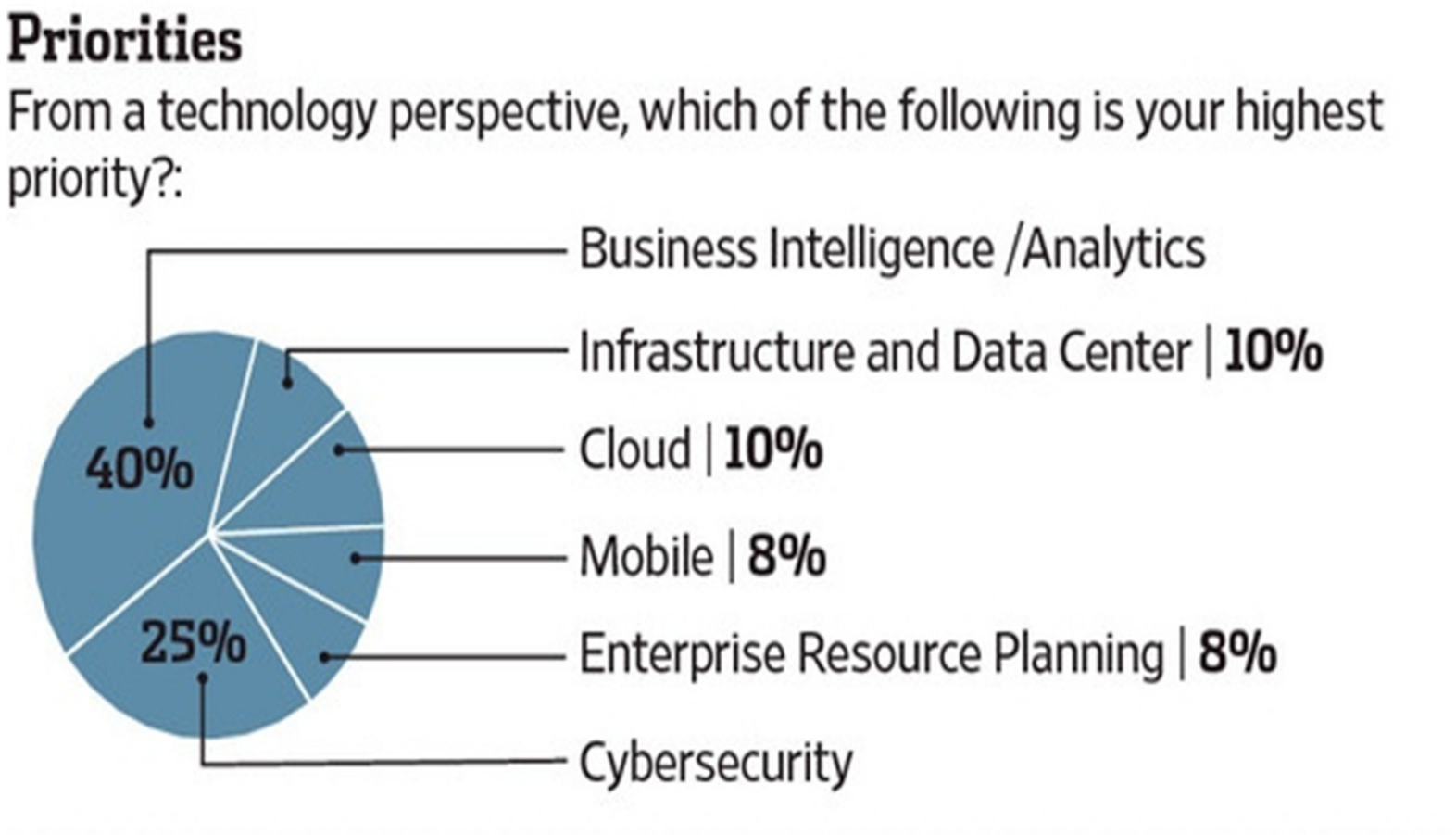
Metrics That Matter – Security Risk Analytics

Amad Fida, Founder and CEO - Brinqa

February 20th, 2014

ISACA
Trust in, and value from, information systems
Denver Chapter

What Matters to CIOs?



http://online.wsj.com/news/articles/SB10001424052702304680904579364641778947268?mod=ITP_journalreport_0

Lack of Communication Regarding Security Risk

September, 2013 - Tripwire, Inc., released results from an extensive study focused on the state of risk-based security management with the Ponemon Institute. Key findings from the survey include:

- 64% said they don't communicate security risk with senior executives or only communicate when a serious security risk is revealed
- 47% said that collaboration between security risk management and business is poor, nonexistent, or adversarial
- 51% rated their communication of relevant security risks to executives as "not effective."
- When asked why communicating relevant security risks to executives was not effective:
  - 68% of the respondents said communications are too siloed.
  - 61% said communication occurs at too low a level.
  - 61% aid the information is too technical to be understood by non-technical management.
  - 59% said negative facts are filtered before being disclosed to senior executives and the CEO

http://www.prweb.com/releases/2013/9/prweb11095496.htm

Analytics is the process of **Signal** Detection

"You gotta help me stop looking up stuff I don't actually care about."

