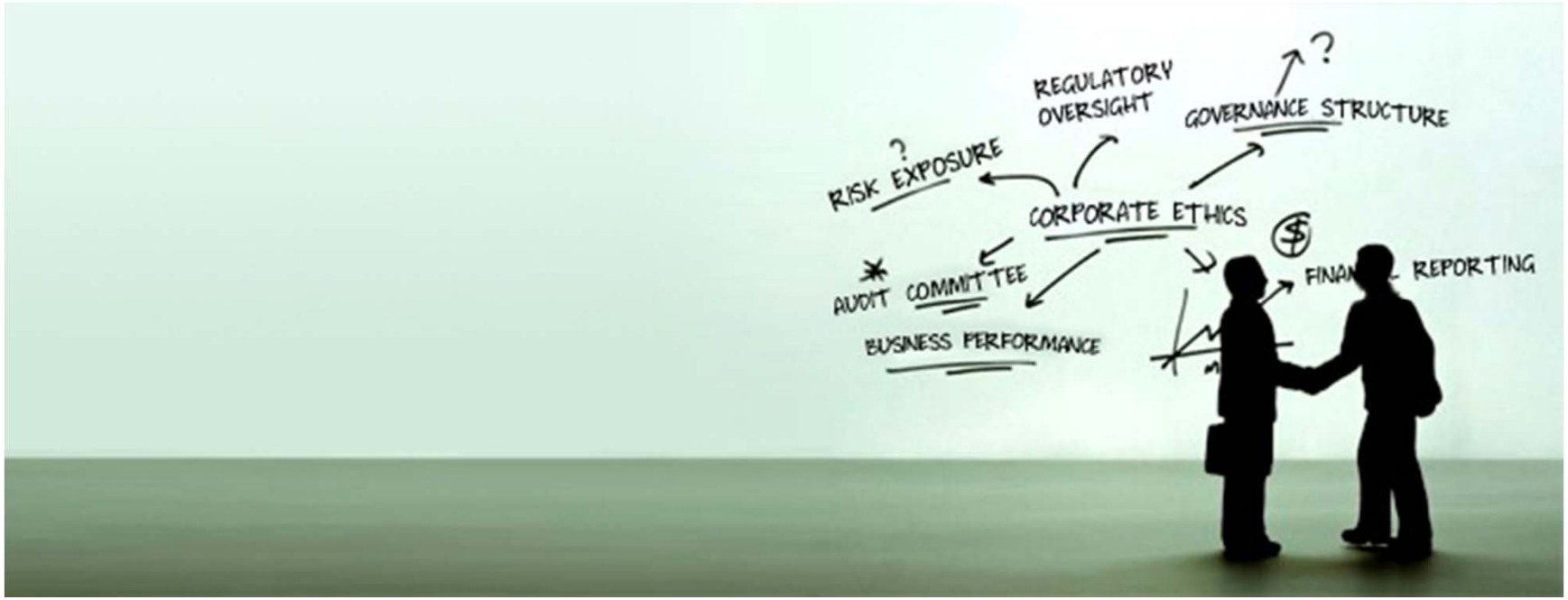
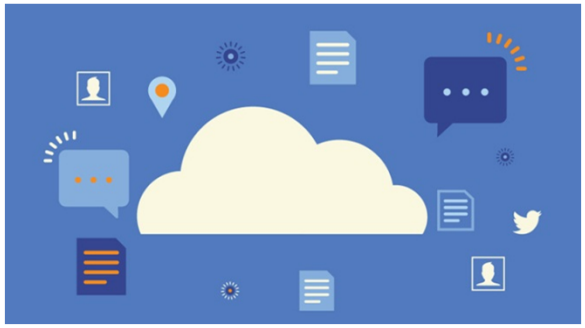


