#SHAREorg

SHARE
Technology · Connections · Results

Security Intelligence, Audit and Compliance for the Mainframe

Rich Skinner, CISSP
Brinqa
Director of Risk Analytics & Big Data
rskinner@brinqa.com

August 15, 2013
Session: 13722

SHARE in Boston

Agenda

- Today's Security Landscape
- Challenges on Enterprise Security, Risk
- Metrics, Measurements, and Showing Value
- Case Studies
- Mainframe = Holy Grail, Fort Knox
- zEnterprise Security Benefits
  - Intelligence, Audit, and Compliance
- Q&A

2 Key Points from Rich's Mainframe Security experience

- 1. zEnterprise is the most **SECURABLE** platform in the World
  - Have to set it up properly
  - Have to continuously monitor and audit
  - Only as strong as the weakest link

- 2. Leveraging zEnterprise for a Security, Risk Center can help reduce Enterprise Risk
  - Highest security certified system in the commercial space
  - Designed and architected for TRUSTED business use over 40+ Years

2013 Security, Risk Landscape

SHARE
Technology · Connections · Results

RSA CONFERENCE | Where The World Talks Security

FINANCIAL SERVICES | Information Sharing and Analysis Center

SC CONGRESS

EDUCAUSE

Gartner Summits

black hat

ISACA®
Trust in, and value from, information systems

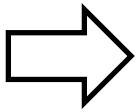
Pulse Protect: The IBM Security Forum
Pulse2013
Optimizing the World's Infrastructure
March 3 – 6
MGM Grand – Las Vegas, NV

IBM System z Security Conference

VANGUARD
SECURITY & COMPLIANCE 2013 | SECURE YOUR ENTERPRISE at

Current State of Risk 'Intelligence'

Cause	Effect
Manual and Inconsistent data collection	**Ambiguous and unreliable interpretation of risk**
No central risk repository or historical data	**Uncorrelated and redundant data included in risk analysis**
Subjective risk measurement and prioritization	**Valuable time and resources wasted addressing non-critical risks**
Lack of business context and no holistic view of risk	**Inability to measure improvements and predict threats**



How to improve Intelligence = Analytics

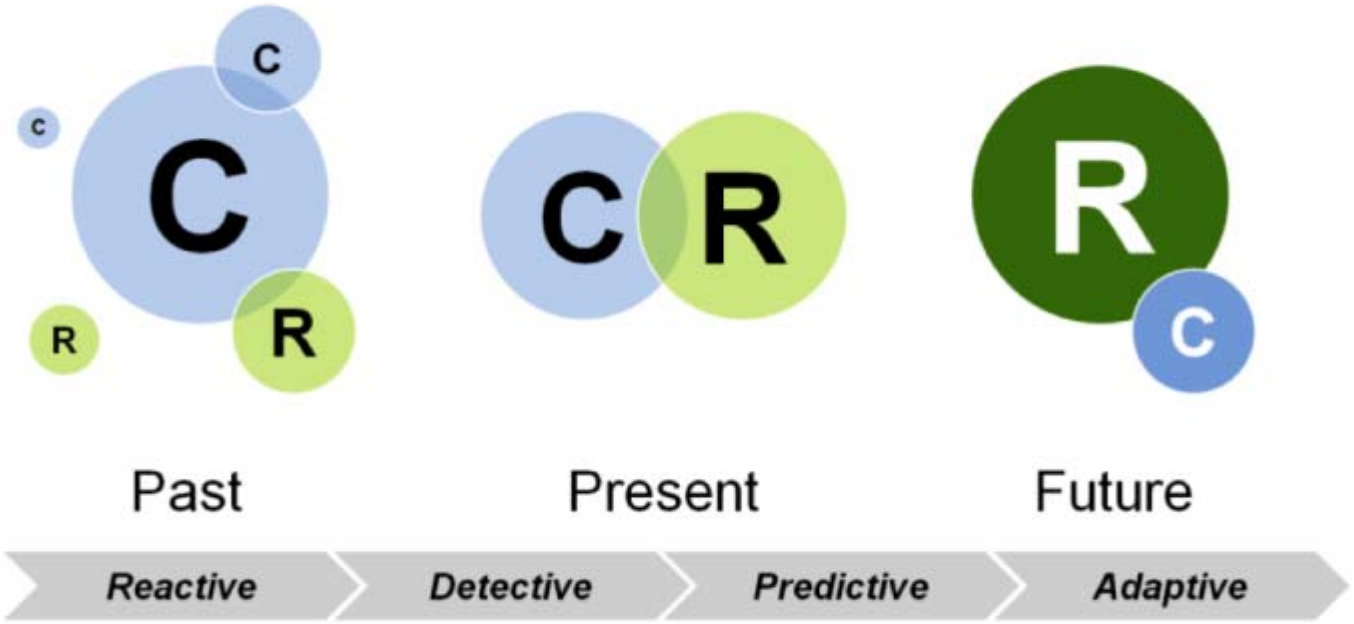
What Is “Analytics”?

Analytics *is the discovery and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistic, computer programming and operations research to quantify performance*.

http://en.wikipedia.org/wiki/Analytics

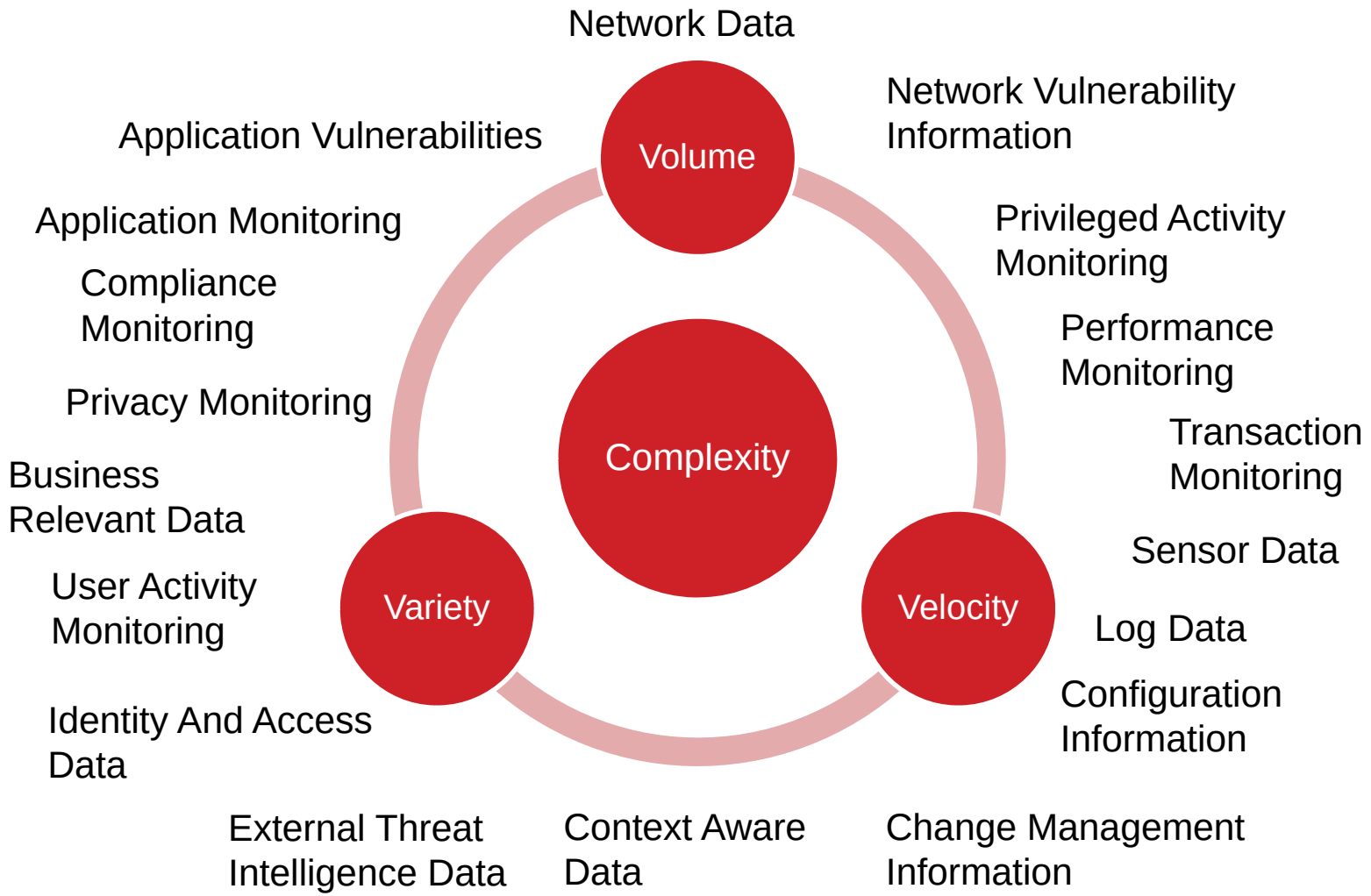
Why Do You Need Risk Analytics?

