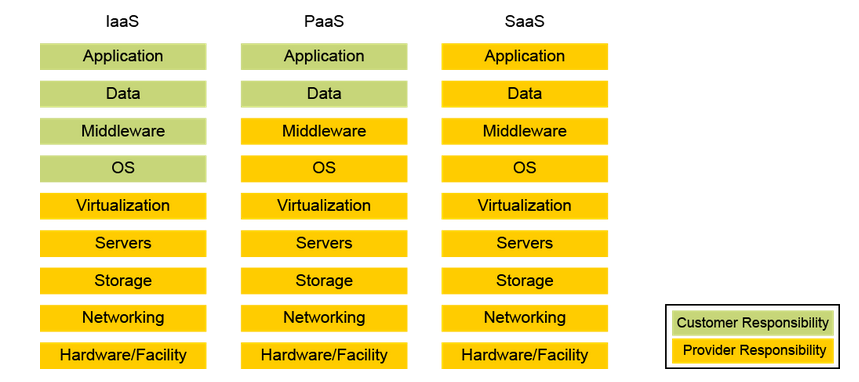
**Cloud Computing**

**Benefits**

* decreased IT staff
* lower hardware cost, and lower operating cost.
* decreased development time
* offering scalability and elasticity: as resources can be provisioned and de-provisioned rapidly, decommissioning cloud resources quickly after they are no longer needed
* better reliability and help prevent against data loss.

**Cloud Service Models**



**Cloud Deployment Models**

**Private**

* In-house managed cloud. Many companies utilize only a private cloud because of data security requirements.
* Industries such as financial, government, and healthcare have strict requirements on how data is secured, which often requires them to keep information within their firewall.
* A company has much more control and insight in a private cloud environment, however, there may not be any cost savings since they are still responsible for the IT staff, hardware, and operations.

**public cloud**

* defined as cloud services from a provider that are hosted outside of a company's walls.
* The cost of utilizing cloud services from a provider is offset by lowering the number of required IT staff and the amount of hardware that needs to be purchased and lowering the operations cost.
* large public cloud providers that offer IaaS, PaaS, Saa solutions: Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Alibaba Cloud, and Dimension Data.
* smaller companies that have public cloud offerings are: Rackspace, OpenStack, and IBM Cloud.
* Another popular public cloud offering is Apple's iCloud, which is utilized by most all iPhone and iPad users.

**Hybrid cloud**: mixture of private and public cloud services

**Community cloud:** shared between several organizations

**Cloud computing attacks:**

* **Session hijacking**: the attacker sniff traffic and intercept traffic to take over a legitimate connection to a cloud service
* **DNS attack:** the attacker tricks users into visiting a phishing site and giving up valid credentials
* **XSS:** used to steal cookies that can be exploited to gain access as an authenticated user to a cloud-based service
* **SQL injection**: this attack exploits vulnerable cloud-based applications that allow attackers to pass SQL commands to a database for execution
* **DDOS attack**
* **Man-in-the-middle cryptographic attack**: attacker place himself in the communication path between two users.
* **Authentication attack**
* **API attacks:** APIs are configured insecurely.

There is no universal, industry-accepted framework that will provide to customers a common security audit approach for a cloud environment.

Among various documents, it is useful to identify some documents that are used as indispensable foundations:

* **National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53)**
* **NIST Cybersecurity Framework**
* **ISO 27001**

**DevOps, Continuous Integration (CI), Continuous Delivery (CD), and DevSecOps**

**Waterfall Development Methodology (methodologie en cascade)**

* Software and hardware development and project management methodology that has at least five to seven phases that follow in strict linear order
* Each phase cannot start until the previous phase has been completed
* Phases: **requirements, design, implementation, verification, maintenance**
* Advantage: project requirements are agreed upon from the beginning; consequently, planning and scheduling is simple and clear, me
* asuring progress is easy as you move through the phases and hit the different milestones (etape).

Disadvantages:

* it can be difficult for customers to enumerate and communicate all of their needs at the beginning of the project.
* If your end customer is dissatisfied with the product in the verification phase, it can be very costly to go back and design the code again.
* In the waterfall methodology, a linear project plan is rigid and lacks flexibility for adapting to unexpected events.