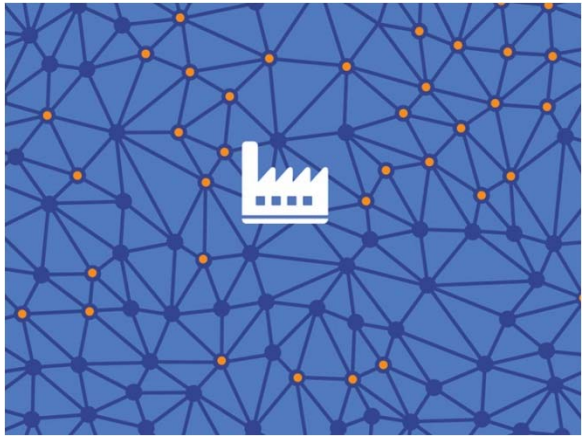
GRC Fundamentals

Vinay Bapna, Associate Vice President - Marketing

MetricStream

GRC in Today's World

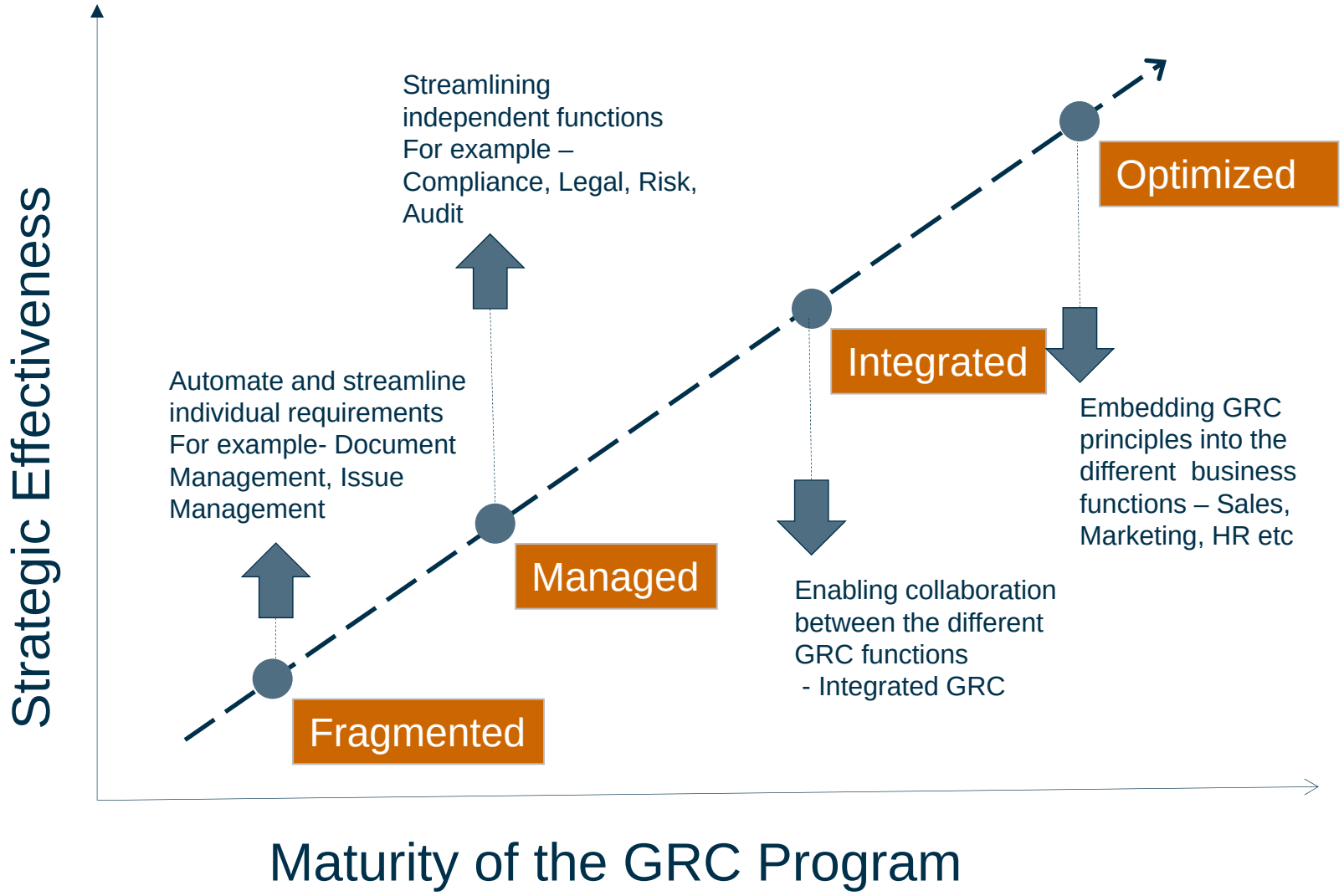




- Performance Focus
  - Risk intelligence has to drive performance in a growing enterprise
- Regulatory Changes
  - Significant business and cost impact on corporations
- Cloud, Social Media, Mobile
  - Emerging risks from faster, unrestricted, information flows
- Complex Global Supply Chain
  - Intertwining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