Compliance Is No Longer the Driver. Risk.



Source: 2013 Gartner

Info Security HAS a Risk Analytics Problem



2013 Global CIO Top 10 Technologies

CIO Technologies	Ranking of technologies CIOs selected as one of their top five priorities in 2013.				
Ranking	**2013**	**2012**	**2011**	**2010**	**2009**
Analytics and business intelligence	1	1	5	5	1
Mobile technologies	2	2	3	6	12
Cloud computing (SaaS, IaaS, PaaS)	3	3	1	2	16
Collaboration technologies (workflow)	4	4	8	11	5
Legacy modernization	5	6	7	15	4
IT management	6	7	4	10	*
CRM	7	8	18	*	*
Virtualization	8	5	2	1	3
Security	9	10	12	9	8
ERP applications	10	9	13	14	2

* Not an option in that year

5 Macro Trends 2013

Security & Risk Professionals Should Focus on 5 Macro Trends

1. The data economy will ensure the dominance of data-centric security
2. **Analytics will help you better predict threats and protect your data**
3. Human elements will drive security re-orgs, training and outsourcing
4. S&R leaders will play a bigger role in customer experience
5. Business resilience is taking on broader corporate implications – security risk, IT failures, data corruption, etc.

Source: 2013 Top Trends to Watch**, Forrester, Inc**.

Risk Analytics + zEnterprise?

brinqa

- Enterprise Risk and Security Analytics
- “Big Data” Platform

- Data Aggregation and Correlation
- Context Aware Risk Models
- Dynamic Dashboards

+

IBM

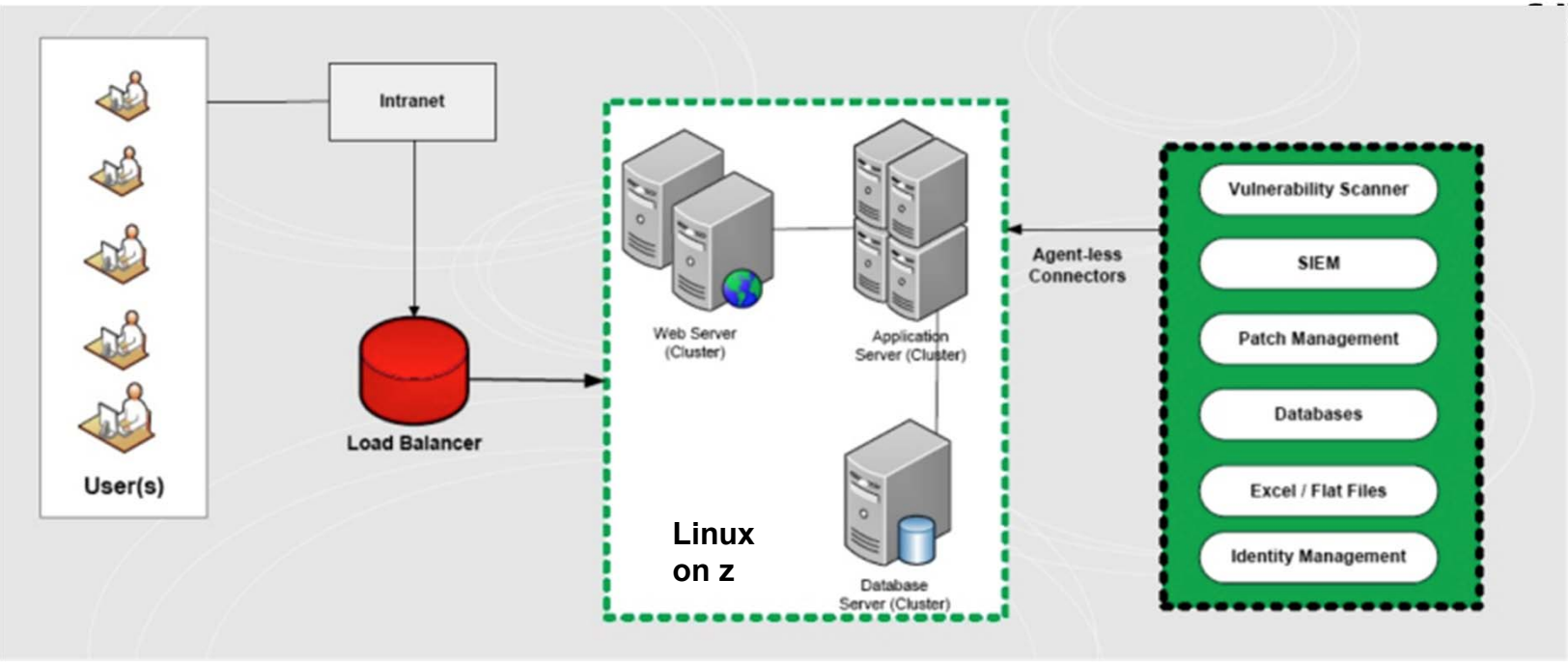
=

IBM Poughkeepsie Linux on z Benchmark Test

- Goals
  - Prove the Brinqa Risk Analytics Platform will deliver mainframe-class results natively
  - Performance of ‘Big Data’ / NoSQL Database
    - Natively on Linux on z. (neo4j)
  - 1 – 6 Million Components Analyzed

