
CAT Security Overview

Safeguarding Data Reported to CAT

Presenters

Soniya Shrivastav
Leader, CAT Leadership Team
Director of Regulatory Initiatives, Legal, NYSE

David Yacono
Chief Information Security Officer
CAT NMS LLC & FINRA CAT LLC

Scott Donaldson
Chief Technology Officer
FINRA CAT LLC

Agenda

1. CAT Overview
2. Security Program Organization
3. Security Framework
4. Secure Architecture
5. Security Controls

CAT Overview

Introduction to CAT

CAT NMS Plan

The Securities and Exchange Commission (SEC) approved Rule 613 under the Securities Exchange Act of 1934, which requires national securities exchanges and national securities associations (collectively, **the Participants**) to submit a national market system plan to create, implement, and maintain a consolidated audit trail ([CAT NMS Plan](#)) that would capture customer and order event information for orders in NMS Securities and OTC Equity Securities (Eligible Securities), across all markets, from the time of order inception through routing, cancellation, modification, execution, and allocation.

The logo for Cboe, featuring a stylized 'C' with a green diamond shape inside the top curve, followed by the word 'boe' in a dark blue sans-serif font.The logo for NYSE, consisting of five vertical blue bars of varying heights, with the letters 'NYSE' in a bold, black, sans-serif font below them.The logo for MIAX, featuring a colorful, swirling circular graphic on the left and the letters 'MIAX' in a bold, blue, sans-serif font on the right, with a trademark symbol.The logo for LTSE, consisting of the letters 'LT' stacked above 'SE' in a white, bold, sans-serif font, set against a dark blue square background.The logo for iex, featuring the lowercase letters 'iex' in a bold, black, sans-serif font, with a small orange square icon to the right.The logo for Nasdaq, featuring a stylized blue 'N' followed by the word 'Nasdaq' in a bold, black, sans-serif font.The logo for BOX OPTIONS, featuring a colorful, stylized cube-like graphic on the left and the letters 'BOX' in a bold, blue, sans-serif font above the word 'OPTIONS' in a smaller, blue, sans-serif font.The logo for FINRA, featuring the word 'FINRA' in a bold, blue, sans-serif font, with a stylized blue graphic to the right, and the text 'Financial Industry Regulatory Authority' in a smaller, black, sans-serif font below it.

CAT Overview

CAT Organizations, Roles & Governance

CATNMS LLC

- Consortium of National Securities Exchanges and National Securities Associations (SROs)

Operating Committee (OpCo)

- Serves as the governing body for CAT and provides review, guidance, and oversight for the overall operations of the CAT
- Industry Advisory Committee provides OpCo with industry perspective and guidance

Leadership Team (LT)

- OpCo designated Participant staff to manage delivery and operations of the CAT

Plan Processor

- Selected by the OpCo to implement and operate the CAT
- FINRA CAT is the Plan Processor. FINRA (parent) provides supporting services pursuant to a shared services agreement.

CISO and CCO

- Fiduciaries of the CAT NMS LLC, to ensure compliance with all Plan requirements, including security.
- Continuously monitor releases and operations
- Recommend and implement improvements

Security Working Group (SWG)

- Working group comprised of CAT CISO as well as CISOs and security experts from each Participant.

SEC

- Oversight of Participants; FINRA CAT is also an SCI entity.

CAT Overview

CAT Data

▶ Definition of CAT Data

- Data derived from Participant Data, Industry Member Data, SIP Data, and such other data as the OpCo may designate:
 - Transaction Data
 - Customer Account Information
 - Customer Identifying Information

▶ Efforts to minimize sensitive data collected

- SEC approved exemptive relief on 3/17 to eliminate collection of key sensitive data
 - SSNs, DOBs, and Account Numbers of individual investors no longer required.
- “I believe this represents an important step in significantly reducing the risk of retail investor identity theft associated with the CAT.”¹ [Chairman Clayton]

¹Chairman Clayton Public Statement, 3/17/2020 (https://www.sec.gov/news/public-statement/statement-clayton-cat-covid-19-nal-cybersecurity-2020-03-17#_ftn1)

CAT Overview

CAT Users

CAT Reporters

- Plan Participants
 - Transmit transaction data, review and repair errors
- Industry Members
 - Transmit transaction, customer and account data; review and repair errors
- Authorized Reporting Agents may report on behalf of an Industry Member CAT Reporter

Regulatory Users

- Includes query tool access for SRO and SEC Regulatory Users
- Separate access and entitlements required for Regulatory Users from the CAT Reporters
- CAT data may only be used for Regulatory Purposes

CAT Overview

Plan Security Requirements

Architectural Level Controls

1. Secure connectivity to CAT
2. Role Based Access Controls (RBAC)
3. CAT Data not accessible via public internet and deployed within the network infrastructure
4. Segregation of CAT compute and network infrastructure from other cloud tenants
5. Customer data segregated from transaction data
6. All data encrypted in flight and at rest including archival data storage
7. Separate Customer query system

Program-Level Controls

1. CISO and CCO Responsibilities
2. CAT Data Access and Confidentiality
3. Datacenter Standards
4. Industry Standards
5. Key Management
6. Penetration Testing (Independent third-party)
7. Breach detection and management policies
8. Review of Participant Security Policies
9. Regular InfoSec Program Review