The Signal and The Noise

Data are neither signal nor noise - data are merely facts. When facts are useful they serve as signals. When they aren't useful, data clutter the environment with distracting noise.

For data to be useful, they must:

- Address something that matters
- Promote understanding
- Provide an opportunity for action to achieve or maintain a desired state

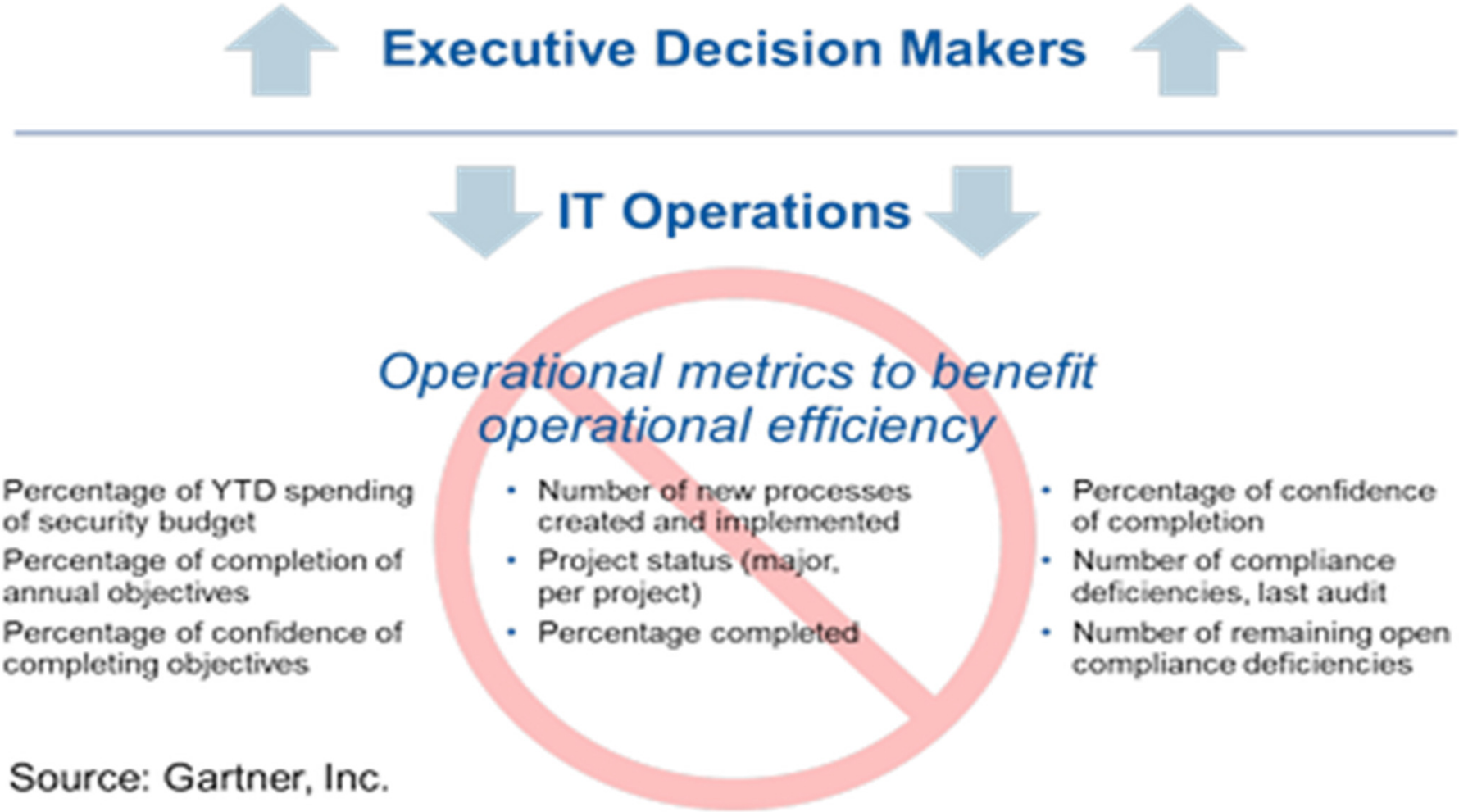
Without these qualities, data is noise.

Why Do We Need Security Risk Analytics?

A common request from the leadership is to report on metrics from various areas that point out which businesses, processes, or systems are most at risk and require immediate attention.

