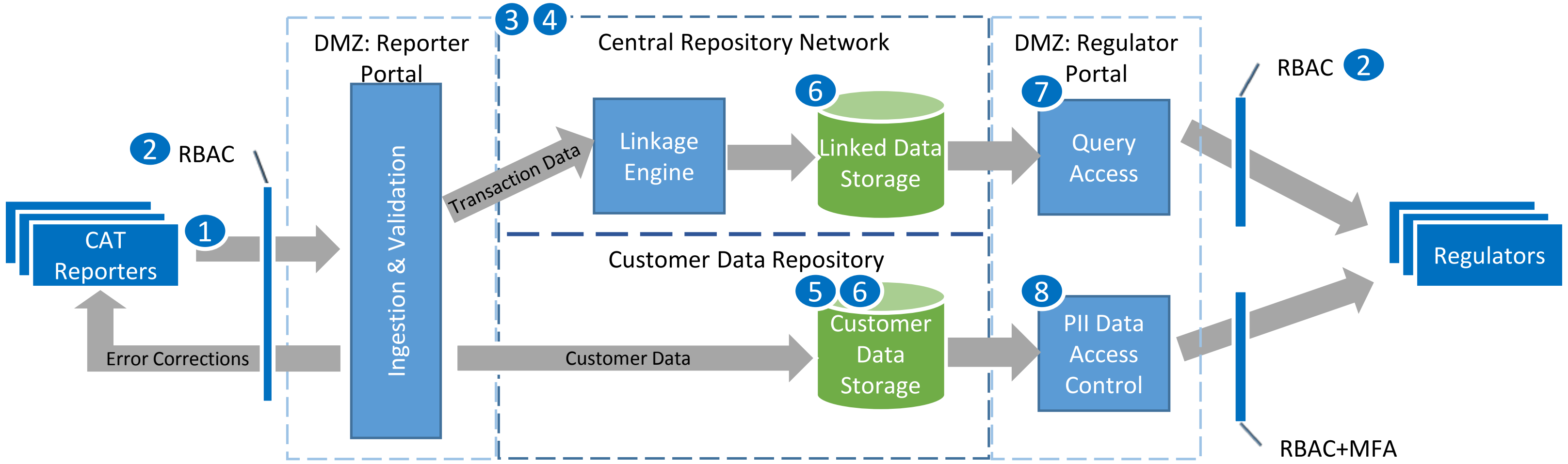
High Level CAT Security Requirements

The below represents some of the high-level security controls required by the CAT NMS Plan. Actual architecture may vary depending on the specific solution provided by the Plan Processor.



Architecture-level Controls

1. Encrypted connectivity to CAT (e.g. private lines, VPNs) (App.D.4.1.1)
2. Role Based Access Controls (RBAC) governing data access; all access logged (App.D.4.1.4)
3. CAT Data not accessible via public internet (App.D.4.1.1, 4.1.3)
4. Segregation of CAT compute and network infrastructure from other cloud tenets (App.D.4.1.3)
5. Customer data segregated into separate database (App.D.4.1.6)
6. All data encrypted in flight and at rest (App.D.4.1.2)
7. No PII data included in query results (App. D.8.1.1, 8.1.3)
8. Separate PII request & retrieval process; Multi-Factor Authentication (MFA) required and all access logged and audited (App.D.4.1.4)

Key

➡ Encrypted Connection

▬ ▬ Isolated Network

🟩 Encrypted Storage

▬ ▬ DMZ Network

Program-level Controls

- The Plan Processor must designate an employee as CISO, with responsibilities including creating and enforcing policies, procedures, and control structures to monitor and address data security issues (6.2.v)
- Documented policies and procedures must be provided for:
  - A comprehensive data security plan, reviewed annually, and including regular penetration testing and code security audits (App.D.4.1)
  - Key management practices, including rotation and revocation(App.D.4.1.2)
  - Access control policies, including auditing, real-time monitoring of all access to CAT transaction and PII data, and data destruction policies (App.D.4.1.2)
  - CRO must annually review and certify all persons with PII access (App.D.4.1.6)
  - Breach detection and management policies, including monitoring and escalation practices, and incident response plan (App.D.4.1.5)
  - Employee data access policies, including background checks, separation of duties, entitlement management, and data access monitoring (App.D.4.1.4)
- All datacenters must be at least SOC-2 certified, with audits at least annually (App.D.4.1.3)
- Compliance with applicable industry standards recommended by NIST, FFIEC, and ISO (App.D.4.2)
- Participants must have policies and procedures to ensure the confidentiality of CAT Data and limit its use to surveillance and regulatory purposes (6.5.f.i.A)