MetricStream

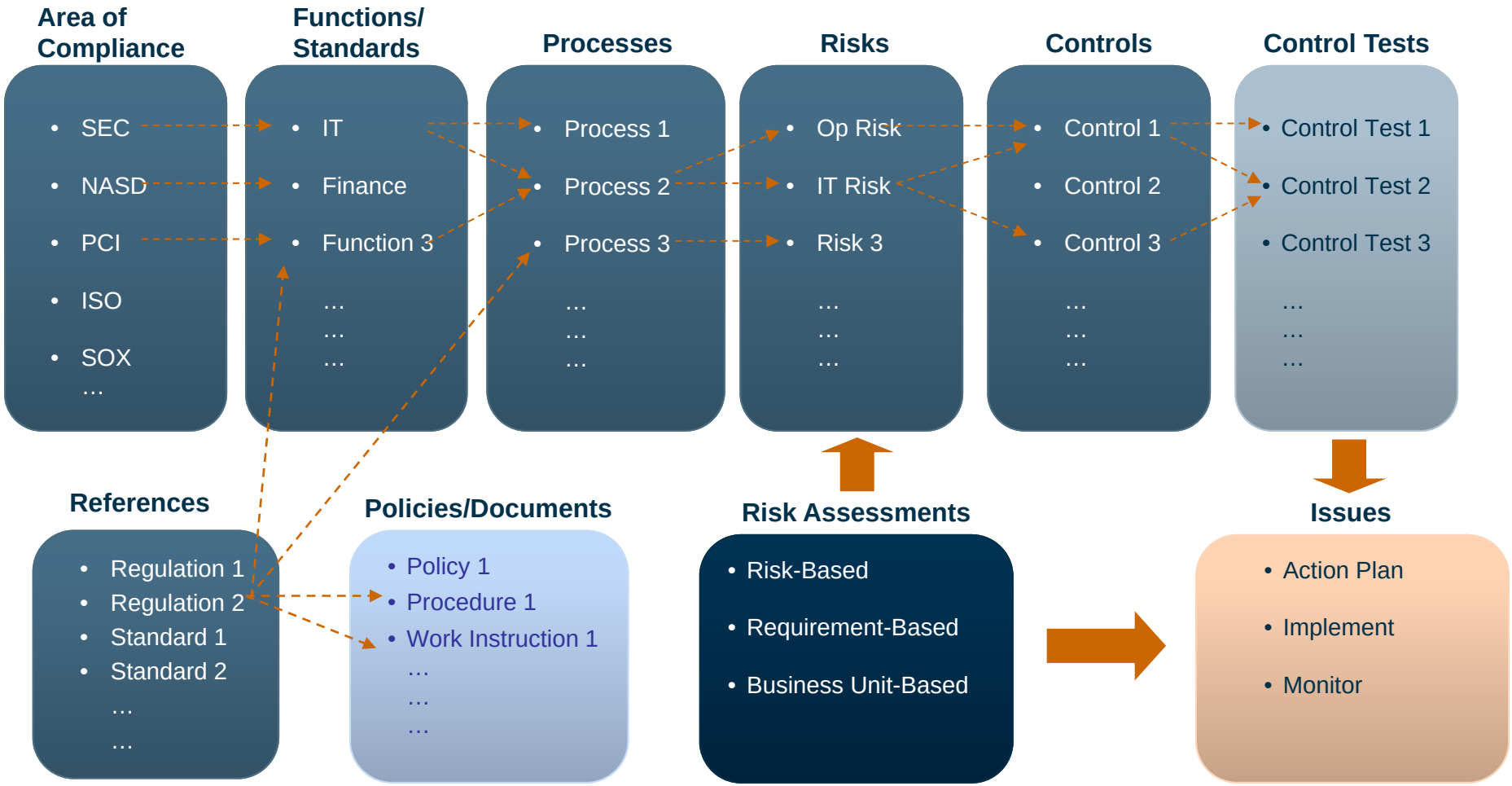
The GRC Journey: Levels of Maturity



MetricStream

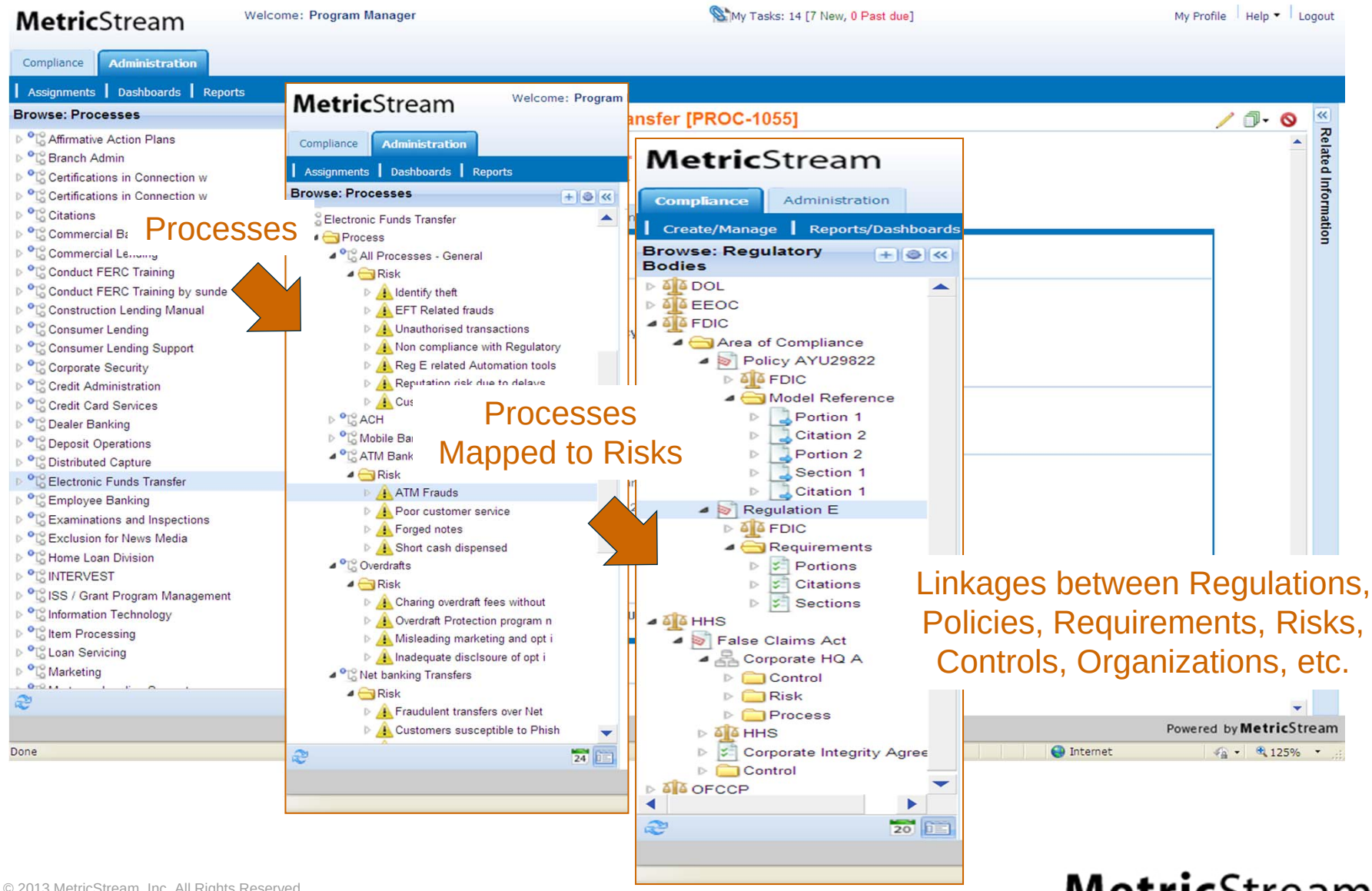
Enabling a Common GRC Taxonomy

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



MetricStream

Data Model: Flexible Relationships and Visualizations



MetricStream

Case Study: Robust Compliance Data Model

Leading Retail Chain

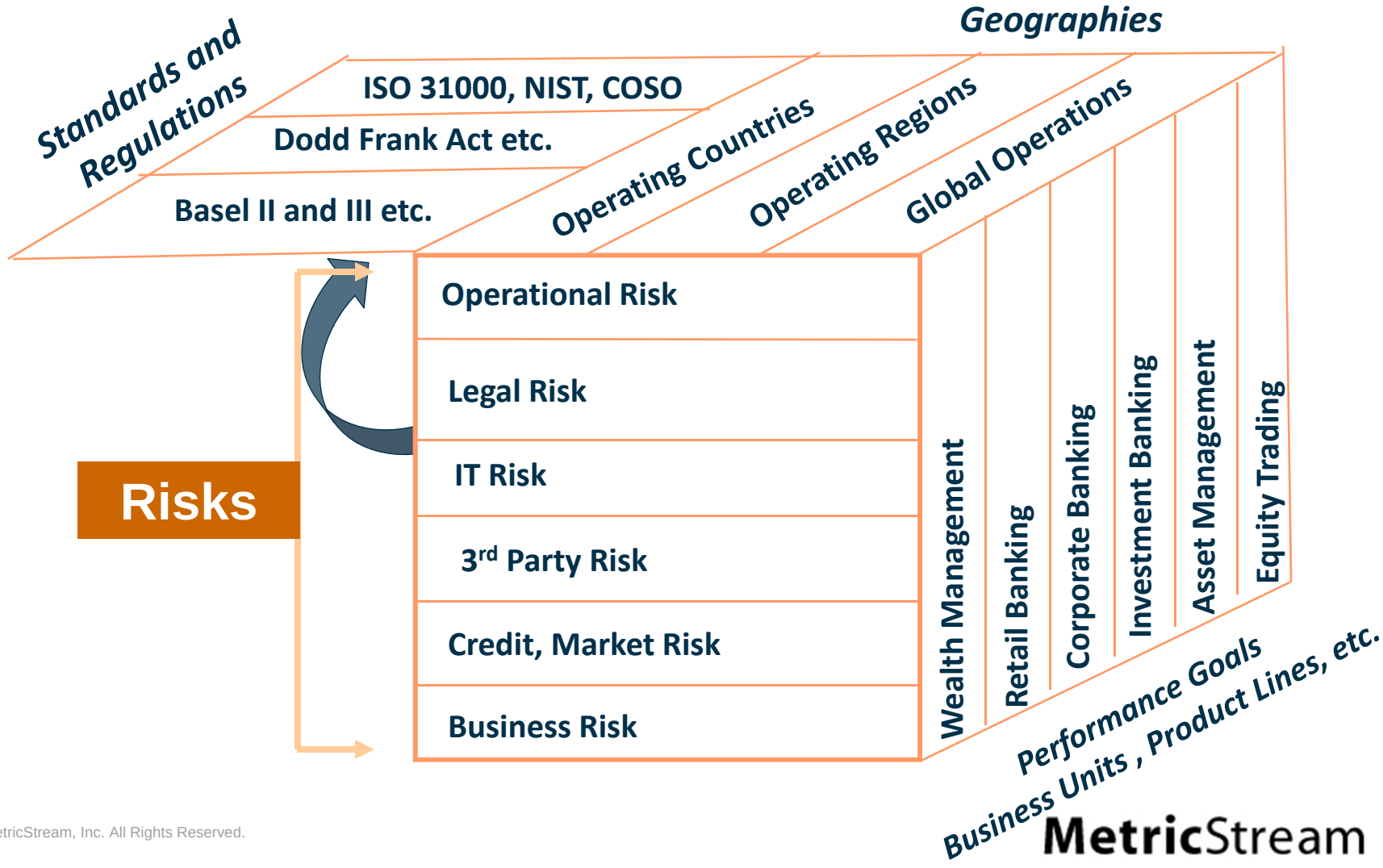
- Streamlining and integrating compliance programs across BUs and functions

