Google Cloud

Architecture Framework:

Security, privacy, and compliance

---

www.thecyphere.com info@thecyphere.com

Learn the key steps to establish **security**, **privacy**, and **compliance** controls within your Google Cloud infrastructure for a resilient and trusted environment.

www.thecyphere.com **info@thecyphere.com**

1. Shared responsibilities and shared fate on Google Cloud

www.thecyphere.com

info@thecyphere.com

Shared responsibility: In the cloud, responsibilities align with workload and services:

a) IaaS: Customers handle most security; providers focus on infrastructure.

b) PaaS: Providers manage more, including the network; customers handle data security.

c)SaaS: Providers own most security; customers manage access and data.

d) FaaS/Serverless: Varies based on the service and event.

Shared fate: Google Cloud assumes responsibility for enhancing security. It provides:

a) Guidance to establish a secure initial cloud environment.

b) Transparent security recommendations, controls, and best practices.

c) Offers resources for a secure Google Cloud setup, minimising misconfiguration-related security risks.

d) Aids in continuous governance of your cloud environment.

www.thecyphere.com

info@thecyphere.com

2. Security principles

- Build security at every level.
- Configure encryption, and limit access wherever possible.
- Design systems for flexibility.
- Document security requirements for each component.

www.thecyphere.com **info@thecyphere.com**

- Remove human intervention and automate deployment.
- Use automated tools to monitor applications and infrastructure.

  Don’t forget the CI/CD pipeline.
- Meet compliance, including PII obfuscation, via automation.

www.thecyphere.com **info@thecyphere.com**

- Adhere to data residency and sovereignty requirements.
- Integrate security into development with early automated code security tests, continuous infrastructure scans, and misconfiguration detection.

3. Manage risk with controls

www.thecyphere.com

info@thecyphere.com

- Perform a risk assessment before creating and deploying resources.
- **Mitigate the identified risks by Technical Controls:** Utilise built-in security features and third-party tools.

Contractual Protections: Define clear legal agreements with your cloud provider, covering security and compliance commitments

Third-party Verifications: Engage third-party audits to verify compliance and security, such as ISO 27017, to ensure industry standards are met.

4. Asset management

- Utilise tools for real-time resource insights and effective asset management.
- Integrate Google Cloud Assets with SIEM.
- Continuously monitor for compliance policy deviations.

5. Identity and access management

- Integrate with identity provider for SSO and configure MFA.
- Employ workload identity federation for external apps.

- Create a dedicated account, set up backup accounts, and enable Multi-Factor Authentication (MFA).
- Follow the 'least privilege' principle, ensuring individuals access only what they need.

- Deploy role segregation and on-demand API calls.
- Review default roles and permissions.
- Automate policy controls.

6. Compute and container security

- Activate secure processing of sensitive workloads and data.
- Disable external IP allocation.
- Monitor compute instances.
- Maintain updated images and clusters, also manage their access.
- Isolate containers within a sandbox.

7. Ensure network security

- Implement explicit trust based controls approach
- Remove default networks in both new and existing projects.
- Protect your application load balancer from unwanted traffic.

www.thecyphere.com **info@thecyphere.com**

- Use firewalls for real-time traffic insights.
- Enhance security and compliance for Compute Engine and Google Kubernetes Engine (GKE) workloads.

8. Data security

- Classify data as Public, Internal, Confidential, and Restricted.
- Implement data governance strategies.
- Set up data storage and user access configurations.

- Ensures data security, privacy, accuracy, availability, and usability.
- Encrypt your data.
- Protect your secrets.

www.thecyphere.com

info@thecyphere.com

9. Secure application deployment

- Automate security vulnerability scanning.
- Enforce approved deployment processes.
- Scan and monitor application code for known vulnerabilities
- Encrypt container images.

10. Manage compliance obligations

- Assess, implement, and monitor regulatory compliance.
- Automate security policies through IaC.

www.thecyphere.com

info@thecyphere.com

11. Implement data residency and sovereignty requirements

- Limiting resource deployment and personnel access.
- Control resource creation and data replication.

www.thecyphere.com

info@thecyphere.com

12. Implement privacy requirements

- Categorise and protect confidential data, including PII.
- Implement IAM access controls.
- Deploy zero-trust controls for cloud resources.
- Stay protected against phishing attacks and malware.

13. Implement logging and detective controls

- Monitor network performance.
- Prevent data exfiltration with Google Cloud's detection and prevention features.
- Do centralise monitoring to enhance threat prevention, detection, and response.

If you find it useful, follow for more updates and share ❤

www.thecyphere.com info@thecyphere.com