- Risk reporting based on business context
- Compliance is no longer the driver
- Risk prioritization rather than risk elimination
- Big data and automation

Operational Metrics are NOT Risk Metrics

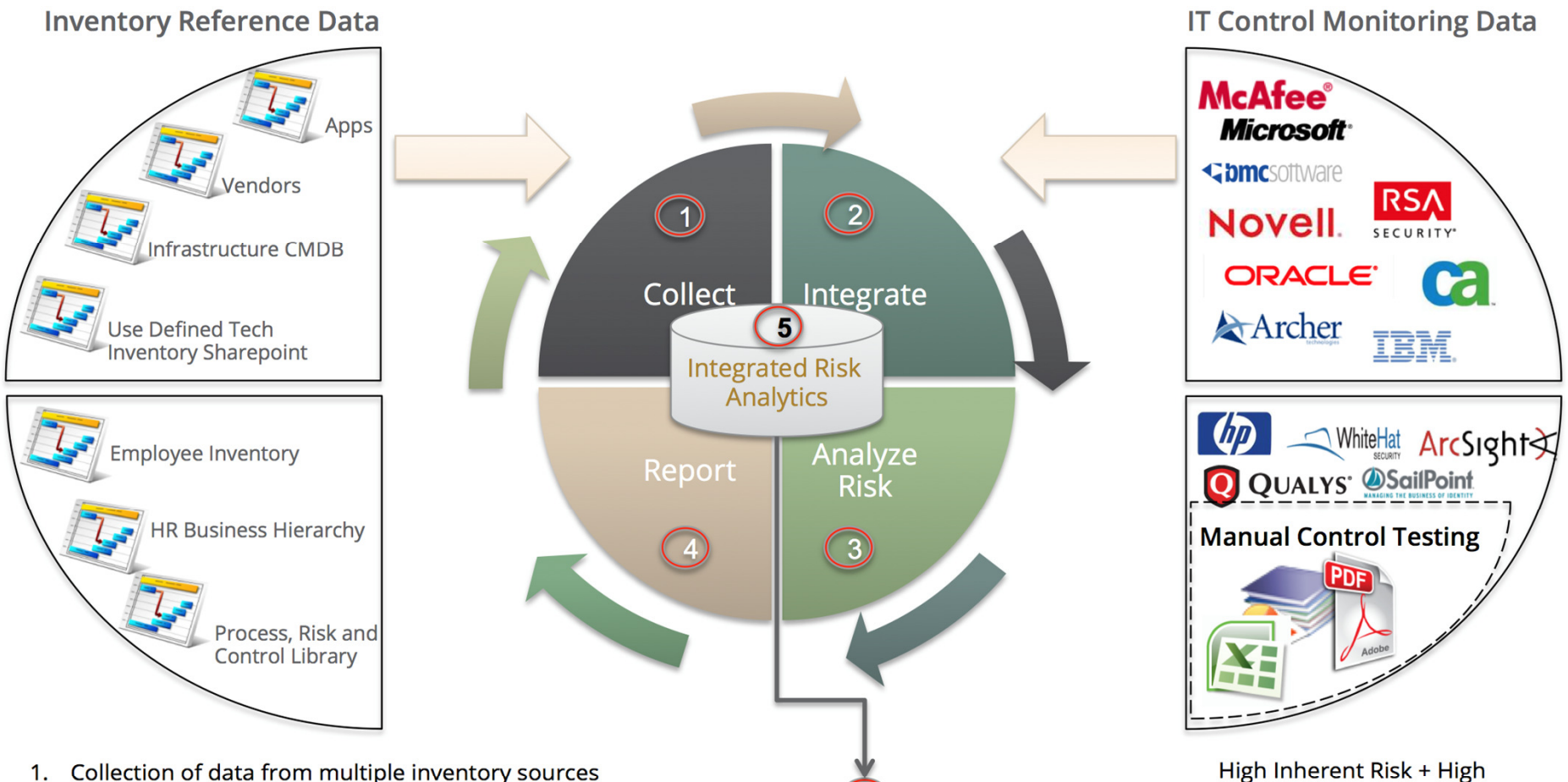


Key Challenges

Key Challenges In Implementing Risk Analytics

- Varied and disparate risk inventories
  - » Uncorrelated and redundant data included in reporting
  - » Prohibits establishing a common inherent risk inventory
  - » No historical data for trending and forecasting
- Manual and inconsistent data aggregation and correlation
  - » Ambiguous and incomplete risk interpretation
  - » Resource and time intensive
- Subjective and non-standard risk measurement
  - » Resources spent addressing non-prioritized issues
  - » Miscommunication and misunderstanding of risk across enterprise
- Operational teams lack understanding of business outcomes
  - » Limits business unit's ability to understand and accept risk
  - » Inability to measure improvements and predict threats
  - » Reactive vs. proactive decision making

Technology Risk Analytics Use Case



1. Collection of data from multiple inventory sources
2. Integration of enterprise-wide control data and manual controls (i.e.,SOC, IT SOX control)
3. Automated risk ranking process
4. Formulate report data into the integrated risk assessment warehouse (central version of the truth)
5. Automatic processing of assessment, analytics, and calculation metrics (prioritize risk, predictive analysis, business intelligence)
6. Produce output to information consumers (e.g. Risk Officers sees patch levels for apps/business)

