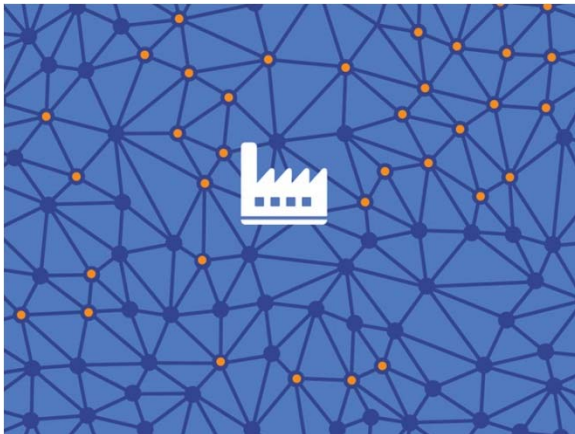


GRC Fundamentals

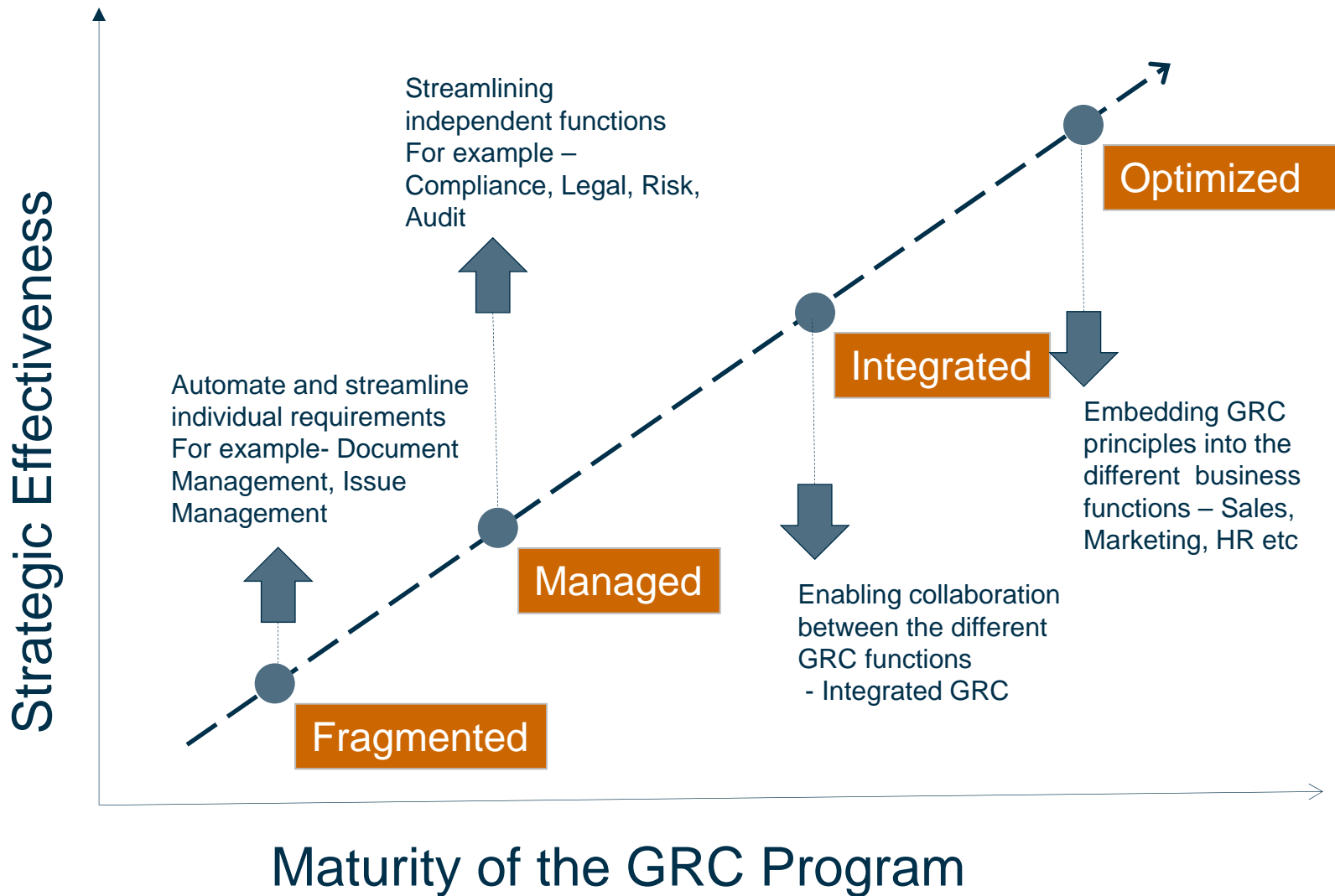
Vinay Bapna, Associate Vice President - Marketing

