

DATA SHEET

GCP Data Protection Strategy Implementation



Why Choose Encryption Consulting LLC?

Encryption consulting is a leading cyber security firm with aspread of expertise across domains in Data Protection, Cryptography and Cloud Security. Encryption Consulting recruits industry best resources with ample amount of experience in Cyber Security with capability to perform comprehensive tasks especially in Data Protection Domains. Cryptography and Key Management are core service areas.

Expertise dedicated for your Cloud Management

Encryption Consulting's team will evaluate the existing GCP Cloud environment and produce an assessment report. Based on the recommendations identified during assessment, implementation plan is designed for GCP Cloud Data Protection. Encryption Consulting's expert team will evaluate and implement the GCP Data Protection Strategy with utmost care and perfection.

Key benefits of GCP Data Protection Implementation

- **Secure Deployment**

Achieve high secure deployment of GCP Data Protection domain-wise matching your requirements.

- **Deep Analysis**

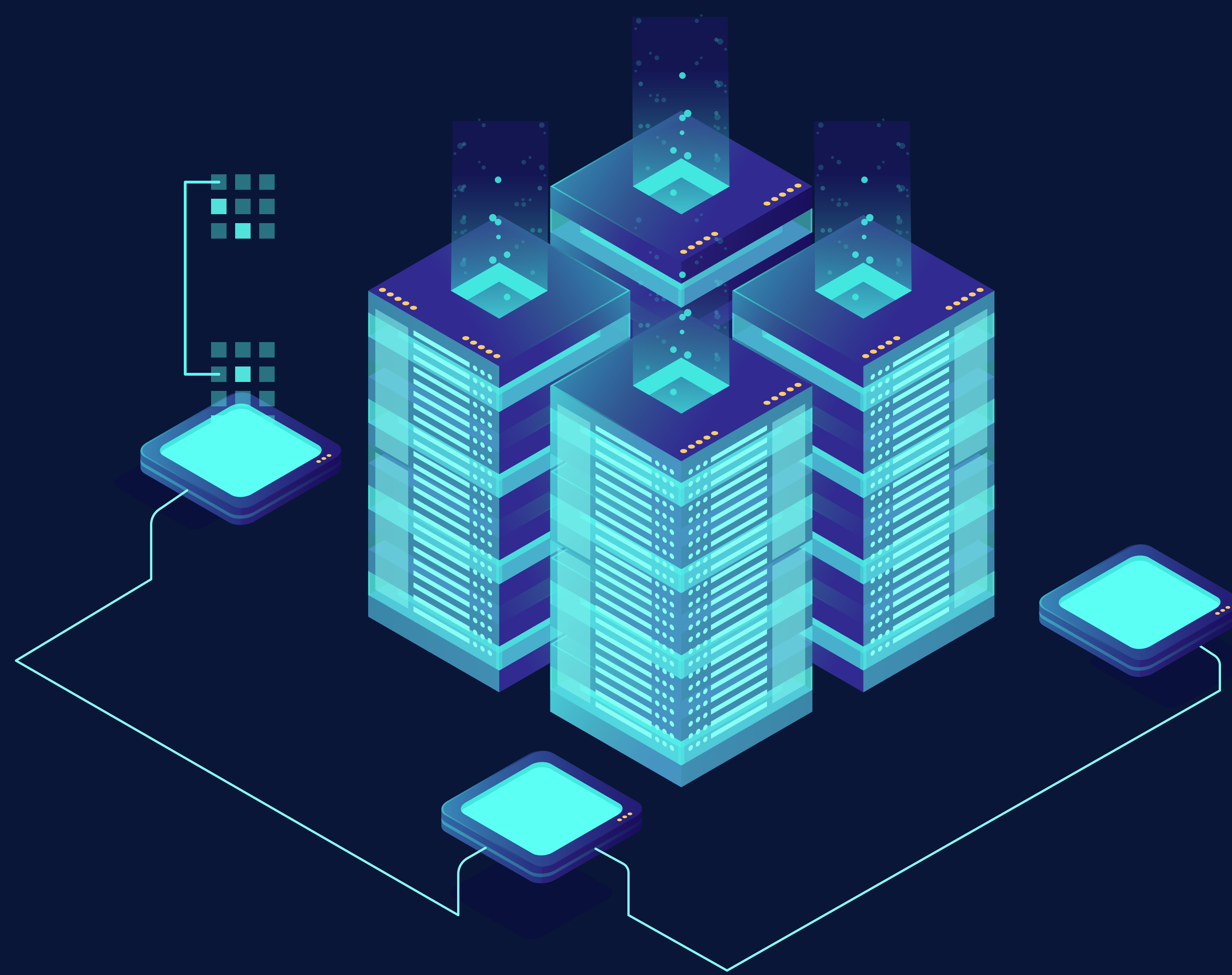
In-depth understanding of your cloud environment with proper assessment and workshops

- **Risk Elimination**

Eliminates risk with expert deployment of Key Management Infrastructure, certificate management and DLP

- **Regulatory Compliance**

Secure and efficient Data Protection implementation by achieving various regulatory compliance such as PCI DSS, GDPR



Our Approach to secure your GCP Environment

Encryption Consulting's team will implement domain-wise Data Protection Strategy based on risk prioritization and timeline. Right from classification of data in GCP cloud to protecting Data in various layers through encryption, DLP across GCP storages such as Cloud Datastore, Cloud SQL, Cloud Spanner, Bigquery etc. We leverage GCP native encryption capabilities in providing an efficient security to your data in support with other Data Protection technologies. We also leverage GCP native tools like GCP IAP, ALTS etc. to take full advantage of the technology.