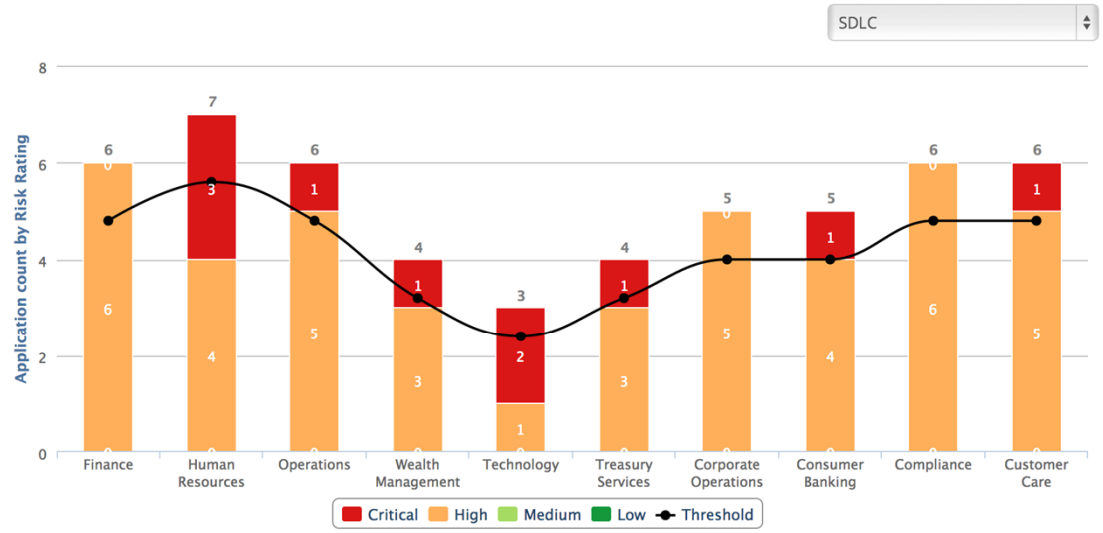
6 Information Consumers

High Inherent Risk + High Risk Control = High Residual Risk (to be escalated)

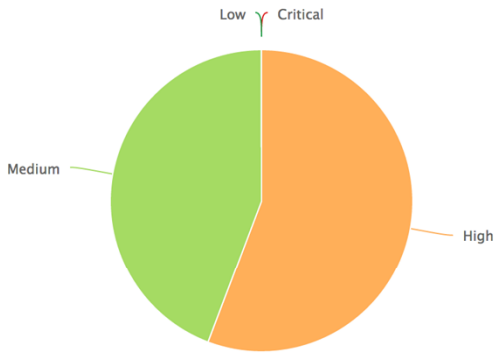
- GRC
- SIROs
- IT Reports
- Information Risk Management
- Other reports

