

“深港澳金融科技师”专才计划一级考试大纲

科目：《云计算与信息安全通识》

一、考查目标

章节	学习目标
第1章 云计算简介	1. 了解云计算的相关定义及特征 2. 掌握云计算的五大关键技术 3. 熟悉云计算的四大部署模型
第2章 云计算市场发展概况	1. 了解云计算的市场规模和未来增长趋势 2. 熟悉云计算的产业格局，如产业链的分布 3. 掌握云计算的三大服务模式：IaaS、PaaS、SaaS
第3章 云计算的发展环境	1. 了解云计算发展的政策现状、市场规模和用户基础需求； 2. 熟悉云计算发展未来规划工作重点、市场热点和用户潜在需求； 3. 分析云计算发展难点、痛点，并构思解决方案。
第4章 云计算在金融领域的应用	1. 了解金融行业云服务需求； 2. 熟悉金融行业云服务方式和部署模式的分类； 3. 举例说明金融行业云实践带来的提升发展和风险挑战。
第5章 金融云发展面临的机遇与挑战	1. 了解金融云发展面临的机遇 2. 了解金融云发展面临的挑战
第6章 信息安全的基本概念	1. 了解信息安全的定义及框架 2. 了解信息安全管理概念及要点 3. 了解企业的信息安全管理内涵 4. 实践信息安全管理体系与标准 掌握信息安全管理法律法规及道德规范
第7章 信息安全产业概况	1. 了解信息安全产业链的服务与市场 2. 了解国内信息安全管理现状 3. 了解国外信息安全管理现状 4. 实践企业员工的信息安全行为管理 掌握企业制定信息安全管理政策要点
第8章 信息安全在金融领域的应用	1. 了解金融领域的信息安全挑战与变化 2. 实践金融领域的信息安全管理方法 掌握提升金融信息安全方法
第9章 金融领域信息安全管理发	1. 了解金融领域信息安全的发展、机遇与挑战

展的机遇与挑战	<p>2. 了解金融领域信息安全管理在各金融平台的发展、机遇与挑战</p> <p>3. 掌握客户、产品与服务、渠道的发展机遇</p> <p>掌握行业竞争、合规监管和人才培育等方面的主要挑战</p>
---------	--

二、考查要点

主要内容	考查要点
云计算基本概念	云计算定义、发展阶段、发展环境。
云计算五大特征的理解	根据 NIST 的定义，云计算具备的五大特征是：按需自主服务、无处不在的网络接入、资源池、快速弹性和按使用付费。
云计算的五大关键技术	虚拟化技术、海量数据分布式存储技术、分布式资源管理技术、编程模型技术、云计算平台管理技术。
云计算的四大部署模型	云计算有私有云、社区云、公有云、混合云四大部署模式。
云计算的三大服务模式	NIST 提出云计算三大服务模式分别是：IaaS、PaaS、SaaS
云计算发展的政策现状	国际云计算政策、国内云计算宏观政策、云计算工作重点、协同治理体系、信用管理、云服务企业信用评级。
云计算发展的市场规模	全球云计算市场规模及趋势、我国云计算市场规模及趋势、云计算发展热点。
云计算发展的用户基础需求	基础需求、扩展需求、优化需求、极致需求
金融云相关政策	《中国银行业信息科技“十三五”发展规划监管指导意见(征求意见稿)》、《可信金融云服务（银行类）》等。
金融云概念	云计算技术核心理念、金融云的定义
金融行业云服务需求	金融云服务使用目的、国内金融云市场规模、服务安全性和可持续性需求。
金融行业上云实践	工商银行案例、招商证券案例、众安保险案例、平安云案例、蚂蚁金融云案例。
金融云应用面临的机遇	传统金融机构金融云应用的广度和深度将进一步提升；将云计算技术赋能中小金融银行将是未来金融云发展趋势；公有云的监管将日趋严格，行业云或更加受监管认可。
金融云应用面临的挑战	业务形态对网络运维和管理提出挑战；行业形态对网络整体架构提出挑战。
信息安全定义	信息安全是指信息系统（包括硬件、软件、数据、人、

