

BSA THIRD PARTY RISK MANAGEMENT

April 11, 2024

Presenter



Stephen King, J.D.

Wolf & Company, P.C

Principal

(617) 428-5448

sking@wolfandco.com



Session Description

2023 into 2024 has been a tumultuous time.

Examiner expectations of governance and oversight have increased in the current regulatory environment. The optimistic view is recent events can serve to help prevent future losses if Risk Intelligent (“RQ”) capabilities can be deployed.

This session will discuss the Bank’s general responsibilities and focus on its role regarding BSA banking topics including third party relationships, change management as well as evolving products and services. We will discuss new and emerging risks in these areas, oversight and examination concerns. We will introduce the principles and recommend how they integrate into the next generation of ERM programs, or #ERMv3.0.



Discussion Agenda

- Current Risk Topics
 - Third Party Risk Management
 - Change Management
 - Evolving Risks
- What Comprises a Risk Intelligence (R^x) Capability
- Contemporary Risk Management Techniques
- Expanded C-suite and Board Reporting



Current Risk Topics

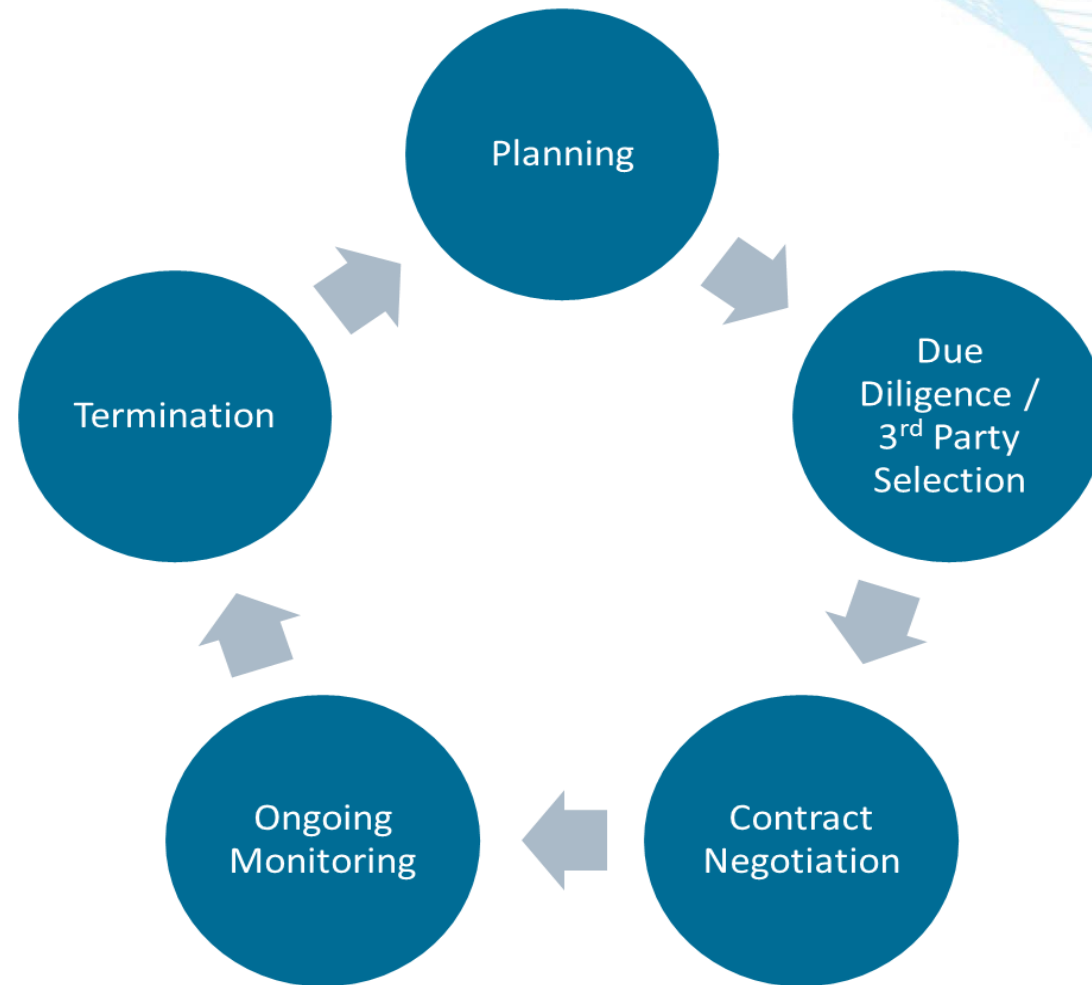
Third Party Risk Management

Types of Third-Party Relationships

- Outsourced Services
- Fintechs
 - SaaS vs BaaS
- Referral Arrangements



Third Party Risk Management



Third Party Risk Management

Planning

- Understand Business Purpose of Arrangement
- Align with Strategic Plan, Risk Appetite
- Identify Benefits, Risks, Impacts
- Establish Formal Approval Process
- Ensure Adequate Oversight Resources



Third Party Risk Management

Due Diligence / 3rd Party Selection

- Align each party's Strategic Plan & Objectives
- Review Due Diligence, including business partners and subcontractors
- Operations, IT, Legal, Finance, Compliance Evaluations
- Customized to Criticality, Complexity



Third Party Risk Management

Contract Negotiations

- Define nature and Scope of Arrangement
- Identify Responsibilities, Performance Standards
- Require Reporting Functions and Retention
- Right to Audit and Remediation
- Contractual Warranties, Indemnifications
- Termination Standards



