MetricStream

GRC
SUMMIT 2017
November 6 - 7, 2017
LONDON

Compliance At the 1st Line of Defense

Subharun Mukherjee – Director, MetricStream

Presenter Details

Subharun Mukherjee
Director
MetricStream

What is Common?

MONEY LAUNDERING

ROGUE TRADING

SPECULATIVE POSITIONS

DATA BREACHES

CHURNING

LOAN FRAUD

PAINTING THE TAPE

MONEY LAUNDERING

CUSTOMER CONDUCT
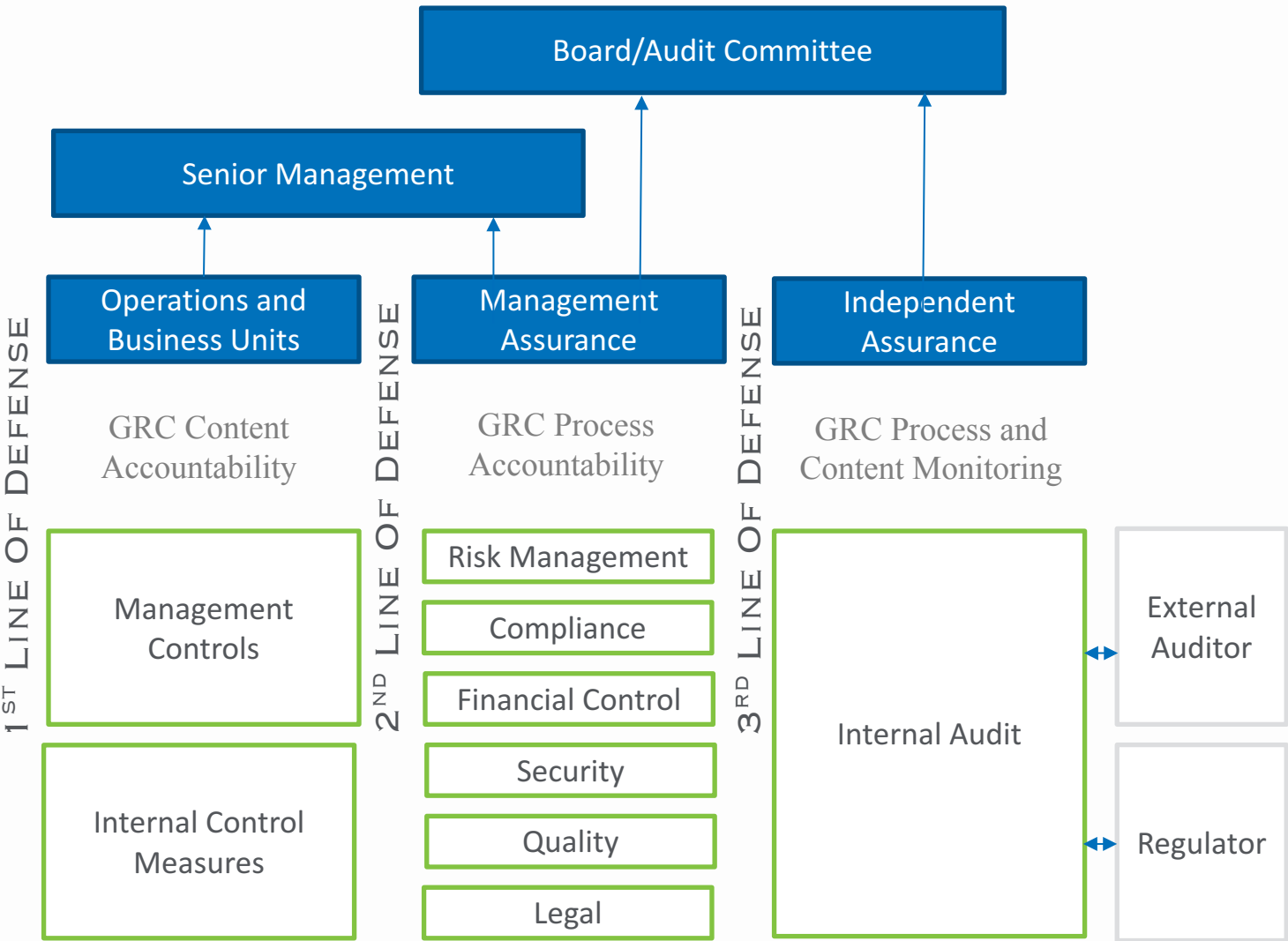
INSIDER TRADING

MIS-SELLING

CARD FRAUD

MARKET MANIPULATION

"Exactly!" said Deep Thought. "So once you do know what the question actually is, you'll know what the answer means."