Context Based Security Risk Metrics

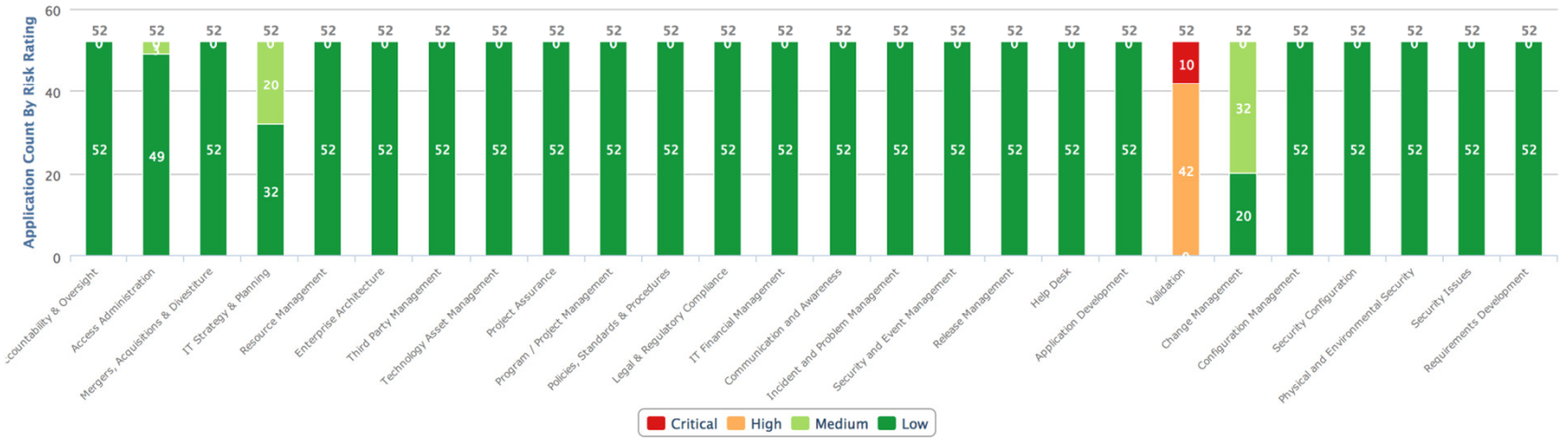
Application Risk By Business



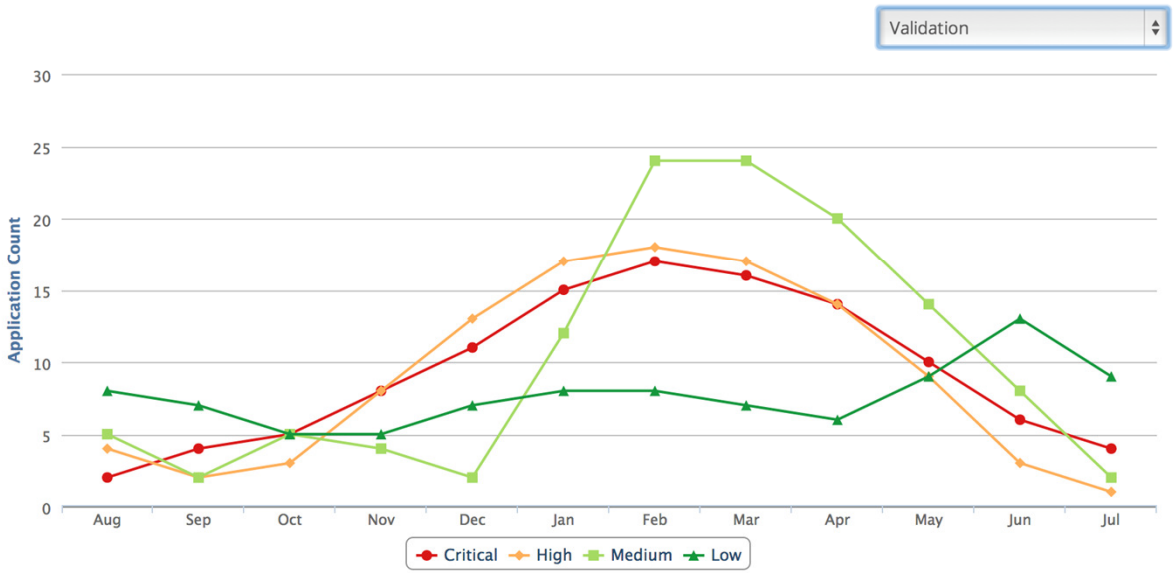
Overall Application Risk Status



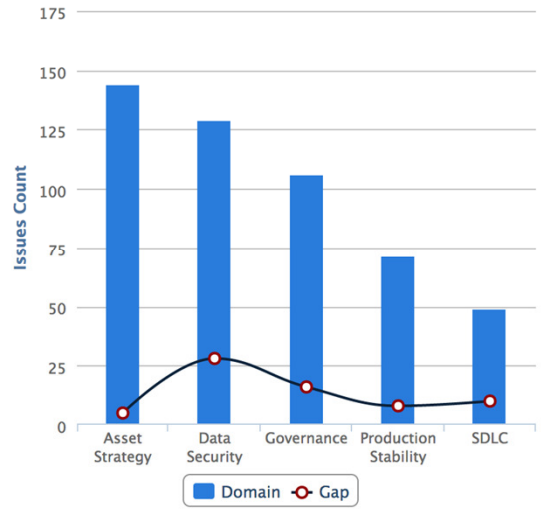
Application Risk By Topic



Application Risk Trend