Third Party Risk Management

Ongoing Monitoring

- Confirm Control Quality and Performance
- Review Performance and Testing
- Identify Material Changes
- Reassess Relationship Against Current Environment
- Integration into Bank Processes
- Establish Acceptable Measurements of Success, Risk, Termination



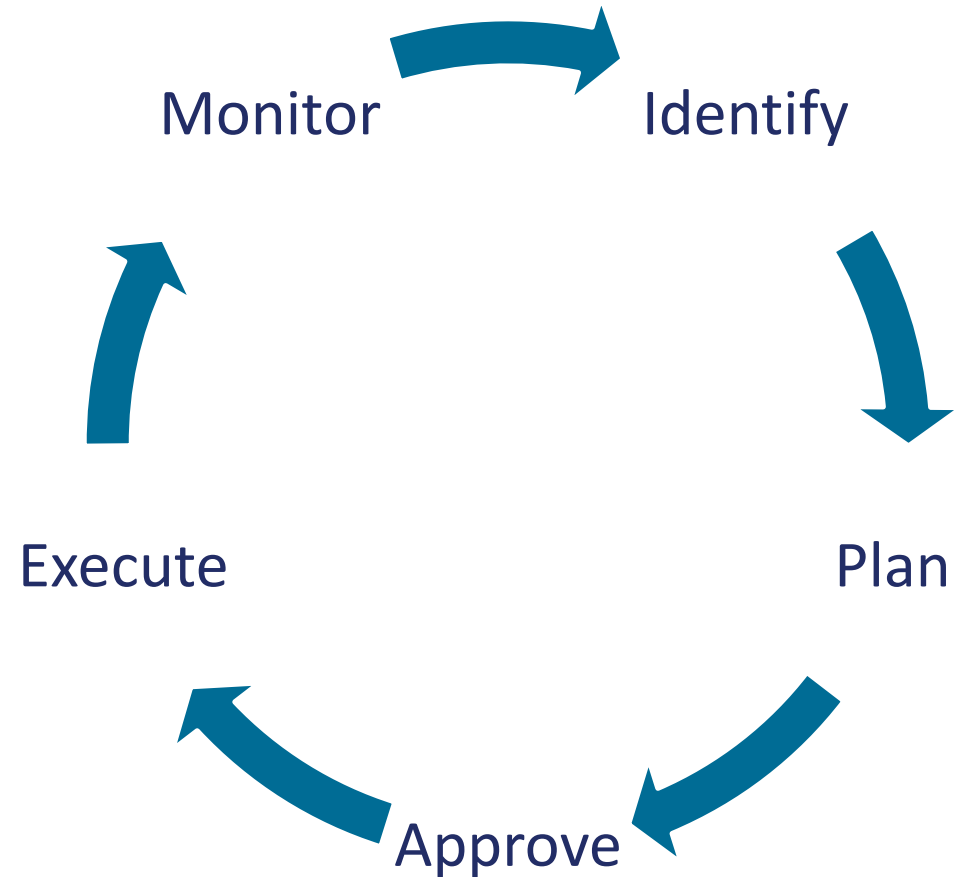
Third Party Risk Management

Termination

- Confirm Thresholds, Measurements
- Establish Remediation, Cure, De-Risk
- Effective Transition of Services
- Ongoing Warranties and Risks



Change Management



Change Management

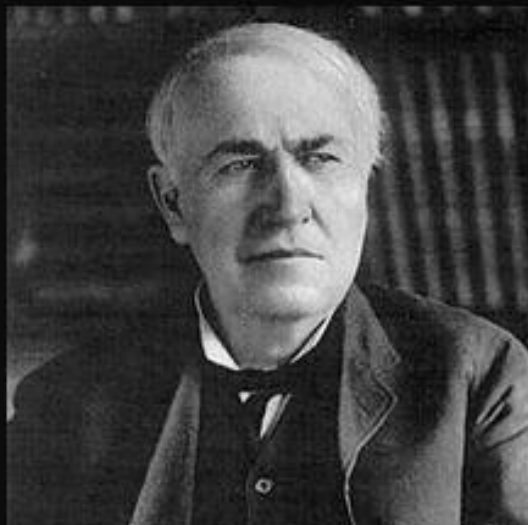
- Identification of Material Changes
- Assess Impact on Bank
- Coordination of Bank Functions
- Revision of Bank Processes and Controls
- Establishment of Measurements
- Reporting Metrics



Evolving Risks

- Increased Examiner Scrutiny
- Economic Uncertainty
- Cybersecurity Risk
- Compliance Risk / Legal Risk
- Talent Management





I have not failed 10,000 times. I have succeeded in proving that those 10,000 ways will not work.

~ Thomas A. Edison

AZ QUOTES

What Comprises a Risk Intelligence (R^Q) Capability

Risk Intelligence (R^Q)

- Goes way beyond inherent risk, controls, and residual risk.
- Risk Acceptance, Risk Mitigation, Risk Transfer, and Exiting the Business is elementary.
- Risk Assessment is critical but no longer sufficient.

Working Definition: Risk intelligence is the ability to identify, assess, and prioritize risks across an organization. It involves analyzing data, monitoring trends, and making informed decisions to mitigate risks. A risk-intelligent organization has integrated risk management into its culture, strategy, and operations.

But we are not all there (yet)!