— Douglas Adams, **The Hitchhiker's Guide to the Galaxy**

3 LoD Model and The 1ˢᵗ Line of Defense

MetricStream

Board/Audit Committee

Senior Management

1ˢᵗ LINE OF DEFENSE

Operations and Business Units

GRC Content Accountability

Management Controls

Internal Control Measures

2ᴺᴰ LINE OF DEFENSE

Management Assurance

GRC Process Accountability

Risk Management

Compliance

Financial Control

Security

Quality

Legal

3ᴿᴰ LINE OF DEFENSE

Independent Assurance

GRC Process and Content Monitoring

Internal Audit

External Auditor

Regulator

Who are the 1ˢᵗ LoD?

- Creates and Sells Products
- Direct contact with customers

Why is the 1ˢᵗ LoD critical?

- This is where the lapse are
- 2ⁿᵈ LoD is Retroactive (at most times)
- They understand the business

Regulatory Landscape - Key Issues For Organizations

1. Scope
Wide Ranging regulations Leads to Disruptive Budgetary Impact

2. Change
Dealing with continuously evolving regulatory requirements

3. Complex
Navigating the complexity of Regulatory Requirements

4. Time
On-time compliance with multiple regulatory timelines

5. Scale
Global impact of different regulations across org. hierarchy

6. Variance
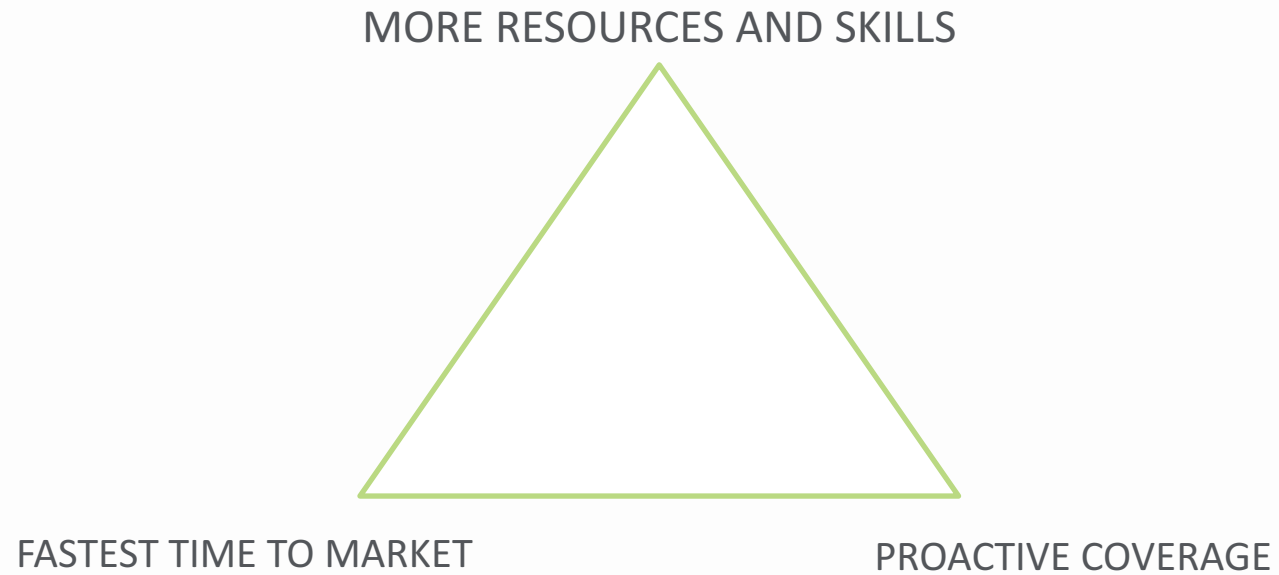Lack of global regulatory convergence resulting in multiple interpretations

6. Resource
Reducing budgets, paucity of manpower, lack of skills

7. Future
Reducing budgets, paucity of manpower, lack of skills

Why Involve the 1ˢᵗ LoD

MORE RESOURCES AND SKILLS

FASTEST TIME TO MARKET

PROACTIVE COVERAGE

What generally happens?

