Chapter 2 - Key Topics

Description	Key Topic Element	Page	Summary
NIST definition of public, private, community, and hybrid clouds	Paragraph	85	**Public Cloud -** Open for public use, examples include AWS, Microsoft Azure, Google Cloud. **Private Cloud** - Used just by the organization on the premises (on-prem) or at a dedicated cloud provider. **Community Cloud** - Shared between two or more clouds or cloud services.
Defining IaaS, PaaS, & SaaS	List	85	**Infrastructure-as-a-Service (IaaS)** - You rent infrastructure, purchase virtual power to execute your software as needed. **Platform-as-a-Service (PaaS)** - Provides everything but the applications, services provided include all phases of System Development Life Cycle (SDLC). Everything but the application. **Software-as-a-Service (SaaS)** - Software is rented to the user, such as Cisco WebEx & Office 365.
Cloud Security Responsibility Models	Section	86	See page for visual example.

Description	Key Topic Element	Page	Summary
The Agile Methodology	Section	89	**Agile Methodology** - Is a software development & project management process where a project is managed by breaking it up into several stages and involving constant collaboration with stakeholders and continuous improvement & iteration at every stage. **Scrum** - Framework which encourages teams to learn through experiences, self organize, and reflect for continuous improvement. Describes a set of meetings, tools, and roles that work in concert to help teams structure and manage work. **Sprints** - Describes a set of meetings, tools, and roles that work in concert to help teams structure and manage work. **Kanban** - Scheduling process system for Lean dev & just-in-time (JIT) manufacturing originally developed by Taiichi Ohno from Toyota.
Understanding what DevOps is	Paragraph	90	**DevOps** - The outcome of many trusted principles — from software development, manufacturing, and leadership to the information technology value stream. **Value Streams** - Product management, Software (or hardware) development, Quality assurance (QA), IT operations, IT operations
CI/CD Pipelines	Section	90	**CI/CD** - When adopting a CI/CD methodology each change in code should trigger an automated build-and-test sequence. Automation provides feedback to developers. **Continuous Integration (CI)** - Developers merge code changes in a central repository multiple times a day. **Continuous Delivery (CD)** - Sits on top of CI and provides a mechanism to automate the entire software release process.

Description	Key Topic Element	Page	Summary
Understanding what serverless computing is	Paragraph	92	**Serverless Computing** - Serverless is an execution model where the cloud provider (AWS, Azure, Google Cloud, and so on) dynamically manages the allocation and provisioning of servers. Run in stateless containers, are ephemeral, & event-triggered. You pay for compute time.
Security Questions to ask cloud service provider	List	95	Who has access? What are your regulatory requirements? Do you have the right to audit? What type of training does the provider offer its employees? What type of data classification system does the provider use? How is your data separated from other users' data? Is encryption being used? What are the service-level agreement (SLA) terms? What is the long-term viability of the cloud provider? Will the provider assume liability in the case of a breach? What is the disaster recovery/business continuity plan (DR/BCP)?
Common Cloud Security Threats	List	97	**Denial of Service (DoS)** - Adversaries use directed, reflected, & amplified DoS & DDoS attacks to cause service disruption. **Session Hijacking** - Occurs when an attacker can sniff traffic and intercept traffic to take over legitimate connections to a cloud service. **DNS Attacks** - These are attacks against DNS infrastructure, DNS poisoning attacks, DNS Zone Transfer attacks. **Cross-site Scripting (XSS)** - Input validation attacks to steal cookies. Redirection of users to known malicious sites. **Shared technology & multitenancy concerns** - Cloud providers typically support a large number of tenants using shared underlying infrastructure. Due to multitenancy more emphasis is placed on configuration, patching, and auditing (especially hypervisors, container management, & orchestration). **Virtual System (VM) Attacks** - If a hypervisor is compromised, all hosted VMs are at risk. In a

Aa Description	☰ Key Topic Element	▼ Page	≡ Summary
			cloud environment, this means multiple customers could be become compromised as well. **Cross-site request forgery (CSRF)** - CSRF attacks exploits the trust an application has in the user. CSRF attacks exploits the trust an application has in the user. **SQL Injection** - This type of attack targets Web Apps and allows attackers to pass SQL commands to databases. **Session Riding** - Orgs may use this term to describe CSRF attacks. Attackers may use the technique to pass unauthorized commands by riding active session by tricking users with emails or links while they are currently logged into a cloud service. **Distributed denial-of-service (DDoS) attacks** - Some argue the cloud is more vulnerable to DDoS attacks since the cloud is shared by many users & organizations. **Man-in-the-middle cryptographic attacks** - An attacker places himself in the middle of two users. Anytime this happens there is a chance the attacker can intercept and modify requests. **Side-channel attacks** - An attacker could attempt to compromise the cloud by placing a malicious virtual machine close to a target cloud server then launching a side-channel attack. **Authentication attacks (insufficient identity, credentials, & access management)** - In hosted and virtual environments authentication is a weak point. Mechanisms used to secure the authentication process and the method of authentication used are frequent targets of attackers. **API attacks** - Mechanisms used to secure the authentication process and method of authentication used are frequent targets of attackers. **Known exploits leveraging vulnerabilities against infrastructure components** - Attackers may leverage known vulnerabilities against virtualization environments,

Description	Key Topic Element	Page	Summary
			Kubernetes, containers, authentication methods, etc