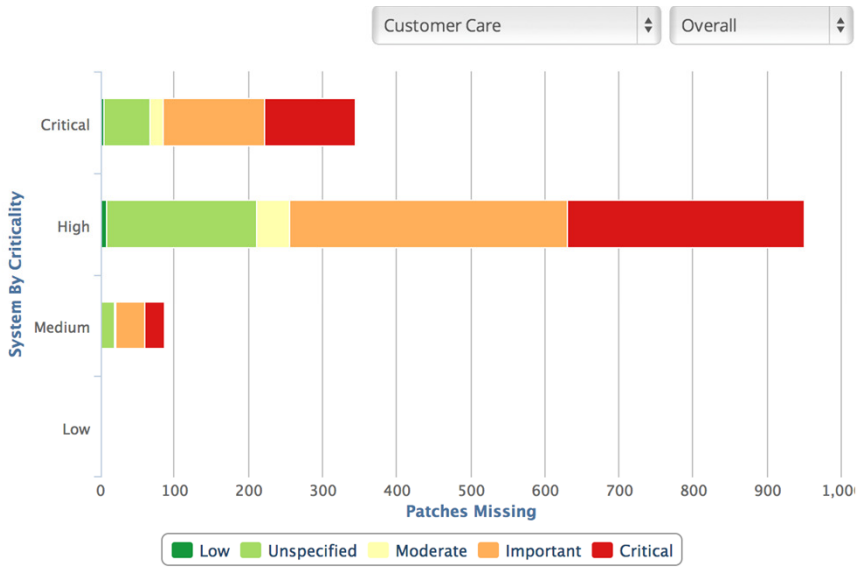


Issues By Domain and Gap

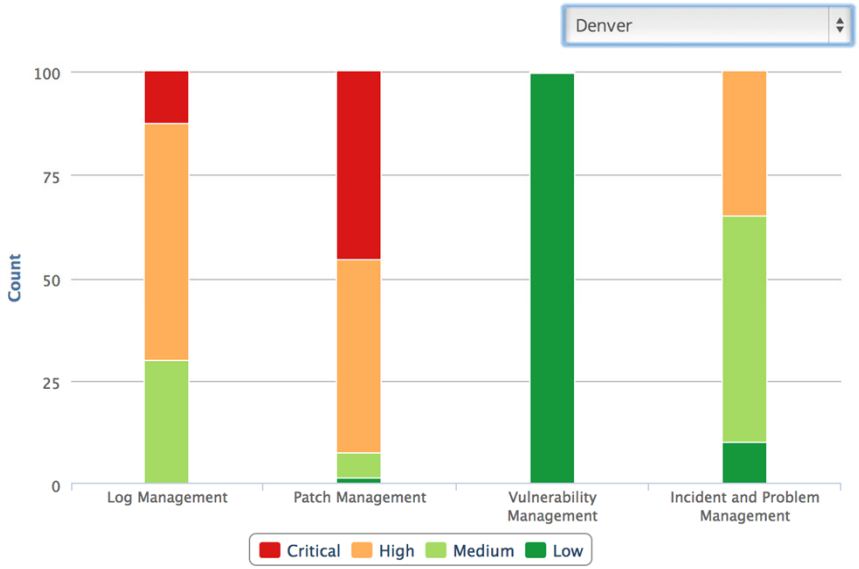


2	295	nyginwebp4.us.xyz.com	18.18%
Non-certified Accounts on Critical Database	Critical Vulnerabilities older than 90 days	Most Impacted Server	Sensitive Database with Critical Vulnerabilities

