**Background**

Goldman Sachs handles significant amounts of sensitive data, including client and financial records, across off-premises environments such as public clouds and third-party providers. The risk of unauthorized access, use, or disclosure in these environments has led to vulnerabilities and audit findings, particularly due to inconsistent encryption practices and poor key management. This document proposes a reference implementation for data encryption at rest in off-premises settings to mitigate these risks, ensure compliance with firmwide policies like DP30\*\*, and support operational needs while protecting data confidentiality, integrity, and availability.

**Definitions**

* **Sensitive Data** - Data classified as DP20 or above per the Firmwide Data Classification Policy, including personally identifiable information (PII), financial records, and proprietary data.
* **Encryption at Rest** - Cryptographic protection of data stored on digital media in off-premises environments, such as cloud databases or third-party storage, to prevent unauthorized access.
* **Off-Premises Environment** - Data residing outside GS datacenters, including public cloud platforms (e.g., AWS, Azure) or third-party provider systems.
* **Production** - Environments supporting business processes, hosted off-premises.
* **Non-Production** - Off-premises environments used for development and testing.
* **Data Asset Owner** - The owner of the primary deployment associated with the data asset, responsible for encryption compliance.

**Considerations when working with data encryption at rest**

* Sensitive data in off-premises environments must be encrypted using firm-approved standards to mitigate breach risks.
* Performance and cost implications of encryption in cloud or third-party systems must be optimized.
* Access controls must align with GS entitlement management to protect encrypted data.

**Risks and Threat Vectors**

| **Class** | **Risk** | **Threat Vector** | **Examples** |
| --- | --- | --- | --- |
| Data | Unauthorized Access | Misconfigured cloud storage | - Unencrypted S3 bucket exposes client PII due to improper settings. |
|  |  | Third-party insider threat | - A third-party provider employee accesses unencrypted backups. |
|  | Key Compromise | Exposure of cloud KMS keys | - Misconfigured IAM roles leak encryption keys on AWS. |
|  |  | Insufficient key rotation | - Stale keys in a third-party system allow decryption of archived data. |
|  | Data Leakage | Unencrypted data sync | - Unsecured API transfers unencrypted data to a third-party service. |
|  | Data Loss | Loss of cloud keys | - Deleted keys render encrypted data in Azure unrecoverable. |
| Operational | Resource Starvation | Encryption overhead in cloud | - High CPU usage from encryption slows cloud application performance. |
|  | System Downtime | Key management failure | - A third-party KMS outage prevents data decryption, halting operations. |

**Areas Requiring Further Review**

* Compatibility of off-premises platforms (e.g., AWS, Azure) with GS-approved cryptography standards.
* Evaluation of third-party provider key management integration with GS KMS.
* Assessment of encryption performance impacts on cloud-based high-traffic systems.
* Review of entitlement controls for off-premises access to encrypted data (e.g., AC-3.106).

**Pending Approvals**

* Approval from Business Sponsors for off-premises encryption workflows (e.g., AC-3.105).
* Sign-off by the Data Protection Oversight Group on cloud compliance with DP30\*\*.
* Authorization from Privilege Managers for RBAC configurations in off-premises environments.

**Requirements**

* Data at rest in off-premises environments (e.g., public cloud or third-party providers) must be encrypted using cryptographic keys and mechanisms compliant with the firm-approved cryptography standard, as per SC-28.1.107.
* Encryption keys must be managed securely with access controls, rotation policies, and audit logging, integrated with a GS-approved Key Management System.
* Data used in off-premises business processes must remain encrypted outside approved workflows.
* Encryption must not compromise performance or availability in off-premises systems.
* Developers must use encrypted off-premises test datasets, masked or anonymized per Tech Risk guidelines.

**Proposal**

| **Feature** | **Immediate** | **Short Term** | **Target** |
| --- | --- | --- | --- |
| Identification of off-premises encryption coverage | - Assess all off-premises storage for sensitive data classification | - Add questions on cloud sensitivity to ARP | - Integrate sensitivity data into AppDir for off-premises assets |
| Separation of Production - Non-Production Encryption | - Document off-premises architecture for review by Technical Owners | - Validate multi-environment separation with third-party providers | - Achieve 100% key separation between off-premises production and non-production |
| Key Management Security | - Use GS-approved KMS for off-premises keys | - Implement automated key rotation in cloud KMS | - Enforce static analysis in SDLC for key security in off-premises deployments |
| Performance Optimization | - Restrict off-premises processes to controlled code bases | - Enable hardware-accelerated encryption in cloud (e.g., AWS Nitro) | - Limit latency increase to <5% in off-premises environments |

**Features and Intermediate Short-Term Targets**

* **Features**:
  + Centralized off-premises KMS with HSM integration for key management.
  + Hardware-accelerated encryption (e.g., AWS Nitro) to reduce cloud performance impact.
  + Real-time audit logging of off-premises encryption events, compliant with AU-3.102.
  + Masked encrypted test datasets for off-premises non-production use.
* **Intermediate Short-Term Targets**:
  + Month 2: Deploy KMS pilot for off-premises with initial key rotation (Infrastructure Team).
  + Month 4: Achieve 50% encryption coverage in off-premises production databases (Database Team).
  + Month 6: Extend encryption to 75% of off-premises non-production environments (DevOps Team).
  + Month 7: Validate backup encryption in off-premises systems (Backup Team).