MALICIOUS | MISINFORMED

THEY KNOW THEY KNOW | THEY DON'T KNOW THEY DON'T KNOW

Different Approaches

MALICIOUS | MISINFORMED

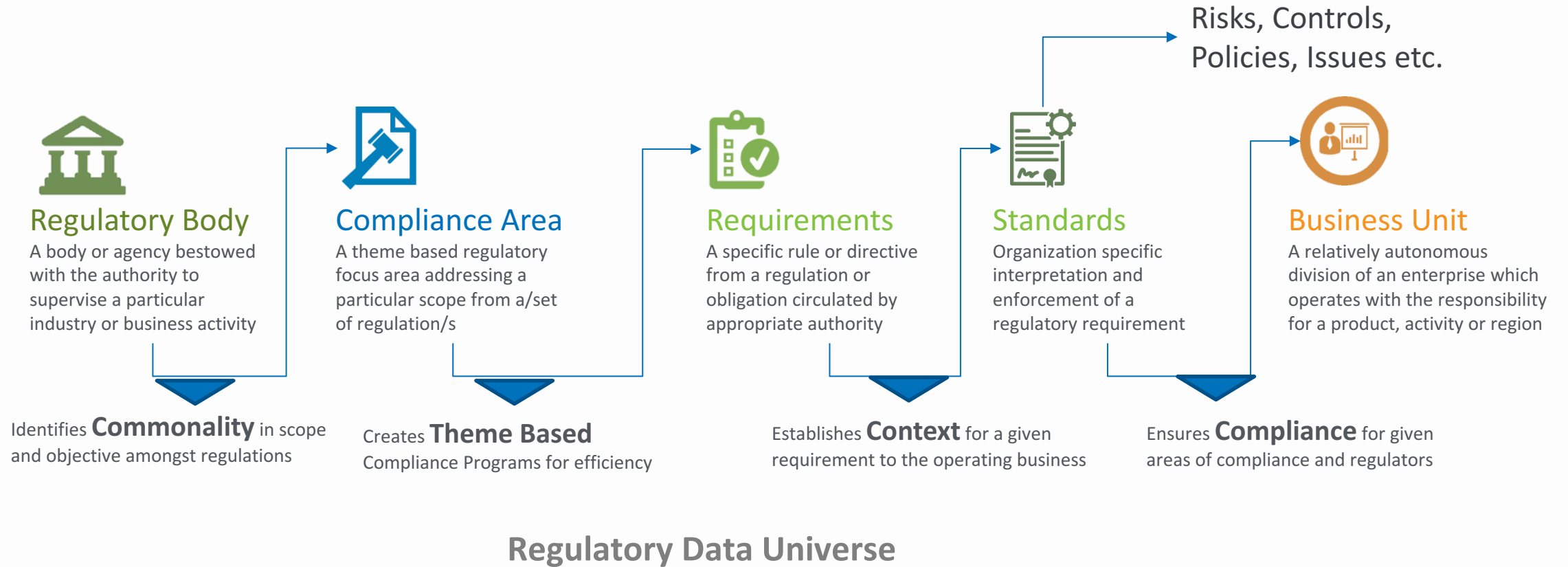BLOCK & TACKLE

Tackle Strategy

3E

ENABLE

- Remove Subjectivity
- Information Availability
- Technology As an Enabler

EMPOWER

- Governance Structure
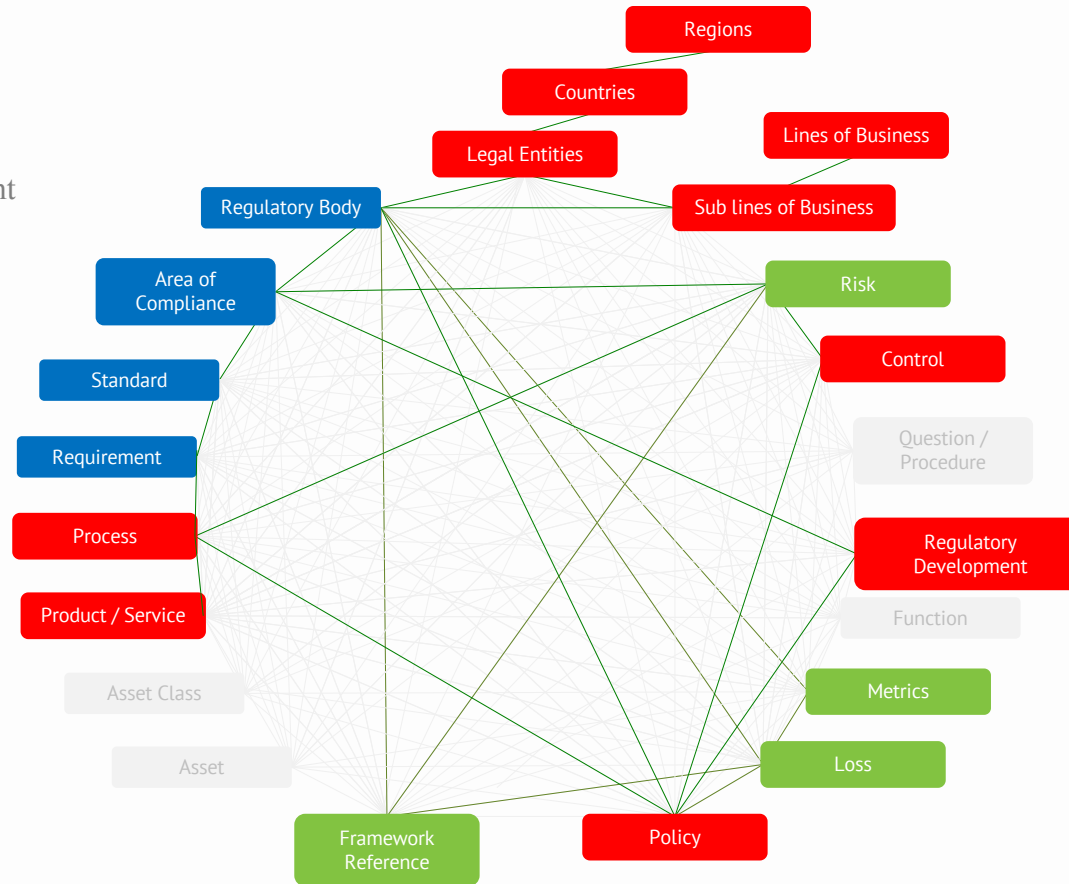- Alignment of Incentives
- Organizational Independence

ENGAGE

- Tone At The Top
- Align with Strategic Objectives
- Skill Development

Enable – Context is King

Risks, Controls, Policies, Issues etc.

Regulatory Body
A body or agency bestowed with the authority to supervise a particular industry or business activity

Compliance Area
A theme based regulatory focus area addressing a particular scope from a/set of regulation/s

Requirements
A specific rule or directive from a regulation or obligation circulated by appropriate authority

Standards
Organization specific interpretation and enforcement of a regulatory requirement

Business Unit
A relatively autonomous division of an enterprise which operates with the responsibility for a product, activity or region

Identifies **Commonality** in scope and objective amongst regulations

Creates **Theme Based** Compliance Programs for efficiency

Establishes **Context** for a given requirement to the operating business

Ensures **Compliance** for given areas of compliance and regulators

Regulatory Data Universe

Enable – Context is King

Example of relationships across the compliance and risk universe driving latent synergies across functional units

Common Data Libraries across Compliance and Risk Universe

Data Libraries of Compliance Universe Associated with the Risk Universe

Data Libraries of Risk Universe Associated with the Compliance Universe

Regions
Countries
Lines of Business
Legal Entities
Sub lines of Business
Regulatory Body
Risk
Area of Compliance
Control
Standard
Question / Procedure
Requirement
Regulatory Development
Process
Function
Product / Service
Metrics
Asset Class
Loss
Asset
Framework Reference
Policy

12

Empower – Provide A Decision Framework

4:20 PM — 10 MINS TO MARKET CLOSE

4:21 PM — 9 MINS TO MARKET CLOSE

4:22 PM — 8 MINS TO MARKET CLOSE

4:27 PM — 3 MINS TO MARKET CLOSE

4:30 PM — MARKET CLOSE

4:20 PM

FUND MANAGER

"Make a trade"

"The size of the trade is four times the size of all trades on the Irish market's index that day taken together"

TRADING FLOOR

TRADER

4:21 PM

"Is this market manipulation?"