**Agile Methodology**

* Software development and project management process where a project is managed by breaking it up into several stages and involving constant collaboration with stakeholders and continuous improvement and iteration at every stage
* Continuous collaboration is key
* Agile use Scrum: scrum described a set of meetings, tools, and roles that work in concert to help teams structure and manage
* Agile uses the Kanban process, Kanban is a scheduling system for lean development and just-in-time manufacturing
* Extreme Programming (EP) is a software development methodology designed to improve quality and for teams to adapt to the changing needs of the end customer

**DevOps**: characterizes a convergence of many technical, project management, and management movements

**Tree general way to devOps**

First way: systems and flow: in this way you make work visible by reducing the work “batch”, sizes, reducing intervals of works, and preventing defects from being introduced by building in quality and control

**Second way:** This way includes a feedback loop to prevent problems from happening again (enabling faster detection and recovery by seeing problems as they occur and maximizing opportunities to learn and improve).

**Third way:** continuous experimentation and learning

**CI/CD Pipelines**

* Continuous Integration (CI) is a software development practice where programmers merge code changes in a central repository multiple times a day
* Continuous Delivery (CD) sits on top of CI and provides a way for automating the entire software release process
* The main goal of the CI/CD processes is to be fully automated, with each run fully logged and visible to the entire team.

**Serverless Buzzword**

Serverless is a cloud computing execution model where the cloud provider (AWS, Azure,  
Google Cloud, and so on) dynamically manages the allocation and provisioning of servers.

**Container Orchestration**

Solution to manage, deploy and orchestrate container in the industry

* **Kubernetes**: Developed by Google, it is platform for creating, deploying, and managing distributed applications
* **Nomad**: A container management and orchestration platform by HashCorp.
* **Apache Mesos**: A distributed Linux kernel that provides native support for launching  
  containers with Docker and AppC images.
* **Docker Swarm**: A container cluster management and orchestration system integrated with the Docker Engine.

**Microservices and Micro-Segmentation**

* **Container**: environment set up within an operating system in which one or more applications may be run, typically assigned only those resources necessary for the application to function correctly.
* **Micro segmentation**: ability to enforce network segmentation in container and VM environments
* Micro-segmentation environment apply zero-trust model
* **zero-trust model** : dictates that users cannot talk to applications and that applications cannot talk to other applications unless a defined set of policies permits them to do so.
* **Contiv** is an open source project that allows you to deploy micro-segmentation policy-based services in container environments

*DevSecOps*

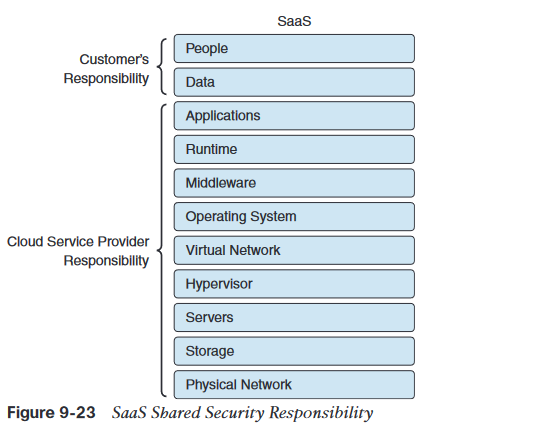
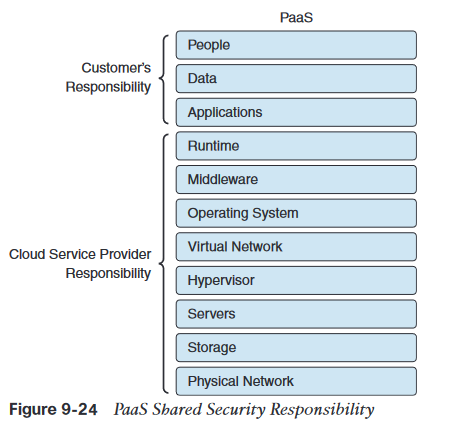
* DevSecOps is a concept used in recent years to describe how to move security activities  
  to the start of the development life cycle and have built-in security practices in the CI/CD  
  pipeline
* **The OWASP Proactive Controls** is a collection of secure development practices and guidelines that any software developer should follow to build secure applications.