**Reference Implementation Proposal**

To address the identified risks and meet the requirements, the following reference implementation for data encryption at rest in off-premises environments is proposed:

1. *Encryption Standards*
   * Use AES-256 in Galois/Counter Mode (GCM) for off-premises data, compliant with FIPS 140-3 and GS cryptography standards.
   * Ensure cryptographic modules are validated by Data Asset Owners for off-premises platforms.
2. *Key Management*
   * Deploy a GS-approved Key Management System (KMS) integrated with off-premises providers (e.g., AWS KMS, Azure Key Vault), using HSMs for key generation.
   * Automate key rotation every 12 months with versioning, enforcing RBAC as per AC-3.111.
   * Maintain audit trails of key operations, aligning with AU-3.102.
3. *Environment-Specific Encryption*
   * *Production*: Enable encryption for off-premises databases (e.g., AWS RDS with TDE), object storage (e.g., encrypted S3 buckets), and third-party systems, validated by Technical Owners.
   * *Non-Production*: Use separate keys for off-premises non-production data, ensuring compliance with production-level controls (e.g., AC-3.105).
   * *Backups*: Encrypt off-premises backups with KMS-managed keys, restricting access to authorized recovery processes.
4. *Performance Optimization*
   * Leverage cloud-native acceleration (e.g., AWS Nitro) to minimize encryption overhead, monitored by Solution Owners.
   * Configure encryption at the storage layer to reduce application changes in off-premises systems.
5. *Access and Audit Controls*
   * Implement RBAC for off-premises decryption, with Privilege Managers reviewing entitlements quarterly (e.g., AC-6.7.100).
   * Log all encryption and decryption operations in a tamper-proof audit trail, integrated with the firm’s central inventory (e.g., AC-24.1).
   * Conduct quarterly validations of off-premises encryption feeds to the central inventory (e.g., AC-24.1.100).
6. *Development and Testing*
   * Provide developers with masked off-premises test datasets, compliant with SA-15.9 and Tech Risk anonymization guidelines.
   * Use off-premises sandboxed environments with KMS-managed keys, preventing self-approval (e.g., AC-3.106).

**Implementation Roadmap**

| **Phase** | **Activity** | **Timeline** | **Owner** |
| --- | --- | --- | --- |
| 1 | Assess off-premises encryption posture and gaps | Month 1 | Security Team |
| 2 | Deploy KMS and integrate with off-premises providers | Months 2-3 | Infrastructure Team |
| 3 | Enable encryption for off-premises production systems | Months 4-5 | Database Team |
| 4 | Extend encryption to off-premises non-production | Month 6 | DevOps Team |
| 5 | Implement backup encryption and key rotation | Month 7 | Backup Team |
| 6 | Conduct compliance audit and address findings | Month 8 | Compliance Team |

**Metrics for Success**

* Percentage of off-premises sensitive data encrypted at rest: Target 100%.
* Number of key compromise incidents: Target 0.
* Performance impact from encryption: Target <5% latency increase.
* Compliance audit findings related to off-premises encryption: Target 0.

**Risk Mitigation**

* *Key Loss*: Maintain redundant off-premises KMS instances and secure key backups.
* *Performance Degradation*: Optimize with cloud acceleration and monitor usage.
* *Unauthorized Access*: Enforce least privilege and monitor key usage, with Privilege Manager oversight.
* *Non-Compliance*: Conduct regular audits against DP30\*\* and GS standards.

**Environment Encryption Matrix**

| **Environment** | **Data Read Sensitive** | **Data Write Sensitive** | **Operational Sensitivity** | **Business Sensitivity** | **Encryption Required** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- |
| Off-Premises Production Database | Y | Y | Y | Y | Y | AES-256 with KMS-managed keys |
| Off-Premises Non-Production Database | Y | N | N | N | Y | Separate keys from production |
| Off-Premises Object Storage | Y | Y | N | Y | Y | Cloud-native encryption (e.g., S3) |
| Off-Premises Backups | Y | N | N | Y | Y | KMS-encrypted archives |
| Off-Premises Development Sandbox | N | N | N | N | N | Use masked or synthetic data |

**Encryption Configuration Matrix**

| **Data Read** | **Data Write** | **Operational** | **Business** | **End User** | **Environment** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- |
| Y | Y | Y | Y | Application | Off-Premises Production Database | TDE with AES-256, KMS keys |
| Y | N | N | N | Developer | Off-Premises Non-Production Database | TDE with separate KMS keys |
| Y | Y | N | Y | Application | Off-Premises Object Storage | Cloud encryption with AES-256 |
| Y | N | N | Y | Admin | Off-Premises Backups | KMS-encrypted archives |
| N | N | N | N | Developer | Off-Premises Sandbox | No encryption; synthetic data |

**Conclusion**

Implementing data encryption at rest in off-premises environments is essential to protect sensitive GS data, ensure compliance with DP30\*\*, and mitigate risks of unauthorized access or data loss. This reference implementation provides a comprehensive framework to encrypt data, manage keys securely, and support development needs without compromising performance or security. By adopting these controls, GS can strengthen its off-premises data protection posture and align with industry and regulatory requirements.