"Will I get into trouble executing this trade?"

"I will lose a large commission if I don't?"

"How Can I ensure that I am following the policy guidelines?"

TRADER

4:22 PM

Triggers Market Manipulation Policy Attestation Survey in MetricStream Policy Management App

- Was the client aware of the size of trade? **YES**
- Was that conversation on a recorded line? **YES**

App Recommends to execute the trade

METRICSTREAM SURVEY MANAGEMENT APP

4:27 PM

Trader executes the trade

Due Diligence on the trade is recorded for future internal and regulatory scrutiny

Commissions on the trade is realized

TRADER

4:30 PM

What was happening?

In parallel an equally big 'opposite trade' order had come from another big fund manager

They wanted to swap a very large volume of shares with one another for accounting reasons

All completely legitimate and above board

Engage - Information is Power

MetricStream

Knowledge Mosaic®

ComplianceOnline
The Largest GRC Advisory Network

State Net®

DATA.GOV
EMPOWERING PEOPLE

Corporate Risk®
>>>>> SOLUTIONS

CLEAR Market Practices

Code of Federal Regulations

DOW JONES

LexisNexis®

SHESHUNOFF | PRATT
INFORMATION SERVICES

SHARED ASSESSMENTS

IT UCF

Regulatory Feeds

News Feeds

Risk/Control Libraries

grc
intelligence.com

Curate

Collaborate on Changes and Subsequent Actions in the Operational Risk Regulatory Framework

Collaborate on market information for deign of products in lines with Conduct related regulations

Operational Risk Management

Regional ORM Regulations

Emerging Risks

KRIs

Changing Compliance Requirements

Publicly Reported Compliance Failures

Emerging Regulatory Consultations

Compliance Management

Third Party Ratings Agency Update

Metrics

Third Party Management

Reported Third Party Breaches

Audit Analytics

Financial Result Announcements

Audit Frame Updates

Internal Audit

EXAMPLES ON USE OF CORRELATIVE INTELLIGENCE

Collaborate on Supplier Audits with Regulatory Intelligence on Risk Profiles

Collaborate Third Party Assessments with Information from Compliance Updates on Third Party related news

LEVERAGING THE INTEGRATED PLATFORM FOR CORRELATIVE INTELLIGENCE

Block Strategy

3R

REGULATE

- Proactive Controls
- Track Indicator Metrics
- Continuous Monitoring

REVIEW

- 2 Eye Principle (maybe 3)
- Ad-hoc reviews
- Investigate possibilities

REINSTATE

- Drive processes
- Attest Regularly
- Inform proactively

Regulate – Catch Them Early (or as they happen)

4.30 PM

30 MINS TO DAY CLOSE

Transaction Records For Entire Day

"How do I ensure that the transactions being performed are following the policy"

FRONT DESK COMPLIANCE OFFICER

RETAIL BANKING FRONT OFFICE

4:31 PM

29 MINS TO DAY CLOSE

"Are all the transactions following the policies?"

"How will I map policies to the transaction types?"

"How do I manage the large volume of transactions"

"If I miss something I will be held liable

FRONT DESK COMPLIANCE OFFICER

4.35 AM

25 MINS TO DAY CLOSE

Triggers Transaction Monitoring Attestation Survey in MetricStream Policy Management App

- What is the transaction type? **YES**
- Is this one of the significant transactions by value? **YES**
- Was the procedure for transaction followed? **YES**

