Internal Audit and GRC: Challenges and Solutions to Alignment

Patrick Potter, GRC Strategist, RSA/EMC

Governance, Risk & Compliance – G23

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

2014 Fall Conference - "Think Big"

CRISC
CGEIT
CISM
CISA

The Challenge

Internal Audit is one of many organizational groups whose mission is to assess risks, evaluate controls, raise issues and improve processes. Other oversight functions with similar charters include Enterprise Risk Management, Compliance, Legal and others. With some common objectives and not-so-common approaches, there is value in aligning methodologies, resources and results. However, Internal Audit has its charter and audit plan and needs to maintain a certain level of independence, so how does Internal Audit strike this balance?

In Case You Didn’t Already Know…

Internal Audit continues to struggle to provide adequate assurance

Compliance will continue to impact

Since 2009

- 131 new major regulations enacted
- $70 billion in costs

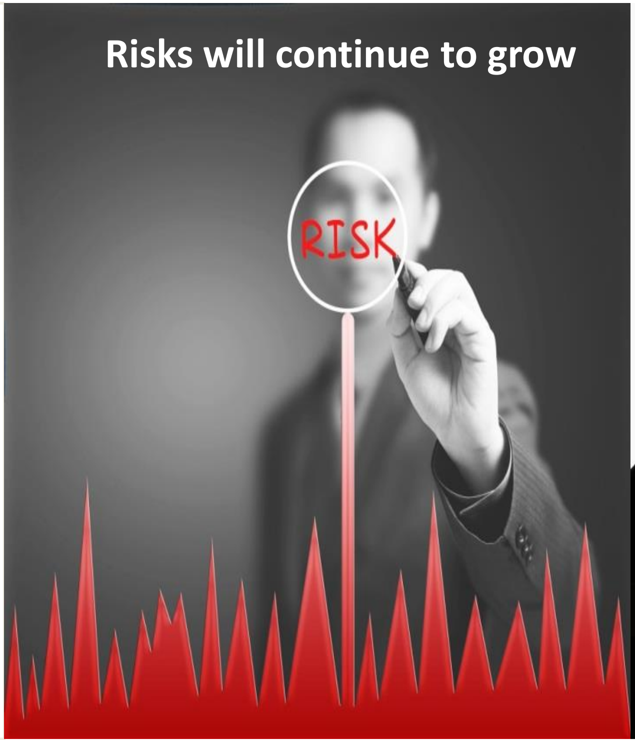
In 2012

- 2,605 new rules
- 69 classified as major
- >$100 Million annual impact

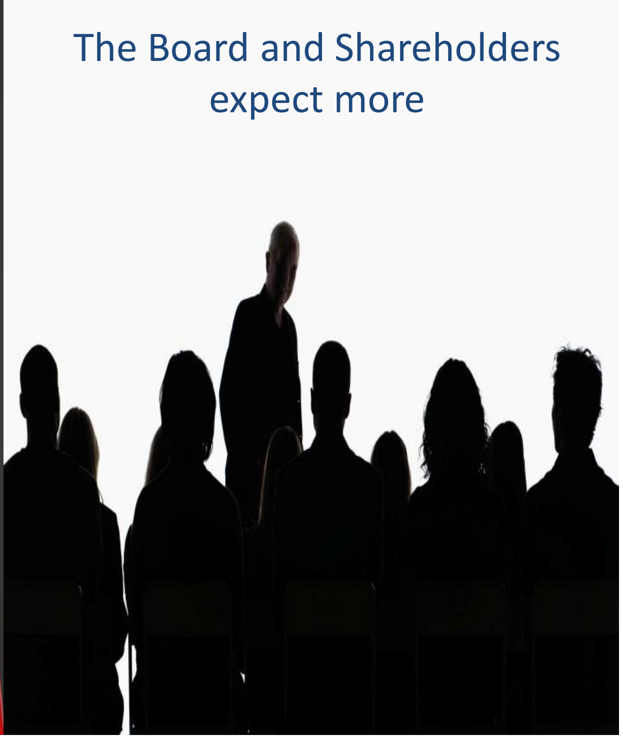
In 2013

- 134 new rules enacted just by the EPA

Source: Heritage Foundation



Risks will continue to grow



The Board and Shareholders expect more

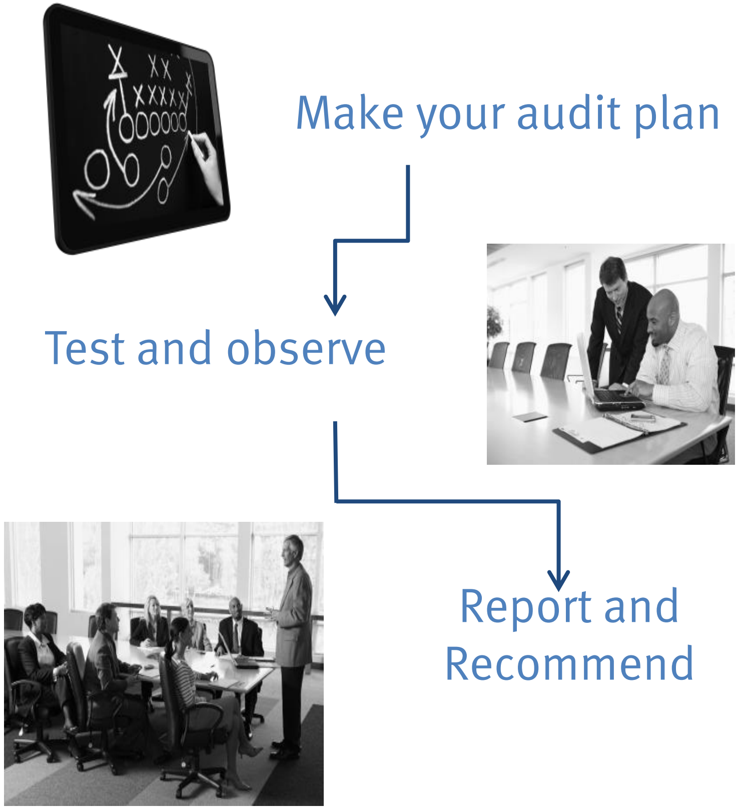
Your Audit Strategy must be **Risk Based**, **Coordinated** and **Connected.**