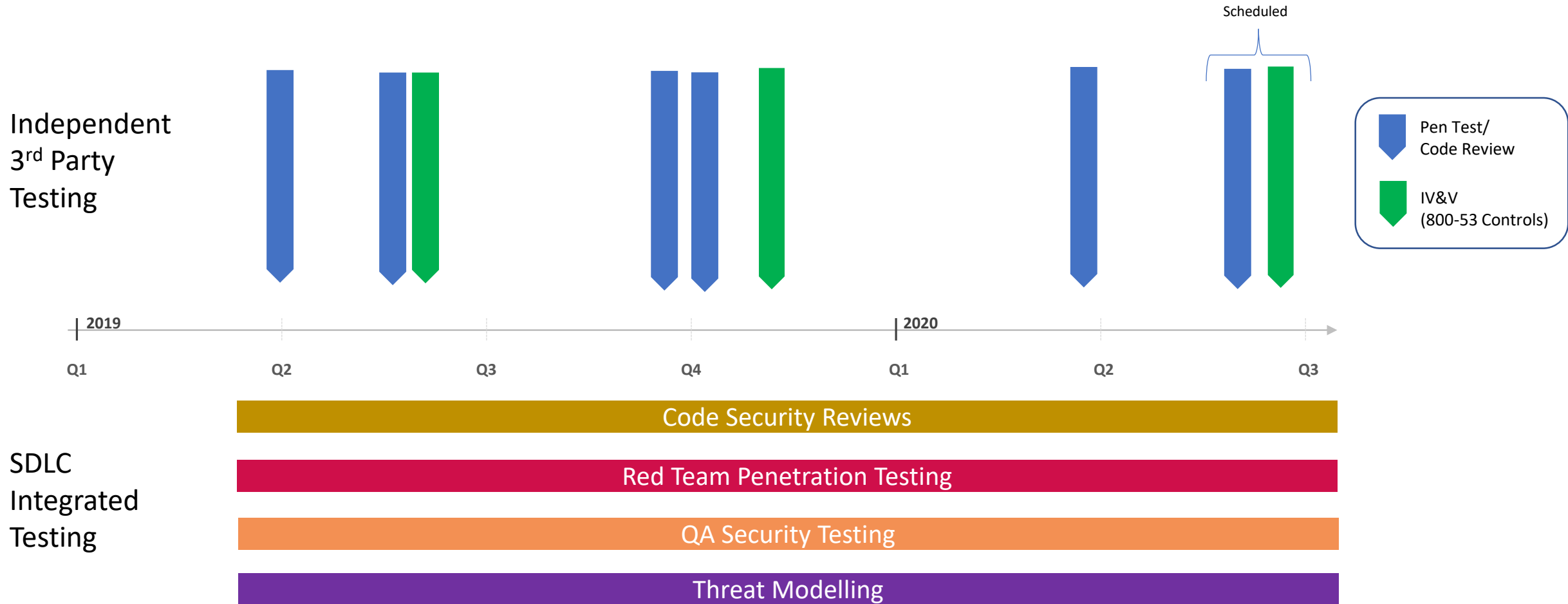
Security Program Organization

Strong Security Team / Independent Validation

- ▶ Plan Processor security capabilities:
 - Dedicated CAT CISO and Security Analysts
 - CAT CISO (and CCO) has fiduciary obligation to Participants (CAT NMS LLC)
 - Secure Systems Architecture
 - Software Security Engineering
 - Threat Hunting, Detection, Response
 - Identity and Access Management
 - Security Policy, Governance & Operational Oversight
 - Security Monitoring, Analysis, & Reporting
- ▶ Experience & Certifications
 - CISSPs, CSSLPs, CTPRPs, ISSAPs, IACRB Pen Testers, Certified Ethical Hackers, A+/Net+/Sec+, and more
- ▶ AWS brings additional breadth/depth
 - Built on industry leading secure cloud platform.
 - Senior Solutions Architect specializing in security committed via Premium Support agreement.
- ▶ Mature and effective policies, tools and processes
- ▶ 3rd Party Tested and Evaluated
 - CAT undergoes annual NIST SP800-53 IV&V
 - Third-party pen test and code review
 - FINRA Parent SOC 2 audits, info sec program assessments. Assessed as outperforming peer organizations and employing industry leading practices.
- ▶ Relationships & memberships provide early access to threat info & analysis

Security Program Organization

Frequent, Ongoing 3rd Party and Internal Security Evaluation



Security Program Organization

Standards, Policies, Oversight

▶ Robust Controls Framework

- NIST SP800-53, in accordance with Plan.
 - Further informed by ISO 27002, NIST Cybersecurity Framework.
 - System Security Plan established.
 - Third-party Independent Verification and Validation; annually as well as with major changes.
- Continuous Monitoring
 - In accordance with NIST SP800-137
- CAT is an SCI System of the Participants. Plan Processor is an SCI entity and operates in compliance with Reg SCI.