- 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

MetricStream

Modeling Organizational Structures and Hierarchies

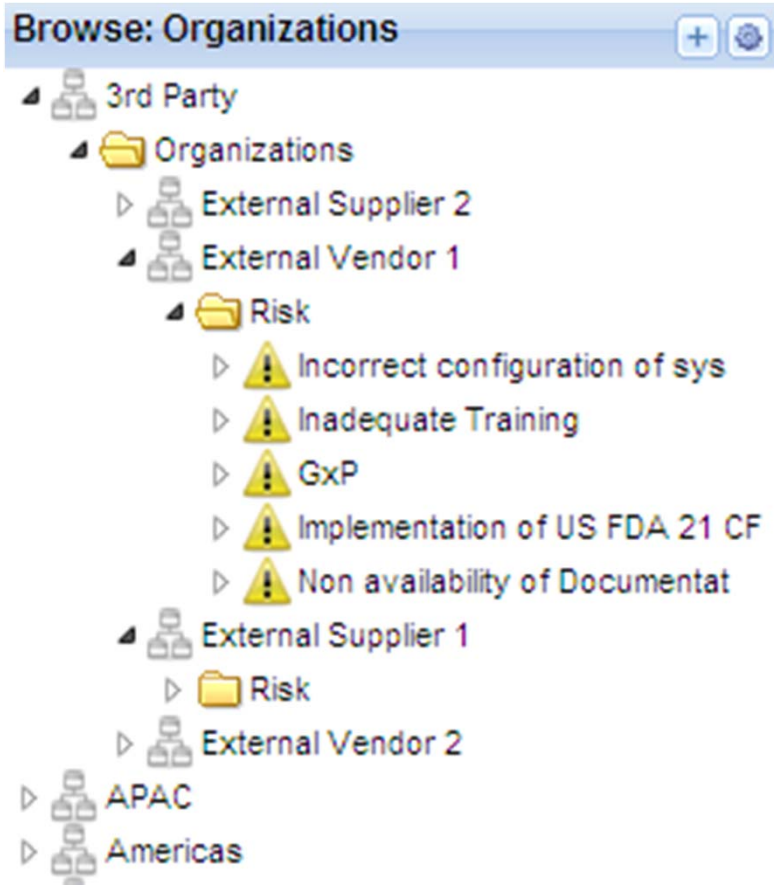
Defining hierarchies and relationships for a centralized view of risk aligned to business performance objectives for enabling decision making