Key Trends Affecting Internal Audit

- ✓ Regulators and external auditors
- ✓ IA must leverage “mega data”
- ✓ IA wants one tool
- ✓ International Auditing and Assurance Standards Board new framework
- ✓ “Competing” with other GRC groups
- ✓ IA assurance in management risk processes
- ✓ Greater scrutiny of audit committees
- ✓ IA strategic partnerships

Where is Internal Audit today?

Static audit planning vs. quickly changing business conditions



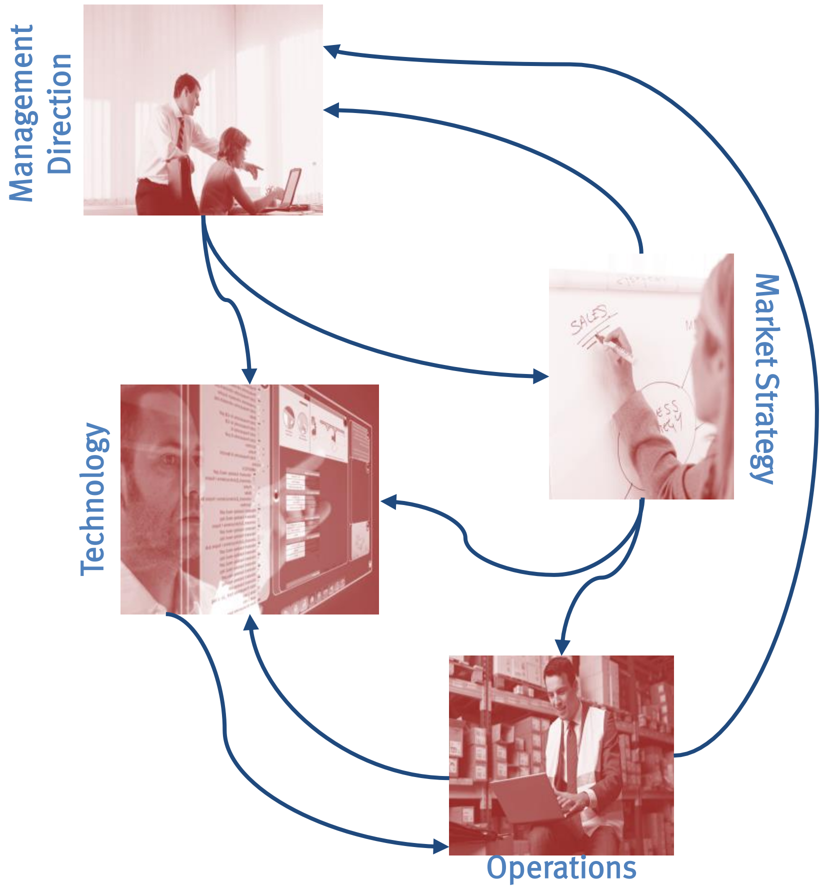
Make your audit plan

Test and observe

Report and Recommend

Today's Audit Strategy

Versus



Management Direction

Market Strategy

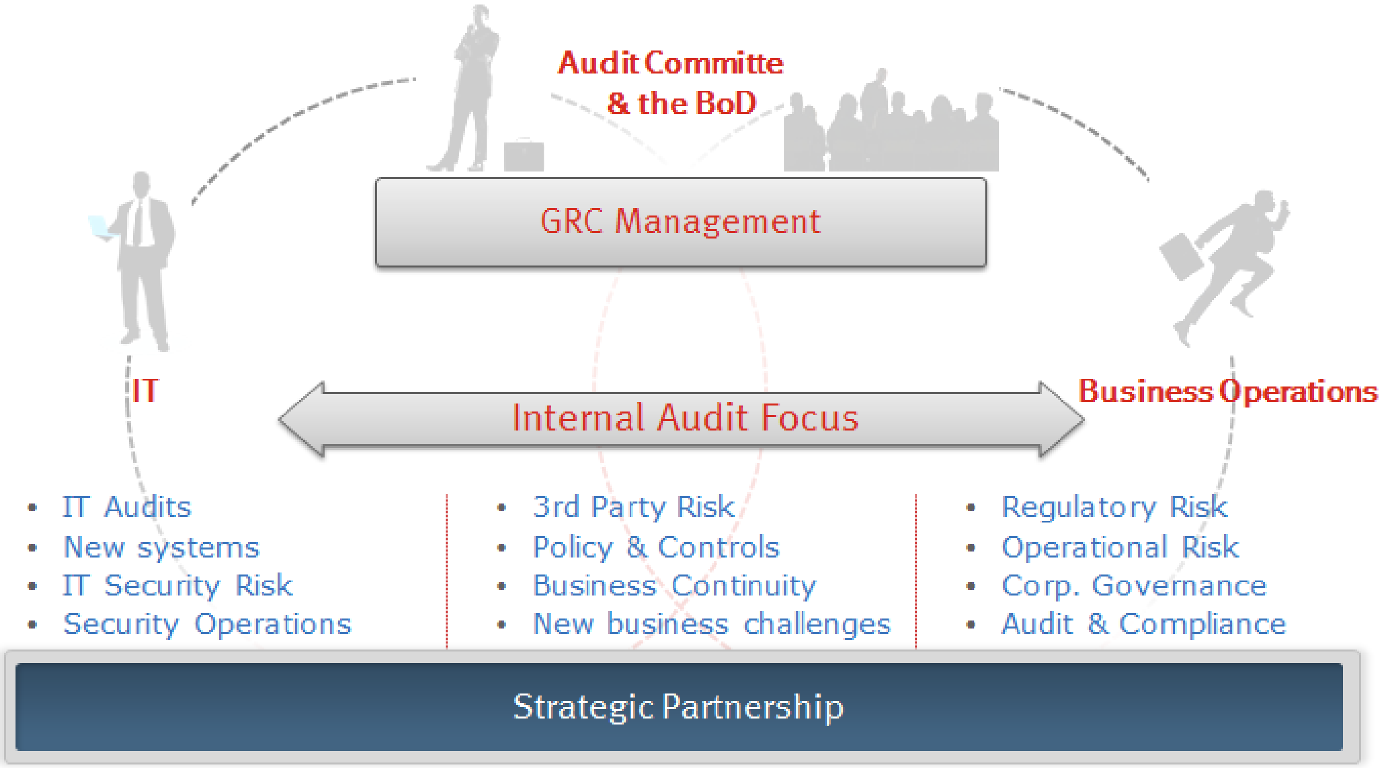
Technology

Operations

Today's Fluid Business

Internal Audit and GRC

GRC = Governance, Risk and Compliance



Audit Committe & the BoD

GRC Management

IT

Internal Audit Focus

Business Operations

- IT Audits