Risk Management Maturity

Know Where You Are, and Where You Aspire To Be

☑ Compliance Risk Management (“Check-the-box”)

“I will do what I am required to keep the regulators happy.”

☑ Integrated Risk Management

“I wish to break down silos and see threats across the organization.”

☑ Strategic Risk Management

“RM is a strategic initiative and should provide us a competitive advantage.”



Risk Monitoring on the ERM Topology Landscape



Evolution to Risk Intelligence
Strategic, market, and operational risks are emerging faster and from more places.

The goal from R^Q is to answer these 3 questions:

1. How do we (and who) monitor for emerging risks?
2. Do we know if both internal and external data sources provide early warning data?
3. Can risk scenarios/events replace or leverage legacy risk assessments?

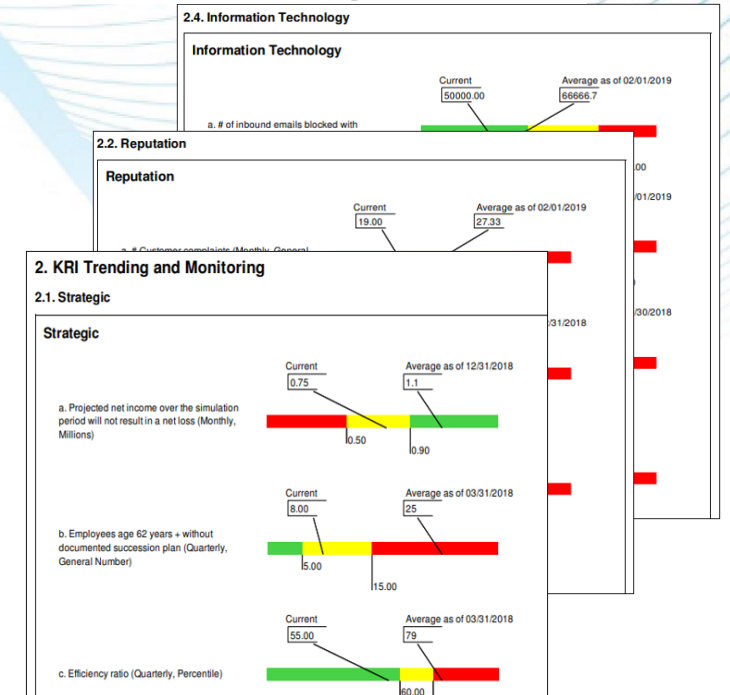
If risk management measures what we know,
risk sensing is an early warning indicator to mitigate risks before they cause harm.

Risk Monitoring Expands to Risk Sensing

1. Compliance Risk Management

Functional Risk Areas	Monitoring Frequency	Current Value	Previous Value	Risk Trend
Strategic				
1. Projected net income over the simulation period will not result in a net loss	Monthly	1	0.25	↓
2. Tier 1 Leverage ratio	Quarterly	13.2	11.8	→
3. CET1 Leverage Capital Ratio	Quarterly	13.4	12	↓
4. Efficiency ratio	Quarterly	55	70	↓
5. Employees age 62 years + without documented succession plan	Quarterly	8	12	→
Reputation				
1. Number of unscheduled branch or office closures	Quarterly	0	1	↓
2. Statements going to the wrong customers due to institution error	Quarterly	3	2	→
3. # Customer complaints	Monthly	10	18	→
4. Annualized Voluntary Turnover Ratio	Quarterly	4.5	1	↑