MetricStream

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



MetricStream

Case Study: Federated GRC Infrastructure

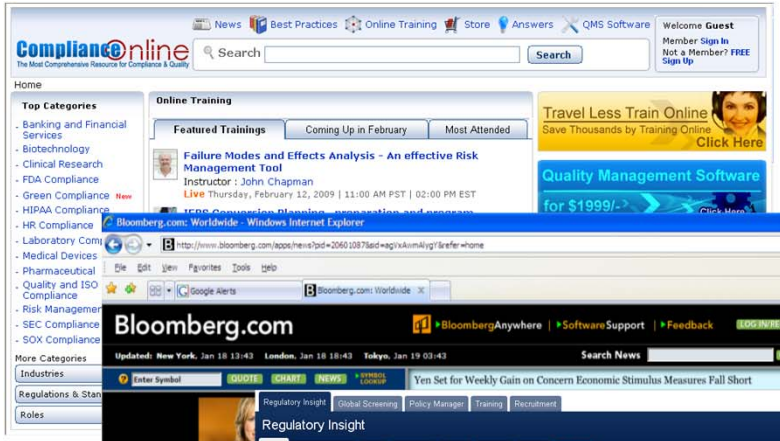
A Fortune 50 Life Sciences Company

- 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

MetricStream

Monitoring Regulatory Changes

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



ComplianceOnline.com

Bloomberg

Complinet

LexisNexis

MetricStream

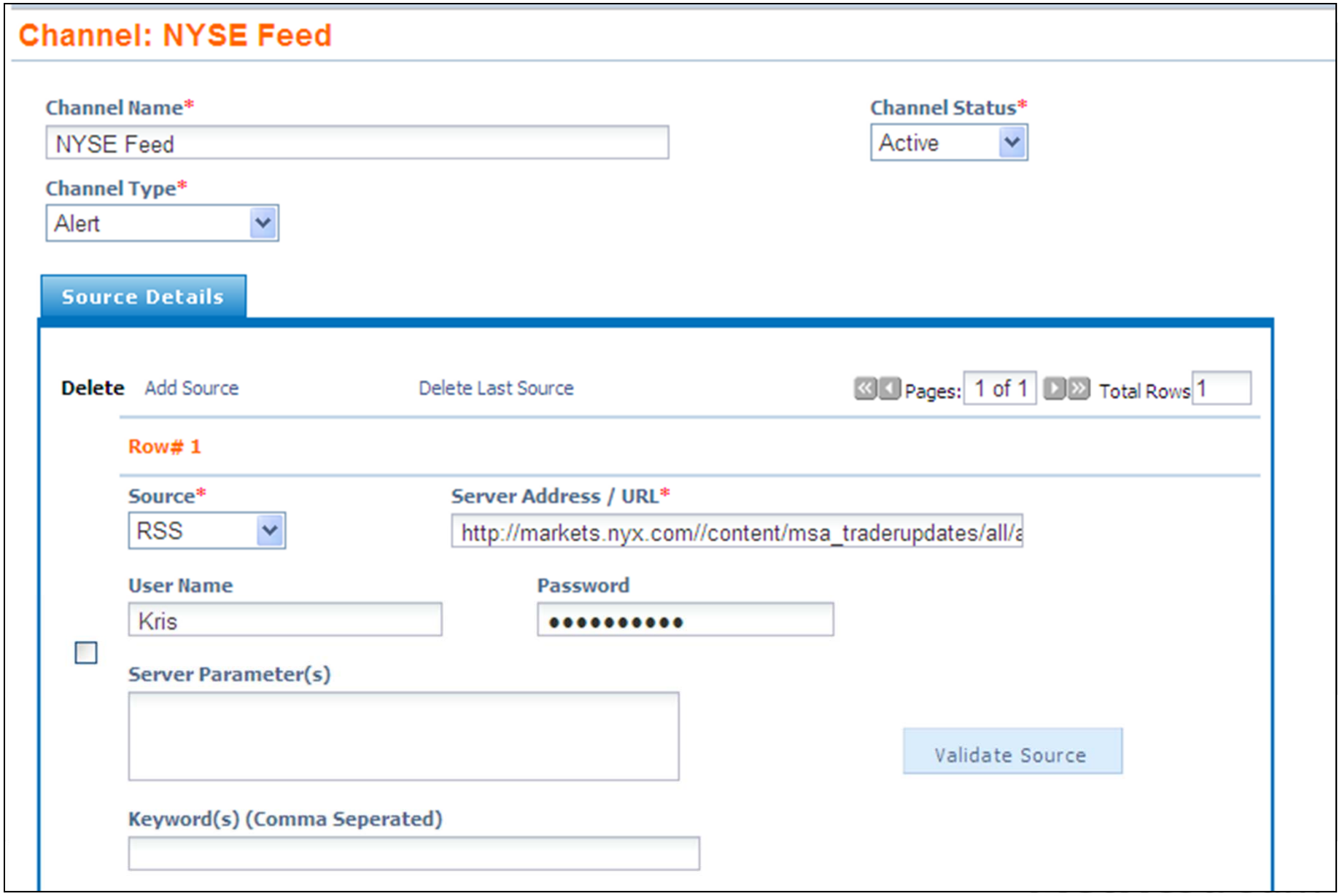
Case Study: Regulatory Monitoring

One of the Largest Banks in Europe

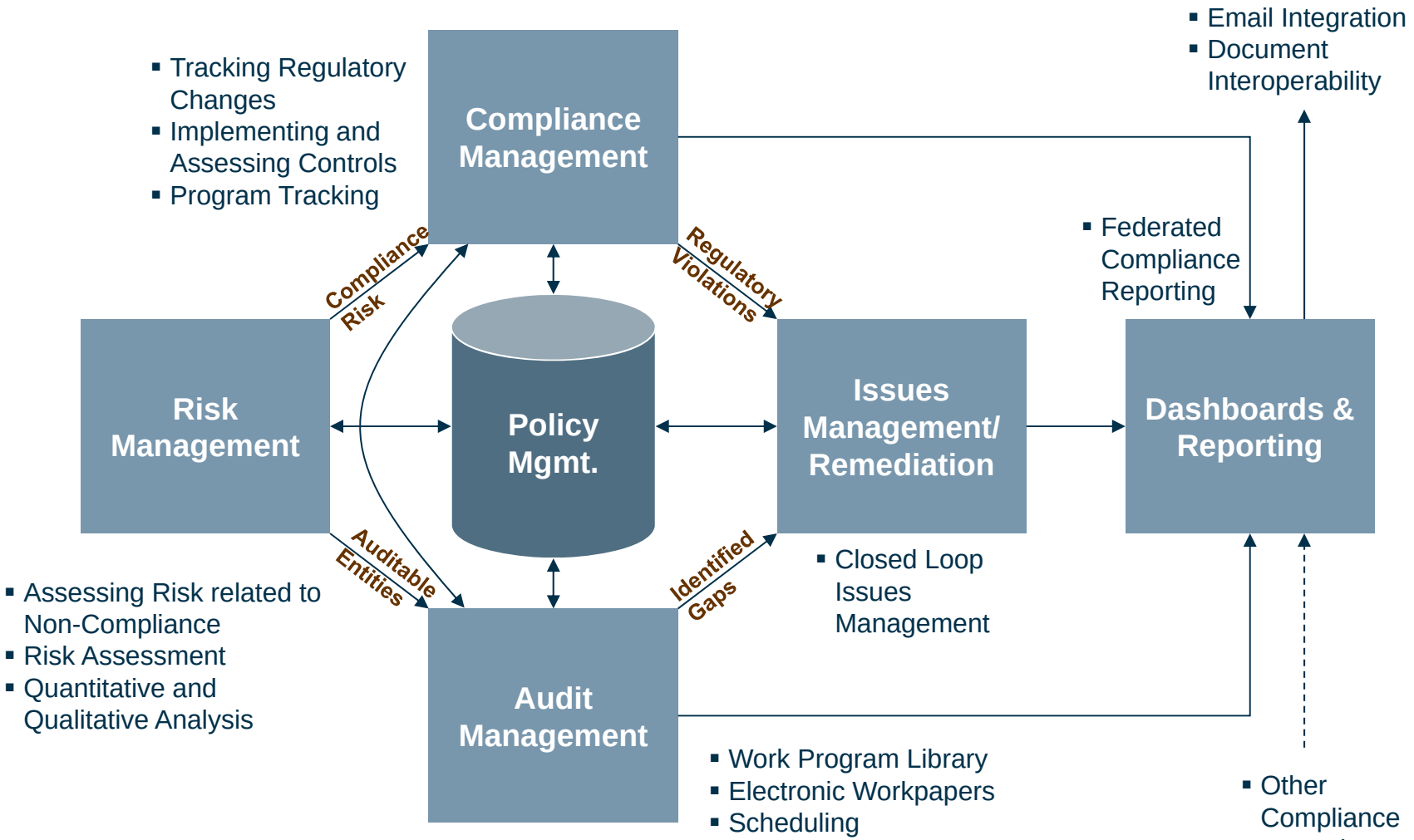
- Streamlined and simplified compliance by integrating risk assessments across countries, functions and processes
- Comprehensively assess and manage risks, establish and monitor controls and meet the demands of regulations across 80 countries
- Integration with external regulatory sources for risk intelligence