- New systems
- IT Security Risk
- Security Operations

- 3rd Party Risk
- Policy & Controls
- Business Continuity
- New business challenges

- Regulatory Risk
- Operational Risk
- Corp. Governance
- Audit & Compliance

Strategic Partnership

Figure 3: Internal Audit and GRC Integration Model

Audit Approaches Need to Change…

to develop a more risk-based approach

Internal Audit

Management

IT

Risk and Compliance Functions

Business Operations

Independent and Reactive

Collaborative and Value Added

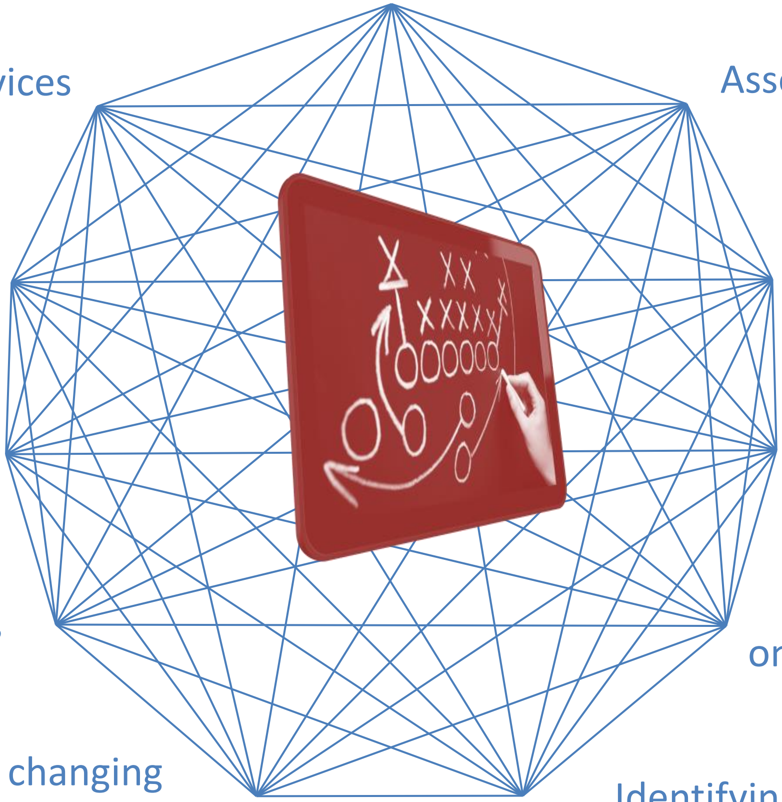
Ideas for Solutions

Align on the “Universe”

- Need an integrated view of business between IA, Risk and Compliance
- No more “Six men touching the elephant” (we all see the universe equally)
- Evaluate the universe consistently (No “tempests in the teapot”)
- Better use of company (all three groups with same approaches) resources