High Level CAT Security Requirements

Architecture-level Controls

❶ **Encrypted connectivity to CAT** (App.D.4.1.1)

- CAT Reporters must use secure methods such as private lines or (for smaller broker-dealers) Virtual Private Network connections

❷ **Role Based Access Controls** (RBAC) (App.D.4.1.4)

- Data access is governed at the attribute level following the “least privileged” practice; all access is logged
- Periodic reports with the current list of authorized users and the date of their most recent access must be provided to Participants, the SEC and the Operating Committee

❸ **CAT Data not accessible via public internet** and deployed within the network infrastructure (App.D.4.1.1)

- If public cloud infrastructure is used, virtual private networking and firewalls/access control lists or equivalent controls such as private network segments or private tenant segmentation must be used to isolate CAT Data from unauthenticated public access
- Remote access to the Central Repository must be limited to authorized Plan Processor staff and must use secure multi-factor authentication

❹ **Segregation of CAT compute and network infrastructure** from other cloud tenants (App.D.4.1.3)

- CAT compute infrastructure may not be co-mingled with other non-regulatory systems
- Systems hosting the CAT processing for any applications must be segmented from other systems as far as is feasible on a network level (firewalls, security groups, ACL’s, VLAN’s, authentication proxies/bastion hosts and similar)
- For systems using inherently shared infrastructure/storage (e.g., public cloud storage services), an encryption/key management/access control strategy that effectively renders the data private must be documented

❺ **Customer data segregated** into separate database (App.D.4.1.6)

- The CAT must capture and store Customer and Customer Account Information in a secure database physically separated from the transactional database

❻ **All data encrypted in flight and at rest** including archival data storage (App.D.4.1.2)

- Data encrypted in flight via TLS/SSL
- Symmetric key encryption must use a minimum key size of 128 bits or greater (e.g., AES-128), larger keys are preferable
- The Plan Processor must describe how PII encryption is performed (e.g. AES-256, 3DES)
- Asymmetric key encryption (e.g., PGP) for exchanging data between Data Submitters and the Central Repository is desirable
- Non-PII CAT Data stored in a Plan Processor private environment is not required to be encrypted at rest

❼ **No PII data included in query results** (App.D.8.1.1, 8.1.3)

- Results will display existing non-PII unique identifiers (e.g., Customer-ID or Firm Designated ID)

❽ **Separate PII request & retrieval process** (App.D.4.1.2, 4.1.4, 4.1.6)

- Multi-Factor Authentication (MFA) capability for all logins (including non-PII) is required to be implemented by the Plan Processor
- All PII access must be logged and audited
- Unencrypted storage of PII is prohibited
- CRO must annually review and certify all persons with PII access

High Level CAT Security Requirements

Program-level Controls

CISO and CCO Responsibilities (6.2.v; App.C.4.a; App.D.4.1.6)

- The Plan Processor must designate an employee as CISO, with responsibilities including creating and enforcing policies, procedures, and control structures to monitor and address data security issues
- Comprehensive data security plan, reviewed annually by the CCO, and including regular penetration testing and code security audits
- The CCO and the CISO shall have access to daily PII reports that list all users who are entitled for PII access, as well as the audit trail of all PII access that has occurred for the day being reported on

CAT Data Access and Confidentiality (6.5.f.i.A; App.D.4.1.4)

- Participants must have policies and procedures to ensure the confidentiality of CAT Data and limit its use to surveillance and regulatory purposes
- User access control policies, including auditing, real-time monitoring of all access to CAT transaction and PII data, and data destruction policies
- Employee data access policies, including background checks, information barriers, separation of duties, internal segmentation, and entitlement management

Datacenter Standards (App.D.4.1.3)

- All datacenters must be at least SOC-2 certified, with audits at least annually

Industry Standards (App.D.4.2)

