

章节	二级目录	三级目录	知识点	页数
D1 云计算概念 和体系架构	1.1 简介			
	1.2 概述	1.1.1 定义云计算	云计算是一种新的运作模式和一组用于管理计算资源共享池的技术	9
			NIST 与 ISO/IEC 定义	9
			抽象/调配	9
		1.1.2 定义模型	五个基本特征（资源池、按需自动配置、广泛的网络访问、快速弹性、提供可测量的服务）	11
			ISO/IEC 1788 六个基本特征、多租户	12
			三个服务模型（SaaS、PaaS、IaaS）	12
			四个部署模型（公有云、社区云、私有云、混合云）	13
		1.1.3 参考和架构模型	服务设施即服务（IaaS）	16
			平台即服务（PaaS）	18
			软件即服务（SaaS）	19

		1.1.3 参考和架构模型	逻辑模型（基础设施、元结构、信息结构、应用结构）	21
	1.2 云安全范围、职责和模型	1.2.1 云安全与合规性范围和职责	共享责任模型	22
			安全工具 1. 公示评估问卷（CAIQ） 2. 云控制矩阵（CCM）	24
		1.2.2 云安全模型	概念模型或框架、控制模型或框架、参考架构、设计模式	24
			云安全流程模型	25
	1.3 重点关注领域	1.3.1 治理域		27
		1.3.2 运行域		28
	1.4 建议			29
	1.5 参考文献			29
D2 治理与企业风险管理	2.0 简介		治理、企业风险管理、信息风险管理、信息安全是管理	30
	2.1 概述	2.1.1 治理	共同责任模式	31
			云治理工具（合同、供应商评估、合规报告）	32

	2.1 概述	2.1.2 企业风险管理	迁移到云端不会改变你的风险承受能力、它只是改变了管理风险的方式。	34
			云风险管理的工具	38
	2.2 推荐		云供应商评估的过程	39
D3法律问题、 合同和电子举 证	3.1 简介			
	3.2 概述	3.1.1 数据保护、隐私权的法律框架		41
		3.1.2 合同与供应商的选择		46
		3.1.3 电子举证		49
D4 合规和审计 管理	4.1 介绍			55
	4.1 概述		GRC （治理、风险、合规性）	56
			合规性确保公司义务的认识和遵守	56
			审计是证明(或反驳)合规性的关键工具	56
		4.1.1 合规	合规性管理是一种治理工具	56

	4.1 概述	4.1.1 合规	共享责任模式；云服务供应商和客户都有责任、但客户始终对自己的合规性负责。	56
		4.1.2 审计管理		58
	4.2 推荐			60
D5 信息治理	5.1 介绍		确保数据和信息的使用遵循组织的策略、标准和战略- 包括监管、合同和商业目标	62
			需求方面影响（多租户、共享的安全责任、所有权、保管）	62
			治理模型（管辖边界和数据主权、适用性规则和隐私政策、销毁和删除数据）	63
	5.2 概要		信息是有价值的信息	63
		5.1.1 云信息治理领域	治理影响（信息分级、信息管理策略、属地和管辖政策、授权、所有权、保管、隐私、合同控制、安全控制）	64
		5.1.2 数据安全生命周期	创建、保存、使用、共享、归档、销毁	65
			数据的逻辑和物理“位置”	66
			授权（谁访问数据、怎么访问）、访问设备	66
	5.3 推荐			68

D6 管理平面和 业务连续性	6.1 介绍		管理平面是传统基础架构和云计算之间唯一最重大的安全差异	69
			云管理平面负责管理资源池中 的资产、而云消费者负责配置他们的资产和部署到云端的资产。	69
		6.1.1 云上的业务连续性和容灾	关注（在某一既定的云提供方内确保连续性和恢复、对云提供方可能出现的中断进行准备和管理、可移植性）	70
			架构	70
			管理平面的安全	72
			提供方和消费者都应该始终只允许用户、应用程序和其他管理平面所需的最少特权	73
			所有特权用户帐户都应使用多因子身份验证(MFA)。	73
			管理安全管理平面（边界安全、客户认证、内部认证和凭证传递、授权和权利、日志，监控和告警）	74
		6.1.2 业务连续性和容灾	逻辑栈（元结构，接触架构，信息架构，应用架构）	76
			混沌工程	77
	6.2 建议			78
D7 基础设施安全	7.0 简介		基础设施安全是在云中安全运行的基础。	80