▶ OpCo / Security Working Group (SWG)

- SWG established by OpCo. SWG makes recommendations to Operating Committee.
- Comprised of FINRA CAT CISO as well as CISOs and security experts from each Participant. SEC also an observer to the SWG.
 - Substantial breadth/depth of Infosec expertise; hundreds of years combined experience

▶ Security Policies

- Full suite of cybersecurity policies, including:
 - Data Security
 - Insider Risk
 - Incident Management
 - Logging and Monitoring
 - Application Security

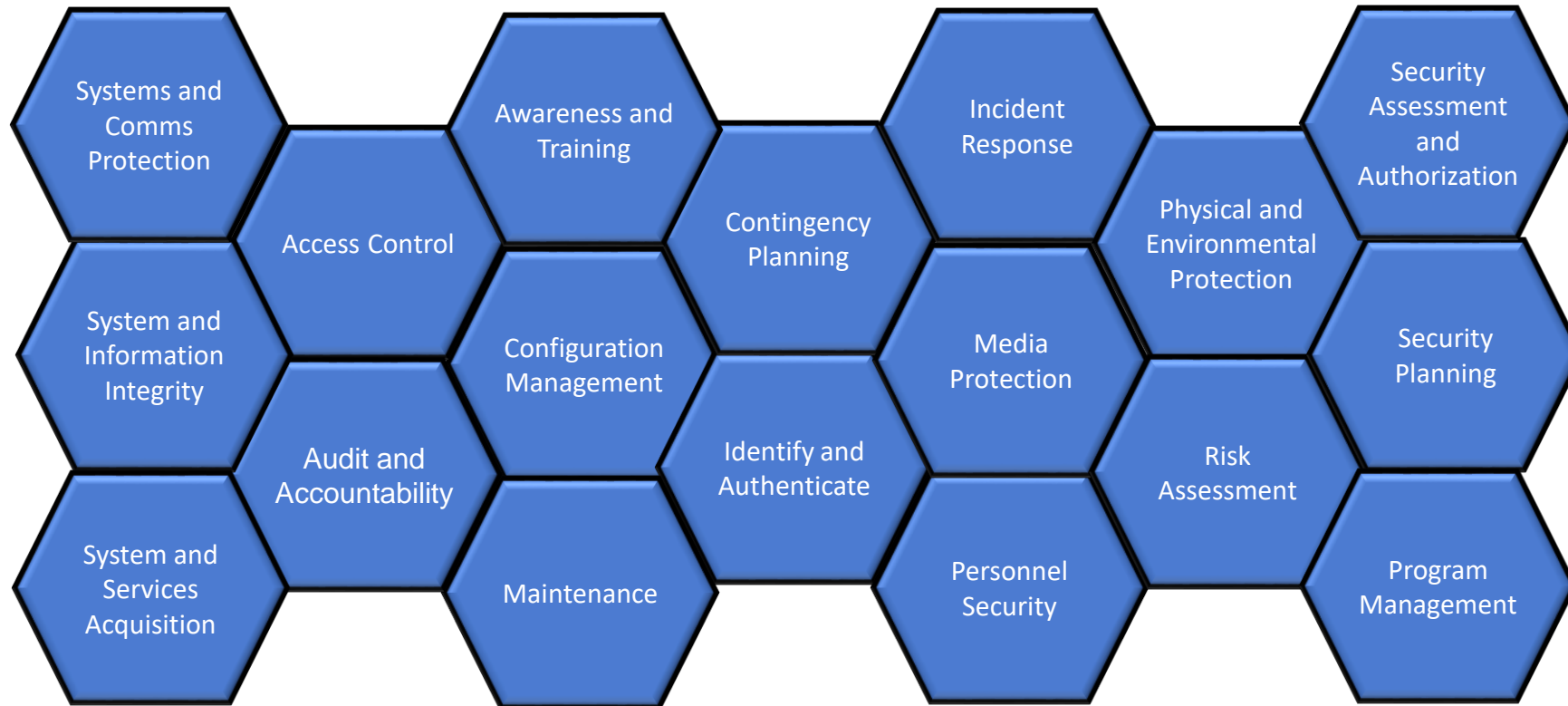
Security Program Organization

AWS is Secure, Well-governed Foundation

- ▶ AWS complies with broad array of industry and international security standards; maintains relevant independent certifications
 - PCI DSS Level 1 (Payment Card Industry Data Security Standard)
 - ISO 27001 (International Standard for Information Security Management)
 - DIACAP (DoD Information Assurance Certification and Accreditation Process)
 - FISMA (Federal Information Security Management Act) / NIST SP800-53
 - FedRAMP (Federal Risk and Authorization Management Program)
 - ITAR (International Traffic in Arms Regulation)
 - FIPS 140-2 (Federal Information Processing Standards for Cryptographic Modules)
 - SEC Rule 17a-4(f)
 - CSA (Cloud Security Alliance)
 - MPAA (Motion Picture Association of America Security Best Practices)
 - HIPAA (Health Insurance Portability and Accountability Act)
 - AICPA SOC1, Type II report (SSAE 16/ISAE 3402; formerly known as SAS70)
 - AICPA SOC2, Type II report (Security Trust Principles)
 - AICPA SOC3 (SysTrust Certification)