GRC in Today's World



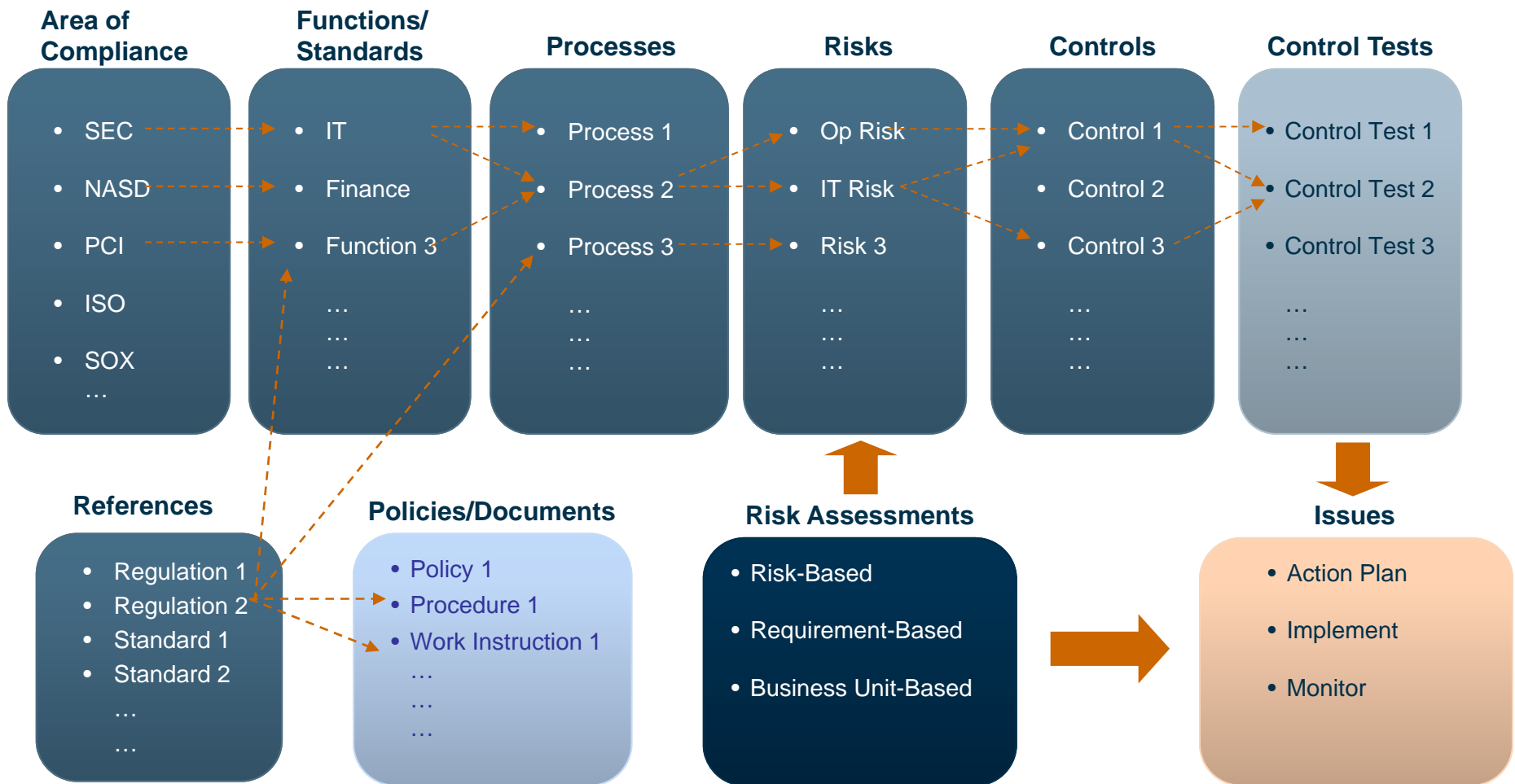
- **Performance Focus**
 - Risk intelligence has to drive performance in a growing enterprise
- **Regulatory Changes**
 - Significant business and cost impact on corporations
- **Cloud, Social Media, Mobile**
 - Emerging risks from faster, unrestricted, information flows
- **Complex Global Supply Chain**
 - Intertwining of risks and escalation of incidents

The GRC Journey: Levels of Maturity



Enabling a Common GRC Taxonomy

Defining a common GRC taxonomy that provides a baseline across the organization as well as a federated model that allows aggregation and roll-ups