MetricStream

GRC Intelligence: Content Cloud

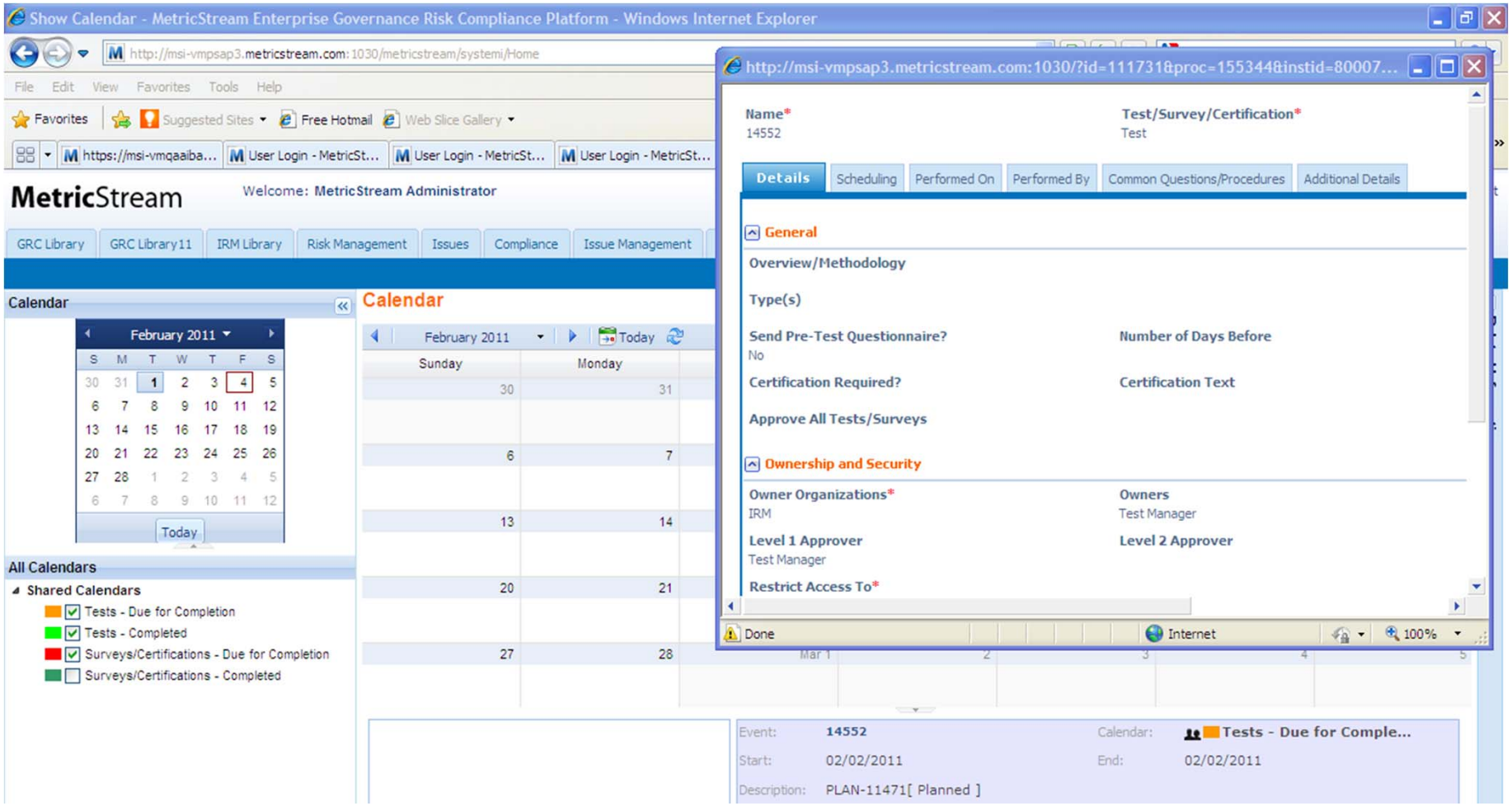


Enabling Collaboration Across GRC Functions



MetricStream

Enabling Collaboration: Calendar, Emails, Workflows



Compliance Survey Collaboration

MetricStream

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

MetricStream

Social Media Risk and Compliance Management

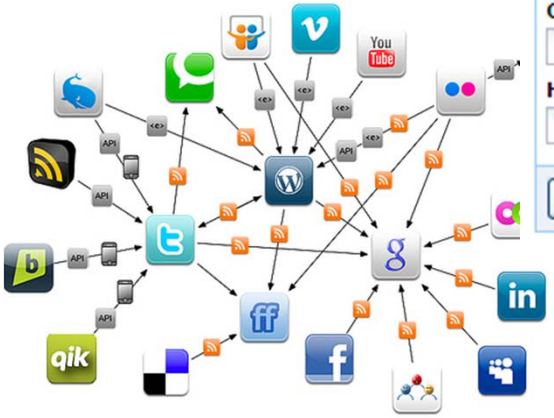
Security Intelligence Report

Tweet Text: Toner Posted By:

Submit | Clear All Load Preference

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 *
https://www.facebook.com/USAA

Config file *
/app/socialgrc/config/CEI.properties

Hadoop DFC root URL *
hdfs://node1.socialgrc.metricstream

Submit | Cancel

Edit Risk Analyzer Rules

Risk Name *
Select One

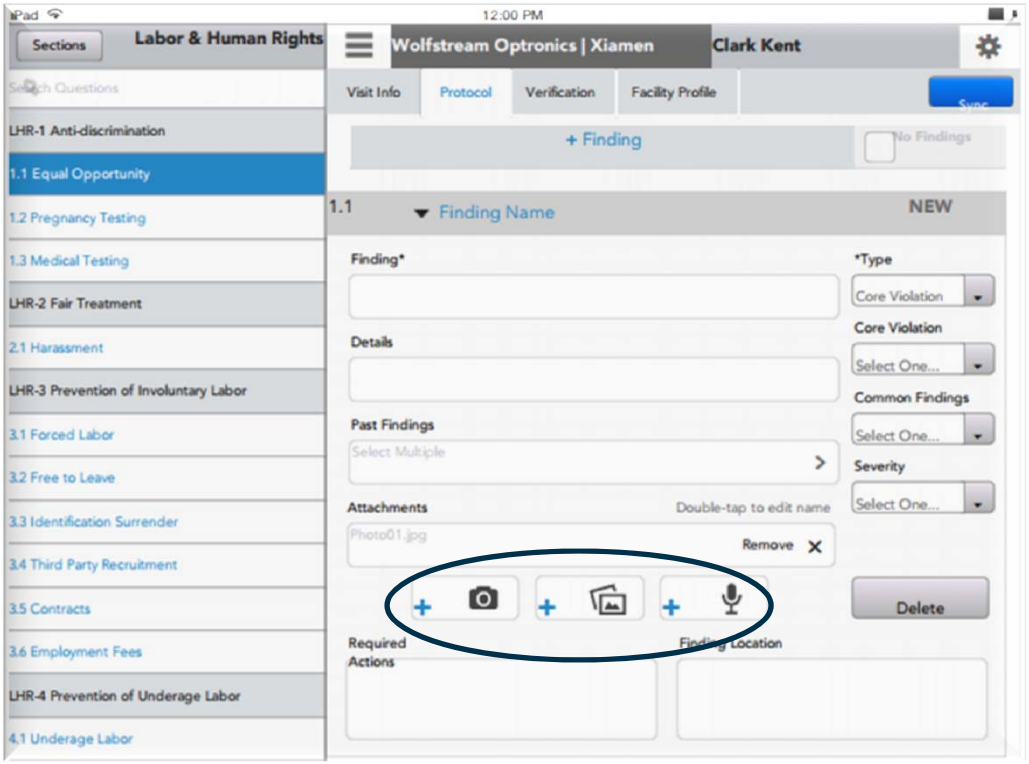
- Select One
- Financial Risk
- IP Loss
- Information Security Risk
- Infrastructure Stability Risk
- Lack of Governance
- Litigation Risk
- Metrics Integrity Risk
- Personal reputation Loss
- Regulatory Risk
- Reputation Risk
- Safety Risk
- Sensitive Data loss