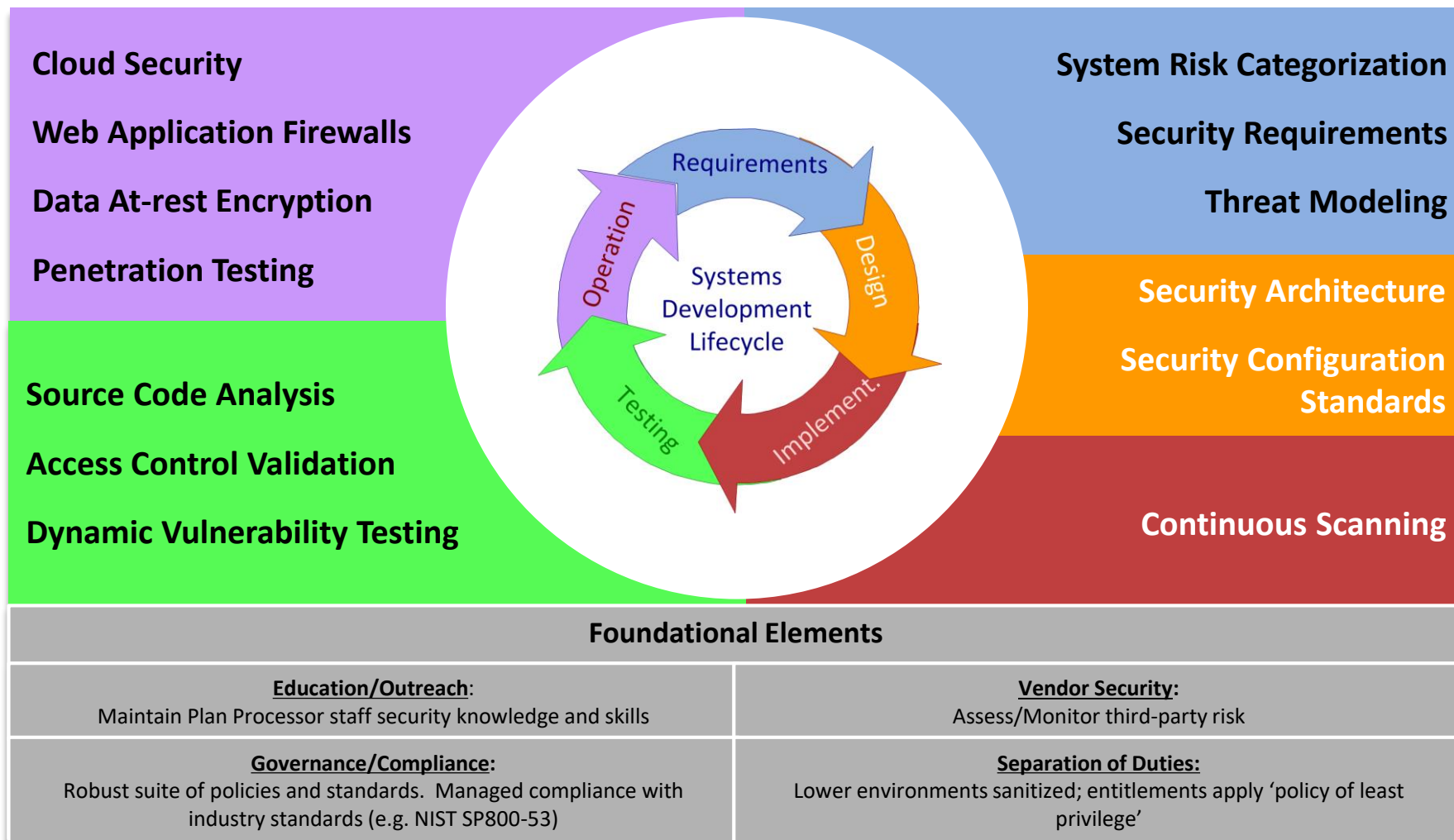
Security Program Framework

NIST SP800-53



Security Program Framework

Security-integrated Development Lifecycle



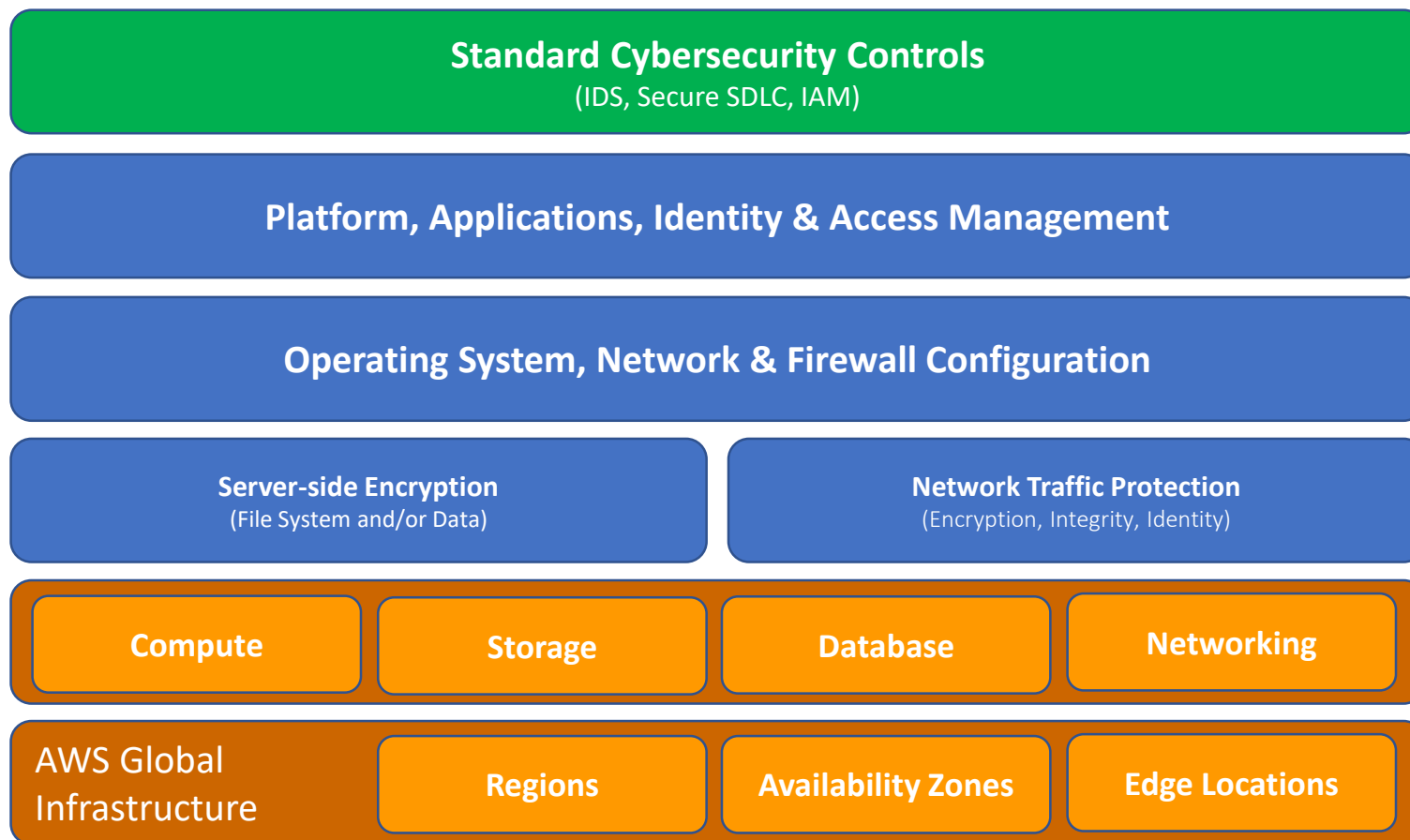
Security Program Framework

Cloud-Powered Security

Security **“ABOVE”** the cloud
Secure software design, assurance
Access Management