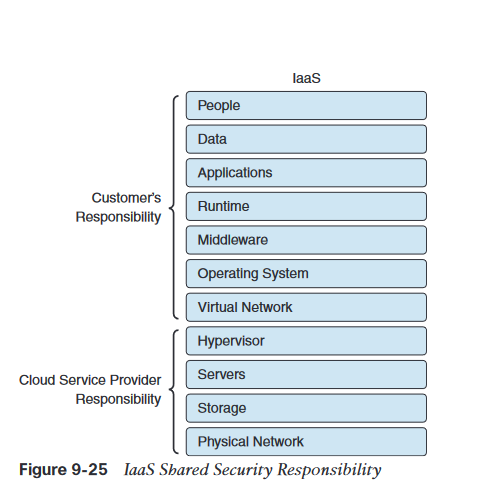
**OWASP Top 10 Proactive Controls:**  
1. Define Security Requirements  
2. Leverage Security Frameworks and Libraries  
3. Secure Database Access  
4. Encode and Escape Data  
5. Validate All Inputs  
6. Implement Digital Identity  
7. Enforce Access Controls  
8. Protect Data Everywhere  
9. Implement Security Logging and Monitoring  
10. Handle All Errors and Exceptions

Software assurance tools and methods

* Findsecbugs is a tool designed to find bugs in applications created in the Java programming language
* SonarQube is a tool that can be used to find vulnerabilities in code, and it provides support for continuous integration and DevOps environments.
* Fuzz testing, or fuzzing, is a technique that can be used to find software errors (or bugs)  
  and security vulnerabilities in applications, operating systems, infrastructure devices, IoT  
  devices, and other computing devices (ex: mutiny fuzing framework, American fuzzy, peach)

**Customer vs Provider Security responsibility**



**Pacth management in the cloud**

* Patch management in the cloud is also a shared responsibility in IaaS and PaaS environments, but not in a SaaS environment.
* SaaS environment: the CSP is the one responsible for patching all software and hardware vulnerabilities.
* IaaS environment, the CSP is responsible only for patching the hypervisors, physical compute and storage servers, and the physical network.

**Security assessment in the cloud**

When performing penetration testing in the cloud, you must first understand what you can  
do and what you cannot do. Most CSPs have detailed guidelines on how to perform security  
assessments and penetration testing in the cloud.

**Questions to ask cloud service provider**: who has access, what are the provider’s regulatory requirements, do you have the right audit…..

**Cisco security solutions that can help protect the cloud**

* **Cisco umbrella**
* **Cisco email security in the cloud:** is also a cloud-based email security solution provided by Cisco. This allows you to provide protection against threats like ransomware, business email compromise (BEC), phishing, spear phishing, whaling, and many other email-driven attacks.
  + **Forged Email Detection**  
    Cisco Email Security also provides a feature called Forged Email Detection (FED). FED is  
    used to detect spear phishing attacks by examining one or more parts of the SMTP message for manipulation
  + Sender Policy Framework  
    Cisco Email Security also has the **Sender Policy Framework (SPF)** for sender authentication and DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) for domain authentication
  + The cloud-based Cisco Email Security solution also provides a customizable reporting dashboard to access information about encrypted email traffic, including the delivery method used and the top senders and receivers.
  + The Cisco Email Security cloud service also **supports S/MIME.** Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standards-based method for sending and receiving secure, verified email messages.
* **Cisco Cloudlock,** is the solution is a **cloud access security broker (CASB)**. A CASB provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.
* **Cisco Stealthwatch cloud**
* **AppDynamics Cloud Monitoring:** provides end-to-end visibility of applications and can provide insights about application performance.
  + AppD is able to automatically discover the flow of all traffic requests in your environment by creating a dynamic topology map of all your applications.
  + Also provides cloud monitoring