Data Model: Flexible Relationships and Visualizations

The screenshot displays the MetricStream web application interface. At the top, it says 'Welcome: Program Manager' and 'My Tasks: 14 [7 New, 0 Past due]'. The main navigation bar includes 'Compliance' and 'Administration' tabs, with sub-tabs for 'Assignments', 'Dashboards', and 'Reports'. The left sidebar shows a 'Browse: Processes' tree with various categories like 'Affirmative Action Plans', 'Branch Admin', etc. The main content area is divided into three overlapping windows:

- Left Window:** 'Browse: Processes' showing a tree structure under 'All Processes - General' with sub-categories like 'Risk', 'ACH', 'ATM Bank', 'Overdrafts', and 'Net banking Transfers'. An orange arrow points from the text 'Processes' to this window.
- Middle Window:** 'Transfer [PROC-1055]' showing a 'Browse: Regulatory Bodies' tree with categories like 'DOL', 'EEOC', 'FDIC', 'Area of Compliance', 'Model Reference', 'Regulation E', 'Requirements', 'HHS', and 'OFCCP'. An orange arrow points from the text 'Processes Mapped to Risks' to this window.
- Right Window:** A detailed view of a regulatory body, showing 'Regulation E' with sub-items like 'FDIC', 'Requirements', 'Portions', 'Citations', and 'Sections'. An orange arrow points from the text 'Linkages between Regulations, Policies, Requirements, Risks, Controls, Organizations, etc.' to this window.

Additional text annotations include 'Processes' with an arrow pointing to the left window, 'Processes Mapped to Risks' with an arrow pointing to the middle window, and 'Linkages between Regulations, Policies, Requirements, Risks, Controls, Organizations, etc.' with an arrow pointing to the right window.