Systems with Known Missing Patches



System Issues by Datacenter



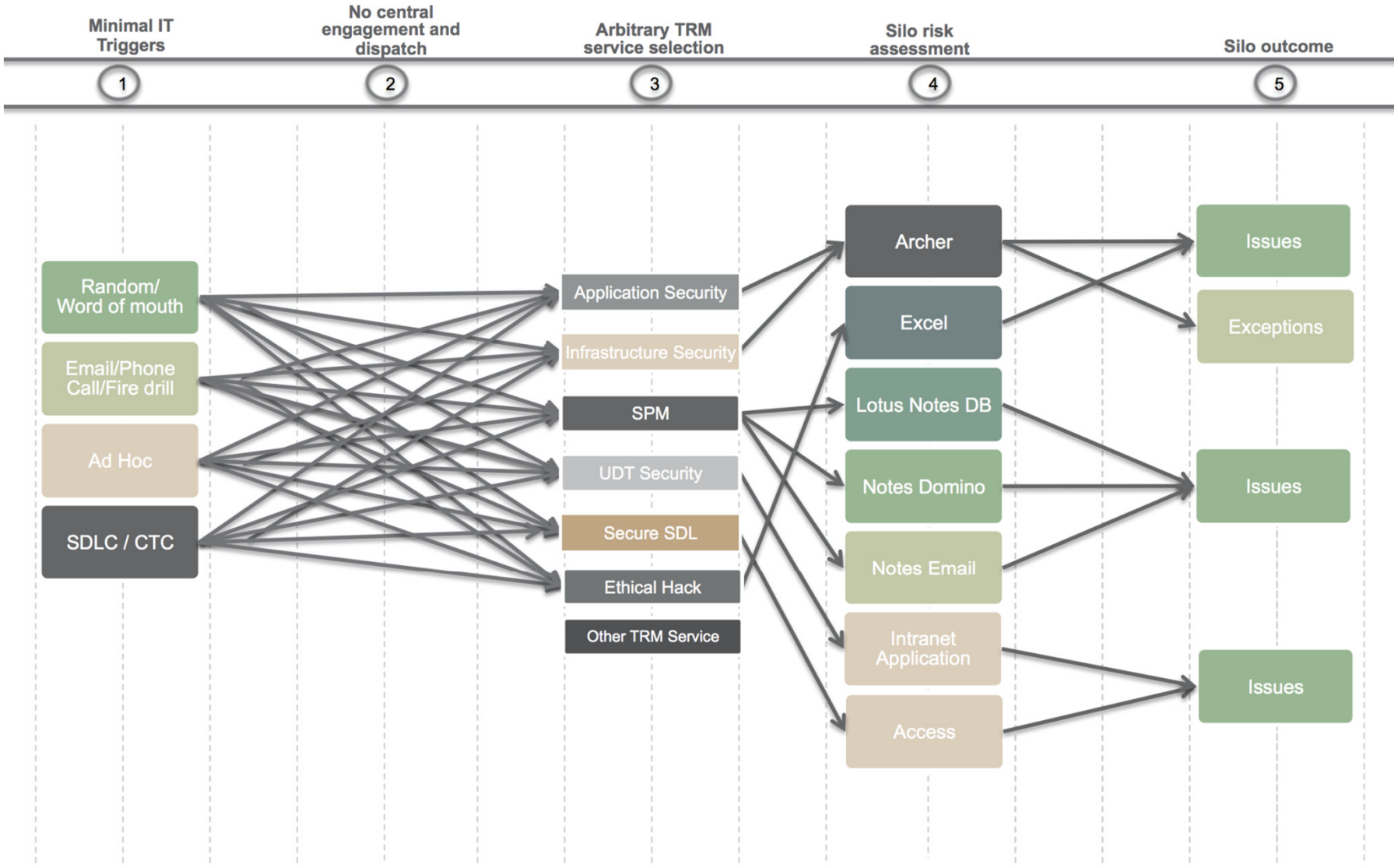
Customer Case Study

World's Largest Deposit Bank - Challenges

Technology Risk Management (TRM) group was utilizing multiple tools and processes to support TRM deliverables. The previous state was not intuitive for non-TRM users, produces redundant efforts, and expends resources on lower criticality projects/applications/infrastructure. Specific examples included:

1. Inability to provide businesses with repeatable risk metrics
2. Inability to provide actionable remediation plans with accountable and responsible parties
3. Inaccurate IT inventories make it difficult to understand the environment
4. Lack of standardized triggers/gates/hooks for someone to be pointed to TRM
5. Lack of centralized decision making process to determine what gets assessed and what gets deferred
6. 21 TRM assessments/services result in overlapping and non-applicable control testing
7. Assessments not looking at all available data