2. Integrated Risk Management

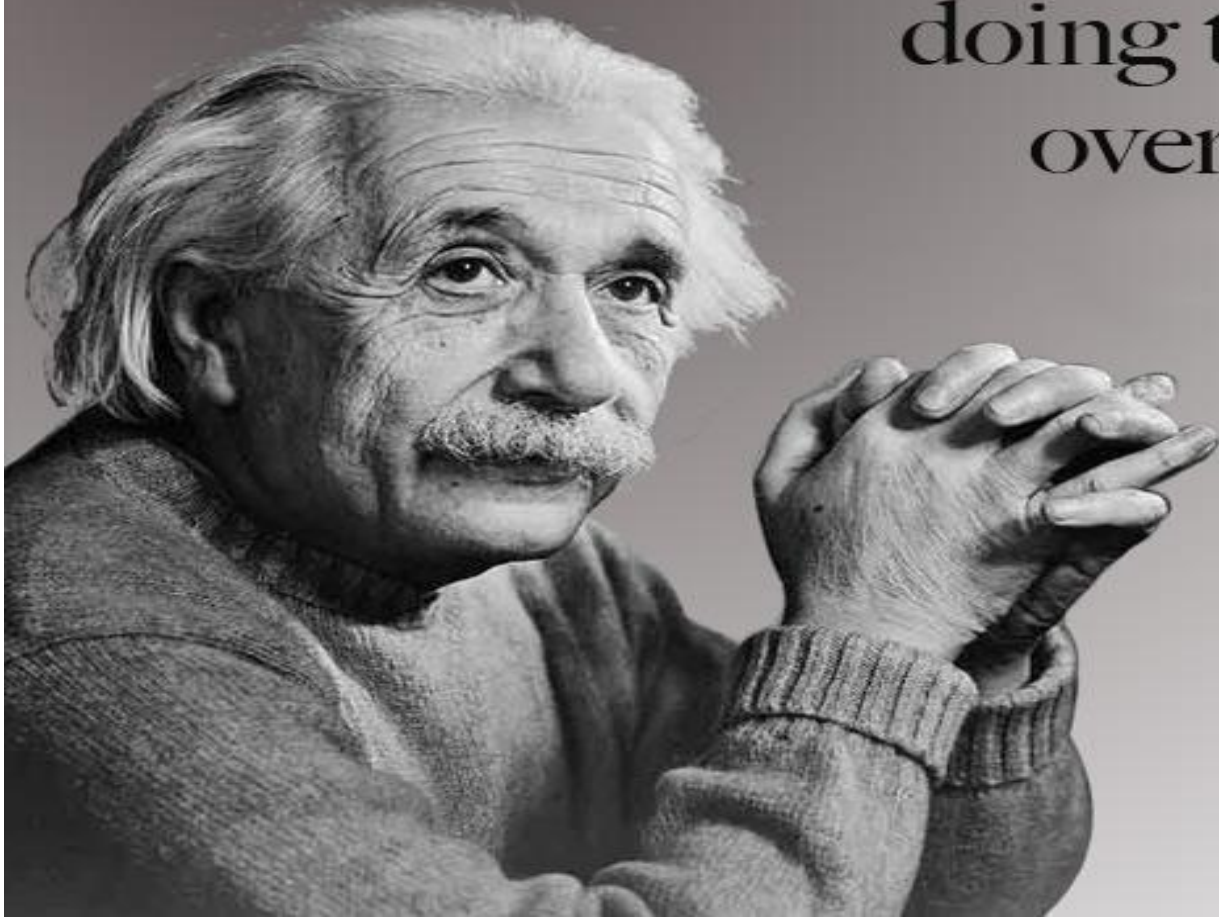


3. Strategic Risk Management and R^Q Organizations



Risk Sensing Capability requires Predictive Risk Intelligence (PRI)*

- ④ Wide Angle Focus
 - Define threat scenarios and develop Early Warning Indicators (EWI similar to KRI)
- ④ Outside-in Perspectives
 - External analysis and external data as it may be less biased than internal analysis
- ④ Listening Posts
 - Data and analysis on customer sentiments, employee sentiments, and regulatory sentiments
- ④ Tracking and Triggers
 - Real-time metrics (not historical key performance indicators and financial results)
- ④ Practical Applications
 - Integrated to ERM and risk governance, not a new, potentially siloed reporting mechanism



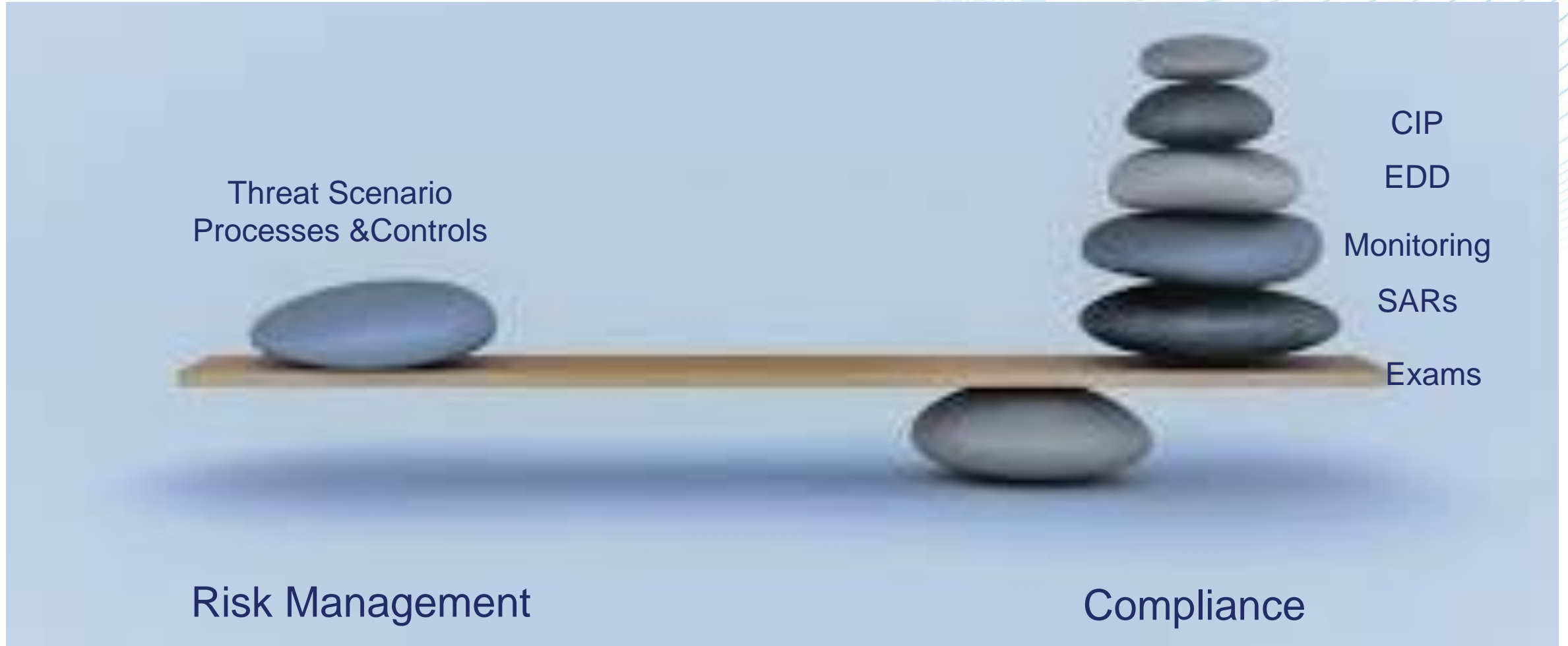
INSANITY:
doing the same thing over and
over again and expecting
different results.