	物理环境及其基础设施) 受到保护, 不因偶然的或者恶意的原因而遭到破坏、更改、泄漏, 系统连续可靠正常地运行, 信息服务不中断, 最终实现业务连续性。
信息安全基本属性	机密性、完整性、可用性、可控性和不可否认性
信息安全理念演进	通信安全发展阶段、计算机安全发展阶段、信息安全发展阶段、信息安全保障发展阶段。
信息系统的构成	计算机硬件、软件、网络与通信设备、信息资源、信息用户和规程。
信息安全的构成	技术体系: 主要包括技术机制与技术管理, 技术机制涉及信息系统运行环境和系统安全相关技术, 技术管理包括安全策略与服务、密钥管理、审计相关的状态检测和入侵监控。 组织机构体系: 涉及机构、岗位和人事相关内容。 管理体系: 涉及制度、培训和法律相关内容。
信息安全保障三要素	人、技术、管理
信息安全需求	物理安全、系统安全、网络安全、数据安全、应用安全、安全管理。
信息安全基础技术	病毒检测与清除技术、安全防护技术、安全审计技术、安全检测与监控技术、解密与加密技术、身份认证技术。
信息安全服务类别	安全咨询服务、等级测评服务、风险评估服务、安全审计服务、运维管理服务、安全培训服务。
资质认证	信息安全产品测评、信息系统认定、信息安全服务资质认定、信息安全专业资质认定。
信息安全标准组织	国际标准化组织和国际电工委员会 (International Electro technical Commission, IEC)、国际电信联盟电信标准分局 (ITU Telecommunication Standardization Sector, ITU-T)
信息系统安全的五个等级	公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17895-1999《计算机信息系统安全保护等级划分准则》被认为我国信息安全标准的奠基石。准则将信息系统安全分为 5 个等级: 自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。
信息安全道德规范	整体原则、兼容原则、互惠原则。
信息安全产业链	硬件、软件、信息安全服务。
中国信息安全重点应用领域	政府、电信、银行、能源、军队等。
国内信息安全战略与政策文件	2016 年 12 月, 国家互联网信息办公室正式发布《国家网络空间安全战略》, 这是我国第一次向全世界系统、

	明确地宣布和阐述对于网络空间发展和安全的立场和主张，是指导国家网络安全工作的纲领性文件。
金融信息安全需求	《金融行业信息系统信息安全等级保护实施指引》适用于金融机构（包括其分支机构）的系统规划建设部门，包括应用开发、系统使用、系统运行、内部监察、安全管理、审计等部门。也可作为信息安全职能部门进行监督、监察和指导的依据。 金融行业技术类安全要求根据其保护的侧重点不同，可将基础控制点分为以下四种：信息安全类（S类）、服务保障类（A类）、通用安全保护类（G类）、金融行业增强安全保护类（F类）。
信息安全发展的四个阶段	基本防护阶段、适应性防护阶段、主动防护阶段、自主可控阶段。
信息安全管理定义	信息安全管理(Information Security Management, ISM)是全方位、整体性的工作，必须涵盖三个层面——管理层面、技术层面、实体层面。信息安全管理描述了企业或组织保护资产机密性、完整性和可用性免受威胁和漏洞影响所需要实施的措施。
信息安全的三大支柱	人员(people)、程序(process)、技术(technology)
企业信息安全管理包括的主要内容	企业信息安全战略规划、企业信息安全治理、企业信息安全政策制度、企业员工信息安全管理、企业信息安全的风险管理。
信息安全管理体系	信息安全管理体系(Information security management system, ISMS)是一套系统式管理企业敏感数据的策略和程序。ISMS的目标是通过主动限制安全漏洞的影响来最小化风险并确保业务连续性，有助于有效的风险管理和缓解策略。
信息安全管理标准	ISO/IEC 27001(前身为 BS 7799-2) 的标准着重于如何实施 ISMS，并在 2002 年版本要求企业使用一种为 Plan-Do-Check-Act 的循环性方法来持续改进信息安全政策，简称 PDCA 循环。
信息系统安全五个保护等级	自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。
信息安全法律法规	共四类：通用性法律法规、惩戒信息犯罪的法律、针对信息网络安全的规定、规范信息安全技术及管理方面的规定。
信息安全道德规范三原则	整体原则、兼容原则和互惠原则。
国内信息安全管理面临的主要问题	管理层面：组织建设、制度建设和人员意识。 法律法规层面：法律法规体系还尚处制定及规划阶段，使现有的法律法规不完善，部分法律法规建设跟不上信息技术发展的需要。
国外信息安全管理面临的主要问题	缺乏专责信息安全人员，缺乏保护个人隐私信息相关法规，黑客及恶意软件威胁日增，缺乏足够预算以提

	升信息安全管理作为等。
信息安全管理的发展机遇与挑战	主要从众筹平台、网络借贷平台、移动支付平台、供应链金融等方面入手，了解各细分领域信息安全管理面临的机遇与挑战。

三、试卷内容本科目建议重点知识结构占比

云计算的五大特征	6%
云计算的五大关键技术	6%
云计算的四大部署模型	6%
云计算的三大服务模式	6%
信息安全基本属性	6%
信息安全的构成	6%
信息安全保障三要素	6%
企业信息安全管理包括的主要内容	6%
信息安全管理面临的问题	6%
信息安全管理面临的机遇与挑战	6%
合计	60%

建议上述 10 个主要内容占比不低于 6%，合计不低于 60%。