Case Study: Robust Compliance Data Model

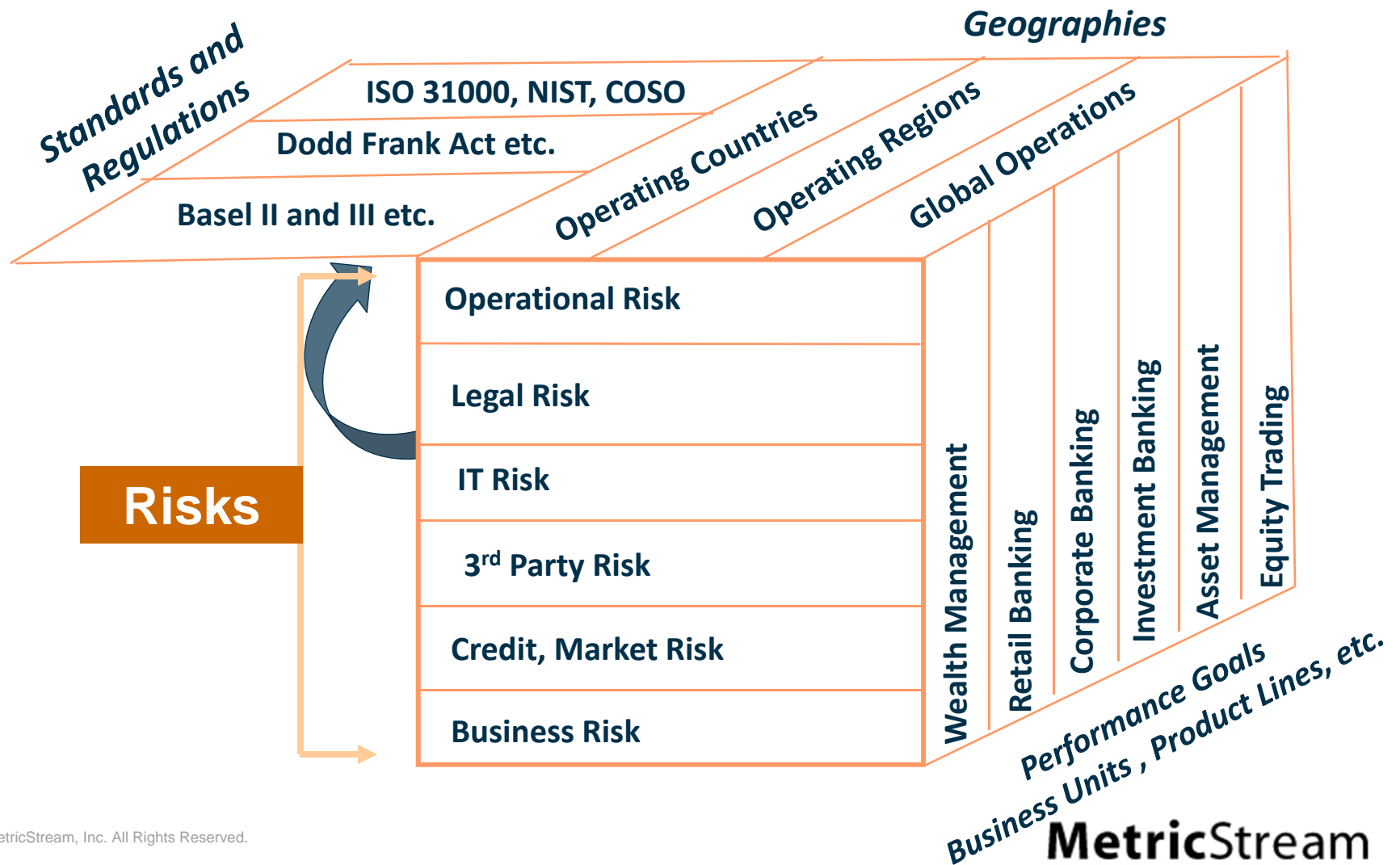


Leading Retail Chain

- Streamlining and integrating compliance programs across BUs and functions
- Integrated framework to streamline compliance with HR policies and procedures, training and certification requirements, privacy policies, diversity affairs, legal requirements, risk management, internal audit, IT security and SOX

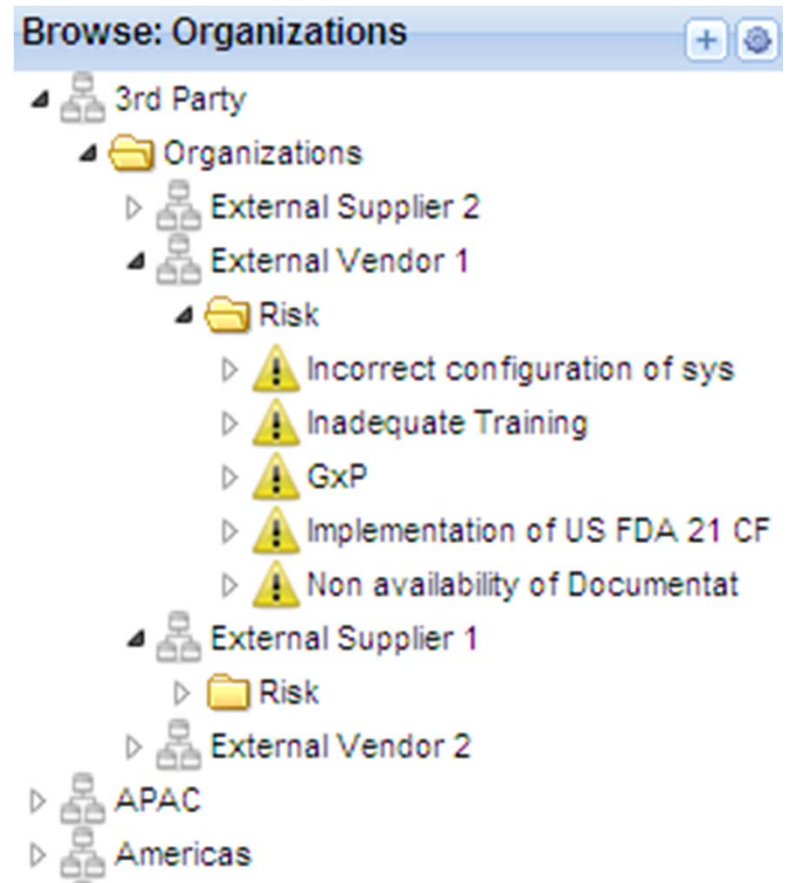
Modeling Organizational Structures and Hierarchies

Defining hierarchies and relationships for a centralized view of risk aligned to business performance objectives for enabling decision making



GRC and the Organization's DNA

- Federated architecture
 - Centralized controls and visibility
 - Decentralized processes and ownership
 - Supporting complex, multi-dimensional relationships
- Large scale adoption
 - Extended enterprise participation
 - Simplified user experience
 - Collaboration, personalization, mobile access



Case Study: Federated GRC Infrastructure



A Fortune 50 Life Sciences Company

- Federated GRC framework across 400 business units
- Regulatory, Operational and IT compliance - driven by the board
- Harmonization of controls across the enterprise and subsidiaries
- Finance, IT, privacy, security, marketing, sales, safety, environment and quality

Monitoring Regulatory Changes

- Update policy and compliance activities
- Impact analysis and mapping
- Triggering assessments, policy updates

The collage displays four overlapping web browser screenshots:

- ComplianceOnline.com:** Shows a navigation menu with categories like Banking and Financial Services, Biotechnology, Clinical Research, FDA Compliance, Green Compliance, HIPAA Compliance, HR Compliance, Laboratory/Compliance, Medical Devices, Pharmaceutical, Quality and ISO Compliance, Risk Management, SEC Compliance, and SOX Compliance. It also features 'Online Training' and 'Featured Trainings'.
- Bloomberg.com:** Shows a news article titled 'Yen Set for Weekly Gain on Concern Economic Stimulus Measures Fall Short' with a sub-headline 'Regulatory Insight'.
- Complanet:** Features a 'Spotlight' section with the headline 'Madoff based suit adds risk for brokers, advisers' and a 'My CourtLink' section with a search bar and filters.
- LexisNexis:** Displays a search results page with sections for 'Recent Searches', 'Recent Dockets & Documents', and 'Today's Alerts'.

Search Term	Matches
howard v - PGC	134 docket matches
Untitled Search 11/9/2006	0 docket matches
Howard University - VA multiple	0 docket matches
NJ Statewide - Eric Olson	16 docket matches
NJ Atlantic - eric olson	1 docket matches
June 2	0 docket matches
IOEE 2	0 docket matches
Untitled Search 11/7/2006	2 docket matches
IOEE	0 docket matches
VA - Wal-mart	1 docket matches

Case Study: Regulatory Monitoring



One of the Largest Banks in Europe

- Streamlined and simplified compliance by integrating risk assessments across countries, functions and processes
- Comprehensively assess and manage risks, establish and monitor controls and meet the demands of regulations across 80 countries
- Integration with external regulatory sources for risk intelligence