~ Albert Einstein

WWW.SEVENQUOTES.COM

Contemporary Risk Management Techniques

RISK vs. COMPLIANCE



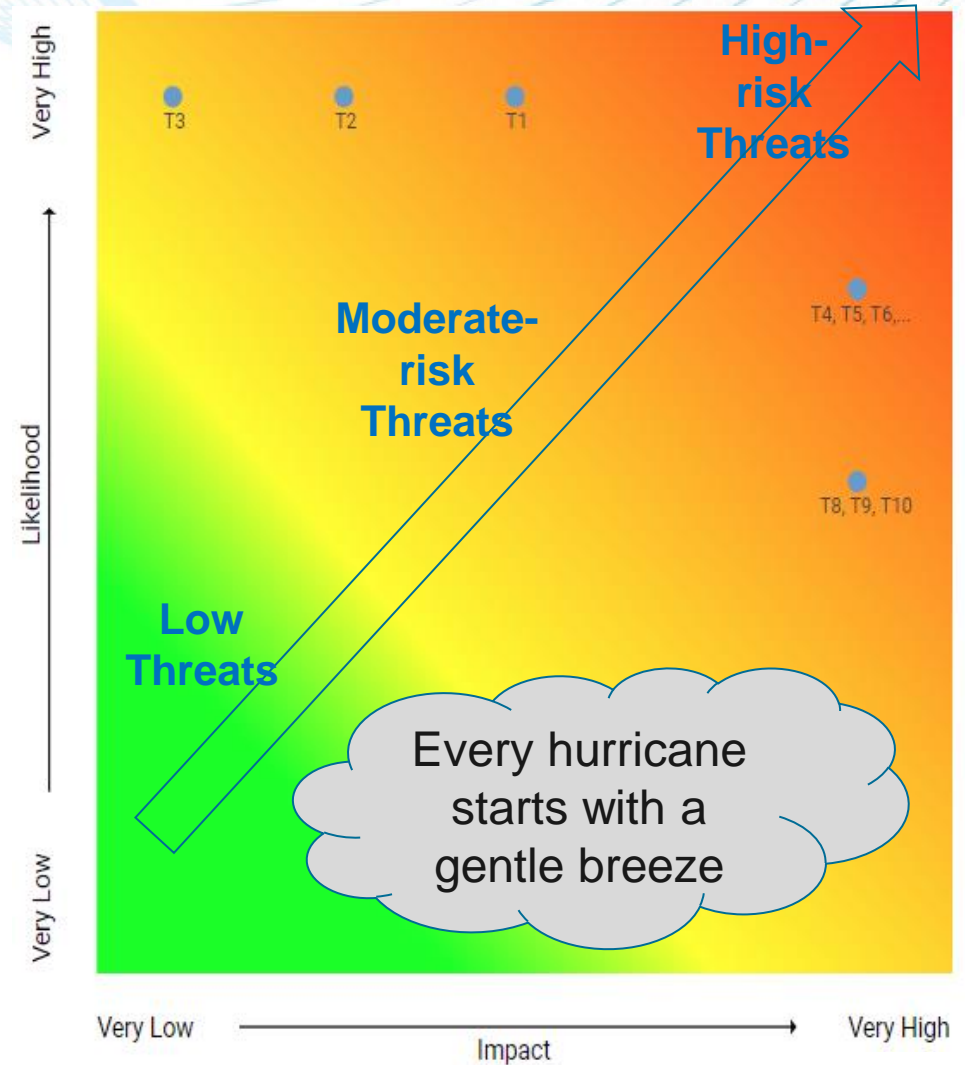
Risk Management – Laying the Foundation

1. Sample Threat Topology for Scenarios



Product/Service: Functional Risk Area:

Inreat ID	Threat Name	Product/Service	Risk Area
T1	Reputation / Material changes in customer relations and perceptions	Audit Services	Liquidity
T2	Reputation / Material changes in customer relations and perceptions	IT Assurance (RMS)	Liquidity
T3	Reputation / Material changes in customer relations and perceptions	Internal Audit (RMS), WolfPAC (RMS), Compliance ... Read More >>	Liquidity
T4	Risk to strategic objectives	IT Assurance (RMS), Audit Services, Internal Audit ... Read More >>	Strategic
T5	Economic environment (Strategic)	Audit Services	Strategic



Risk Management – Laying the Foundation

2. Risk Appetite

The degree of risk that will be acceptable in pursuit of business objectives

What are the risks we are both Willing and Unwilling to take?

Category	No Appetite	Lesser Appetite	Balanced Appetite	High Appetite
Compliance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Liquidity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Strategic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Int Rate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

RISK MANAGEMENT – LAYING THE FOUNDATION

1. RISK APPETITE - EXAMPLE

Qualitative statements

- We will strive to offer value to our customer while maintaining a viable business-lending program in accordance with the asset/liability policy.
- We will maintain the quality of the loan portfolio and minimize the losses associated with high-risk loans by establishing parameters to govern the maximum and minimum amounts of loans to be held in the Institution's loan portfolio.