D7 基础设施安全	7.1 概述		基础设施两个层面（构建云的基础资源，云用户管理的虚拟/抽象基础设施）	80
	7.2 云网络虚拟化		服务网络、存储网络、管理网络	81
	7.3 云网络带来的安全变化	7.3.1 虚拟设备的挑战		83
		7.3.2 SDN的安全优势	隔离更容易、SDN防火墙	84
		7.3.3 微分段和软件定义的边界	只在需要时连接这些网络，降低爆炸半径	85
			SDP三个组件（SDP客户机、SDP控制器、SDP网关）	85
		7.3.4 云提供商或私有云的其他注意事项	多租户环境的分区和隔离	86
			供应商还必须向云用户暴露安全控制措施，以便他们能够正确配置和管理其网络安全 性。	87
		7.3.5 混合云的考虑	混合云连接架构是“堡垒”或“中转”虚拟网络	87
		7.4 云计算与负载安全		计算抽象类型（虚拟机、容器、基于平台的负载、无服务器计算）
	7.4.1 云对负载安全的改变			
	7.4.2 不可变负载增强安全性		安全性提升与需求	91

D7 基础设施安全	7.4 云计算与负载安全	7.4.3 云对标准负载安全控制的影响		92
		7.4.4 负载安全监控和日志的变化		93
		7.4.5 脆弱性评估的改变		94
		7.4.6 云存储安全		94
	7.5 建议			94
D8 虚拟化和容器	8.0 简介			95
	8.1 概述		安全控制层次（虚拟化技术本身的安全性、虚拟资产的安全控制）	96
		8.1.1 与云计算相关的主要虚拟化类别	云提供者责任是强制隔离并维护安全的虚拟化基础设施	97
			云消费者的主要责任是正确实施部署在虚拟环境中的所有安全措施（安全设置、监控和日志、镜像资产管理、使用专用主机）	98
			云消费者对虚拟化资源的安全控制负责	99
			计算安全性问题（虚拟资源更加短暂并且快速变化，主机级监控/日志可能不适用）	99
			监控和过滤	100

D8 虚拟化和容器	8.1 概述	8.1.2 网络	云提供商主要负责建立安全的网络基础设施并正确配置。	101
			云消费者主要负责合理配置虚拟网络的部署，尤其是虚拟防火墙。	101
		8.1.3 存储	在不同的地方保存了多个数据副本	102
		8.1.4 容器	容器是高度可移植代码执行环境	103
			三个组件（容器执行环境、自动协调及调度控制器、容器镜像或代码的可执行仓库）	103
			容器安全（底层物理基础设施、管理器、镜像仓库、安全性构建到容器内运行的任务/代码中）	103
			容器不一定提供完整的安全性隔离，但一定提供任务隔离。	104
	8.3 建议			104
D9 事件响应	9.0 介绍			106
	9.1 概述	9.1.1 事件响应声明周期	准备（建立事件响应能力，使组织对事件响应作好充分准备）、检测与分析、遏制，根除和恢复、总结	107
		9.1.2 云计算如何影响事件响应	准备	
			云应急工具包	109

D9 事件响应	9.1 概述	9.1.2 云计算如何影响事件响应	检测与分析	109
			遏制、根除和恢复，始终确保云管理平面/元结构远离攻击者	111
	9.2 建议			112
D10 应用安全	10.0 介绍	云计算主要为应用程序带来安全优势	机会（更高的安全基线、响应能力、隔离环境、独立的虚拟机、弹性、DevOps、统一接口）	113
			挑战： 1. 可见性受限-收集与安全相关的数据 2. 增加应用范围-管理平台/元结构安全性，直接影响与该云帐户关联的任何应用程序的安全性 3. 不断变化的威胁模型-威胁模型还需要对云提供程序或平台的技术问题进行调整 4. 降低透明度-不知道外部服务的安全控制	114
	10.1 概述	10.1.1 安全软件开发声明周期和云计算简介	安全的设计和开发、安全部署、安全操作	115
		10.1.2 安全设计与开发	五个阶段（训练、定义、设计、开发、测试）	116
		10.1.3 安全部署	安全性测试可能会潜在的集成到开发和部署中（代码审查、单元测试，回归测试和功能测试、静态应用安全测试(SAST)、动态应用安全测试(DAST)）	117
			对脆弱性评估的影响	118

D10 应用安全	10.1 概述	10.1.3 安全部署	对渗透测试的影响	119
			部署管道安全	119
			基础架构作为代码和不可变的影响（由于这些环境是由一组源文件定义自动构建的，所以它们也可以是不可变的。）	120
		10.1.4 安全操作	生产环境的管理平台应该比开发环境更严格的锁定、即使使用不可变的基础设施，仍应该积极监控通过基线的生产环境的变化和偏差	120
		10.1.5 云如何影响应用程序设计和架构	默认隔离、不可变的基础设施、增加使用微服务、PaaS和“无服务器”体系结构	121
			软件定义安全、事件驱动安全	121
		10.1.6 云提供商的其他注意事项		122
		10.1.7 DevOps的崛起和作用	安全意义和优势（标准化、自动化测试、不可变、改进审计和变更管理、SecDevOps/DevSecOps 和 Rugged DevOps）	122
	10.2 建议			123
	11.0 引言		加密是最重要的一种控制手段	123
		11.1.1 数据安全控制	控制什么数据进入云端、保护和管理云中的数据、执行信息生命周期管理安全	124
		11.1.2 云数据存储类型	对象存储、卷存储、数据库、应用程序/平台	125