GRC Intelligence: Content Cloud

Channel: NYSE Feed

Channel Name*

NYSE Feed

Channel Status*

Active

Channel Type*

Alert

Source Details

Delete Add Source

Delete Last Source

Pages: 1 of 1 Total Rows 1

Row# 1

Source*

RSS

Server Address / URL*

http://markets.nyx.com//content/msa_traderupdates/all/a

User Name

Kris

Password

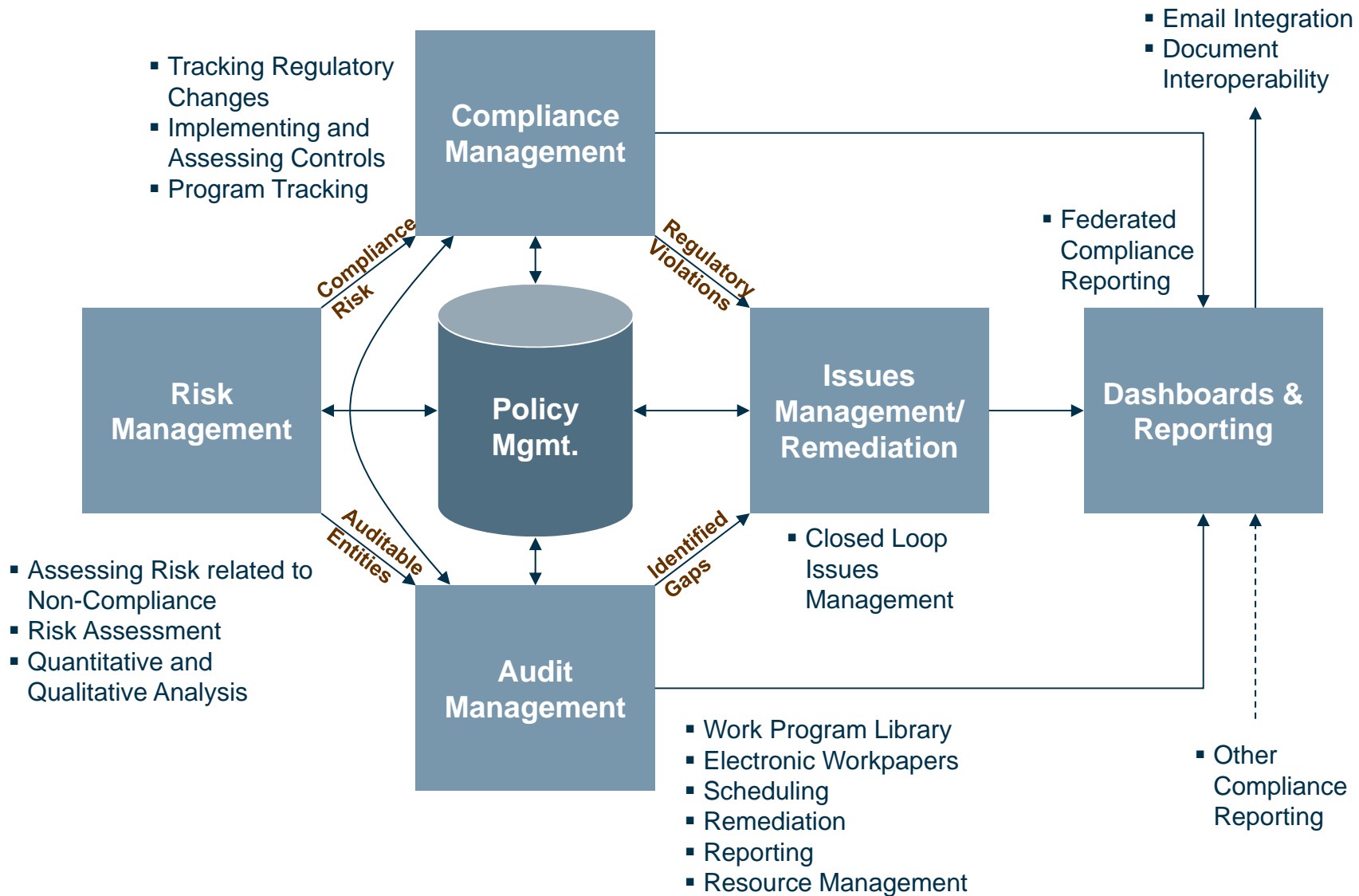
●●●●●●●●

Server Parameter(s)

Validate Source

Keyword(s) (Comma Separated)

Enabling Collaboration Across GRC Functions



Enabling Collaboration: Calendar, Emails, Workflows

The screenshot displays the MetricStream Enterprise Governance Risk Compliance Platform interface. The main window shows a calendar for February 2011, with a detailed view of a test event (ID 14552) scheduled for February 2, 2011. The event details include:

- Name:** 14552
- Test/Survey/Certification:** Test
- General:**
 - Overview/Methodology
 - Type(s)
 - Send Pre-Test Questionnaire? No
 - Certification Required?
 - Approve All Tests/Surveys
- Ownership and Security:**
 - Owner Organizations*: IRM
 - Level 1 Approver: Test Manager
 - Restrict Access To*

The calendar view shows a grid for February 2011, with the 2nd of the month highlighted. A legend for 'All Calendars' indicates that orange squares represent 'Tests - Due for Completion', green squares represent 'Tests - Completed', red squares represent 'Surveys/Certifications - Due for Completion', and dark green squares represent 'Surveys/Certifications - Completed'. The event details at the bottom of the screen show: Event: 14552, Start: 02/02/2011, End: 02/02/2011, Description: PLAN-11471[Planned], and Calendar: Tests - Due for Comple...

Compliance Survey Collaboration



Next Gen GRC Platform Capabilities

- Big Data Analytic Capabilities
- Contextual Risk Intelligence and Advanced Analytics
- Advanced AppStudio for Configuration
- Multi-platform Mobility Support
- Cloud-based Solution
- Readiness for Enterprise

Social Media Risk and Compliance Management

Security Intelligence Report

Tweet Text: Posted By:

Report Data as of: 08/22/2012 10:29 AM

Posted By	Tweet Text ^	Posted On	Source
AmazonFriend2	Hewlett Packard -HP- Color Laserjet 4500N (C4194A) original Toner-Kartusche -...	Tue, 07 Aug 2012 03:08:18 +0000	twitterfeed
AmazonIdol12	Hewlett Packard -HP- Color Laserjet 1500LXI (C970*A) original Toner-Kartusche...	Tue, 31 Jul 2012 14:32:42 +0000	twitterfeed
BockDelon	Genuine NEW Hewlett Packard CC530A Smart Print Black Toner Cartridge: Genu...	Tue, 31 Jul 2012 17:50:00 +0000	twitterfeed
Briedndw	LD © Remanufactured Yellow Laser Toner Cartridge for Hewlett Packard (HP) C...	Wed, 01 Aug 2012 02:22:02 +0000	twitterfeed
CluB0yeso	HP Toner Black, CE505A: Pages 2300Kompatibel mit: HP/Compaq LaserJet - P20...	Wed, 01 Aug 2012 01:23:02 +0000	twitterfeed