Monitoring, threat management

Security **“IN”** the cloud
Hardened configs, monitoring
Microsegmentation
Operational Separation of Duties,
Monitoring

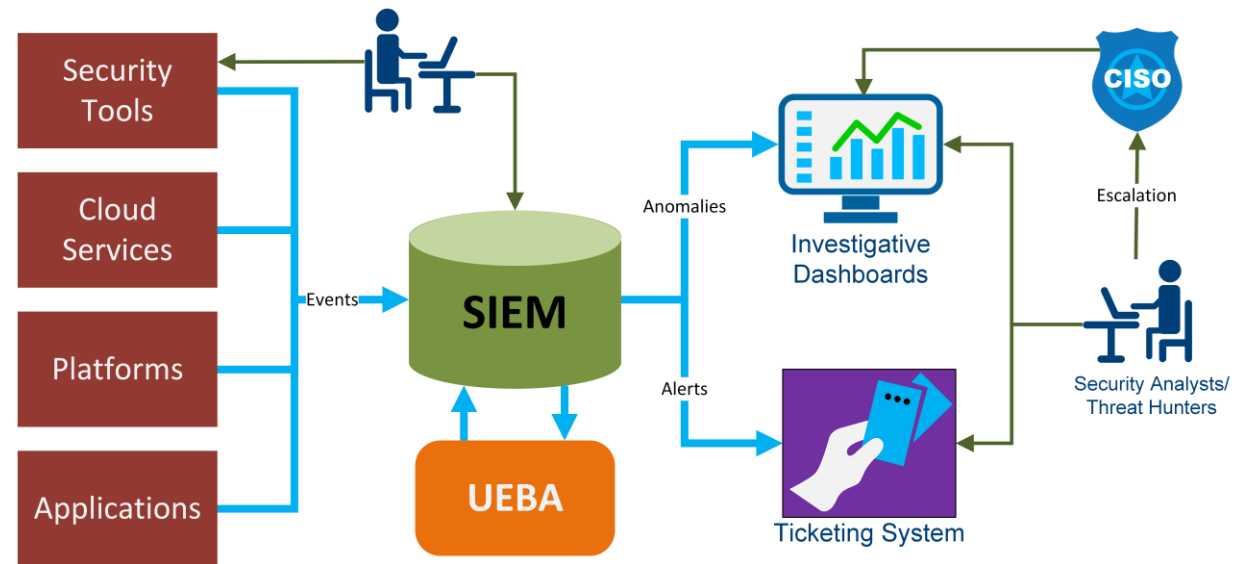
Security **“OF”** the cloud
AWS native controls.
FINRA CAT validates and monitors
through its mature third-party risk
management program.