- Environment:
  - zEnterprise EC12 2827-HA1
  - 2 CPs, 1 zVM LPAR, 16 GB Memory

Sample Implementation Model

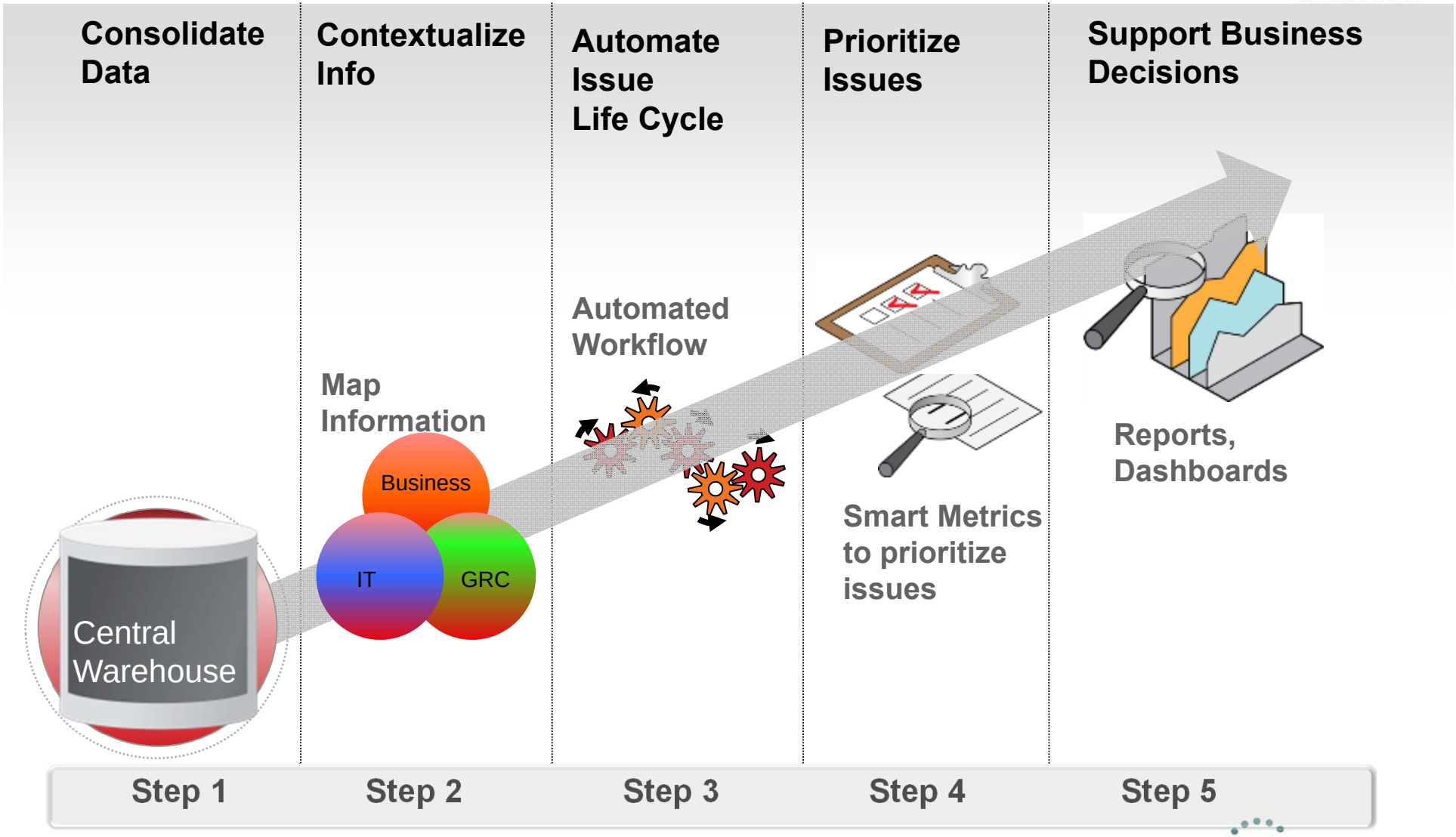


- A clustered web server load balanced using a load-balanced router. The web, app and database servers can be deployed on Linux on z or zOS
- A clustered application server on which Brinqa is deployed
- Brinqa can be deployed on a complete IBM Stack
  - Operating System – *Linux on z, zOS, or AIX*
  - Application Server – *WebSphere v7+*
  - Database – *DB2*

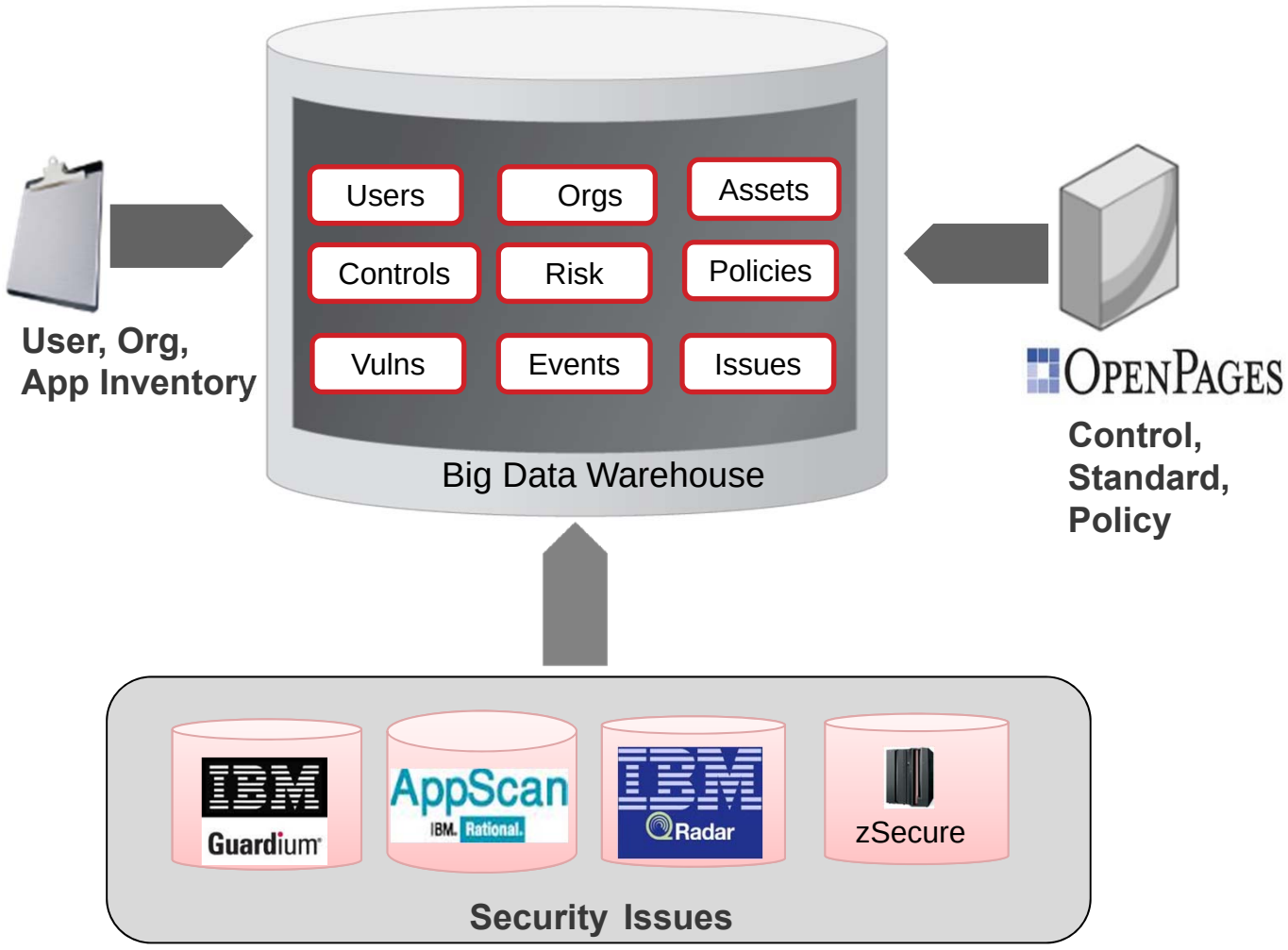
Results and the Future is Bright!

- **Results:**
  - Analytics Platform and NoSQL Database Performed Beyond Expectations
  - **400% Improvement** in Performance over previous distributed environments!
  - Less than 30mins on zEnterprise compared to 2 hours for Analytics Processing on Distributed
  - Allows analytical models to run in near real-time compared to batch
- **Future Testing**
  - Scale the amount of concurrent USERS to over 500
  - zOS Performance
- **Future Activities**
  - Working Closely with IBM on Webcasts, Sales & Marketing Activities, Conference Presentations, Magazine Articles
  - Welcome Future Engagements with the Mainframe NY Community

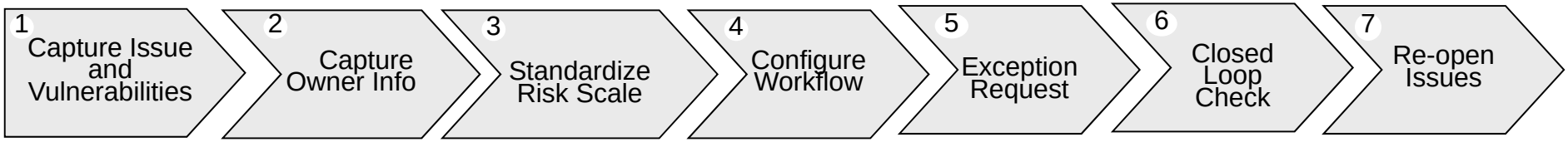
Sample Risk Methodology



Consolidate & Contextualize Data



Step 3 - Issue Lifecycle



- Import issues and vulnerability data from various system using connectors

- Use the HR Hierarchy to capture manager chain
- Use HR info to contact owner
- Capture manager details for escalations
- Obtain job titles and discuss logical role groupings

- Create standard risk scale (e.g. HML, CHMLI)
- Map all issue severity / priorities to the standard risk scale

- Configure issue lifecycle workflow for data source/ Department
- Configure email templates
- Configure escalation and notification rules
- Launch issue lifecycle workflow

- Configure exception request workflow
- Approval chain by risk scale
- Map exception to **Policies** imported

- Monitor issue in system
- If issue closed validate with source data collected from target system
- Reinitiate issue workflow after exception duration exceeded

- Reinitiate issue workflow after exception duration exceeded
- Re-open issues if closed loop check fails

Step 3 – System Metrics

Metric	Parameters	Calculation	Indicator
% of Critical Apps/ Assets	• Count of critical applications • Vuln count • Business criticality – weight between 1 - 5	(Vulns/ Total Apps) * Criticality)/ Weighted Average)* 100	
Issue count by LOB Owner	• Issues captured from various security system • Org Hierarchy	Issue lookup based on Org Hierarchy	
Mean time to mitigate	Detection date , mitigate date	**Σ (**Date of mitigation – Date of Detection) / Count (Mitigated issues)	
% of system with known issues	• Count of systems • Count of issues / problems	(Count(Systems without known Issues) / Count of scanned systems)* 100	
Mean cost to mitigate	• Hours required to mitigate • Hourly rate of an employee • Other mitigation costs • Mitigated count	**Σ** (Hours to mitigate*Hourly Rate+ Other mitigation cost) / Count (Issues)	
% of system mitigated	• Systems with mitigated issues • Total number of systems • Other mitigation costs • Mitigated count	**Σ** (Hours to mitigate*Hourly Rate+ Other mitigation cost) / Count (Issues)	