Quantitative metrics

- Total investment in corporate bonds and notes $\leq 10\%$ of the Institution's assets.
- The Institution shall not permit any person or entity to borrow or guaranty, directly or indirectly, an amount(s), in the aggregate, which $> 1\%$ of its total assets.
- Ratio of the Non-Qualified Real Estate Loans to the net worth of the Institution $< 125\%$.
- "Criticized asset" loans $\geq 15\%$ of customer business loans.

RISK MANAGEMENT – LAYING THE FOUNDATION

2. RISK APPETITE - EXAMPLE

Policy

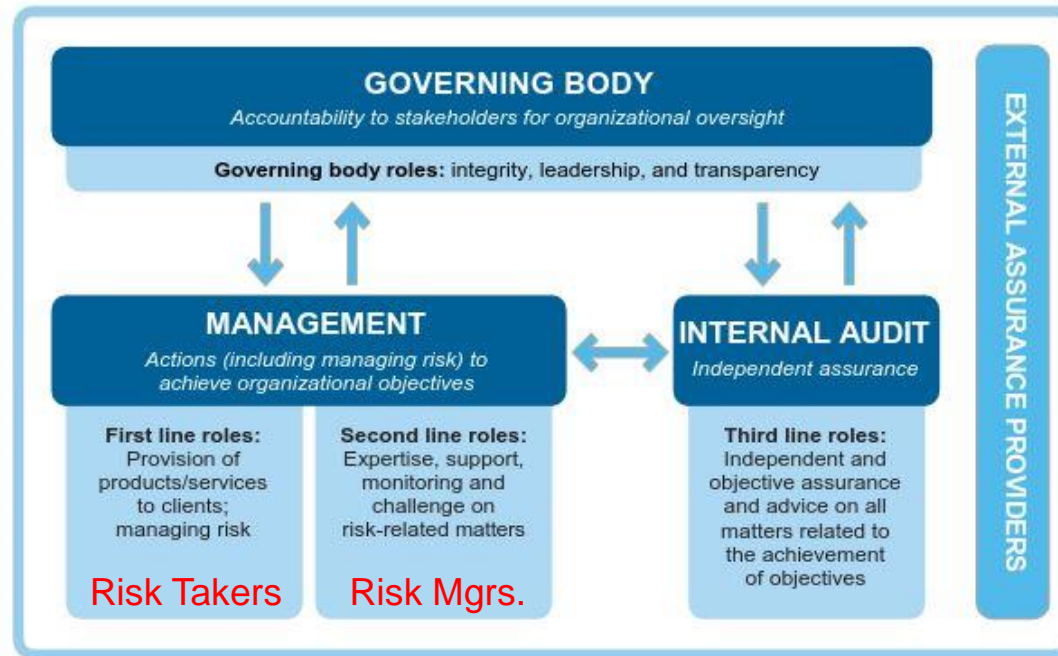


ERM or Risk Mgmt. Policy:

1. Purpose
2. People
3. Committee(s)
4. Processes
5. Reporting

Risk Management Framework

The IIA's Three Lines Model



- ✓ First Line are the "Risk Takers"
- ✓ Second Line are the "Risk Managers"
- ✓ Third Line is Independent Audit

Oversight



- ✓ Direct Board Reporting (tradition of Exec. Session)
- ✓ Required Exec. Mgr. Role (or designated role)
- ✓ Training Resources and Succession Planning

Expanded C-suite and Board Reporting

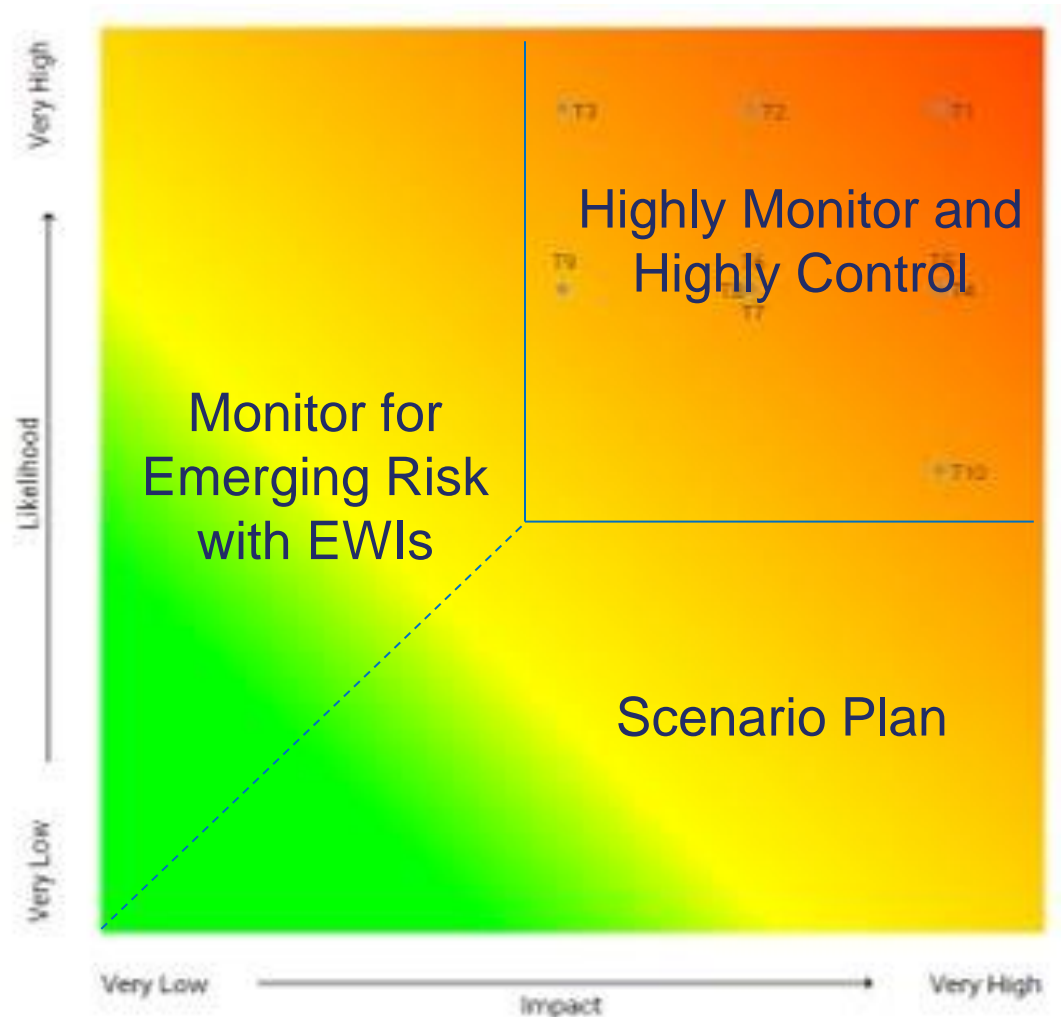
Ensure CRO Independence and Credible Challenge