Security Program Framework

Threat Detection, Monitoring, & Alerting

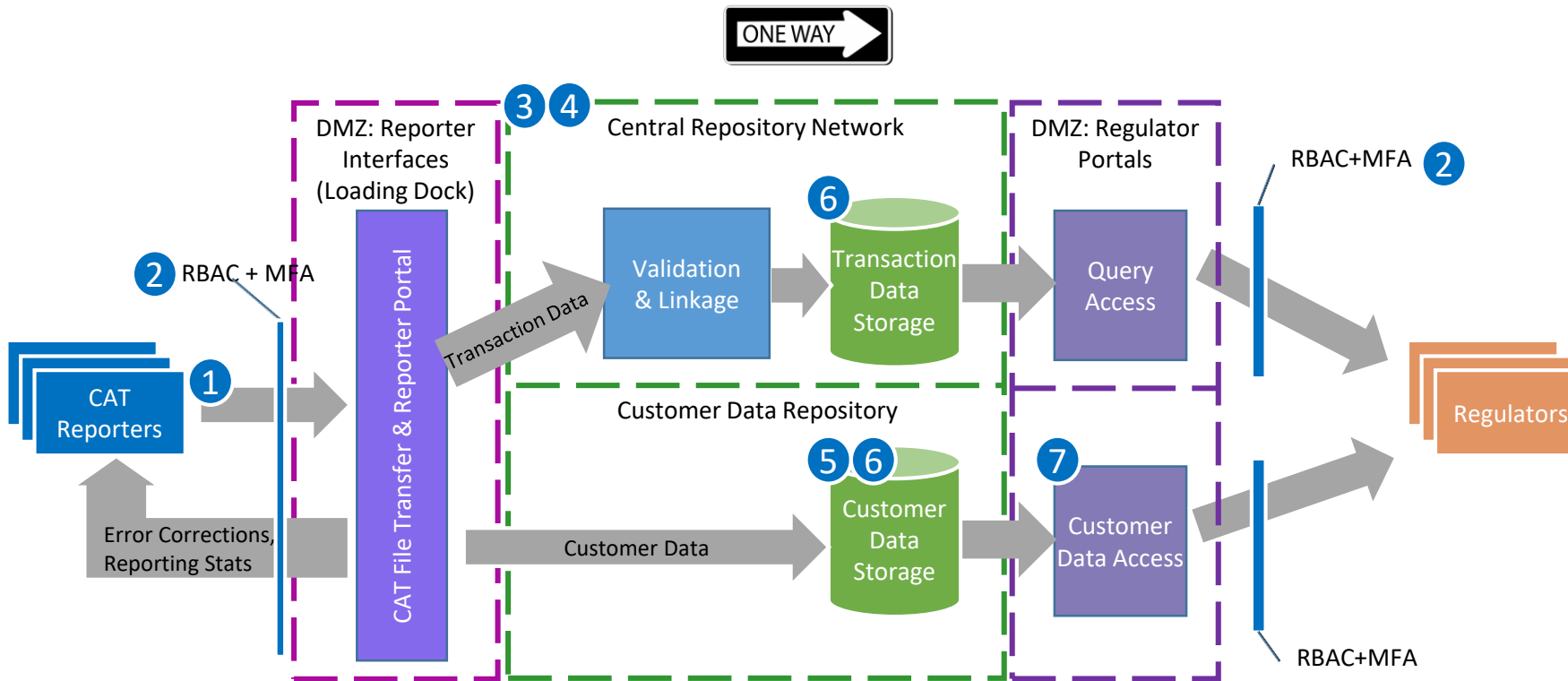
- ▶ Multiple automated Threat Intelligence Feeds
- ▶ Extensive logging (breadth and depth)
 - Security Tools
 - Cloud services
 - Platforms
 - Applications
- ▶ Security Information and Event Management (SIEM)
 - Collection, analysis, and reporting
 - Behavioral Analytics (UEBA)
 - Continuous Monitoring (NIST SP800-137)
 - Dashboard, Alerting
 - Ticketing, triage, resolution.



Rapid and effective ability to detect and respond to malicious activity.

Secure Architecture

Architectural Features Enhance Security



Key

→ Encrypted Connection



Encrypted Storage

--- Isolated Network

--- DMZ Network

Network Isolation

- Industry Members: Private Lines, AWS PrivateLink, Secure Reporting Gateway
- Participants: Private Line
- Reporters separated from Regulators
- Reporter Interfaces cannot access the Central Repository
- Separate network segments DMZs, Central Repository, & Customer Data

Encryption – All Data

- In Transit
- At Rest

Authentication & Entitlement

- Multi-factor Authentication (MFA)
- Granular Role Based Access Control (RBAC)

Extensive, Granular Logging

- Security Information & Event Management (SIEM)
- User and Entity Behavior Analytics (UEBA)

Test Environment

- Full replication of architecture; incl. security.