Connecting the dots

A connected, dynamic process will succeed



Tied to corporate objectives

Assets mapped to products and processes

Business Processes reflect risk impacts

Monitoring and managing key risks

Testing controls once/continuous monitoring

Identifying new risks

Leveraging changing people/roles

Monitoring your vendors

Updated policies and procedures

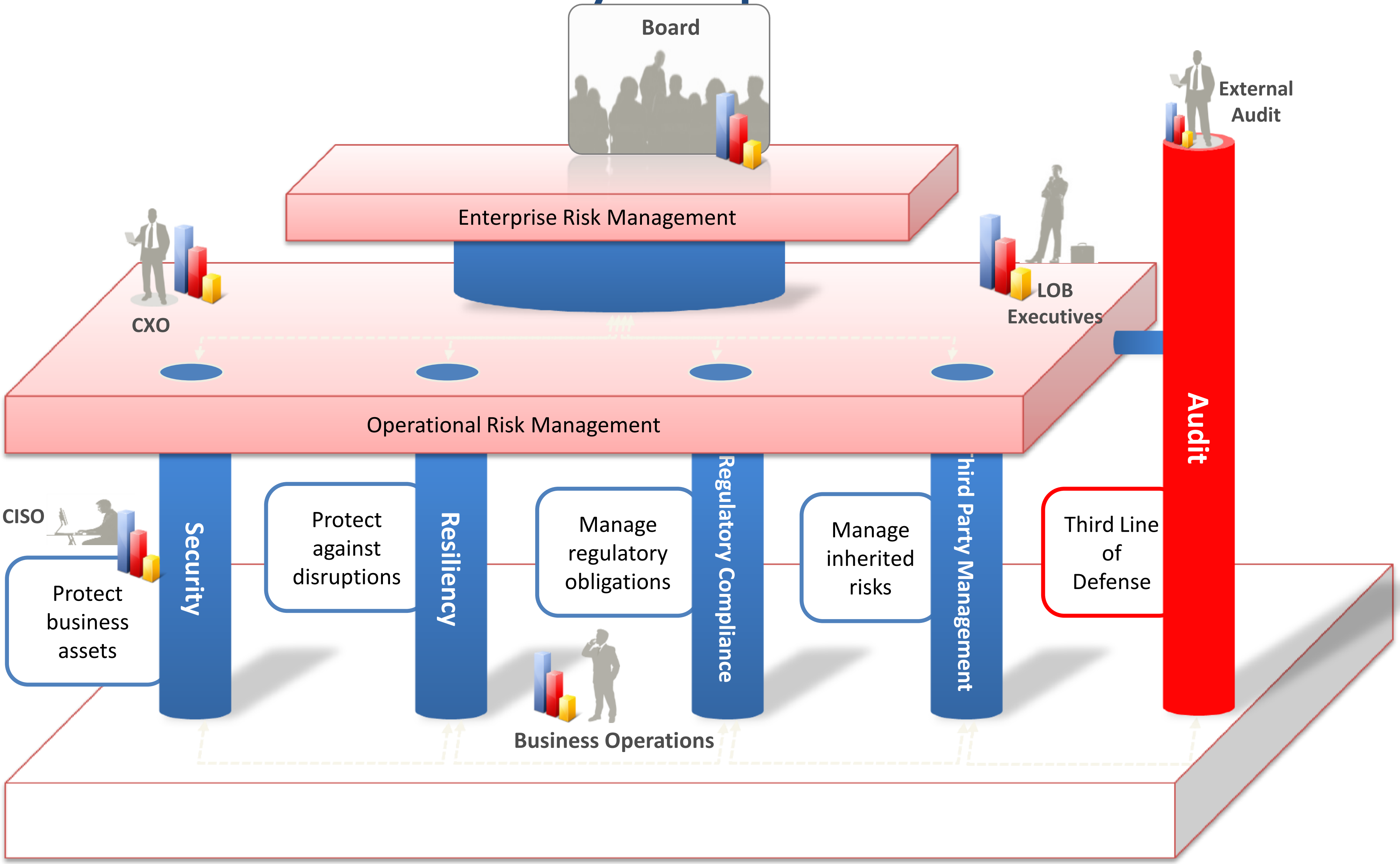
Managing new and changing Rules & Regulations

Most critical products/services identified

Let Others Do the Dirty Work

- **Ops/Enterprise Risk Management** – Identify, assess, manage and monitor risks
- **Compliance** – Evaluate compliance with regulations and internal requirements
- **Legal** – Identify regulations, interpret requirements, determine exposure

Audit– A Key Aspect of GRC



Board

Enterprise Risk Management

CXO

LOB Executives

External Audit

Operational Risk Management

Audit

CISO

Protect business assets

Security

Protect against disruptions

Resiliency

Manage regulatory obligations

Regulatory Compliance

Manage inherited risks

hird Party Management

Third Line of Defense

Business Operations

Leverage your ORM/ERM Group

Good

- Meet ORM, understand their process and how they assess and mitigate risk
- Review their findings and mitigation activities

Better

- Incorporate ORM results into annual risk assessment and audit scoping

Best

- Align risk assessment methodologies between ORM
- Use ORM KRIs for dynamic risk assessment
- Align on findings and remediation plans

Leveraging Compliance Groups

Good

- Meet Compliance, understand their process and how they assess and mitigate risk
- Review their findings and mitigation activities