- Direct Board Reporting (similar to Internal Auditor)
- Board Committee Executive Session
- Explicit Succession Planning

Add Board Risk Scenario Discussions

Results From: a) High Impact Low Likelihood Threats, and
b) Emerging Risks



Scenario Planning Techniques

- Can utilize models and table-top exercises
- Keep it simple (at first)
- Assemble the right people
- Work with the right data
- Develop comprehensive strategies
- Refresh scenarios frequently

Emerging Risk Monitoring Techniques

- Top down, By Line of Service, and By Department (engage other people)
- Report over time, and monitor direction of risk
- Develop indicators to alert for small changes

RISK MANAGEMENT – LAYING THE FOUNDATION IN SUMMARY – KNOW WHERE YOU ARE, AND WHERE YOU ASPIRE TO BE

☑ Compliance Risk Management (“Check-the-box”)

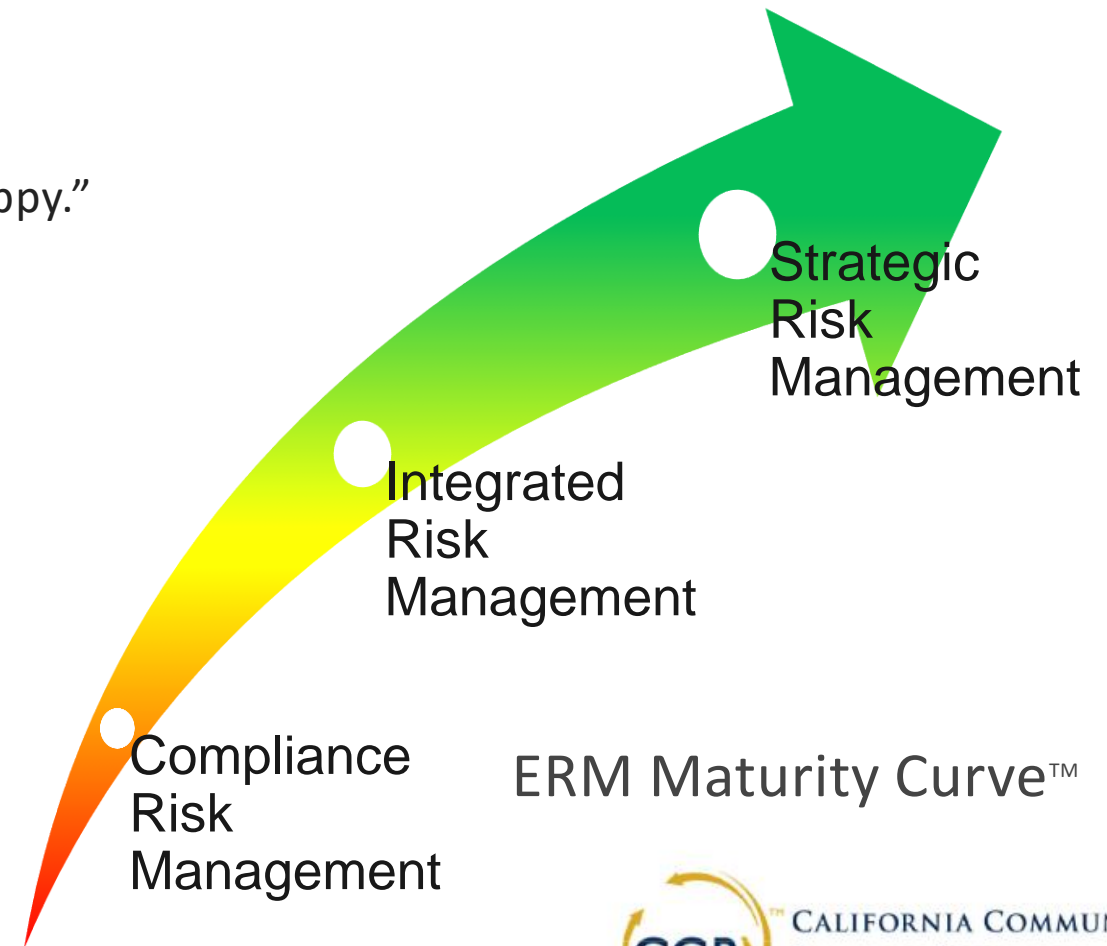
“I will do what I am required to keep the regulators happy.”