Step 4 - Risk Prioritization Example

Mainframe Security Risk Analytics = Business Context, End to End Process Scoring, Reporting, Trends, Analysis

Mainframe Security, Auditing (zSecure)

Database Monitoring (Guardium)

SIEM (qRadar)

zEnterprise Infrastructure

RACF, ACF2, TopSecret

DB2, IMS

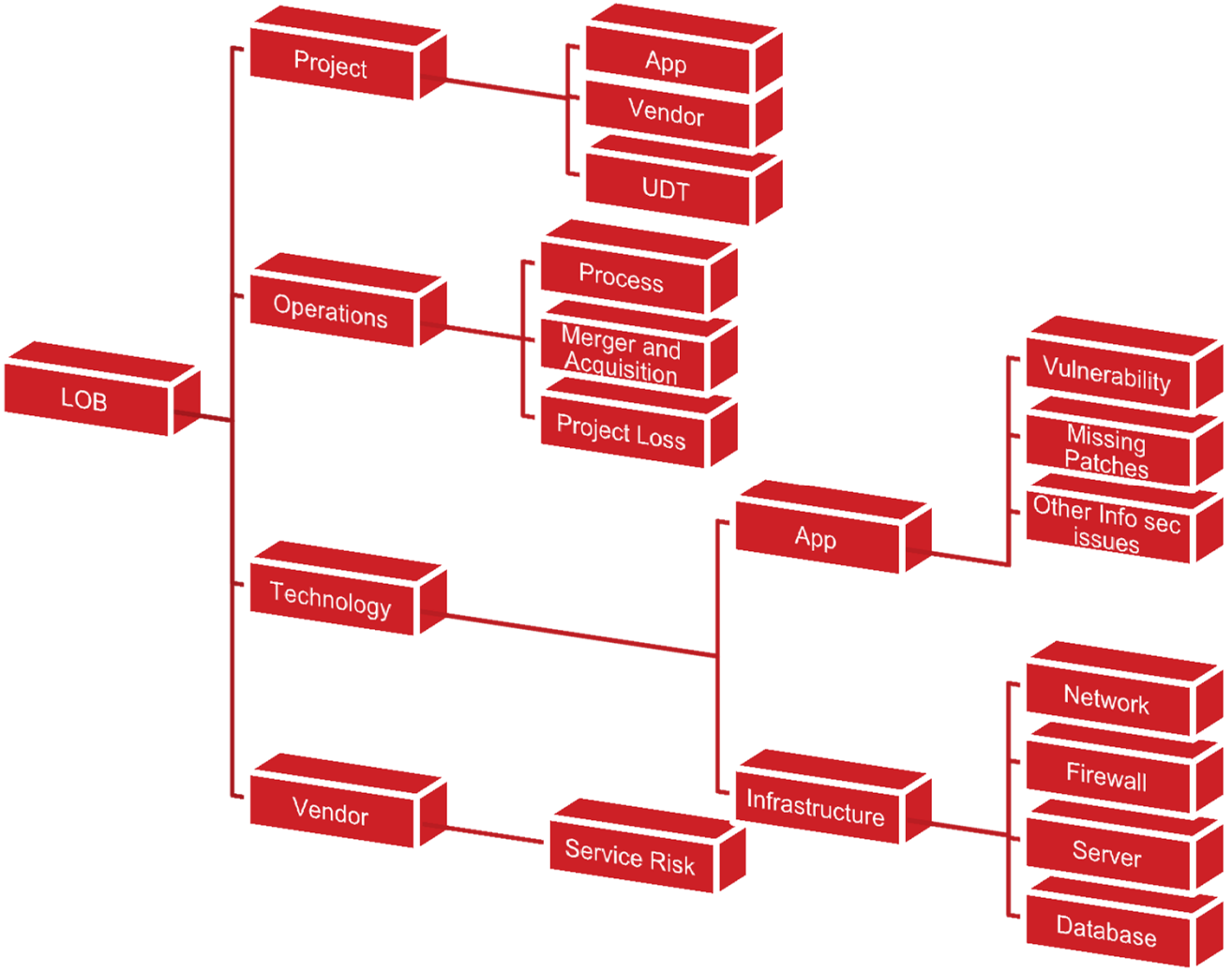
CICS

SMF

zOS, Linux on z

Applications

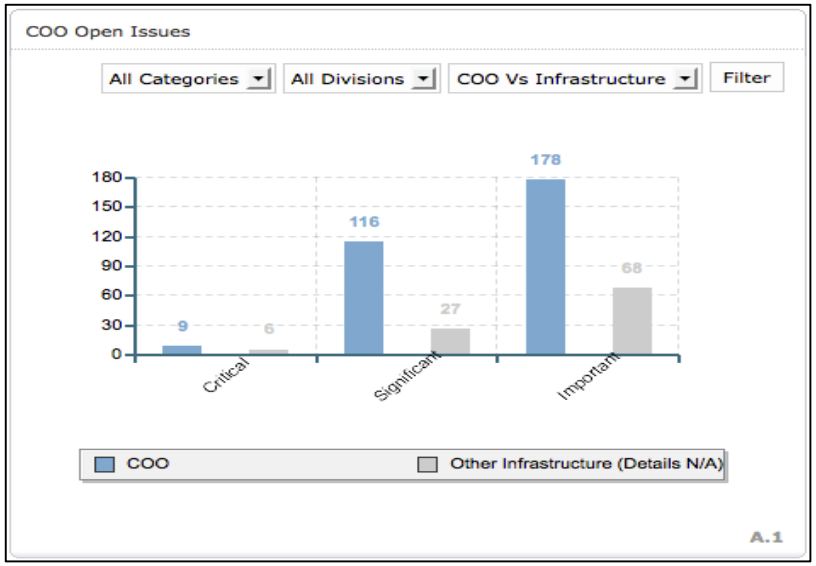
Step 5 - Reporting

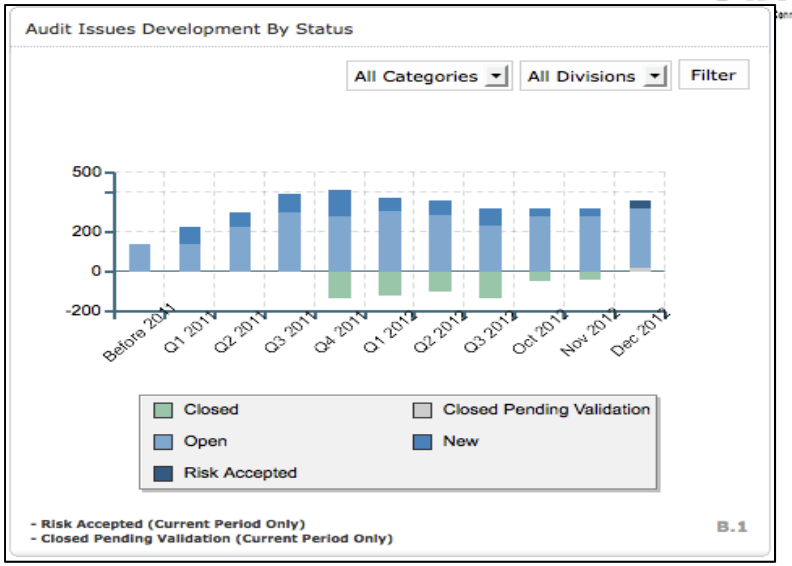


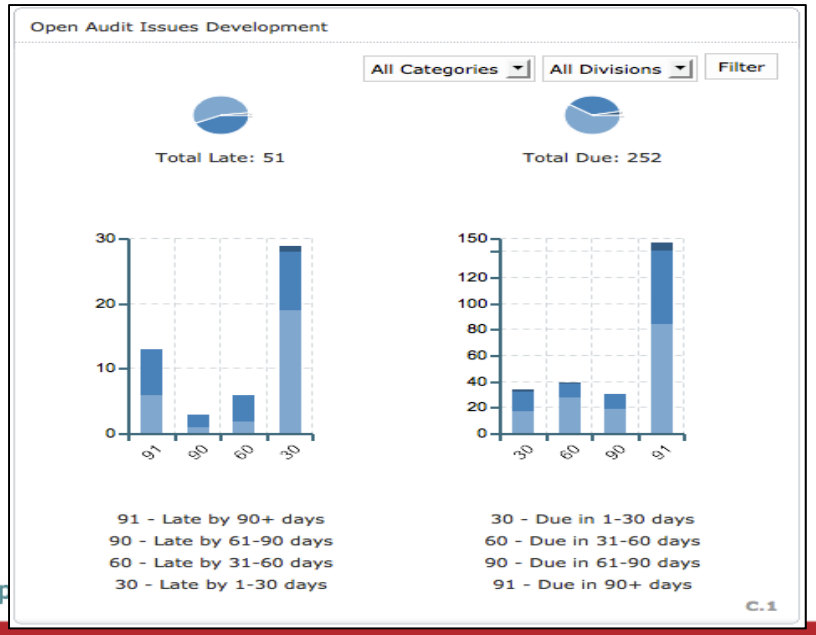
Aggregate data and report risk at highest level with ability to drill down to details