Configure social site access

Social site URL *

Config file *

Hadoop DFC root URL *

Edit Risk Analyzer Rules

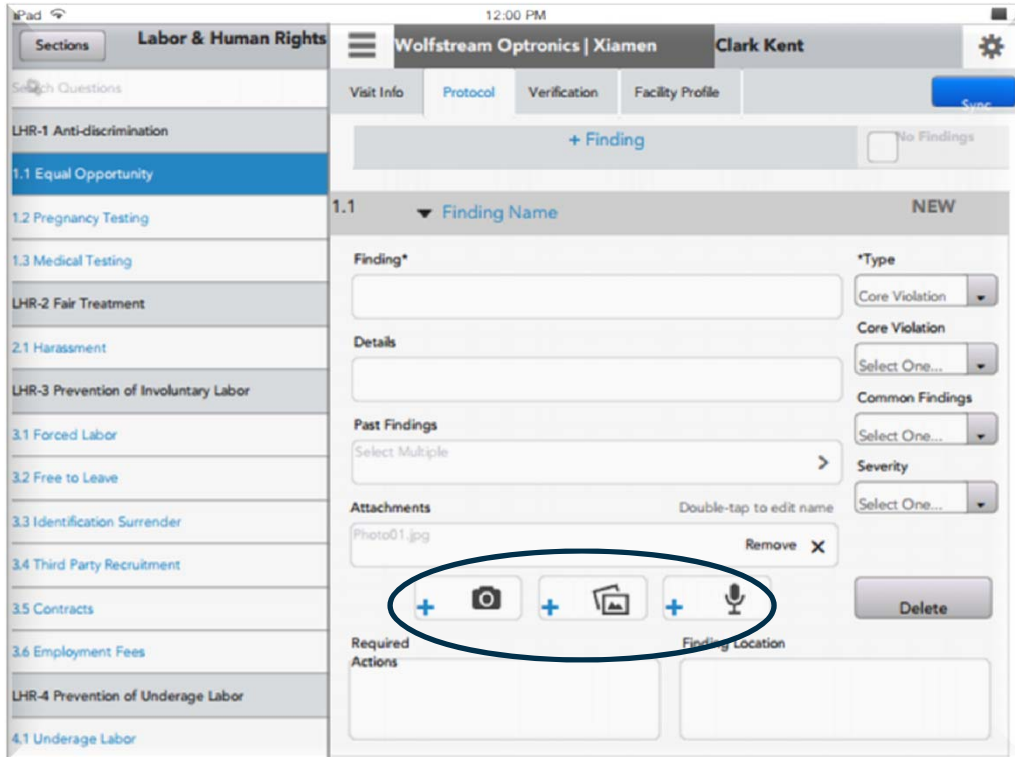
Risk Name *

- Select One
- Financial Risk
- IP Loss
- Information Security Risk
- Infrastructure Stability Risk
- Lack of Governance
- Litigation Risk**
- Metrics Integrity Risk
- Personal reputation Loss
- Regulatory Risk
- Reputation Risk
- Safety Risk
- Sensitive Data loss

Operation	Categories
contains	UPSET_noun
contains	UPSET_noun
contains	LOSS_verb
contains	LOSS_verb

Total Rows: 4 Pages: 1

Leveraging Native Mobile Capabilities



Questions

- Land Contract**
Is there a written contract for land use in place?
- Variance #**
Variance # (if applicable)
- In-Season Monitoring Log**
Is in-season monitoring log up-to-date?
- GPS Coordinates**
After GPS coordinates are recorded, do you see any coordinates red flagged (i...)
- Corner Markers**
Is each corner of the regulated release site marked with a physical marker?
- Isolation**
Is approved isolation requirement (to nearest planted sexually compatible cr...)
- Volunteers**
Is the approved isolation zone free of any sexually compatible volunteers?
- Work (Service) Co...**
Is there a written contract for the work to be done between DAS and the third...?
- Movement/Release Permit/...**
Is there a copy of the movement/release permit for the regulated release site?

1000-PF Assessment

ON Include GPS Coordinates

Cancel Copy

Questions

- Land Contract
Yes
- variance #
Yes-record # in comments if not in task details
- In-Season Monitoring Log
No
- GPS Coordinates
No

Tasks

- [Complete Checklist]- Simpson, David - IN, Benton (PF)/ 5854-PF Assessment
- [Complete Checklist]- AUD - IPAD Validation [PF]/ 5678-PF Assessment
- [Complete Checklist]- Validation for the GPS coordinates/ 5555-PF Assessment
- [Complete Checklist]- Simpson, David - IN, Benton (PF)/ 5412-PF Assessment
- [Complete Checklist]- AUD - IPAD Validation [PF]/ 5207-PF Assessment
- [Complete Checklist]- Tyler Horn-Santa Clara-CA/ 1001-PF Assessment