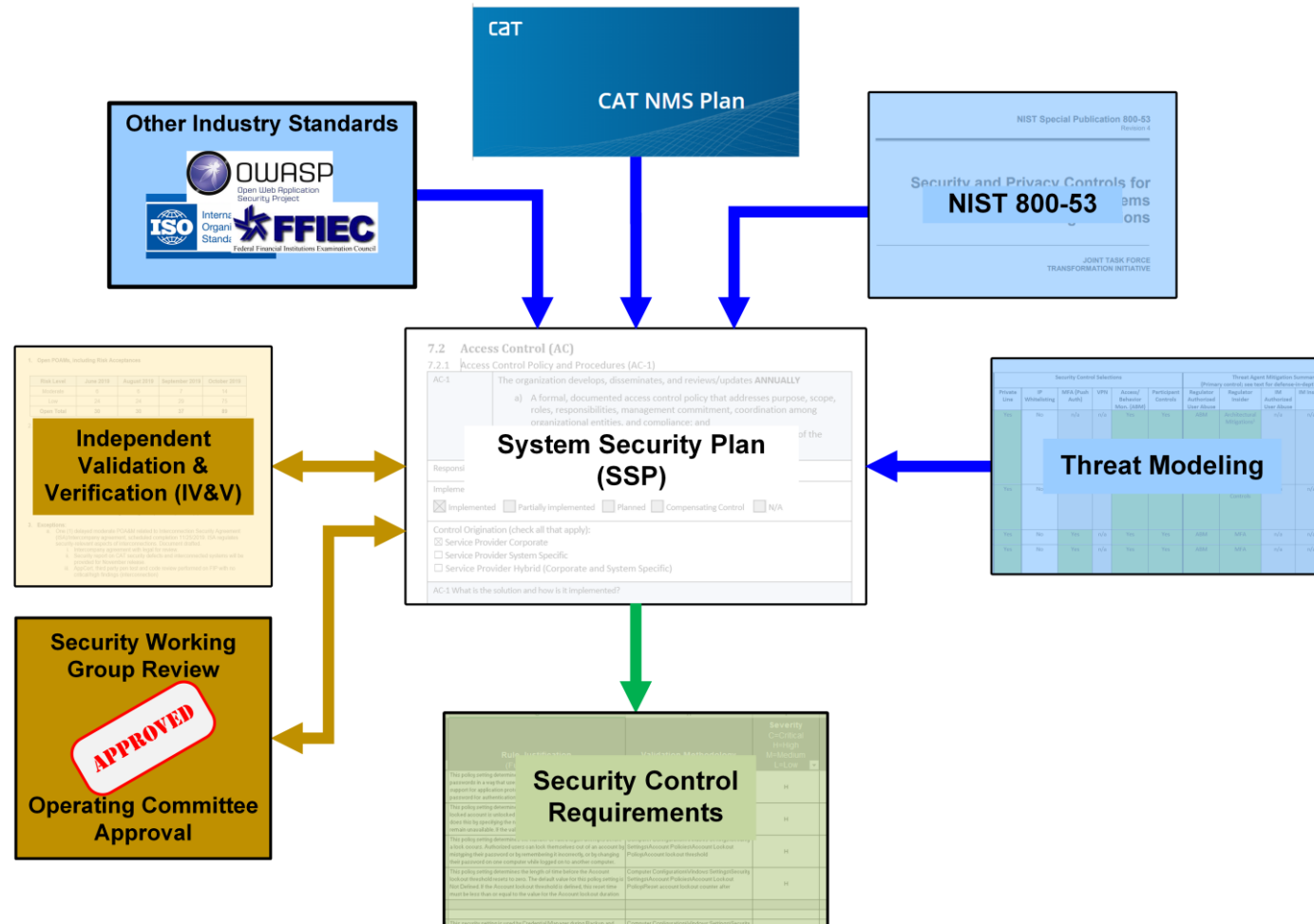
Secure Architecture

Separation of Customer and Transaction Data

- ▶ **Separate AWS Accounts**
- ▶ **Separate Development and Operations Teams**
- ▶ **Separate User Interfaces**
- ▶ **Separate Entitlements**
- ▶ **Customer/Account Data Separately Encrypted from Transaction Data (also encrypted)**

Security Control Highlights

Control Selection and Decision Making



Security Control Highlights

Staffing and Vendor Security

- ▶ Plan Processor Staffing and Operations: **US Only**
 - AWS regions used to store/process CAT Data
 - Only US-based development and operations staff
- ▶ Vendors
 - Third-party Risk Assessment prior to onboarding.
 - Ongoing monitoring
 - Critical vendors subject to intensive oversight

Security Control Highlights

Connectivity

- ▶ Two categories of secure connectivity offered:

	Private Line	CAT Secure Reporter Gateway
Industry Member Reporting	IM machine-interface reporting	Interactive (human) access to Industry Member Reporter Portal for small-scale reporting/corrections; status.
Plan Participant Reporting	All Reporting	N/A
Regulator Use	All Access	N/A

- ▶ What is the CAT Secure Reporter Gateway (SRG)?
 - Only for **small scale**, manual reporting/corrections; status.
 - Industry Member uses existing Internet connectivity.
 - User authenticates (MFA) to SRG; only authenticated traffic routed to Reporter Portal
 - Communication occurs over VPN to SRG.

Security Control Highlights

Authentication

▶ Multi-factor Authentication (MFA) required

- All Regulator and Industry Member Logins
 - Regulator/Query Tools
 - Reporter Portals
 - Industry Member Secure Reporting Gateway

▶ Two factors:

- Something you know: Username/Password
- Something you have: Registered mobile device / hard token

▶ Secure, state-of-the-art MFA approach

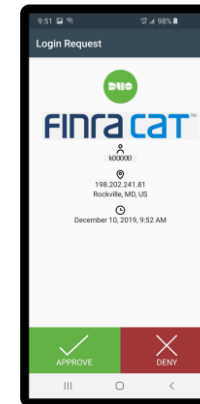
- Push authentication; Time-based One Time Passcodes
- No deprecated technologies used (e.g. SMS codes)

▶ Protects against

- Unauthorized access by Regulator insiders
- Any interaction with the Reporter Portal, other than by authorized individuals.