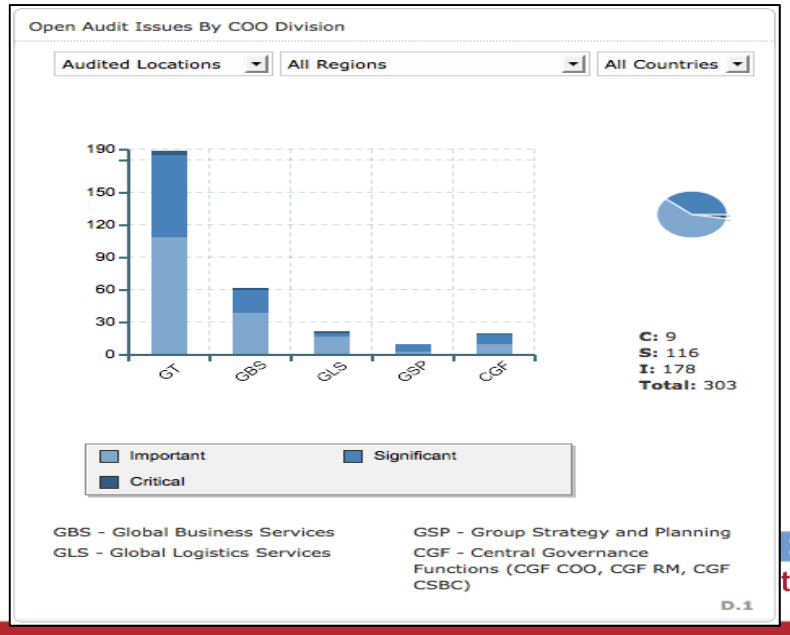
Application Risk Metrics

Audit Metrics



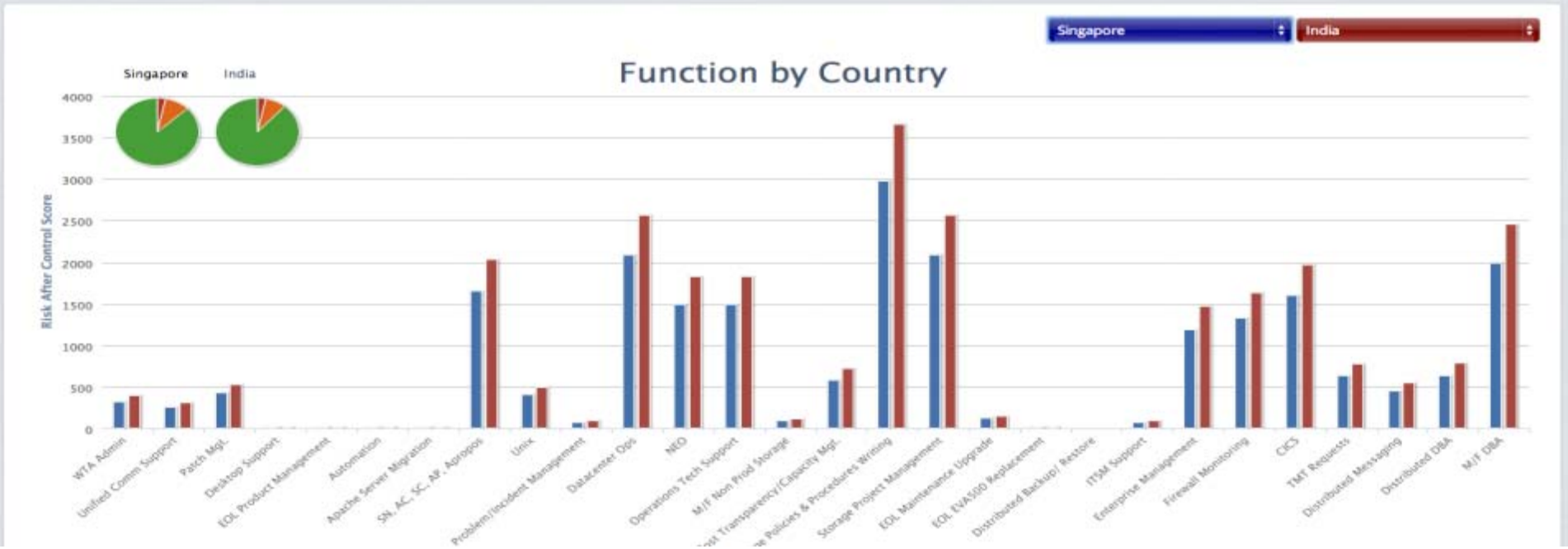






Country Risk Metrics

5.4	WTA Admin	-7.9 %	Philippines	2.5 %
Times Risky	Function-Highest Risk	Offshore-Risk Change	Country-Highest Risk	Onshore-Risk Change



Benefits

- **~65% reduction in issue/incident remediation efforts**
- **~55% reduction in assessment efforts**
- **~70% reduction in information gathering efforts**

- Common view of all risk (IT, Financial, Operations, Legal etc.)
- Prioritization of issues by risk to organization
- Consistent and clear communication of risk posture
- Effective and efficient resource utilization

- Ability to predict and respond to threats
- Automated, relevant and efficient risk assessments
- Monitor and track continuous improvements
- Ad-hoc and dynamic risk reports for executives and stakeholders to make intelligent decisions

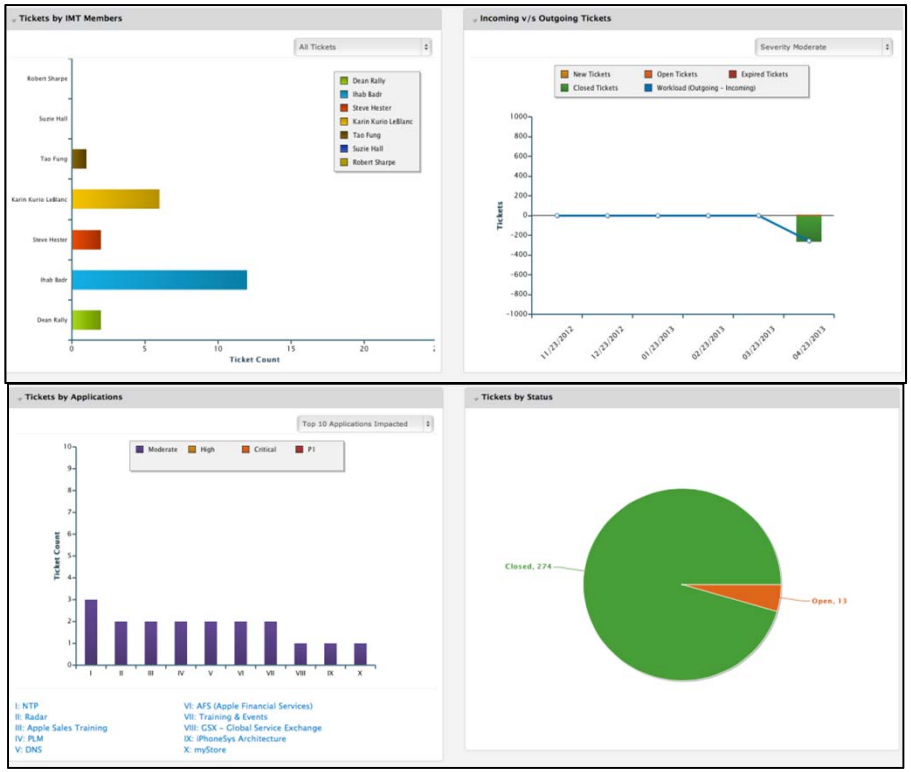
Case Study #1

Customer Profile

- Fortune 50 global technology company
- Over a million reported vulnerabilities from various systems
- Lack of visibility and identification of key risk areas

Brinqa Solution

- Nightly processing of vulnerabilities within the system
- Consolidation and remediation by Application instead of individual vulnerabilities
- Quantitative risk analysis
- Central warehouse for all issues, risks and findings
- Closed loop remediation for host vulnerabilities