Sections

Labor & Human Rights



Wolfstream Optronics | Xiamen

Clark Kent



Search Questions

Visit Info

Protocol

Verification

Facility Profile

Sync

LHR-1 Anti-discrimination

1.1 Equal Opportunity

1.2 Pregnancy Testing

1.3 Medical Testing

LHR-2 Fair Treatment

2.1 Harassment

LHR-3 Prevention of Involuntary Labor

3.1 Forced Labor

3.2 Free to Leave

3.3 Identification Surrender

3.4 Third Party Recruitment

3.5 Contracts

3.6 Employment Fees

LHR-4 Prevention of Underage Labor

4.1 Underage Labor

LHR-1 Anti-discrimination

1.1 Equal Opportunity

Implementation

3

Compliance

3

Suppliers shall not discriminate against any worker based on race, color, age, gender, sexual orientation, ethnicity, disability, religion, political affiliation, union membership, national origin, or marital status in hiring and employment practices such as applications for employment, promotions, rewards, access to training, job assignments, wages, benefits, discipline, and termination.

Suggested Documents

Bacon ipsum, dolor sit amet, ut et duis, meatball commodo ham salami, labore bacon, officia id excepteur, Velit doner meatball, deserunt.

Special Consideration

Bacon ipsum, dolor sit amet, ut et duis, meatball commodo ham salami, labore bacon, officia id excepteur, Velit doner meatball, deserunt.

Information Sources

[+ Finding](#)

No Findings



Search Questions

Visit Info Protocol Verification Facility Profile Sync

LHR-1 Anti-discrimination

+ Finding No Findings

1.1 Equal Opportunity

1.1 Finding Name NEW

1.2 Pregnancy Testing

1.3 Medical Testing

LHR-2 Fair Treatment

2.1 Harassment

LHR-3 Prevention of Involuntary Labor

3.1 Forced Labor

3.2 Free to Leave

3.3 Identification Surrender

3.4 Third Party Recruitment

3.5 Contracts

3.6 Employment Fees

LHR-4 Prevention of Underage Labor

4.1 Underage Labor

Finding*

*Type

Details

Core Violation

Past Findings

Common Findings

Attachments Double-tap to edit name

Severity

Required Actions

Finding Location

Measuring Value of GRC - Reduced Risk

- **Better risk mitigation**
 - Speed of Decision Making
 - Reaction time to loss events reduced
 - Example: credit card data security breach – PCI non-compliance
 - Ability to understand co-relations of risks
- **Assured compliance**
 - Effective tracking and reporting
 - Detection and closure of gaps and deficiencies
 - Example: Penalty for noncompliance with laws
- **Effective risk detection and assessment**
 - Know where to focus, right prioritization
 - Translate assessment into actionable recommendations
 - Example: Positional intellectual property liability

Measuring Value of GRC - Lower Ongoing Costs

- Reduction on
 - Eliminate redundant and irrelevant activities
 - Harmonization of controls (for example Cobit, ISO 27002, PCI, SOX)
 - 20-40% reduction
- Rationalizing Resources
 - Consolidation and better resource utilization – lesser manual work
 - Improved assurance with current staff
- Reduction in external costs of assurance
 - Less use, more effective use with easy access to information
 - Estimated 25% savings in External Costs of Assurance
- Lower IT costs
 - Common infrastructure across various assurance groups
 - Faster compliance by system consolidation, information visibility

Measuring Value of GRC - Better Business Decisions

- Reputation Management
 - Preserving brand and shareholder value
 - Unmanaged incident, compliance issue - millions in reputation damage
- Revenue Management
 - Ensuring you don't lose your customers
 - Customer loss - millions in revenue loss
- Visibility
 - Faster decision making
 - Pre-empted controls can result in hundreds of thousands in savings
- Transparency
 - Risk intelligence to board and investors
- Strategic Value
 - Align IT to business
 - Business performance gains through process standardization

Succeeding at Integrated GRC: Role of Platform

- **Configurability**
 - Modify data model, workflows, reporting for specific business needs
- **Extensibility**
 - Start in one area, extend seamlessly into others
- **Enterprise readiness**
 - Reliability, Availability, Scalability, Cloud and On-Premise Support
- **Multi-level security & access controls**
 - Multiple layers of hierarchy, business units spanning geographies
- **Integration mechanisms**
 - Big Data, Web Services, file upload, database, message bus, etc.

Summarizing: Next Steps in GRC

- **Common information model**
 - Multiple sites, regulations, functions, countries
- **Collaboration driven**
 - Standardized data collection to eliminate errors and inconsistencies
 - Manage compliance, risk and audits as a central function
- **Integrated and real-time information flow**
 - Leveraging internal and external sources
- **Decision making and performance management**
 - Easy access to analytics - with minimal manual work
- **Tied to a closed-loop remediation, corrective actions processes**
 - Seamless integration between compliance, risk and audit process



Thank you