App Identifies anomalies in the transactions for the day

METRICSTREAM POLICY MANAGEMENT APP

4:55 PM

5 MINS TO DAY CLOSE

All significant daily transaction records are validated

Any frauds or anomalies noticed are appropriately escalated

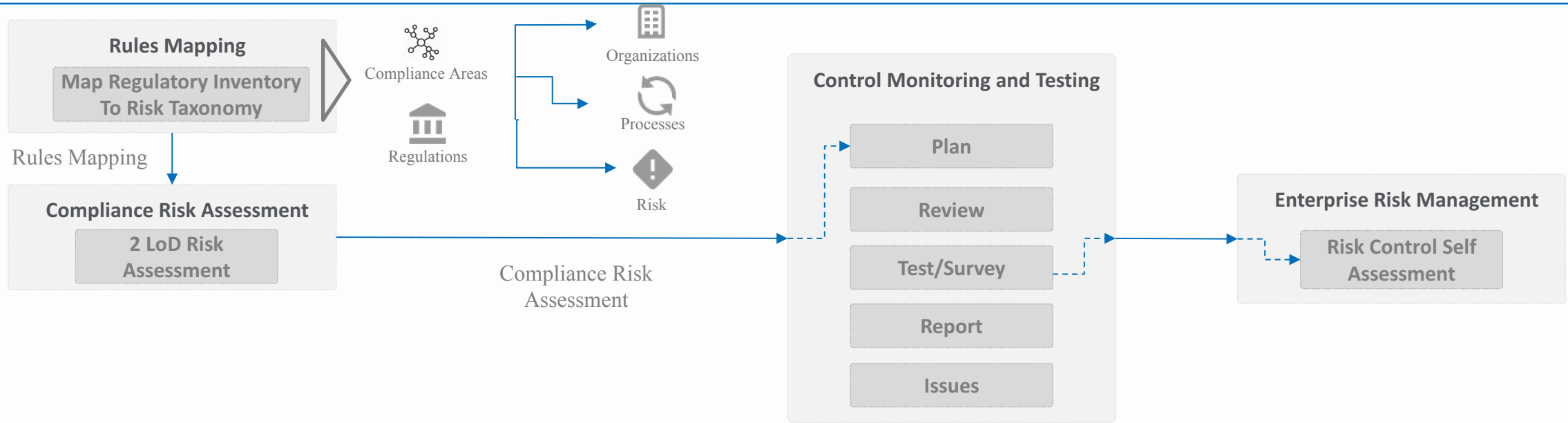Records are stored for regulatory scrutiny

FRONT OFFICE STAFF

5:00 PM

DAY CLOSE

What was happening?

Transactions made during the day need to be validated by the front office staff to endure that they followed all the policies for the high value transactions