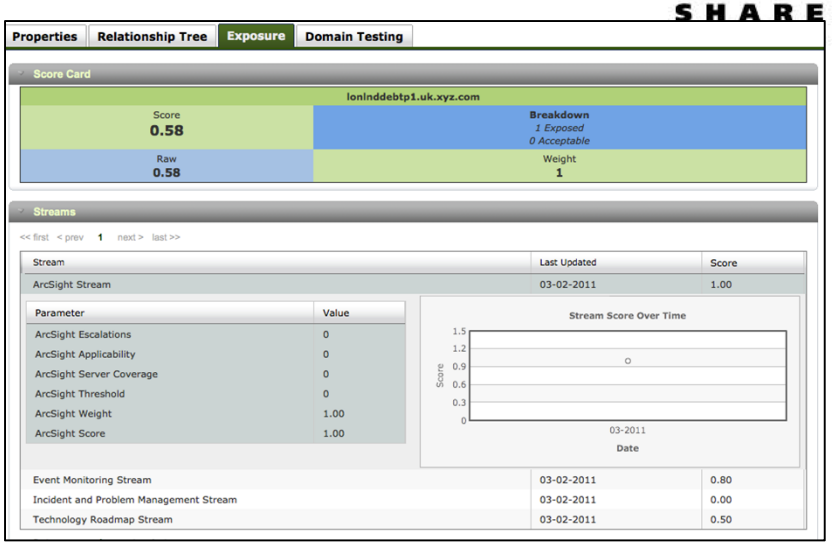
Case Study #2

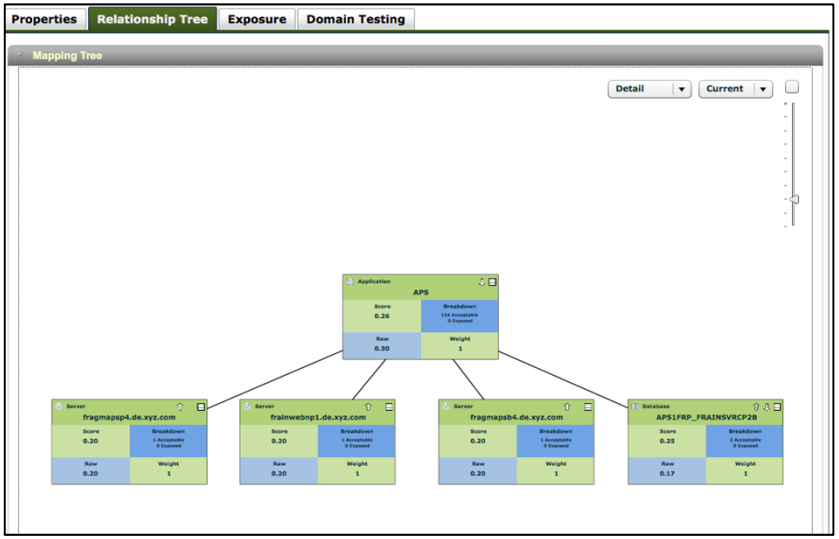
Customer Profile

- Fortune 100 global financial institution
- 2400 critical applications
- Lack of visibility and identification of key risk areas
- Costly labor to address thousands of issues/findings yearly

Brinqa Solution

- Portal to report infrastructure components and applications
- Integrated asset model to show the relationship between applications and supporting infrastructure
- 800 Critical Applications, 17000 servers, 1000 databases
- Simulation analysis to produce reports based on scenarios





Case Study # 3

Customer Profile

- 7th largest bank in the world
- $1.4 trillion in assets under management
- $27 trillion under custody and administration
- Responsibility for reporting risk across 21 services
- Very difficult to standardize and report risk for various areas
- Various assessments over many different business lines

Brinqa Solution

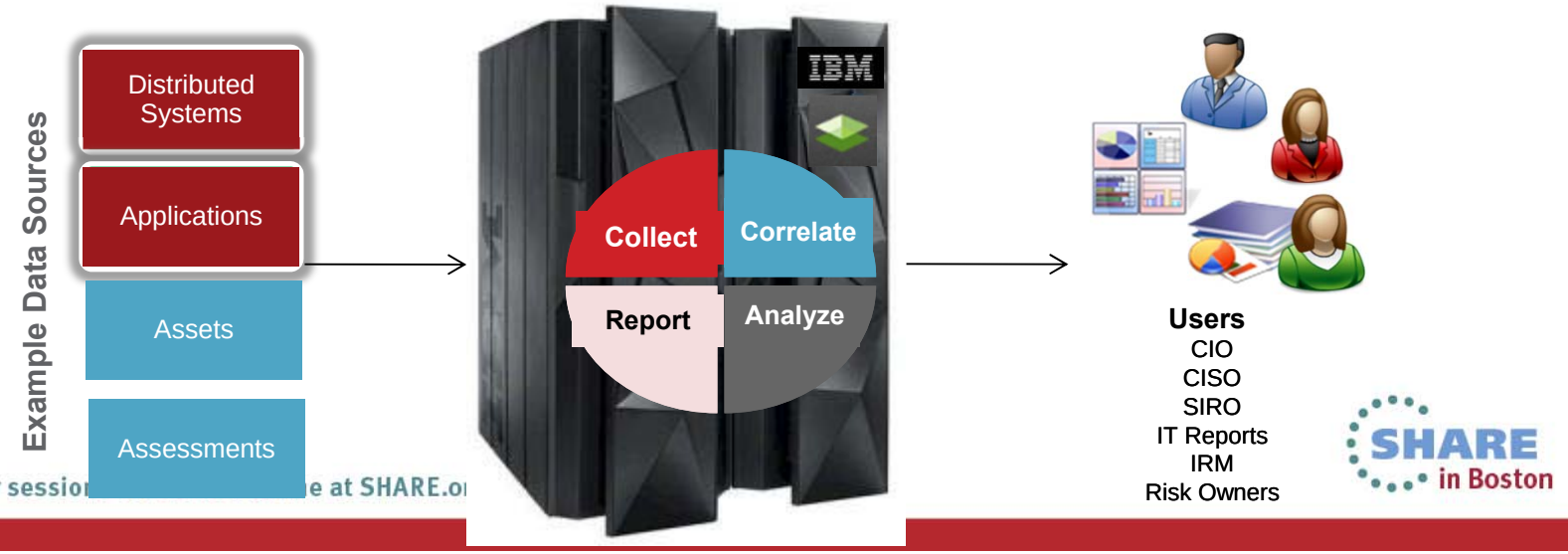
- Risk Analytics to centralize, integrate and report on various services
- Data aggregation through connector framework
- Automated and consistent assessments that lead to greater efficiencies
- A repository of risks that gave the departments a standardized library
- Risk normalization and prioritization
- Consolidated reporting for the multiple departments; aggregated risk scores and reporting by distinct areas

Brinqa Security Risk Analytics. zOS and Linux on z.

- Measures Security, Risk of Mainframe + Distributed
- Business Impacts, Trends, Processes based on end to end view

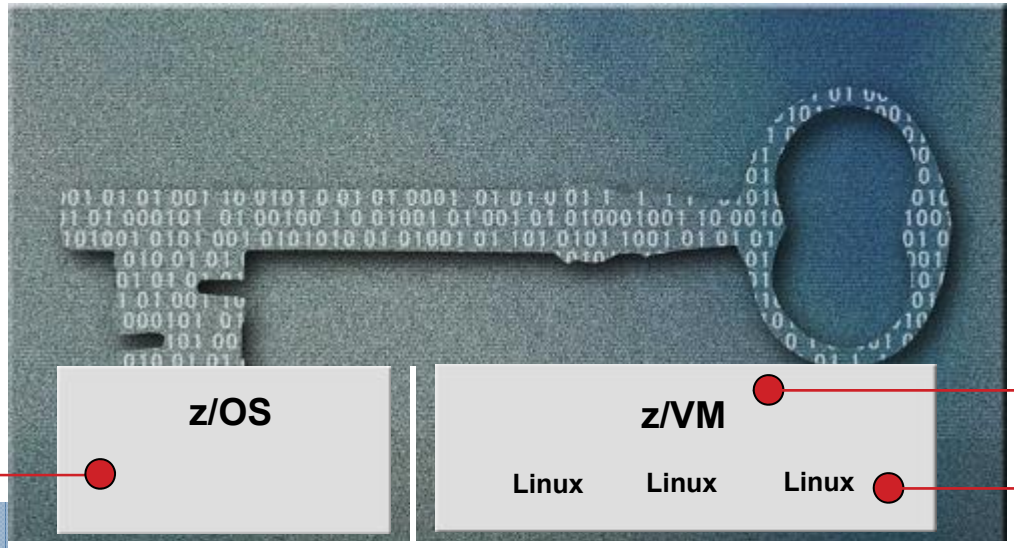
- Enhanced visibility: User, DB Monitoring, Security / Audit events, Assets
- Risk, Security Remediation and Treatment Workflows

