信息安全风险评估、信息安全运维、信息安全工程建设、信息安全应急等信息安全服务的基本方法和实践技能；

2.2.6 掌握信息安全等级保护各个关键环节，理解和掌握 5 个安全等级的基本要求；

2.2.7 熟悉 IT 服务项目管理；

2.2.8 理解和掌握信息技术基础知识。

3．考试题型

3.1．信息安全服务工程师（满分 100 分，60 分及格）

3.1.1 单项选择题

3.1.2 简答题

3.2．信息安全服务高级工程师（满分 120 分，72 分及格）

3.2.1 单项选择题

3.2.2 简答题

3.2.3 案例分析题

二、考试范围

信息安全服务工程师和信息安全服务高级工程师考试都涵盖信息安全总体保障、政策法规与标准、信息安全服务以及信息安全等级保护，信息安全服务高级工程师还包括 IT 服务项目管理。

1．信息安全总体保障

1.1．信息安全基本概念和发展规律

了解信息安全基本概念和发展规律。

1.2．国家和北京市信息安全保障

了解我国信息安全保障工作方面存在的主要问题、总体要求、主要原则和主要任务。

了解国家和北京市网络与信息安全组织领导情况。

2．政策法规与标准

2.1．政策法规

掌握国家及北京市信息安全主要政策法规，包括《中华人民共和国保守秘密法》（中华人民共和国主席令第 28 号）、《中华人民共和国计算机信息系统安全保护条例》（国务院第 147 号令）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号）、《国务院关于大力推进信息化发展和切实保

障信息安全的若干意见》（国发〔2012〕23 号）、《信息安全等级保护管理办法》（公通字〔2007〕43 号）、《国家密码管理局关于印发〈信息安全等级保护商用密码管理办法〉的通知》（国密局发〔2007〕11 号）、《关于建立国家信息安全产品认证认可体系的通知》（国认证联〔2004〕57 号）、《关于加强信息安全管理体系认证安全管理的通知》（工信部联协〔2010〕394 号）、《中华人民共和国工业和信息化部公告》（2011 年第 21 号）、《商用密码条例》（国务院第 273 号令）、《中华人民共和国电子签名法》、《电子认证机构管理办法》（信产部第 35 号令）、《电子政务电子认证服务管理办法（试行）》（国密局发〔2009〕7 号）、《关于信息安全产品实行政府采购的通知》（财库〔2010〕48 号）、《国家网络与信息安全协调小组〈关于开展信息安全风险评估工作的意见〉的通知》（国信办〔2006〕5 号）、《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技〔2008〕2071 号）、国务院办公厅关于印发《国家网络与信息安全事件应急预案》的通知（国办函〔2008〕168 号）、《国务院办公室关于印发〈政府信息系统安全检查办法〉的通知》（国办发〔2009〕28 号）、《北京市信息化促进条例》（北京市人民代表大会常务委员会公告第 63 号）、《北京市公共服务网络与信息系统安全管理规定》（北京市人民政府第 163 号令）、《北京市政务与公共服务信息化工程建设管理办法》（北京市人民政府第 67 号令）、《北京市党政机关计算机网络与信息安全管理办法》（京办发〔2001〕27 号）、《北京市关于开展信息安全等级保护工作的实施方案》（京公网监字〔2007〕788 号）、《北京市政务数字证书使用管理办法》（京信息办函〔2005〕46 号）、《关于加快政务署子证书推广应用的通知》（京信息办函〔2006〕151 号）、《北京市党政机关信息技术外包服务机构申请信息安全管理体系认证安全审查程序（暂行）》（北京市经信委 2013 年第 1 号通告）、《北京市经信委关于做好信息技术服务外包安全管理工作的通知》（京经信委〔2013〕203 号）、《关于开展信息安全服务能力评估和推荐工作的通知》（京信息办函〔2004〕34 号）、《北京市电子政务与重要行业信息安全服务能力评定条件（2013 年版）》、《北京市财政局.北京市经济和信息化委员会.北京市质量技术监督局转发财政部、工业和信息化部、质检总局、认监委关于信息安全产品实施政府采购的通知》（京财采购〔2010〕754 号）、《关于加强我市电子政务信息系统灾难恢复工作的意见》（京信安协〔2006〕3 号）、《北京市网络与信息

安全事件应急预案》（2012 年修订）（京应急委发〔2012〕23 号）、《北京市通信保障和信息安全应急指挥部关于加强本指挥部及办公室建设有关工作的通知》（京信安应急指〔2008〕1 号）、《北京市信息安全容灾备份中心使用管理规定》、《北京市政府信息系统安全检查实施办法》（京政办发〔2010〕25 号）等。.