Better

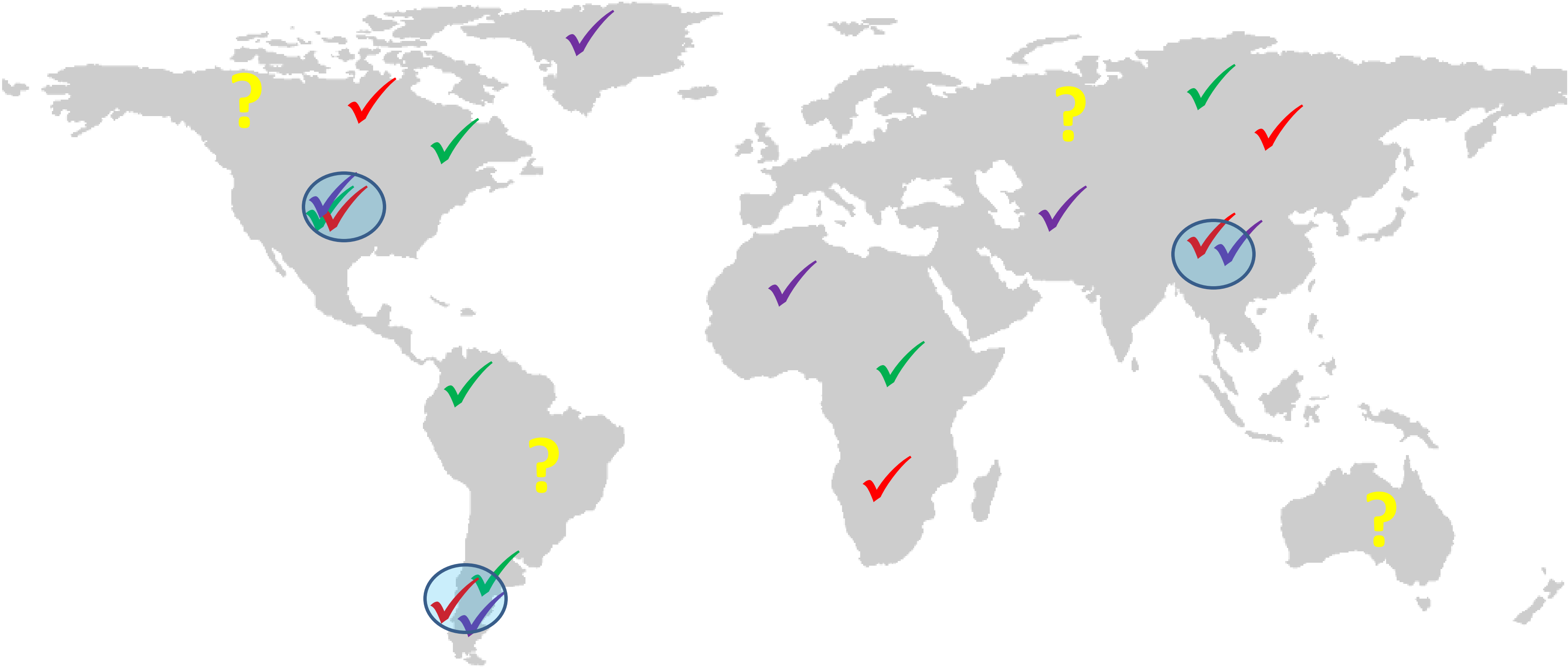
- Incorporate testing results into annual risk assessment and audit scoping

Best

- Align audit plans and control testing
- Use KPIs for continuous control monitoring
- Align on findings and remediation plans

Develop a Heat Map

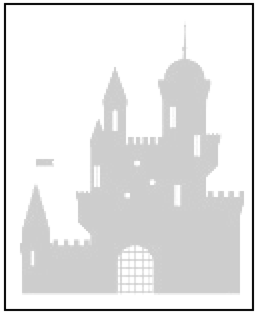
Coverage by Internal Audit, Risk and Compliance



Areas of duplication or no coverage appear

Challenges to Alignment

- Looking at the whole discloses gaps, or areas no one group is focused on
  - Similar activities with different and sometimes competing priorities
  - Duplicate resources, processes and misaligned objectives
  - Political, geographic, or financial (e.g., funding) factors
- It's all new to everyone
  - Protect the empire
  - Working against each other, not intentionally



What do we do now and who takes the lead?

Replace Your Audits with Data Analytics

Supplement your audits and adjust your audit plan with dynamic key risk and control indicators

Business Priority

↓

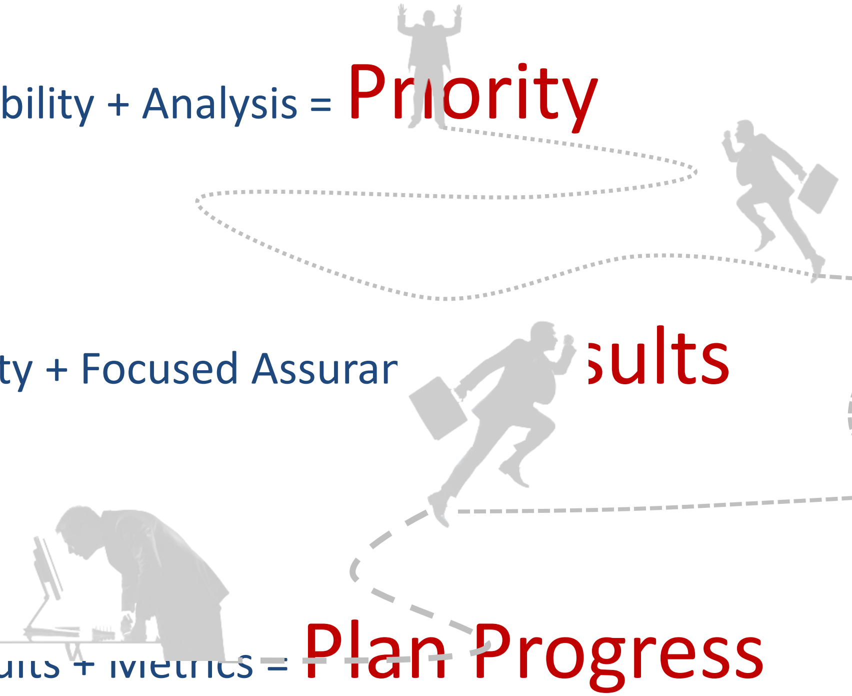
Analysis

↓

Action

↓

Metrics



Visibility + Analysis = Priority

Priority + Focused Assurar sults

Results + Metrics = Plan Progress

From Onsite Audits to Continuous CIs

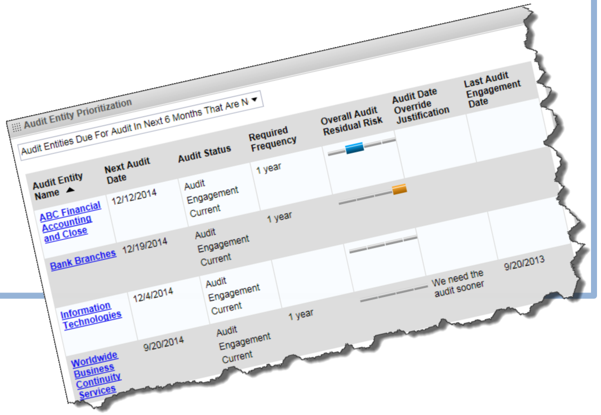
Internal Audit group for a Fortune 100 financial services company modified its approach to auditing financial offices based on continuous controls monitoring

