This document presents **three alternative AWS account structures** to replace the **forced 3-account consolidation model**. The proposed solutions address key concerns, including **security, compliance, performance optimization, AWS quota management, cost transparency, and scalability**. These proposals ensure better **workload isolation** and **operational efficiency**, while avoiding the pitfalls of the forced consolidation approach.

**2. Issues with the Forced 3-Account Consolidation**

The forced 3-account consolidation model introduces significant risks and inefficiencies, as outlined below:

| **Key Concern** | **Forced Proposal (Issues)** | **Optimized AWS Model (Benefits)** |
| --- | --- | --- |
| **Security & Compliance** | Mixed SOC & non-SOC workloads increase audit risks. | Dedicated AWS accounts reduce attack surface & simplify SOC compliance. |
| **Performance & Scalability** | Resource contention in TradeCube affects execution speed. | Pre-booking and post-booking workloads are isolated, ensuring low-latency execution. |
| **AWS Quotas & Limits** | EC2, Lambda, and API Gateway limits can throttle services. | More AWS accounts avoid quota bottlenecks, ensuring smooth operations. |
| **Cost Transparency** | Business units cannot track costs separately in a single account. | Each AWS account aligns with business functions, enabling accurate chargebacks. |
| **Risk Mitigation** | Outages in one AWS account affect all workloads. | Disaster Recovery AWS accounts ensure business continuity. |
| **Big Data & AI Scalability** | AI/ML models and trade execution share compute resources, reducing efficiency. | Separate AWS account for AI/ML risk analytics, ensuring independent scaling. |
| **Single Point of Failure (SPOF)** | If Nessie fails, all other applications relying on it also fail. | More AWS accounts ensure independent failover mechanisms, reducing overall impact. |

**Why the Forced Proposal Increases Complexity Instead of Reducing It**

The **forced 3-account consolidation** is expected to **increase complexity and cost**, rather than reduce it:

* **Deployment Risks**: Centralizing workloads in a few accounts **creates bottlenecks** and **resource contention** during deployment.
* **Higher Maintenance Overhead**: Managing shared infrastructure across multiple teams **increases dependencies and operational complexity**.
* **More Cost Due to Scaling Issues**: Instead of reducing costs, **scaling within a single account means higher service quota requests**, leading to **potential throttling and operational inefficiencies**.
* **Security Risks**: Mixing **SOC and non-SOC workloads** in the same account **expands the attack surface** and complicates regulatory audits.

**3. Proposal 1: Compliance & Workload Isolation Model**

This approach ensures **regulatory workloads remain separate**, and **pre-booking/post-booking workloads do not interfere**.

**✅ AWS Account Structure**

| **AWS Account Name** | **Applications (Seals Assigned)** | **Why This Works?** |
| --- | --- | --- |
| **1. Pre-Booking & Trade Execution (CPOF)** | F&O Clearvision, CDT COMPASS, CDT Allocation Tool Suite, TradeSphere (Trade Processing), Trinity Cleared Derivatives UX, OTC Cleared Derivatives Affirmation Services, GMI Booking Adaptor | Keeps trade execution isolated, ensuring low-latency performance. |
| **2. Post-Booking & Risk Management (Non-CPOF)** | F&O GeMM, CDT JEDI, Instruction Generation Service, Data Aggregation & Distribution Service | Ensures post-booking services do not impact execution performance. |
| **3. Regulatory & Compliance (Encore Account)** | CDT Engineering Controls & Regulatory Reporting, Regulatory Reporting Workbench, CDT Exchange Balancing, Union II | Compliance-focused AWS account, ensuring full SOC isolation. |
| **4. External & Client-Facing Services** | CDT Client Experience (Public-Facing) | Only SOC-external workload, reducing attack surface. |
| **5. Treasury & Financial Operations** | Osprey, Javelin, Condor (OTC Clearing), BOLT (Brokerage Ops), CaCTuS | Keeps financial operations & billing independent for better cost tracking. |
| **6. Core Ledger & Books (Highly Regulated, Separate SEAL)** | GMI (Core Books & Records SEAL) | Sensitive ledger data remains secure. |
| **7. Data Analytics & Nessie (Replaces Data Warehouse & RDC)** | Nessie (CDT Data Warehouse + Reference Data Cache), Clearing Data Analytics & MIS | Centralized data analytics & reporting for efficiency. |

**4. Proposal 2: Business-Aligned Multi-Account Model**

This model **groups applications by business operations**, making account ownership clearer and reducing cross-team dependencies.