2.2．安全标准

熟悉信息安全等级保护、信息安全风险管理、信息安全管理体系、信息安全容灾备份与应急管理等国家信息安全主要标准，包括：《信息安全技术.政府部门信息安全管理基本要求》（GB/T.29245－2012）、《信息安全技术.基于互联网电子政务信息安全实施指南》（GB/Z.24294－2009）、《计算机信息系统安全保护等级划分准则》（GB.17859－1999）、《信息安全技术.信息系统安全等级保护基本要求》（GB/T.22239－2008）、《信息安全技术.信息系统安全等级保护定级指南》（GB/T.22240－2008）、《信息安全技术.信息系统等级保护安全设计技术要求》（GB/T.25070－2010）、《信息安全技术.信息系统安全等级保护实施指南》（GB/T.25058－2010）、《计算机场地安全要求》（GB/T.9361－1988）、《计算机场地通用规范》（GB/T.2887－2000）、《电子计算机机房设计规范》（GB.50174－1993）、《信息安全技术.办公设备基本安全要求》（GB/T.29244－2012）、《信息安全技术公共及商用服务信息系统个人信息保护指南》（GB/Z.28828－2012）、《信息技术信息技术安全管理指南》（GB/T.19715.1－2005、GB/T.19715.2－2005）、《信息技术.安全技术.信息安全管理体系要求》（GB/T.22080－2008）、《信息技术.安全技术.信息安全管理实用规则》（GB/T.22081－2008）、《信息安全技术.信息系统安全管理要求》（GB/T.20269－2006）、《信息安全技术.信息安全风险管理指南》（GB/Z.24364－2009）、《信息技术.安全技术.信息技术安全性评估准则》（GB/T18336.1－2008、GB/T.18336.2－2008、GB/T.18336.3－2008）、《信息安全技术.信息安全风险评估规范》（GB/T.20984－2007）、《信息安全技术.信息系统灾难恢复规范》（GB/T.20988－2007）、《信息技术.安全技术.信息安全事件管理指南》（GB/Z.20985－2007）、《信息安全技术.信息安全事件分类分级指南》（GB/Z.20986－2007）、《信息安全技术.信息安全应急响应计划规范》（GB/T.24363－2009）等。

3．信息安全服务

3.1．信息安全服务基本概念和分类

了解信息安全服务基本概念和分类。

3.2．信息安全管理咨询服务

理解信息安全管理体系相关概念。

理解信息安全管理体系构成，掌握信息安全体系建立过程。

3.3．风险评估

理解风险评估与信息安全等级保护的关系。

掌握《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）等标准。

重点掌握风险评估过程和方法。

能根据风险提出合理的风险处理建议。

3.4．信息安全运维管理

理解信息安全运维管理模型及要素。

3.5．信息安全工程建设

理解信息安全工程生命周期和流程管理。

掌握信息安全工程建设实施过程和方法，了解工程监理。

3.6．应急响应服务

掌握信息安全事件应急响应过程。

理解应急预案的设计、演练、维护、变更管理。

理解应急响应体系建立流程：编制应急响应计划、建立预防预警机制、规定应急响应流程、设置应急响应保障措施。

4．信息安全等级保护

4.1．信息安全等级保护实施过程关键环节

熟悉定级备案工作的相关政策、标准和原则，掌握信息系统安全保护等级划分方法和定级备案工作流程。

熟悉安全建设整改工作依据的政策、标准，掌握安全建设整改工作内容和步骤。

理解等级保护安全测评依据、要求、作用和流程。

了解监督检查内容、分类和实施要求。

4.2．信息系统安全等级保护基本要求

理解和掌握物理安全、网络安全、主机安全、应用安全、数据安全的技术要求控制点。

理解和掌握安全管理制度、安全管理机构、人员安全管理、系统建设管理、

系统运维管理控制点及要求项，重点掌握三级控制点。

4.3．信息系统安全等级保护建设整改

掌握信息安全等级保护设计技能，理解不同级别信息系统安全计算环境、安全区域边界、安全通信网络、安全管理中心设计目标、设计策略、设计技术要求。

掌握新建信息系统等级保护方案总体安全设计方法、设计步骤、设计方案与实施方案内容。

理解已建信息系统安全整改工作基本流程.、系统改建实施方案设计等内容。

理解信息系统安全管理整改流程和安全整改责任，掌握安全管理机构、人员、制度，系统建设管理，系统运维管理等整改内容。

5．IT 服务项目管理

5.1．基本概念和方法

理解 IT 服务项目管理基本概念、基本方法及基本理论体系。

5.2．IT 服务设计、转换、运营和改进

熟悉掌握 IT 服务设计的概念、需求识别、方案设计及成本预算。

理解 IT 服务转换概念，掌握服务转换计划、启动、执行及验收。

熟悉掌握 IT 服务运营业务关系管理、人员要素管理、流程要素管理、技术要素管理质量管理及信息安全管理。

掌握服务改进方法、服务测量及服务报告。

5.3．IT 服务项目生命周期和管理知识体系

了解 IT 服务项目生命周期概念、项目启动、项目规划、项目执行和监控及项目收尾。

了解 IT 服务项目管理知识体系，包括项目范围管理、项目时间管理、项目成本管理、项目质量管理、人力资源管理、项目沟通管理、项目风险管理及项目采购管理。

5.4．IT 服务项目类别和 IT 服务项目群管理

了解 IT 服务分类及常见 IT 服务项目类型。

了解项目组织、项目考核及项目经理考核的相关内容。

6．信息技术基础知识

理解和掌握信息技术基础知识。