Security Controls in Cloud System Architecture

Overview

Security controls are essential components in a cloud system architecture. They protect cloud-based assets, manage risks, and ensure regulatory compliance.

Categories of Security Controls

- **Preventive Controls** â€“ Stop threats before they occur (e.g., encryption, access control).
- **Detective Controls** â€“ Identify and detect incidents as they happen (e.g., monitoring, logging).
- **Corrective Controls** â€“ Respond and recover from incidents (e.g., backup, disaster recovery).

Key Security Controls

Control	Description
Identity & Access Management (IAM)	Manage user access to resources using roles, policies, and authentication mechanisms.
Encryption	Protect data at rest and in transit with encryption algorithms and key management.
Network Security	Use firewalls, segmentation, VPNs, and security groups to control network traffic.
Monitoring & Logging	Track events, detect anomalies, and maintain audit trails for compliance and investigations.
Vulnerability Management	Perform regular security assessments and patching to reduce risks from known threats.
Data Loss Prevention (DLP)	Implement controls to prevent unauthorized data exfiltration or exposure.
Incident Response	Define and enforce procedures for responding to security incidents effectively.

Cloud Security Model Layers

- **Infrastructure Layer** â€“ Physical and virtualization controls.
- **Platform Layer** â€“ OS hardening, API security, and middleware controls.
- **Application Layer** â€“ Secure coding, application firewalls, and input validation.
- **Data Layer** â€“ Encryption, masking, and secure data storage practices.

Sample Cloud System Architecture Diagram

[Insert architecture diagram here]

Conclusion

Implementing layered and robust security controls is critical for safeguarding cloud environments against evolving threats and ensuring data confidentiality, integrity, and availability.