- Promotes zEnterprise to a central part of Enterprise Security, Risk Initiatives
  - Centralized, Secure, Scalable, Resilient
- New Workload Java-based Architecture. zOS / Linux on z. (IFL, zIIP / zAAP)
- Increased Analytics Performance: Benchmark Results



System z Evaluations & Certifications

The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/VM

- Common Criteria
- z/VM 5.3
- EAL 5+ for CAPP and LSPP
- System Integrity Statement

z/OS

- Common Criteria EAL4+
  - with CAPP and LSPP
  - z/OS 1.7 → 1.10 + RACF
  - z/OS 1.11 + RACF (OSPP)
  - z/OS 1.12 + RACF (OSPP)
- Common Criteria EAL5
  - z/OS RACF 1.12 (OSPP)
- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services
- FIPS 140-2
  - System SSL z/OS 1.10 →1.12
  - z/OS ICSF PKCS#11 Services – z/OS 1.11
- Statement of Integrity

Linux on System z

- Common Criteria
- SUSE SLES10 certified at EAL4+ with CAPP
- Red Hat EL5 EAL4+ with CAPP and LSPP
- OpenSSL - FIPS 140-2 Level 1 Validated
- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

Virtualization with partitions

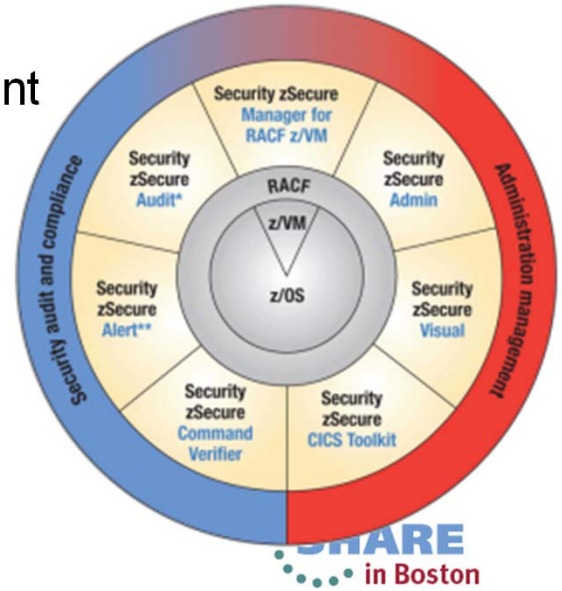
- System z9 EC and z9 BC System z10 EC and z10 BC
- Common Criteria EAL5 with specific target of evaluation -- LPAR: Logical partitions
- zEnterprise 196 & zEnterprise 114
- Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions

Cryptography

- Crypto Express2 & Crypto Express3 Coprocessors
  - FIPS 140-2 level 4 Hardware Evaluation
  - Approved by German ZKA
- CP Assist
  - FIPS 197 (AES)
  - FIPS 46-3 (TDES)
  - FIPS 180-3 (Secure Hash)

Technology can help

- Define the security policy in monitoring tools
  - Operating system and security settings against baselines
  - Operating system and security changes against baselines
  - Data access against standards
  - Access by technicians should fit production profile
  - etc.
- In case of conflict
  - Deny the action, prevent the change from taking place, or
  - Issue a real-time message to data security officer, or
  - Generate an exception report for review by management
- Document
  - Baseline or security standard
  - Exceptions and transgressions

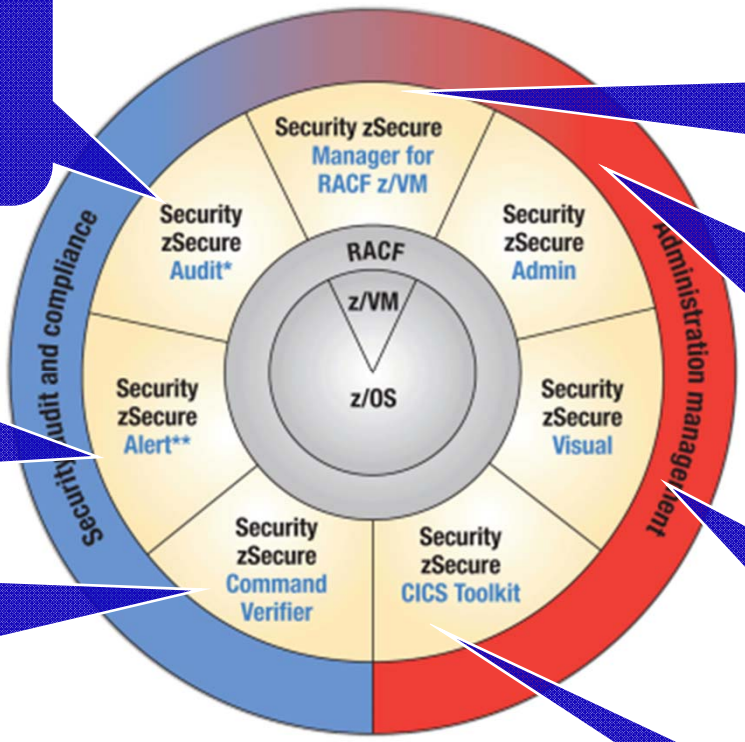


IBM Security zSecure suite products and benefits

Vulnerability analysis for your mainframe infrastructure. Automatically analyze and report on security events, detect security exposures, and integration with SIEMs.

Real-time mainframe threat monitoring permits you to monitor intruders, identify misconfigurations that could hamper your compliance efforts, and report to SIEMs.

Policy enforcement solution that helps enforce compliance to company and regulatory policies by preventing erroneous commands



Combined audit and administration for RACF in the z/VM environment including auditing Linux on System z

Enables more efficient and effective RACF administration, using significantly fewer resources. Provides RACF cleanup, database merge, database compare and RACF offline

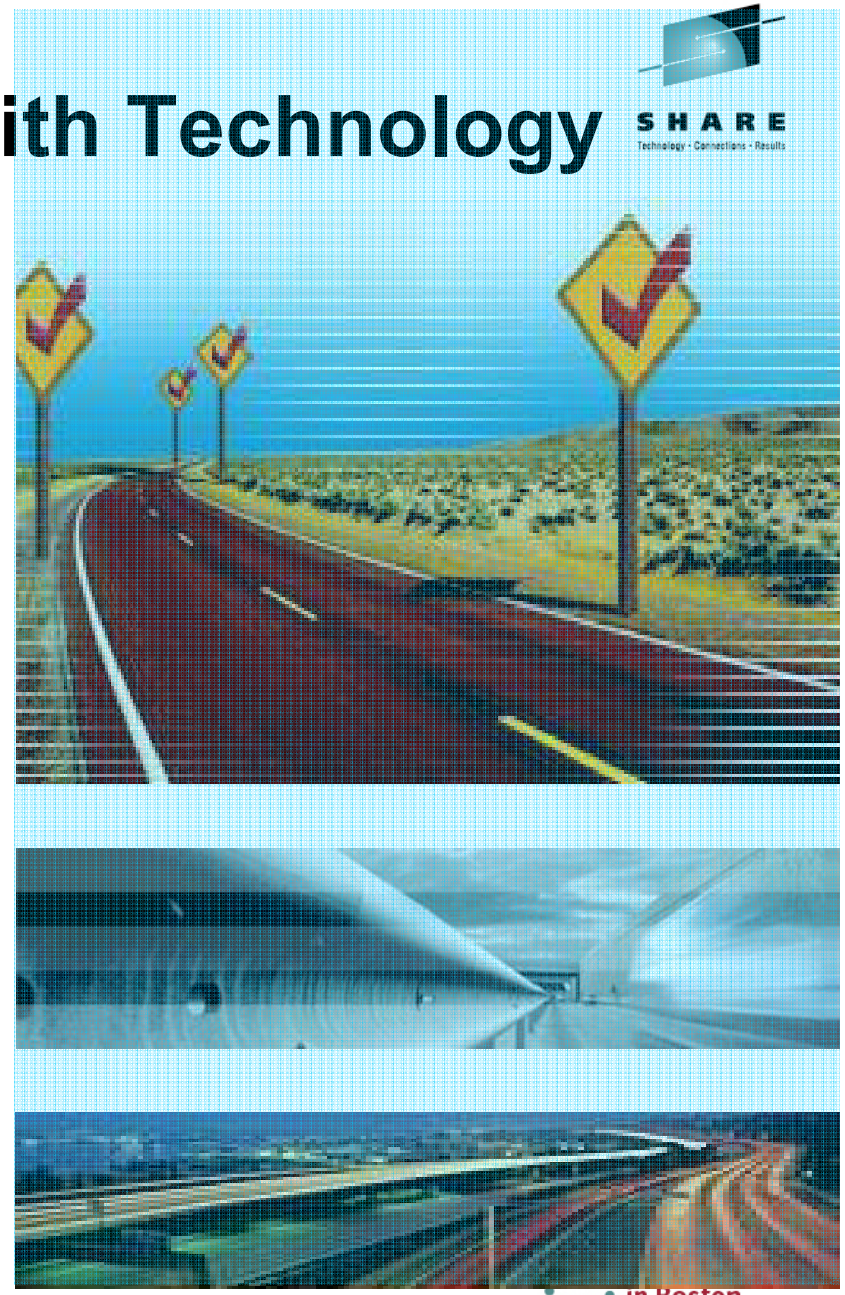
Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Provides access RACF command & APIs from a CICS environment, allowing for additional administrative flexibility