BEFORE

- Internal Audit randomly selected from 10k financial offices to perform surprise audits
- Surprise audits were done because of financial negotiable instruments on hand
- IA counted negotiable instruments and reconciled to the GL.
- IA verified accuracy of lost items, aging and follow steps to reconcile differences

AFTER

- IA reviewed metrics showing aged, outstanding and unreconciled financial items
- IA monitored these continuous control indicators (CCI) on a regular basis
- When aged, outstanding and unreconciled items reached certain thresholds, IA investigated

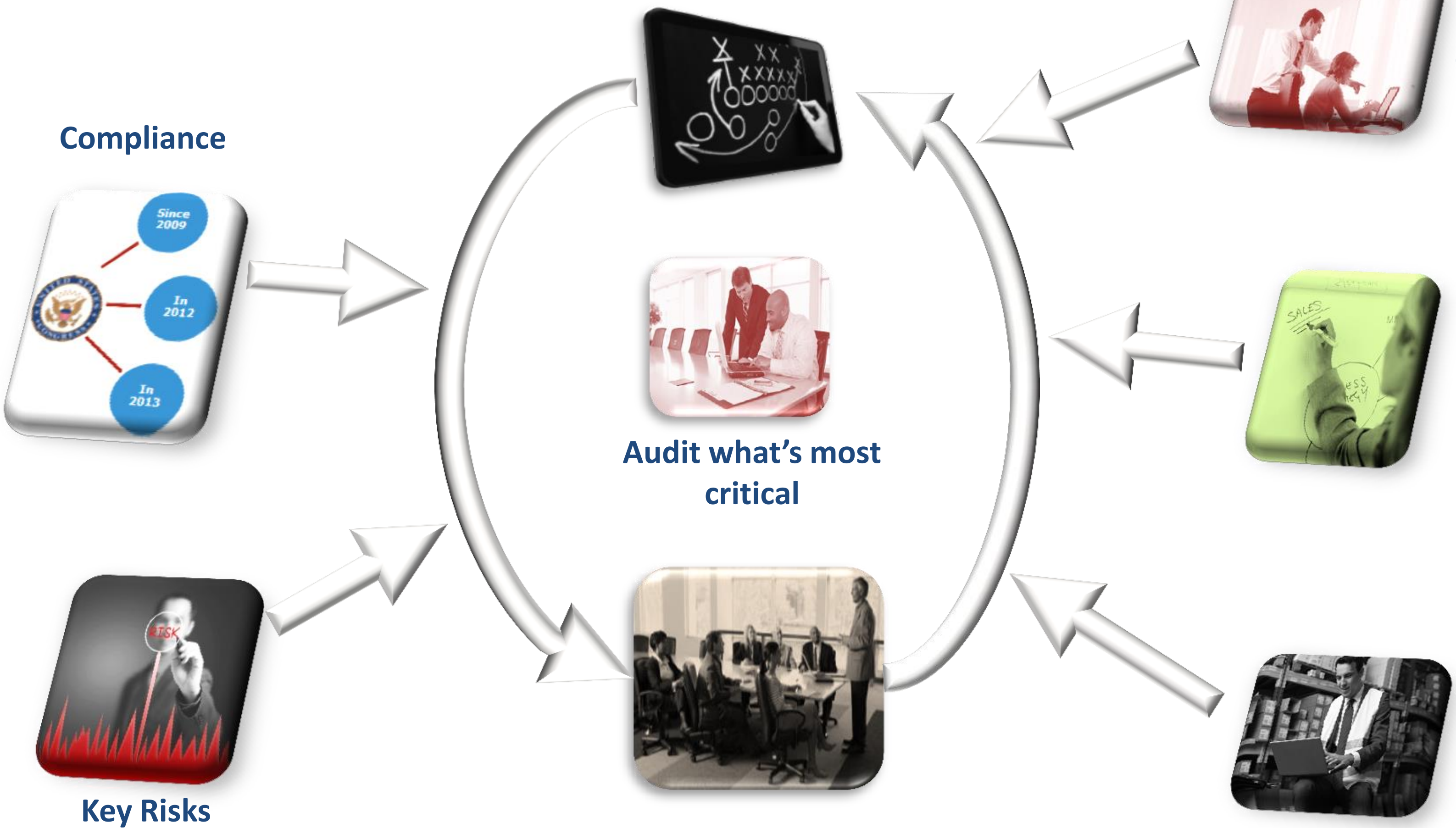


Audit Entity Prioritization

Audit Entities Due For Audit In Next 6 Months That Are N ▾

Audit Entity Name ▲	Next Audit Date	Audit Status	Required Frequency	Overall Audit Residual Risk	Audit Date Override Justification	Last Audit Engagement Date
ABC Financial Accounting and Close	12/12/2014	Audit Engagement Current	1 year	🟦		
Bank Branches	12/19/2014	Audit Engagement Current	1 year	🟧		
Information Technologies	12/4/2014	Audit Engagement Current				
Worldwide Business Continuity Services	9/20/2014	Audit Engagement Current	1 year		We need the audit sooner	9/20/2013