DATA – AT – REST PROTECTION

GCP Discovery

Data at rest scans will be performed across GCP Cloud environment to identify sensitive data and develop Data Flow Diagrams (DFD), Inventory

AES256/AES128 Encryption (DB)

Databases are protected through a FIPS 140-2 validated encryption module using either AES256 or AES128

Disk – Level Encryption

Static data residing on GCP storages such as disks with in clusters and back ups can be protected through standard AES-256 u

DATA – IN – TRANSIT PROTECTION

Authenticating Endpoints

Data sources and destinations are verified along with validation of human or process pings. Google IAM is used for access control

Cloud DLP)

Data in transit can be protected by implementing CASB solution in cloud and also by protecting endpoint machines with Endpoint DLP. We evaluate and implement appropriate vendor for your environment

Network Traffic Encryption

Encryption is done in the transport and network layer. Cloud Key Management can be configured to manage keys and certificates

DATA – IN – USE PROTECTION

Field – Level Encryption

DZone Security column level encryption can be implemented to protect dynamic web sensitive data while meeting compliance requirements

Application Layer Transport Security(ALTS)

GCP ALTS ensures all Remote Procedure Calls(RPCs) are protected. It uses state-of-the-art cryptographic primitives

Tokenization & Obfuscation

Our experts will implement Tokenization and Obfuscation to protect highly critical sensitive data stored in GCP cloud. This ensures compliance with GDPR

Deliverables

Implementation deliverables vary as per the client requirements and engagement scope. Please find below sample deliverables for high level view:

- GCP Workbook
- Service documentation
- Regulatory requirements and assessments framework
- Training and awareness documentation
- Executive summary report

Client References

1. Global Reinsurance Company

Background

A leading Reinsurance company sought out Encryption Strategy implementation for GCP . Client requirement was to provide a phase-wise implementation as per risk prioritization plan.

What we did

- Designed requirements framework for assessing GCP Cloud environment and identifying risk appetite.
- Developed implementation plan based on workshop outcomes and risk prioritization.
- Implemented Application Layer Transport Security (ALTS) as per the assessment outcomes.
- Developed service documentation with standards for future reference.

Outcomes/impact

- Encryption strategy report.
- GCP Encryption implementation guide.
- Service documentation.

2. Global Agri-tech Corporation

Background

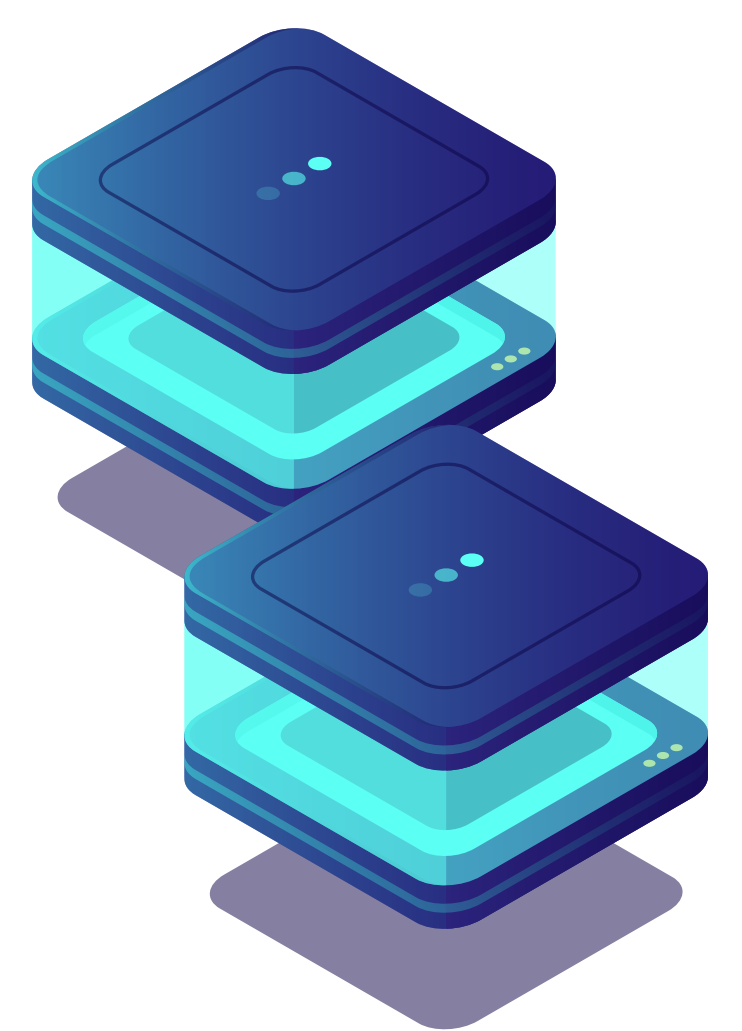
A global Agri-tech corporation decided to perform an overall GCP Data Discovery and Data Classification across the organization. They wanted to develop Critical Data Inventory and Data Flow Maps for GCP Cloud data.

What we did

- Performed document review to identify existing storage locations.
- Conducted workshops with critical crown jewel business stakeholders to identify “Critical Data Elements” and data flow process.
- Mapped and developed Data Flow Maps depicting the sensitive data flow and security controls implemented.
- Created a global data inventory with critical data assets and elements.

Outcomes/impact

- Data Flow Maps.
- Critical Data Inventory.
- Data Lineage Document.



Why Encryption Consulting LLC?



Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security



Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure



Hardware Security Module – HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.



Certificate Lifecycle

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases



Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?



Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us