Any anomalies noticed are escalated to ensure faster resolution or reversal

Review – CMAT Is a Case In Point

Rules Mapping

Map Regulatory Inventory To Risk Taxonomy

Rules Mapping

Compliance Risk Assessment

2 LoD Risk Assessment

Compliance Areas

Regulations

Organizations

Processes

Risk

Compliance Risk Assessment

Control Monitoring and Testing

Plan

Review

Test/Survey

Report

Issues

Enterprise Risk Management

Risk Control Self Assessment

RULE MAPPING

- Mapping Regulatory Body To Areas of Compliance

- Areas Compliance Mapped to Requirements and Standards

COMP. RISK ASSESSMENT

- Identify Compliance Risks

- Assess Compliance Risks by the 2nd Line of Defense
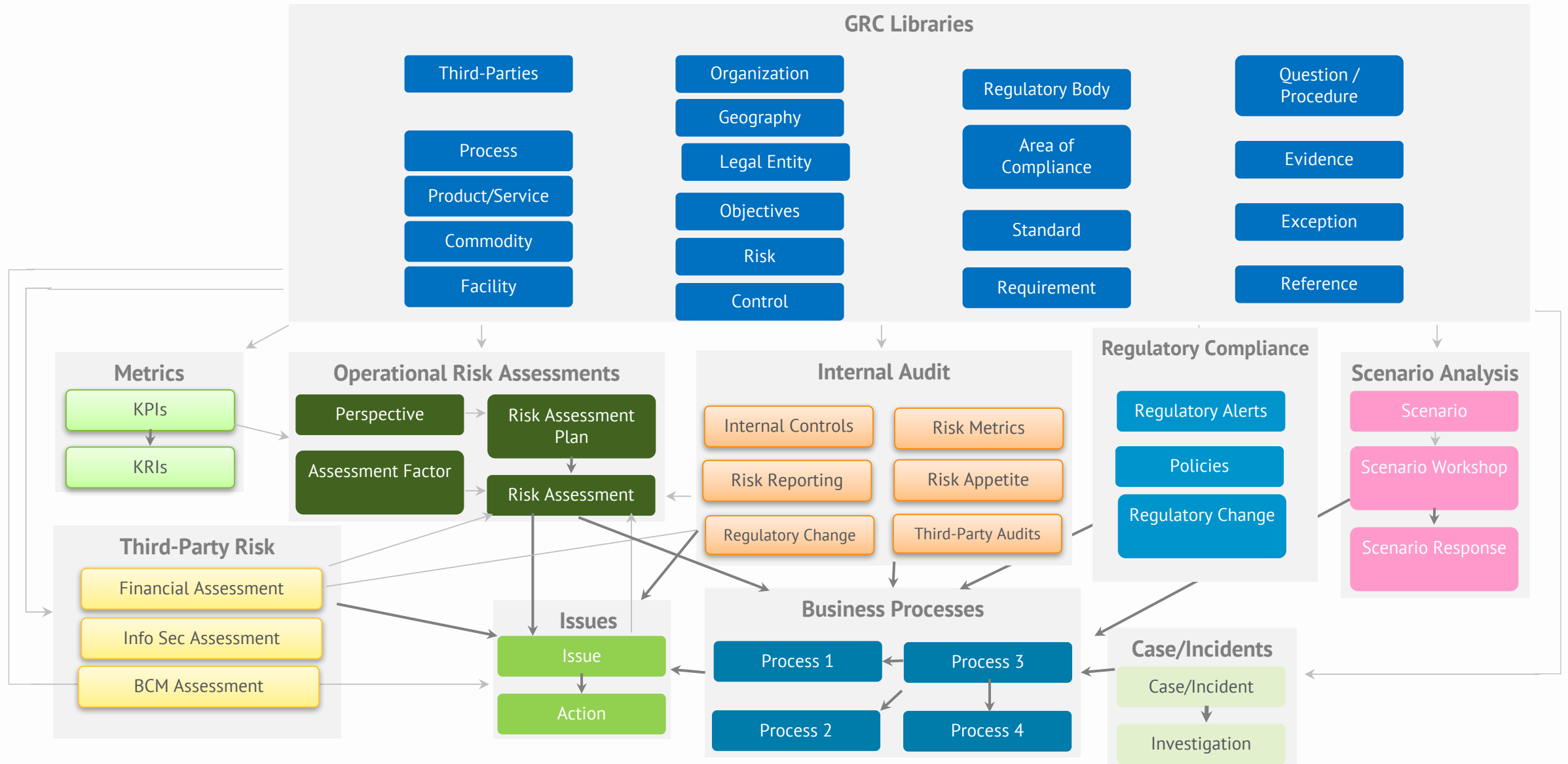
- Report Risk Scores

CONTROL MONITORING AND TESTING

- Plan – Control testing program based on risk based planning

- Review – Align Control Testing Resources and Time

- Test – Conduct control tests by the 2.5 Line of Defense groups

- Report – Control test reports around control effectiveness

- Issues – Track open issues to closure

ENTERPRISE RISK MGMT.

- Control test results from CMaT is used for Risk control Self Assessment

- Control Rating from CMAT is used to calculate residual risk scores

Reinstate – Establish Multiple Checkpoints

MetricStream

GRC Libraries

- Third-Parties
- Process
- Product/Service
- Commodity
- Facility

- Organization
- Geography
- Legal Entity
- Objectives
- Risk
- Control

- Regulatory Body
- Area of Compliance
- Standard
- Requirement

- Question / Procedure
- Evidence
- Exception
- Reference

Metrics
- KPIs
- KRIs

Operational Risk Assessments
- Perspective
- Risk Assessment Plan
- Assessment Factor
- Risk Assessment

Internal Audit
- Internal Controls
- Risk Metrics
- Risk Reporting
- Risk Appetite
- Regulatory Change
- Third-Party Audits

Regulatory Compliance
- Regulatory Alerts
- Policies
- Regulatory Change

Scenario Analysis
- Scenario
- Scenario Workshop
- Scenario Response

Third-Party Risk
- Financial Assessment
- Info Sec Assessment
- BCM Assessment

Issues
- Issue
- Action

Business Processes
- Process 1
- Process 3
- Process 2
- Process 4

Case/Incidents
- Case/Incident
- Investigation

The Future

Business Advisor

1 Extending Limited Resources
Extending the compliance function

2 Proactively Stop Incidents
Prevent misinformed and malicious lapses

3 Build Market Confidence
Stronger confidence on data and processes

4 Robust Relationship with Business
Find the elusive elixir of balance

5 Increases Brand Value
Contribute towards business objectives

Q&A

MetricStream

GRC
SUMMIT **2017**
November 6 - 7, 2017
L O N D O N

Continue the conversation online
#GRCSummit

Thank You!

GRC for **High Performers**