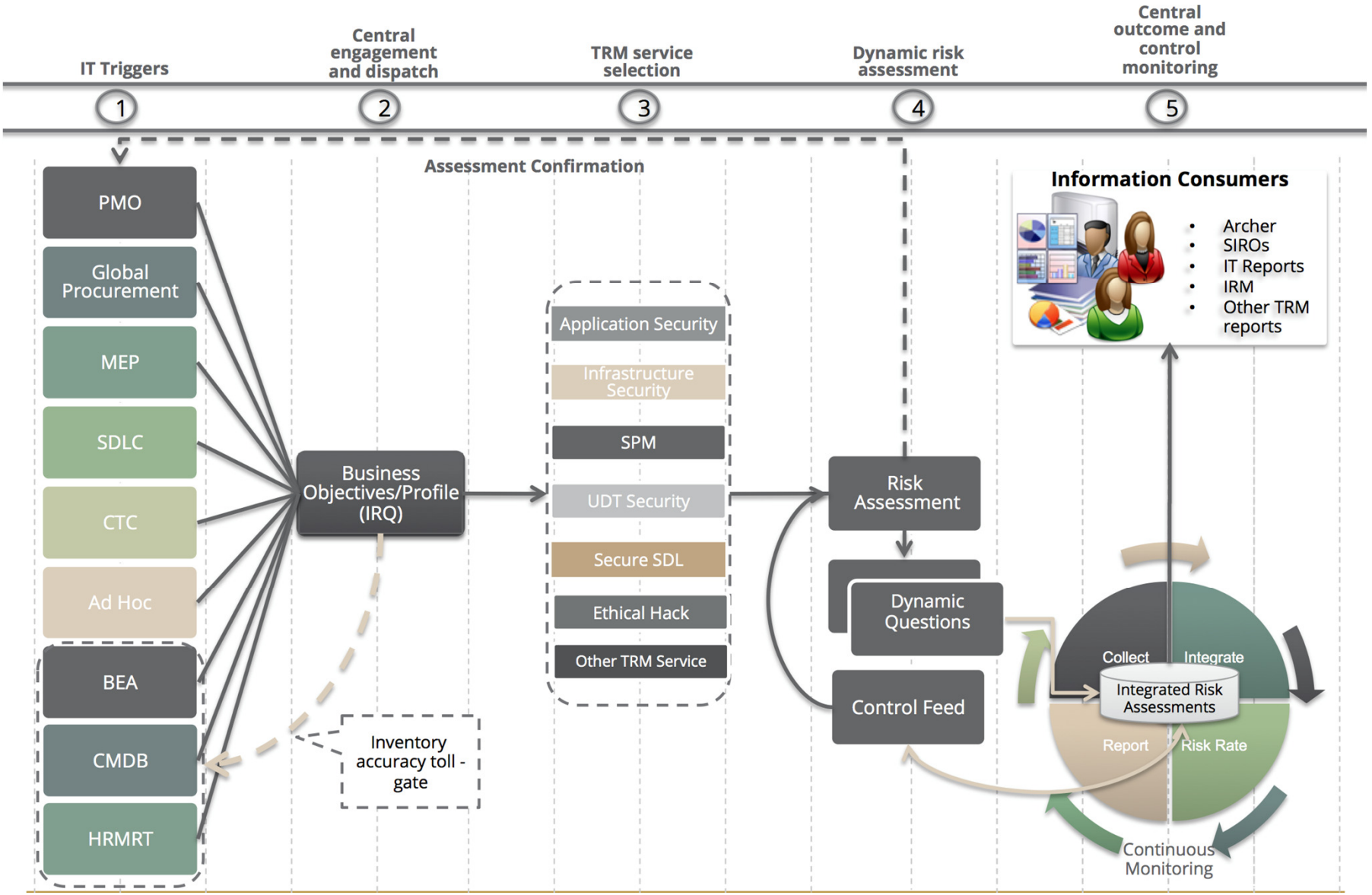
Without Risk Analytics



Solution

1. Leverage up to date IT inventories and collaborate with IT to improve quality
2. Create a standardized process for everyone to engage TRM
3. Create a centralized decision making process to determine what gets assessed and what gets deferred
4. Streamline 21 assessments/services to avoid overlapping and out of scope questions
5. Leverage IT monitoring tools to validate risk assessment answers and enable near-time visibility of IT controls
6. Use a centralized technology risk assessment repository to reduce complexity, improve operational efficiency, and focus remediation expenditures
7. Load historical risk assessment data into the centralized risk assessment repository

With Risk Analytics

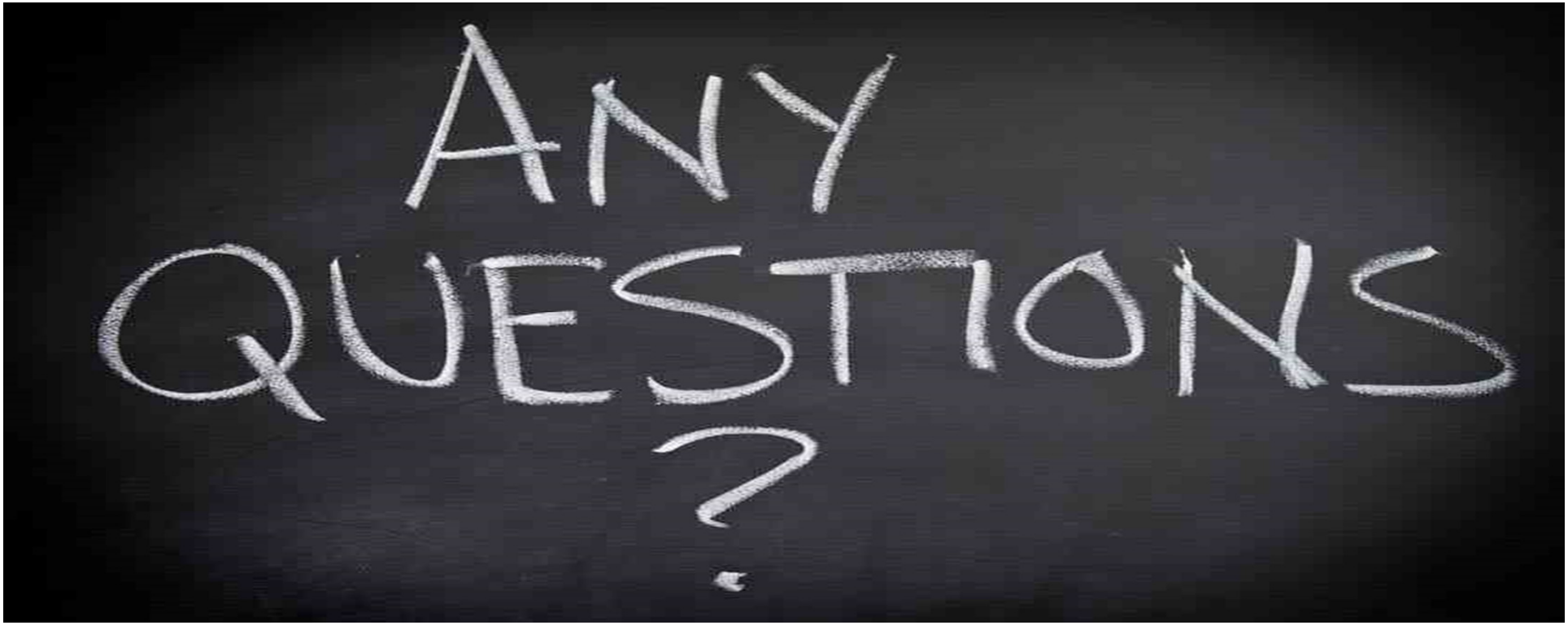


Benefits

1. Standardized, streamlined, and centralized TRM processes to improve consistency
2. Facilitated TRM collaboration between different groups for better decision making.
3. Incorporated data from existing IT Controls (e.g. patch management, DLP, etc.)
4. Achieved sustainable constant monitoring of current technology risks for the enterprise, not just one time assessments (e.g., 24-hour risk reporting cycle similar to Market and Ops Risk)
5. Provided granular self service view/pivot of technology risk information for a department, business unit, and entire enterprise
6. Historical and predictive technology risk simulations using customer's data in context

About Brinqa

Brinqa provides an operational risk analytics platform for aggregation, correlation, analysis and reporting of risk data in heterogeneous environments. The solution delivers insightful analysis and intelligent reporting for informed decisions and improved operational effectiveness.



Contact Information:

Amad Fida – Founder and CEO
afida@brinqa.com
Katy Loughney – Director of Risk Analytics, West
kloughney@brinqa.com