☑ Integrated Risk Management

“I wish to break down silos and see threats across the organization.”

☑ Strategic Risk Management

“RM is a strategic initiative and should provide us a competitive advantage.”



Concluding Remarks

Practical Considerations

1. Adopt a Product/Service Orientation to the Enterprise Risk Analysis
 - End-to-end service delivery from the customer's perspective, not the Bank's operations
 - The 3 Cs (communication + compilation + coordination)
 - Integration of of risk pillars (no more siloes)
2. Mature Risk Assessments to Scenario Assessments (based on RA results)
3. Develop Capital at Risk Measurement: Better Threat Impacts that are monetized, add control test results, and add *new* EWI to KPIs and KRIs

Observations

R^X Organizations move up the ERM maturity Curve. Acquired skills and abilities:

- Risk Sensing – getting insights not currently measured
- Portfolio Management (e.g., Product and Service)
- Risk Governance – Enterprise Level, not risk pillar-based (e.g., Technology, Operations, Credit, or Balance Sheet ALM)



Final Thought

“ Amateurs built the ark;
professionals built the Titanic. ”

Unknown



Bottom Line

Let's not delay in trying new approaches. We can't fix anything unless we are moving (forward).

Thank You



Stephen R. King, JD

Principal

Regulatory Compliance Services

✉ Skings@wolfandco.com

☎ 617-428-5448

OVERVIEW

Stephen serves as a Principal in the Regulatory Compliance Services group where he guides clients through the myriad of federal and state banking statutes from both an operational and legal perspective. Stephen is responsible for managing a team of professionals to ensure the successful delivery of compliance services to Wolf clients. Steve regularly presents compliance and governance program issues, strategies, techniques and trends at national and regional conferences for industry professionals.

Stephen joined the Firm in 1996 and over thirty years of experience as an advisor, facilitator and resource to financial institutions, fintechs, investment companies, and mortgage industry professionals

INVOLVEMENT

California Community Banking Network

New York Bankers Association Government Relation and
Lawyers Committee

New Jersey Bankers Association Compliance & CRA Committee



QUESTIONS



Appendices

WHO WE ARE

1911

WOLF & CO.
ESTABLISHED

400+

PROFESSIONALS



3 OFFICES IN:

- ✓ Boston, MA
- ✓ Springfield, MA
- ✓ Princeton, NJ



SERVICES OFFERED IN:

- ✓ Audit
- ✓ Tax
- ✓ Risk Management

WOLF
& COMPANY, P.C.

An Association Of Legally Independent Firms



SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.



ADVISORY

- [Business Continuity Planning](#)
- [Cybersecurity](#)
- [Data Analytics & Management](#)
- [Digital Transformation](#)
- [Enterprise Risk Management](#)
- [Environment, Social & Governance](#)
- [Internal Audit](#)
- [IT Audit](#)
- [Model Risk Management](#)
- [Outsourced Accounting Solutions](#)
- [Regulatory Compliance](#)
- [Strategic Planning](#)



ASSURANCE

- [Employee Benefit Plan Audits](#)
- [Financial Statements Audits](#)
- [HITRUST](#)
- [PCI DSS](#)
- [SOC Reporting](#)



TAX

- [Business Tax](#)
- [Federal](#)
- [International](#)
- [State & Local](#)
- [Private Client Group](#)



vSUITE

- Virtual risk management consulting services
- Virtual Chief Information Security Officer (vCISO)
 - Virtual Chief Privacy Officer (vCPO)
 - Virtual Chief Risk Officer (vCRO)
 - Virtual Vendor Management



WOLFPAC

Integrated risk management SaaS suite



DENSECURE

Advanced cyber threat experts

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Application Penetration Testing
- Network Penetration Testing
- Red Team Assessment
- Social Engineering
- Threat Emulation

WOLF
& COMPANY, P.C.

den
secure
by wolf & company, p.c.



WOLF
& COMPANY, P.C.

CCBN CALIFORNIA COMMUNITY
BANKING NETWORK

WOLFPAC INTEGRATED RISK MANAGEMENT® SOFTWARE

WolfPAC Integrated Risk Management helps banks & credit unions build a modern, scalable enterprise risk management program.



WolfPAC Pro™

The modular risk management platform used by hundreds of institutions for more than a decade:

- ✔ Bring consistency to your risk management program without the hassle of GRC systems
- ✔ Leave spreadsheet-based risk assessments behind for good
- ✔ Save time & money by increasing efficiency



WolfPAC Essentials™

The streamlined solution designed for use by smaller institutions:

- ✔ Business continuity planning
- ✔ Information Technology risk management
- ✔ No implementation fees
- ✔ Third-party (vendor) risk management

WOLF & COMPANY ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

INSIDE Public
Accounting

TOP 100
Accounting Firms

accountingTODAY

TOP 100
Accounting Firms
#2 BEST LARGE FIRM to
Work For Nationwide

TOP FIRMS:
New England

BOSTON
BUSINESS JOURNAL

- ⊙ Area's Best Places to Work
- ⊙ Area's Most Admired Companies
- ⊙ Area's Fastest Growing Private Companies
- ⊙ Area's Largest I.T. Consulting Firms

Forbes

America's Best
Tax and Accounting
Firms of 2022, 2021