**✅ AWS Account Structure**

| **AWS Account Name** | **Applications (Seals Assigned)** | **Business Domain** |
| --- | --- | --- |
| **1. Trade Processing & Execution** | F&O Clearvision, TradeSphere, CDT Allocation Tool Suite, Trinity Cleared Derivatives UX, OTC Cleared Derivatives Affirmation Services | Market & Trading |
| **2. Post-Trade & Risk Management** | F&O GeMM, CDT JEDI, Instruction Generation Service, Data Aggregation & Distribution Service | Risk & Analytics |
| **3. Regulatory & Compliance (Encore)** | Regulatory Reporting Workbench, CDT Engineering Controls & Regulatory Reporting, CDT Exchange Balancing, Union II | Regulatory Reporting |
| **4. Client Experience & External** | CDT Client Experience (Public-Facing Only) | Customer Engagement |
| **5. Treasury, Billing & Clearing Operations** | Osprey, Javelin, Condor, CaCTuS | Finance & Billing |
| **6. Books & Records (Highly Regulated SEAL)** | GMI (Core Books & Records SEAL) | Ledger & Audit |
| **7. Data Analytics (Nessie & RDC)** | Nessie (CDT Data Warehouse + Reference Data Cache), Clearing Data Analytics & MIS | Centralized Analytics |

**5. Proposal 3: High-Performance Scalability Model**

This model **ensures AWS quotas are not exceeded** while **maximizing performance**.

**✅ AWS Account Structure**

| **AWS Account Name** | **Applications (Seals Assigned)** | **Performance Considerations** |
| --- | --- | --- |
| **1. High-Performance Trade Processing** | F&O Clearvision, TradeSphere (Trade Processing), CDT Allocation Tool Suite, OTC Cleared Derivatives Affirmation Services | Dedicated for low-latency, high-throughput trading workloads. |
| **2. Analytical & Post-Trade Data Management** | F&O GeMM, CDT JEDI, Instruction Generation Service, Data Aggregation & Distribution Service | Ensures post-trade data processing scales independently. |
| **3. Regulatory Compliance & Audit** | Regulatory Reporting Workbench, CDT Engineering Controls & Regulatory Reporting, CDT Exchange Balancing, Union II | Strictly compliance workloads to avoid regulatory issues. |
| **4. Public-Facing Client Services** | CDT Client Experience (Public-Facing Only) | SOC-external workload kept separate for security. |
| **5. Treasury & Financial Operations** | Osprey, Javelin, Condor, CaCTuS | Financial operations have dedicated AWS resources. |
| **6. Highly Secure Books & Records** | GMI (Core Books & Records SEAL) | Financial ledgers are isolated to prevent data breaches. |
| **7. Nessie (Replaces Data Warehouse & RDC)** | Nessie (CDT Data Warehouse + Reference Data Cache), Clearing Data Analytics & MIS | Data analytics scalability is ensured. |

**6. Conclusion: Why More AWS Accounts are Beneficial**

✅ **Security & Compliance:** More AWS accounts allow SOC workloads to remain completely isolated, reducing security risks.  
✅ **Performance Optimization:** Dedicated accounts prevent resource contention and AWS service quota issues.  
✅ **Cost Allocation & Operational Efficiency:** Business units can track costs separately.  
✅ **Scalability:** Scalable workloads (AI/ML, Data Analytics, Trade Processing) can operate without affecting other services.  
✅ **Avoiding Single Point of Failure (SPOF):** If Nessie fails, workloads in other AWS accounts remain operational.

**Recommendation**

More AWS accounts should be created based on **workload type, business function, and regulatory needs** to ensure **long-term operational stability and security**.