D11 数据安全和加密	11.1 概述	11.1.2 云数据存储类型	数据分散（分为碎片）	125
		11.1.3 管理数据迁移	迁移监视云使用情况和任何数据传输（CASB、URL 过滤、DLP）	126
			保护云数据传输安全	127
		11.1.4 保护云中数据	云数据访问控制（管理平面、公共和内部共享控制、应用程序级别控制）	128
			存储(At-Rest)加密和令牌	129
			IaaS加密： 1. 卷存储加密（实例管理的加密、外部管理加密） 2. 对象和文件存储（客户端加密、服务器端加密、代理加密）	130
			PaaS 加密： 1. 应用层加密 2. 数据库加密 3. 其他	131
			SaaS 加密： 1. 提供商管理的加密 2. 代理加密	131
			密钥管理(包括客户管理的密钥)：HSM /设备、虚拟设备/软件、云 提供商服务、混合	131

D11 数据安全和加密	11.1 概述	11.1.5 数据安全架构	应用架构影响数据安全。云提供商提供的功能可以减少攻击面，但确保要求强大的元结构 安全性	132
		11.1.6 监控、审计和告警	确保将您的日志存储在安全的位置，如专用日志记录帐户。	133
		11.1.7 其他数据安全控制	数据丢失防护（CASB(云访问和安全代理)、云提供商功能)	133
			数据屏蔽和测试数据生成（测试数据生成、动态屏蔽）	134
		11.1.8 执行声明周期管理安全	管理数据位置/驻留、确保合规性、备份和业务连续性	134
	11.2 建议			134
D12 身份、授权和访问管理	12.0 介绍		联邦	136
		12.0.1 云上IAM的差异	将某种形式的实体(人、系统、代码 等)映射到与各种相关联的可验证身份属性(可以根据当前情况改变)，然后根据授权决定他们 能做什么或不能做什么。	136
	12.1 概述		实体、身份、标识符、属性、人物角色、角色、认证、多因素认证(MFA)、访问控制、授权、权利、联邦身份管理、授权源、身份提供者、依赖方	137
		12.1.1 云计算的IAM标准	安全鉴别标记语言(SAML)2.0、OAuth、OpenID、可扩展访问控制标记语言(XACML)、跨域身份管理系统(SCIM)	139
		12.1.2 管理云计算的用户和身份	Free-form, Hub and Spoke	142

D12 身份、授权和访问管理	12.1 概述	12.1.3 认证以及凭证	云计算对身份验证的最大影响是使用多因素强身份验证的强烈需求	143
			MFA多种选择（硬件令牌、软令牌、带外密码、生物识别技术）	144
		12.1.4 授权和访问管理	授权是被允许做某事、访问控制作为授权允许或拒绝的一种表现、权利将身份映射到授权和任何必需的属性	144
			云以多种方式影响权利、授权和访问管理	145
		12.1.5 特权用户管理		146
	12.2 建议			146
D13 安全即服务	13.0 介绍		安全即服务(SecaaS)	147
	13.1 概述	13.1.1 SecaaS的潜在优势和问题	潜在优势（云计算优势、人员配置和专业知识和智能共享、部署灵活性、客户无感知、伸缩和成本）	147
			潜在问题（能见度不足、监管差异、处理监管的数据、数据泄漏、更换供应商、迁移到SecaaS）	148
		13.1.2 现提供的安全及服务主要分类	身份，授权和访问管理服务	149
			联合身份代理(Federated Identity Brokers)，不同云服务之间建立IAM。	149
			云访问安全代理(CASB，又称云安全网关)	149

D13 安全即服务	13.1 概述	13.1.2 现提供的安全及服务主要分类	Web 安全(Web 安全网关)	150
			电子邮件安全	150
			安全评估	150
			Web 应用程序防火墙(WAF)	151
			入侵检测/防御(IDS / IPS)	151
			安全信息与事件管理(SIEM)	151
			加密和密钥管理	152
			业务连续性和灾难恢复	152
			安全管理	152
			分布式拒绝服务保护	152
	13.2 建议			152
D14 相关技术	14.0 简介			154

D14 相关技术	14.1 概要	14.1.1 大数据	高海量化、高快速化、高多样性	154
			分布式数据收集、分布式存储、分布式处理	154
			安全性和隐私方面的考虑、数据收集、密钥管理、安全功能、身份识别和访问管理、PaaS	156
		14.1.2 物联网(IoT)		157
		14.1.3 移动		158
		14.1.4 无服务器计算		158
	14.2 建议			160