It’s Ok for Your Audit Plan To Be a Moving Target



Dynamic audit plan

Compliance

Business Objectives

Market Strategy

Audit what’s most critical

Key Risks

Report and Recommend

Business Criticality

Bad Reasons Not To Automate

5 – I can’t justify the spend to the execs

4 – My boss likes the system we use

3 – We don’t want to learn another system

2 – No one in risk or compliance will use it

1 – We’ve always done it this way

Reduce Burden on the Business

Synchronize findings and remediation plans between audit, Risk and Compliance

Incorporate more BU control self-assessments, continuous control and key metrics monitoring

Present a coordinated front to regulators

Coordinate schedule with Risk and Compliance teams

Considerations: Audit Planning

- Emerging issues we’re not prepared to deal with
- Do we have the right resources to achieve the audit plan?
- Measuring whether the plan is covering enough of the company’s risk profile
- Regional intricacies our IA group can’t address either geographically or topically

More Considerations

- Was the audit plan based on the right evaluation of risk (IA and Risk might have different methodologies – who's right?)
- Duplicating or conflicting plans w/Risk and Compliance groups
- Right mix of compliance vs. risk entities, topics and procedures (reactive vs. proactive)
- Will it satisfy external constituents, such as regulators, external auditors, audit committee

Audit what's most critical

IA and GRC Maturity Model

Advantaged	IA establishes common risk and assurance methodologies between audit, risk and compliance. Determines priorities based on potential impacts on common objectives, and coordinates audit work. Creates a combined view of findings for coordinated monitoring. Performs project and department level quality assessments, identifies gaps and makes improvements.
Transforming	IA monitors and reports on all findings and remediation plans on a consistent basis. Overlays business and risk context to findings to drive criticality and escalation. Relates findings to policies, standards, and procedures to identify systemic issues. Documents policy changes needed from findings and uses policy exceptions as a source for future control testing.
Managed	IA evaluates criticality of business processes and IT infrastructure and relationships between them, and maps auditable entities to the business hierarchy and infrastructure. Compares audit entity risk assessments to management's view of risk
Transitioning	IA identifies better documents the audit universe of the business hierarchy, products/services, business processes, IT infrastructure, locations and people. IA performs audit entity assessments, creates an audit plan and reports on completion. Templates and audit program libraries are used for engagements and staffing is better coordinated
Siloed	Internal Audit performs the basic lifecycle (audit planning and execution). IA is isolated and mainly compliance-based. Multiple, unrelated tools are used and reporting is very difficult.