Total Rows: 4 Pages: 1

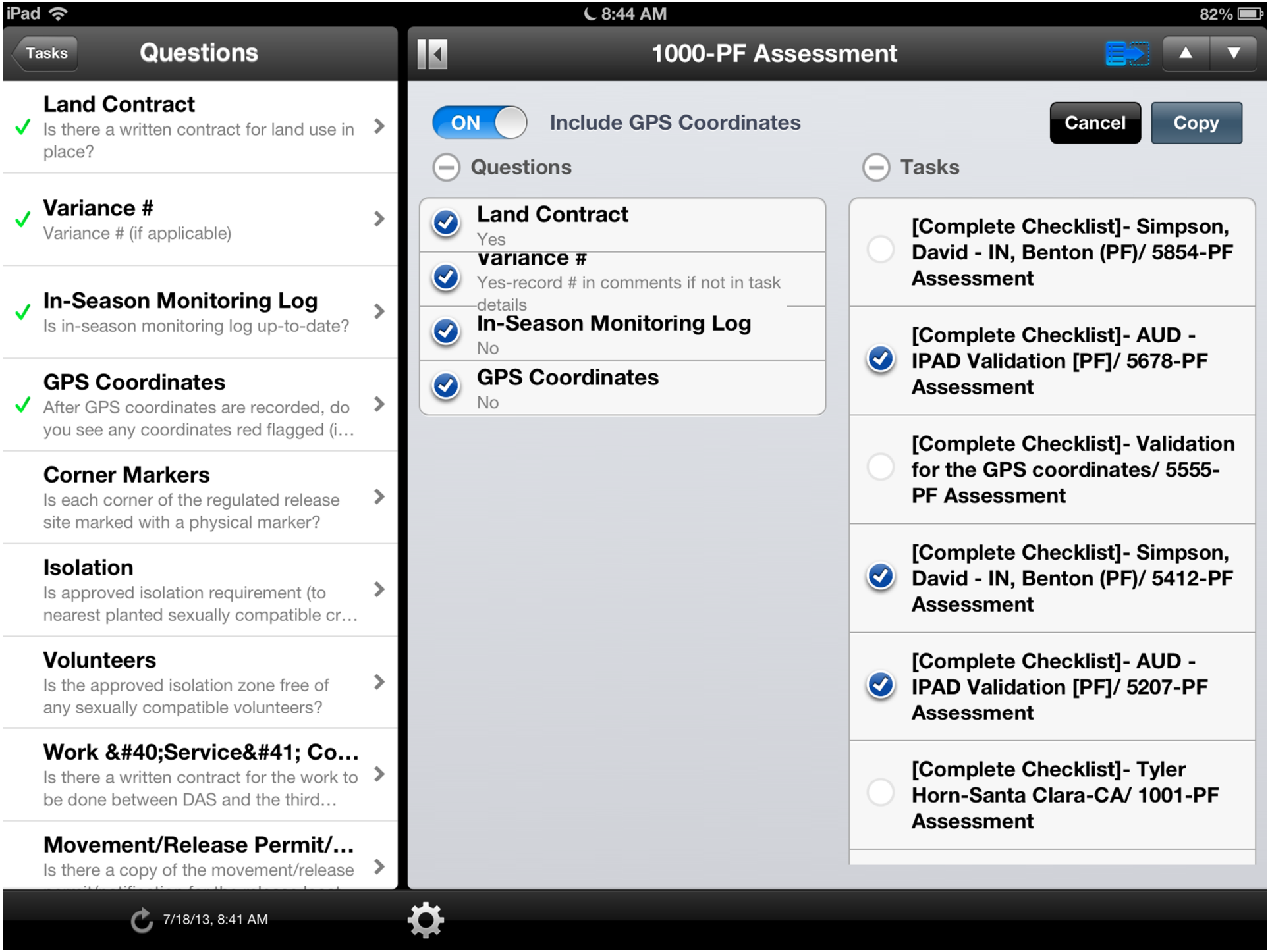
			Operation	Categories
			contains	UPSET_noun
			contains	UPSET_noun
			contains	LOSS_verb
	at least	2	contains	LOSS_verb

