Cloud Security Architecture Principles Checklist

Below are key principles for a rock-solid cloud security architecture, divided into four main categories: risk assessment and management, security framework development, compliance integration, and operational resilience.

Risk assessment and management	
☐ **Identification of users and assets**	Inventory cloud users, resources, associated roles, and access levels.
☐ **Business context, policies, and risk strategy**	Align cloud strategy with business context, policies, and risk thresholds.
☐ **Vulnerability and threat identification**	Continuously assess your cloud environment for known vulnerabilities and emerging threats.
☐ **User identity and access management**	Gain visibility and control over user authentication, roles, and privileges.
☐ **Activity monitoring**	Observe system behavior in real-time to detect anomalies, policy violations, and indicators of compromise.
Security framework development	
☐ **Security controls**	Implement guardrails to protect users, data, and infrastructure.
☐ **Configured responsibilities and security standards**	Define roles and expectations for managing security across services.
☐ **Data encryption**	Apply encryption protocols to protect all sensitive data at rest and in transit.

Compliance integration	
☐ **Data protection standards**	Ensure alignment with HIPAA, GDPR, and other regulatory frameworks.
☐ **Visibility across cloud deployments**	Maintain transparency across public, private, and hybrid clouds.
☐ **Regular verification**	Perform scheduled audits and security checks to validate adherence.
Operational resilience	
☐ **Monitor traffic in and out of the cloud**	Track ingress and egress points to detect anomalies.
☐ **Segment the architecture**	Isolate workloads to reduce the blast radius of an attack.
☐ **Automate cloud security tasks**	Use automation to enforce policies, remediate issues, and streamline workflows.
☐ **Ensure architecture flexibility**	Design with adaptability in mind for future needs and emerging threats.