Your Rise to the Top

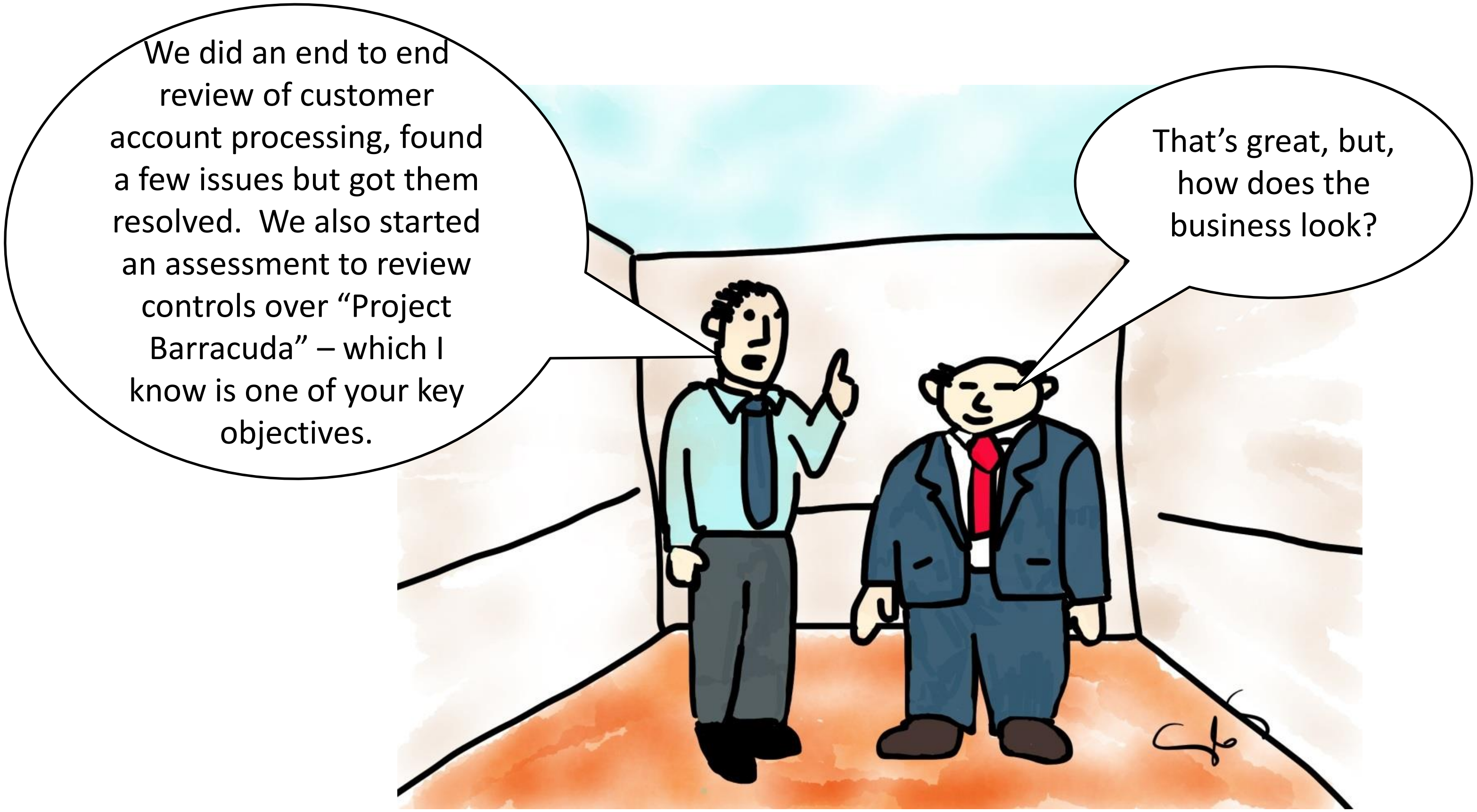
Today’s World

The CEO & BCM manager ride the elevator…

We performed 12 audits this quarter and found 56 control deficiencies.
That’s great, but, how does the business look?

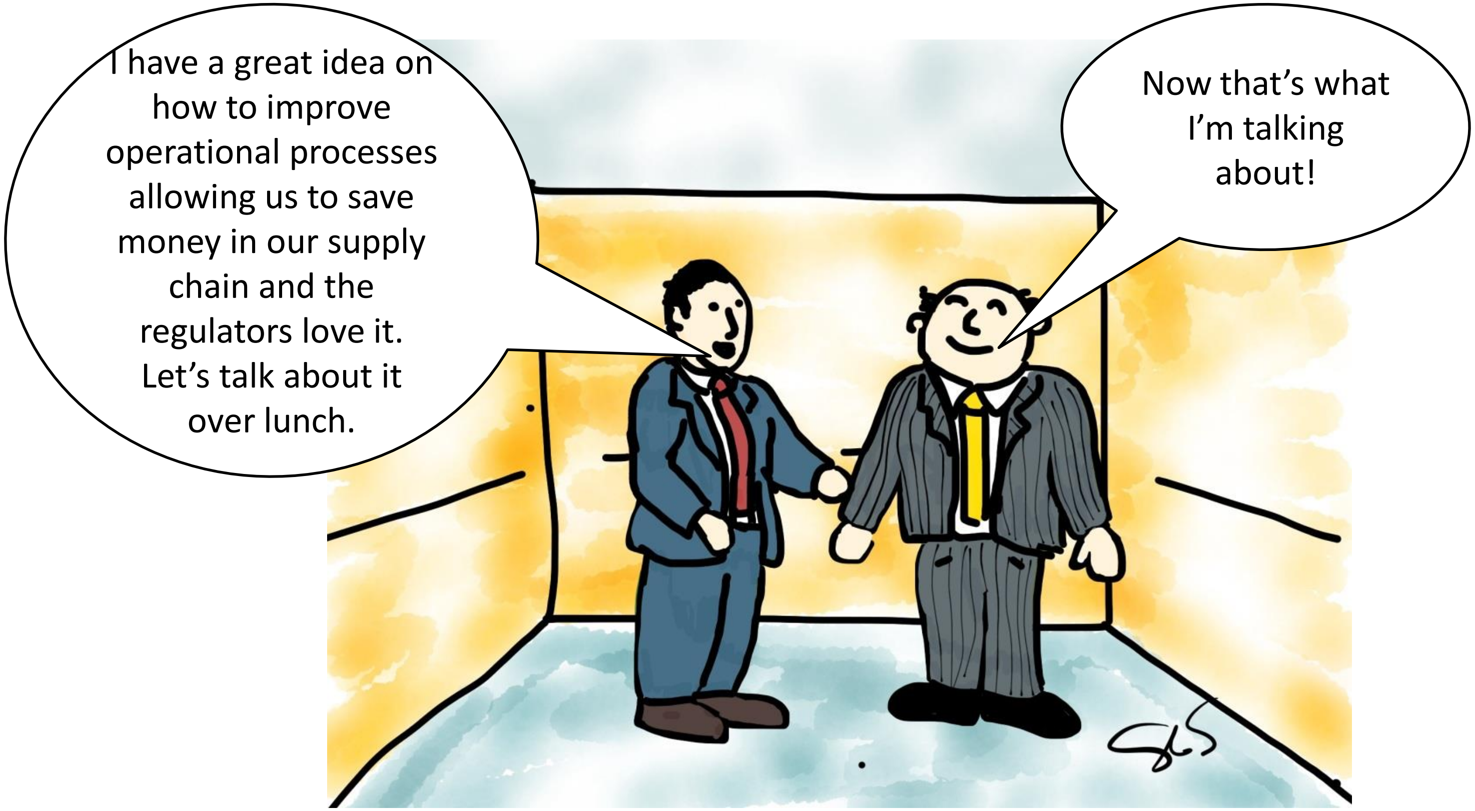
Resiliency Enabled

The CEO & audit manager ride the elevator…


We did an end to end review of customer account processing, found a few issues but got them resolved. We also started an assessment to review controls over “Project Barracuda” – which I know is one of your key objectives.
That’s great, but, how does the business look?

Resiliency, a Competitive Advantage

The CEO & **Business Resiliency** manager ride the elevator…


I have a great idea on how to improve operational processes allowing us to save money in our supply chain and the regulators love it. Let's talk about it over lunch.
Now that's what I'm talking about!

Thank You