**Something
You Know**



**Something
You Have**

Security Control Highlights

Data Protection

At Rest



Pervasive Use of Encryption

Security Control Highlights

Targeted Monitoring

- ▶ CAT-specialized Security Monitoring
 - Explicit Plan requirements
 - Threat-determined requirements
- ▶ Enabled by Threat, Detection, Monitoring, and Alerting Framework
 - Extensive Component-level Logging
 - Security Tooling
 - Behavioral Analytics
- ▶ Plan Requirements: Access and Monitoring
 - Every instance of access to the Central Repository is logged (query and reporting)
 - Full audit trail of data access is maintained

Regulator Security

Security of Accessed Data

▶ Participant InfoSec Policies Comparable to CAT

- CAT CISO Review of Participant Infosec Policies (per Plan)
- Based on 800-53
 - Completed for active Participants; new Participants reviewed during onboarding.
 - Annual review
- Participants subject to SEC oversight

▶ CAT Security Awareness Training

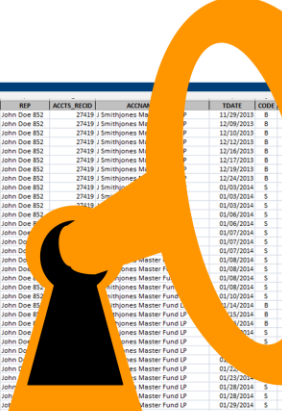
- Each individual regulatory user takes prior to getting access; annual retake to retain access.
- Topics include:
 - Data can be used only for regulatory purposes
 - Protecting CAT Data from unauthorized access/use
 - Secure handling of CAT Data
 - Recognizing and reporting security issues

▶ Safeguard of Information Affidavit

- Each individual SRO regulatory user with access to Central Repository must sign an affidavit
 - *“I acknowledge if I breach my obligations under this Affidavit, I am subject to liability as provided by the CAT NMS Plan and my Authorizing Organization may take disciplinary action including termination of my employment or consultancy.”*

▶ Regular Access Reports to Participants, SEC

Closing



ACCT#	BRN#	PROPERTY	EXEMPT	Estm Name	Perm CD	REP	ACCT#	BRN#	ACCOUNT	DATE	LOAN	AMOUNT	INCOME			
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	11/29/2013	B	115	28078.5	1503.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/09/2013	B	175	14879.5	1503.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/10/2013	B	16	17126.5	733.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/12/2013	B	7	18521	128.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/16/2013	B	2	18928.5	2003.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/17/2013	B	7	10582.5	154.25		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/19/2013	B	84	10428.5	2003.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	12/24/2013	B	205	10803.5	603.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/03/2014	S	50	10328	24.25		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/02/2014	S	100	2018.05	404.05		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/03/2014	S	50	8470.29	79.25		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/06/2014	S	50	1615.17	29.25		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/06/2014	S	50	210.78	154.25		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/07/2014	S	100	3999.00	394.97		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/07/2014	S	50	885.75	154.25		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/07/2014	S	50	2625.74	24.26		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/08/2014	S	50	1461.72	154.26		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/08/2014	S	50	4805.72	24.26		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/08/2014	S	50	4333.7	79.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/08/2014	S	100	9006.93	51.07		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/10/2014	S	100	5704.96	305.04		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/14/2014	B	210	113341	118.5		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/16/2014	B	196	18931	179.275		
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/16/2014	B	01	147	758.67	4.84	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/16/2014	S	50	11.75	17905.67	134.88	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/16/2014	S	50	8100	1919.81	144.8805	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/16/2014	S	50	88187	43629.23	154.27	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/16/2014	S	50	8141	16003.90	122.5	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/22/2014	S	100	82963	16235.48	72.5	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/22/2014	S	100	8131	17556.85	63.5	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/28/2014	S	150	83953	126473.8	458.7	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/28/2014	S	57	82	8.3	47895.5	178.1
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	100	9774	1774.79	55.25	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	200	10.11	151742.1	1007.9	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	100	9304	14848.84	133.36	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	100	10.209	102047.7	43.38	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	200	10.054	194661	606.99	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	50	8.99	8979.63	154.37	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	100	93481	16575.83	305.17	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	75	10.424	7806.88	117.37	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	100	10.235	102302.7	43.29	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/29/2014	S	75	10.424	7806.88	117.37	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	01/31/2014	S	75	10.816	7382.22	229.78	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	02/07/2014	S	100	8.242	15719.97	155.03	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	02/18/2014	S	100	10.867	162394.2	606.34	
27419	106015	DAVID CRABTREE	Broker Dealer 832	8061 John Doe 832			27419		SmithJones Master Fund LP	02/28/2014	S	100	10.895	16939.6	609.37	

- This presentation will be recorded and available on catnmsplan.com
- E-mail questions to FINRA CAT helpdesk: help@finracat.com