SANS Security Principles

CCSP Series - Chapter # 1

SANS Security Principles Overview

- **Organization:** SANS (sans.org)
- **Services:** Training, templates, CIS control framework
- **Approach:** Risk management, starting with asset inventory
- **Prioritization:** Based on the prevalence of internet threats
- **Applicability:** Solid foundation for securing cloud infrastructure due to cloud's broad network accessibility

Cloud Security Architecture Essentials

1. **Well-Architected Framework:** Best practices for cloud infrastructure management and evaluation

2. **Common Pillars Across CSPs:**
   - **Security:** Identity and access management, encryption, monitoring
   - **Reliability:** System and data accessibility
   - **Performance:** Scalability based on demand

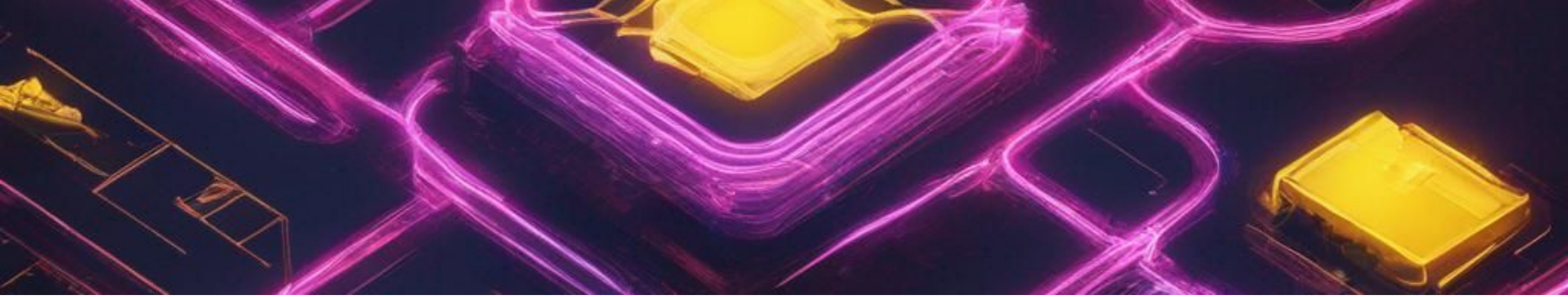
3. **Selection Criteria:** Driven by organizational needs and specific CSP offerings

Cloud Security Alliance Enterprise Architecture

Framework: Aligning IT resources with business requirements

Domains: Business Operation Support Services, IT Operations & Support, Technology Solution Services, Security, and Risk Management

Infrastructure Protection: Focus on identifying tools, processes, and best practices for security



DevOps and Security Integration

- **DevOps:** Bridging development and operations for faster software delivery
- **Importance:** The inclusion of security to identify risks early in the lifecycle
- **Models:** DevSecOps and SecDevOps, advocating for 'shifting left' in security testing
- **Resource:** NIST working group on integrating security in DevOps processes

Evaluating Cloud Service Providers (CSPs)

1. **Criteria Use:** Objective and standardized for easier comparison among CSPs

2. **Standards Utilization:** Voluntary (e.g., SOC 2) vs. mandatory (e.g., PCI DSS)

3. **Regulatory Compliance:** Adjusting to various market-specific standards and legal requirements

International and Industry Standards

ISO 27001 & 27002: Establishing ISMS and related control sets

ISO 27017 & 27018: Extending guidance for cloud services and PII protection

PCI DSS: 12 requirements focusing on payment data security and integrity

Governmental Standards: Complying with high-security services like FedRAMP and UK G-Cloud

Security Compliance and Assurance Programs

- **CSA Security, Trust, Assurance, and Risk (STAR):** Voluntary registry for CSP security and privacy controls
- **System/Product Certifications:**

> - **Common Criteria (CC):** Protection profiles and EALs for information security product evaluation
> - **FIPS 140-2:** Cryptographic module standards for government data security

Cloud Computing Basic Concepts and Architecture

1. **NIST Definition:** On-demand, network-based access to shared computing resources

2. **Service and Deployment Models:** SaaS, PaaS, IaaS; public, private, community, hybrid clouds

3. **Roles:** Cloud service customer, provider, partner, broker, and regulator

Key Cloud Computing Characteristics

On-Demand Self-Service, Broad Network Access, Multitenancy

Rapid Elasticity and Scalability

Resource Pooling

Measured Service

Building Block Technologies for Cloud

- **Virtualization:** Resource sharing using hypervisors
- **Storage:** SANs and NAS, ensuring flexible and scalable storage
- **Networking:** IP-based, high bandwidth, low latency networks
- **Databases:** Diverse types facilitating big data applications
- **Orchestration:** Automating, managing, and integrating cloud resources

Cloud Reference Architecture and Activities

1. **NIST RA Roles:** Consumer, provider, auditor, broker, carrier

2. **Role-Based Activities:** Evaluating, using, managing, compliance assessment, service aggregation, and connectivity

3. **Capability Types:** Application, platform, and infrastructure focus

Cloud Service Categories Breakdown

Software as a Service (SaaS): Turnkey software solutions, managed by CSPs

Platform as a Service (PaaS): Development platforms, tools management shared between customer and CSP

Infrastructure as a Service (IaaS): Hardware and basic infrastructure, more control, and responsibility for the customer

Cloud Deployment Models Defined

- **Public Cloud:** Broad access, managed by third-party providers
- **Private Cloud:** Organization-specific cloud with controlled access
- **Community Cloud:** Designed for organizations with common interests
- **Hybrid Cloud:** Combining different cloud models for flexible solutions
- **Multi-Cloud Strategy:** Using services from multiple CSPs for enriched services

Considerations for Secure Cloud Computing

1. **Interoperability:** Smooth operation across multiple platforms
2. **Portability and Reversibility:** Flexibility in moving data/processes
3. **Availability:** Ensuring robust SLAs for consistent uptime
4. **Security and Privacy:** Data protection across layers of cloud
5. **Resiliency:** Designing failover capabilities for disaster scenarios
6. Performance, Governance, Maintenance, Service Levels

Impact of Related Technologies

- **Data Science and Machine Learning:** Leveraging large data volumes for security insights
- **Artificial Intelligence:** Advancing toward intelligent, human-like computing services
- **Blockchain:** Secure, distributed ledger technology
- **Internet of Things (IoT):** Vast data production requiring new storage and security approaches
- **Containers:** Application portability and security isolation
- **Quantum and Edge Computing:** Emerging areas promising powerful computing and distributed processing

Summary of Cloud Concepts and Design

Understanding cloud services: Real-world implications for security practice

Variety in cloud architecture: Making informed choices based on security needs

Domain 1 knowledge: Essential for safeguarding cloud environments

Practical application: Tailoring technologies to support secure cloud computing

Information Security Buzz

Discover more at our InfoSec Knowledge Hub