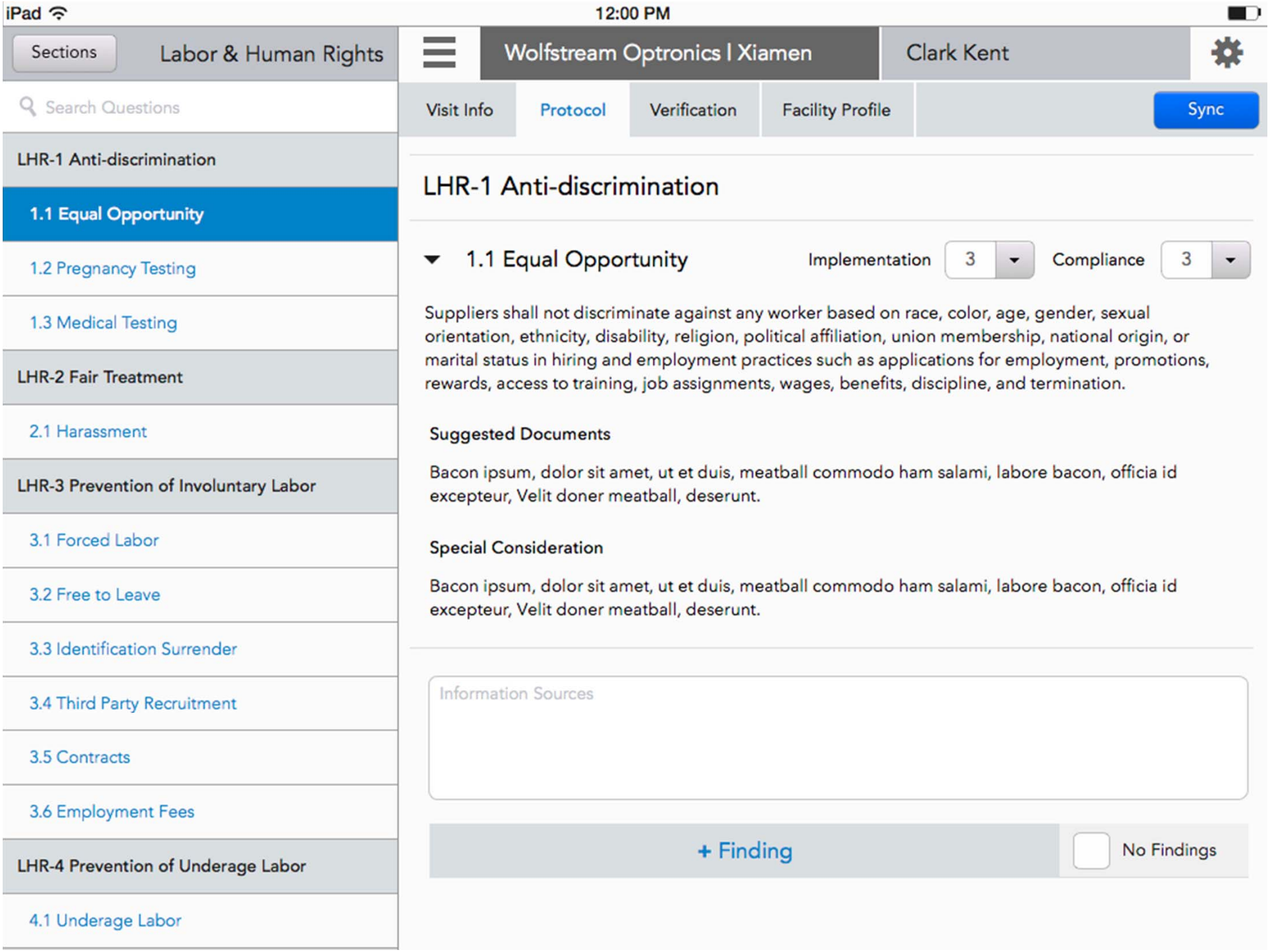
MetricStream

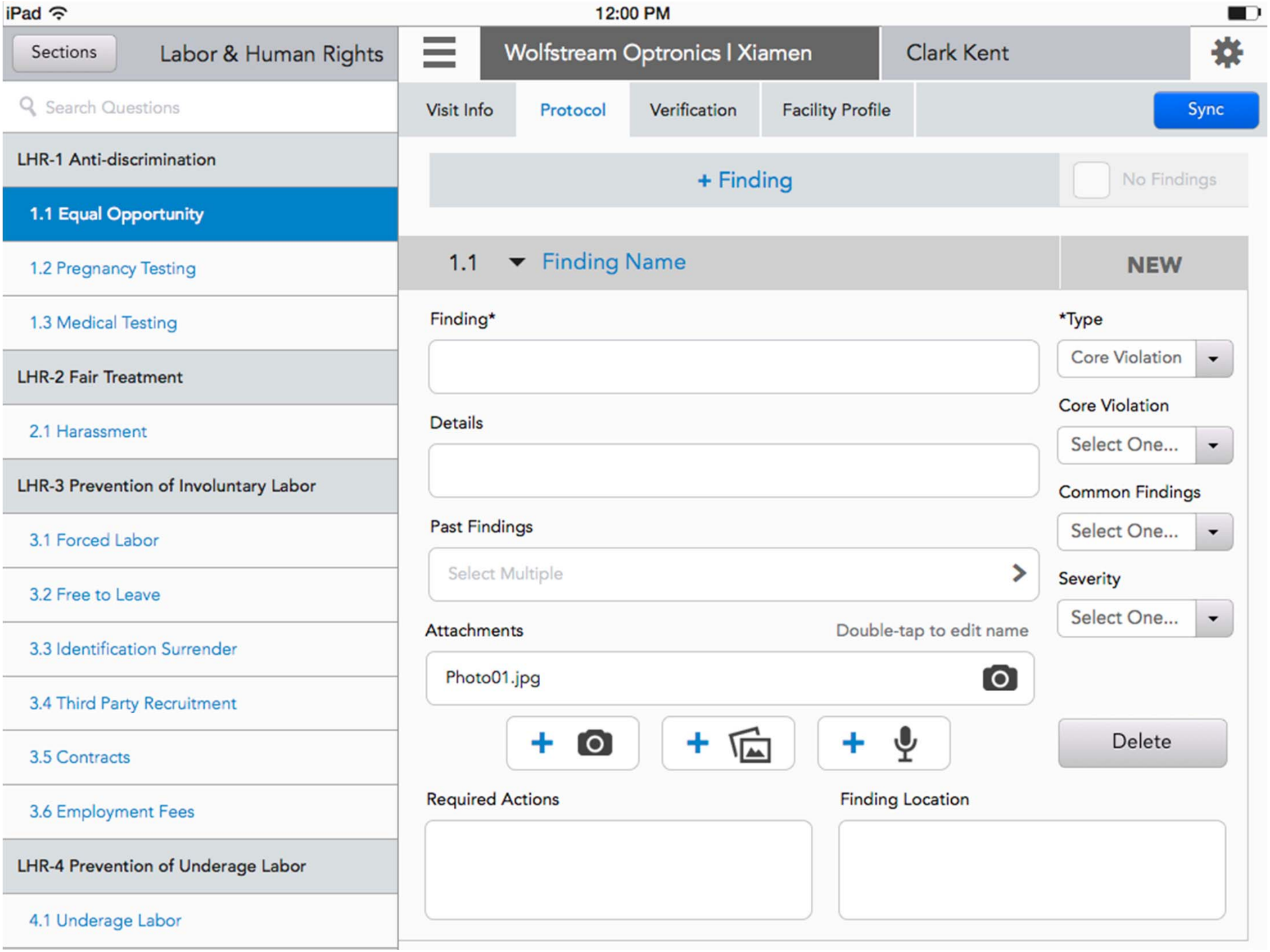
Leveraging Native Mobile Capabilities



MetricStream


iPad
8:44 AM
82%
Tasks
Questions
1000-PF Assessment
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
ON
Include GPS Coordinates
Cancel
Copy
Questions
Tasks
Land Contract
Yes
Variance #
Yes-record # in comments if not in task details
In-Season Monitoring Log
No
GPS Coordinates
No
[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
7/18/13, 8:41 AM


iPad
12:00 PM
Sections
Labor & Human Rights
Wolfstream Optronics I 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


iPad
12:00 PM
Sections
Labor & Human Rights
Wolfstream Optronics I 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
+ Finding
No Findings
1.1
Finding Name
NEW
Finding*
*Type
Core Violation
Core Violation
Select One...
Details
Common Findings
Select One...
Past Findings
Select Multiple
Severity
Select One...
Attachments
Double-tap to edit name
Photo01.jpg
Delete
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

MetricStream

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

MetricStream

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

MetricStream

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.

MetricStream

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

MetricStream

Thank you

MetricStream