Automate audit, monitoring and compliance with repeatable – sustainable processes i.e. STIGS, PCIDSS, SOX and oathers
Simplify security administration and provisioning
Reduce costs, improve ROI, assist in improving z/OS security
Consolidate an centralize security management

Benefits of Automating with Technology

- Facilitate compliance with security requirements and policies
- Leverage seamless integration with an enterprise-wide view of audit and compliance efforts
- Monitor and audit incidents to help detect and prevent security exposures, as well as assess compliance
- Automate routine administrative tasks to help reduce costs and improve productivity
- Understand the security baseline and when it changes to keep security intelligence at it's highest and up to date



Your Conflict: Regulation versus Reality

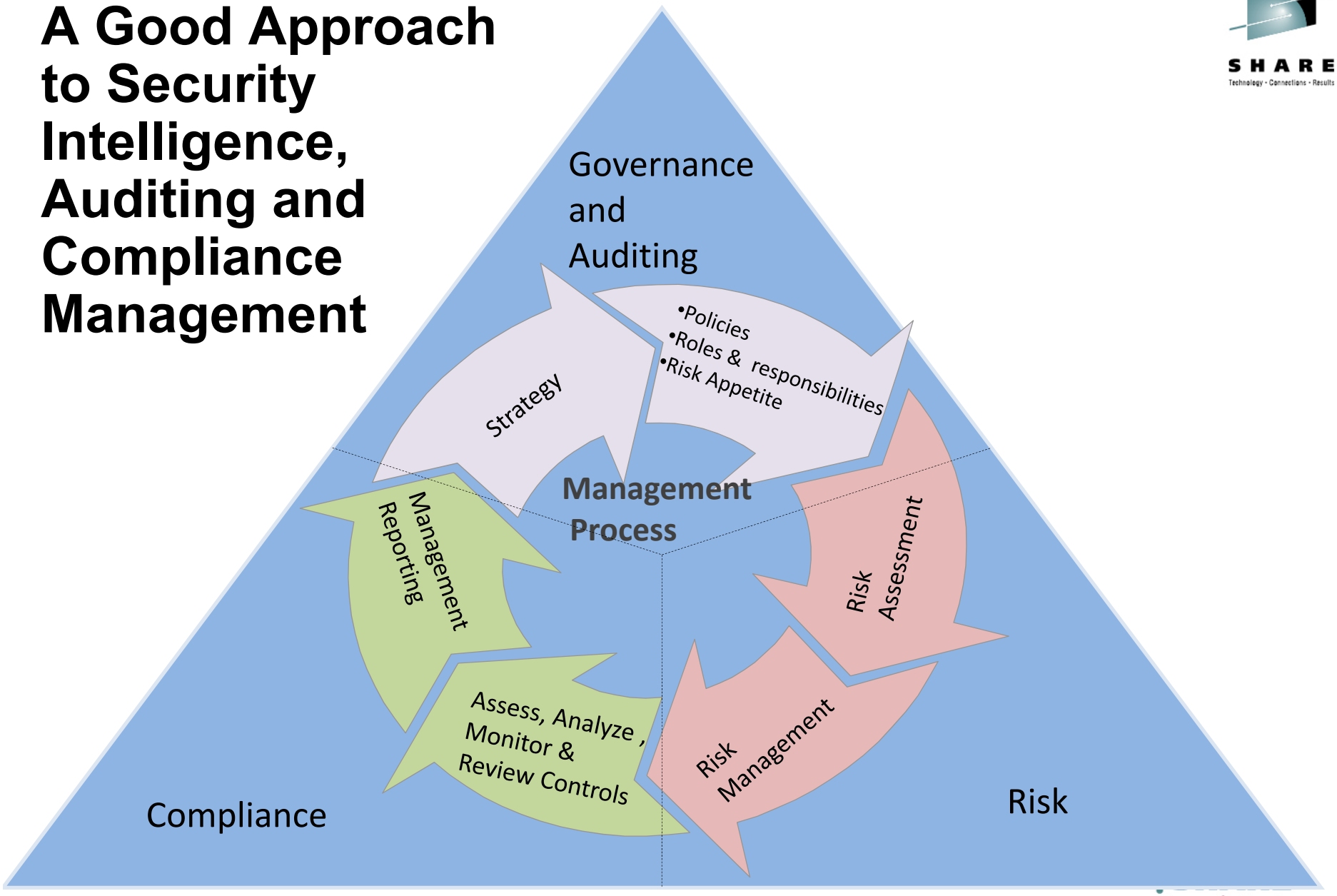
Regulation

- Change management
  - Clearly defined process with approval and reporting
  - Ability to identify changes
- Security management
  - Separation of duties
  - Identification of exposures and mis-configurations
  - Clear audit trail and accountability
- Data security
  - Data confidentiality and integrity
  - Prevent improper access to financial, medical or personal data
  - Monitor access to data by technician, administrator, outsiders

Reality

- Separation of duty impractical tasks with small teams
- Many highly authorized IDs necessary for final go-to technician
- Mainframe installations often rely on “system special” and “uid(0)”
- Red-tape bypassed for high-impact problem resolution
- Manual monitoring impractical due to volume of data
- Human mistakes cause service outages
- Cleanup projects are long running and expensive

A Good Approach to Security Intelligence, Auditing and Compliance Management



About Brinqa

WHO WE ARE	WHAT WE DO	HOW WE DO IT	WHO WE DO IT FOR	WHY WE DO IT
▪ Smart Risk Analytics and management	▪ Provide continuous centralized risk analysis and management solution ▪ Metrics driven analysis	▪ Connects all data across the enterprise ▪ Customizable to business needs ▪ Hands on service team	▪ Chief risk and compliance officers ▪ CISO, CIRO ▪ CIO, COO, CTO ▪ Enterprises	▪ Better business decisions: ▪ proactive vs. reactive ▪ Risk Management and compliance ▪ Peace of mind

"Re-imagine your risk data"

Brinqa Risk Analytics

*Brinqa risk analytics provides organizations **visibility** into all **essential data** and the **metrics** needed to **proactively** offset potential threats.*

- Data Aggregation and Correlation
  - Advanced Correlation
  - Dynamic Surveys
  - Smart Connectors
  - Big Data Architecture
- Context aware Risk Models
  - Best practice based
  - Risk Taxonomies
  - Easily configurable
  - Simulation models
  - Quantitative and Qualitative calculations
  - Adjustable threshold and tolerance levels

- Dynamic Dashboards and Reports
  - Risk prioritization, what-if analysis and trends
  - User defined dashboards and reports
  - Role-based views

References

- American Banker
  - http://www.americanbanker.com/issues/178_145/banks-struggle-to-manage-tech-ops-risk-survey-1060945-1.html
  - http://www.americanbanker.com/issues/178_151/modeling-the-cost-of-doing-nothing-1061133-1.html
- Treasury and Risk
  - http://www.treasuryandrisk.com/2013/08/12/the-case-for-risk-analytics
- ComputerWorld
  - www.computerworld.com/s/article/9241592/Analytics_company_Bringa_puts_a_price_on_risk
- DataInformed
  - http://data-informed.com/bringa-were-the-facebook-of-machine-data-for-risk-security-analytics/
- CMSWire
  - http://www.cmswire.com/cms/information-management/could-bringa-the-facebook-for-data-predict-trouble-long-before-it-occurs-022002.php

#SHAREorg

SHARE

Thank You. Questions?

For More Information please contact:

Rich Skinner, CISSP

Director

Security, Risk Analytics, & Big Data

rskinner@bringa.com

260.312.1958

SHARE in Boston