- Compliance with applicable industry standards recommended by NIST, FFIEC, and ISO
- Plan Processor shall seek membership in the FS-ISAC and other comparable organizations

Key Management (App.D.4.1.2, 4.1.3)

- If public cloud managed services are used, key management surrounding the encryption of that data must be documented (particularly whether the cloud provider manages the keys, or if the Plan Processor maintains that control), as well as policies for rotation and revocation
- PII encryption methodology must include a secure documented key management strategy such as the use of HSM(s)
- Auditing and real-time monitoring of the service for when cloud provider personnel are able to access/decrypt CAT Data, as well as a response plan to address chain of custody must be documented in detail

Penetration Testing (6.2.b.v.H; App.D.4.1.3)

- The Plan Processor must include penetration testing and an application security code audit by a reputable (and named) third party prior to launch as well as periodically as defined in the SLA(s)
- The penetration test reviews of the Central Repository's network, firewalls, and development, testing and production systems should help the CAT evaluate the system's security and resiliency in the face of attempted and successful systems intrusions
- Penetration test reviews shall occur at least every year or earlier, or at the request of the Operating Committee

Breach detection and management policies (App.D.4.1.5)

- Policies should include monitoring and escalation practices, and incident response plan
- The incidence response plan may include items such as: Guidance on crisis communications, Security and forensic procedures, Customer notifications, "Playbook" or quick reference guides that allow responders quick access to key information.

High Level CAT Security Requirements

Data Usage and Regulator Controls

User Roles and Data Access (App.D.4.1.4, 4.1.6, 8.1.3, 8.2.1, 8.2.2)

- Periodic reports detailing the current list of authorized users and the date of their most recent access must be provided to SROs, the SEC and the Operating Committee. The required frequency of this report will be defined by the Operating Committee
- Authorized regulators from SROs and the SEC may access all CAT Data, with the exception of PII data. A subset of the authorized regulators from the Participants and the SEC will have permission to access and view PII data
- The Plan Processor must work with SROs and SEC to implement an administrative and authorization process to provide regulator access. The Plan Processor must have procedures and a process to verify the list of active users on a regular basis
- The user-defined direct query tool must provide an automated delivery method of scheduled query results to the appropriate Participant. Delivery methods must comply with all information security guidelines (encryption, etc.)
- Bulk extraction of data must be consistently in line with all permissioning rights granted by the Plan Processor. Extracted data returned must be encrypted, password protected and sent via secure methods of transmission

Separate PII request & Retrieval process (App.D.4.1.2, 4.1.4, 4.1.6)

- Multi-Factor Authentication (MFA) capability for all logins (including non-PII) is required to be implemented by the Plan Processor
- All PII access must be logged and audited
- Unencrypted storage of PII is prohibited
- CRO must at least annually review and certify all persons with PII access

Data Usage Policies and Procedures (6.1.m; 6.5.f.i.A, f.i.B, f.ii, g)

- SROs must have written policies and procedures reasonably designed to ensure the confidentiality of the CAT Data obtained from the Central Repository and limit the use of CAT Data obtained from the Central Repository solely for surveillance and regulatory purposes
- Effectiveness of related policies and procedures must be reviewed and remediated periodically as needed
- The Plan Processor shall develop and implement a training program that addresses the security and confidentiality of all information accessible from the CAT, as well as the operational risks associated with accessing the Central Repository. The training program will be made available to all individuals who have access to the Central Repository on behalf of the Participants or the SEC, prior to such individuals being granted access to the Central Repository
- All individuals who have access to the Central Repository (including the respective employees and consultants of the Participants and the Plan Processor, but excluding employees and Commissioners of the SEC) must execute a personal "Safeguard of Information Affidavit"
- SROs must implement information barriers for regulatory and non-regulatory staff with regard to access and use of CAT, permit only designated persons to have access to the CAT Data stored in the Central Repository, and impose penalties for staff non-compliance with any of its or the Plan Processor's policies or procedures with respect to information security

Incident Response (6.5.f.iii)

- SROs and SEC shall alert the CAT chief compliance officer as promptly as reasonably practicable, and within 24 hours, in the case of noncompliance with the policies and procedures adopted by an SRO or the SEC or a breach of the security of the CAT