DRIVING EFFECTIVE INTERNAL AUDITS THROUGH COMPLIANCE RISK ASSESSMENTS

CALIFORNIA BANKERS ASSOCIATION

LAUREL SYKES

AMERICAN RIVIERA BANK

Laurel Sykes is EVP and Chief Risk Officer for California-based American Riviera Bank, with offices in the Santa Barbara and San Luis Obispo Counties.

STEPHANIE LYON, ESQ. CRCM, CERP, CAMS

NCONTRACTS

As the VP of Regulatory Content Strategy and Compliance, Stephanie leads a team of industry experts to enhance the Ncontracts suite of integrated risk and compliance solutions. Stephanie is the author of the Upside of Compliance, a practical guide for compliance professionals.

MEREDITH PIOTTI

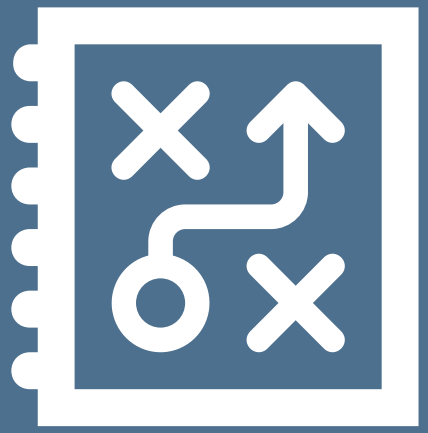
WOLF & COMPANY

Merry Piotti is a Principal within the Advisory Group of a National Accounting Firm assisting over 400 Financial Institutions. She oversees the firm’s data analytics practice.

ROADMAP

- Creating a Compliance Risk Assessment
- Leveraging Risk Assessments in Audit Planning
- Remediation and Corrective Action

CREATING A COMPLIANCE RISK ASSESSMENT



COMPLIANCE RISK ASSESSMENT ELEMENTS

Risk Identification

Risk Measurement

Risk Response

Monitoring

IDENTIFYING COMPLIANCE RISKS

ANALYZE THE REGULATORY LANDSCAPE

- Identify requirements and prohibitions
- Stay on top of reg change
- Don’t forget about state laws and regs such as elder abuse and privacy

KEEP AN INVENTORY WITH LINKAGES AND DATA

- Product, service, activity, department
- Regulator
- Level
- Thresholds

START WITH YOUR INVENTORY

ANTI-MONEY LAUNDERING RISK ASSESSMENT

Customers/Entities

- Transaction Types
- Account Types
- Methods for Interacting (Including Third-parties)

Geography

- Transactions
- Countries and locations

Products/Services

- Third-parties

REQUIREMENTS ARE GROWING

"…BSA compliance risk assessments provide a comprehensive and accurate assessment of the Bank's BSA compliance risk…at a minimum:

a) Analysis and documentation to identify: (i) the quantity of risk associated with third-party activities, (ii) any control weaknesses and gaps, (iii) any deficiencies identified during independent testing, and (iv) mitigating factors related to identified weaknesses; and

b) policies and procedures for developing accurate MIS reporting, including a Money Laundering Risk report… to identify and manage money laundering, terrorist financing, and other illicit finance risks related to the Bank's third-party relationships…"

BEST PRACTICES FOR STRUCTURING COMPLIANCE RISK ASSESSMENTS

Categorizing Risk Assessments by Reg, Product/Service, or Department

What's Recommended by Regulators

Practitioners' Advice

FORMAT MAY BE DIFFERENT DEPENDING ON THE REGULATORY REQUIREMENTS

DETERMINING PROGRAM ELEMENTS

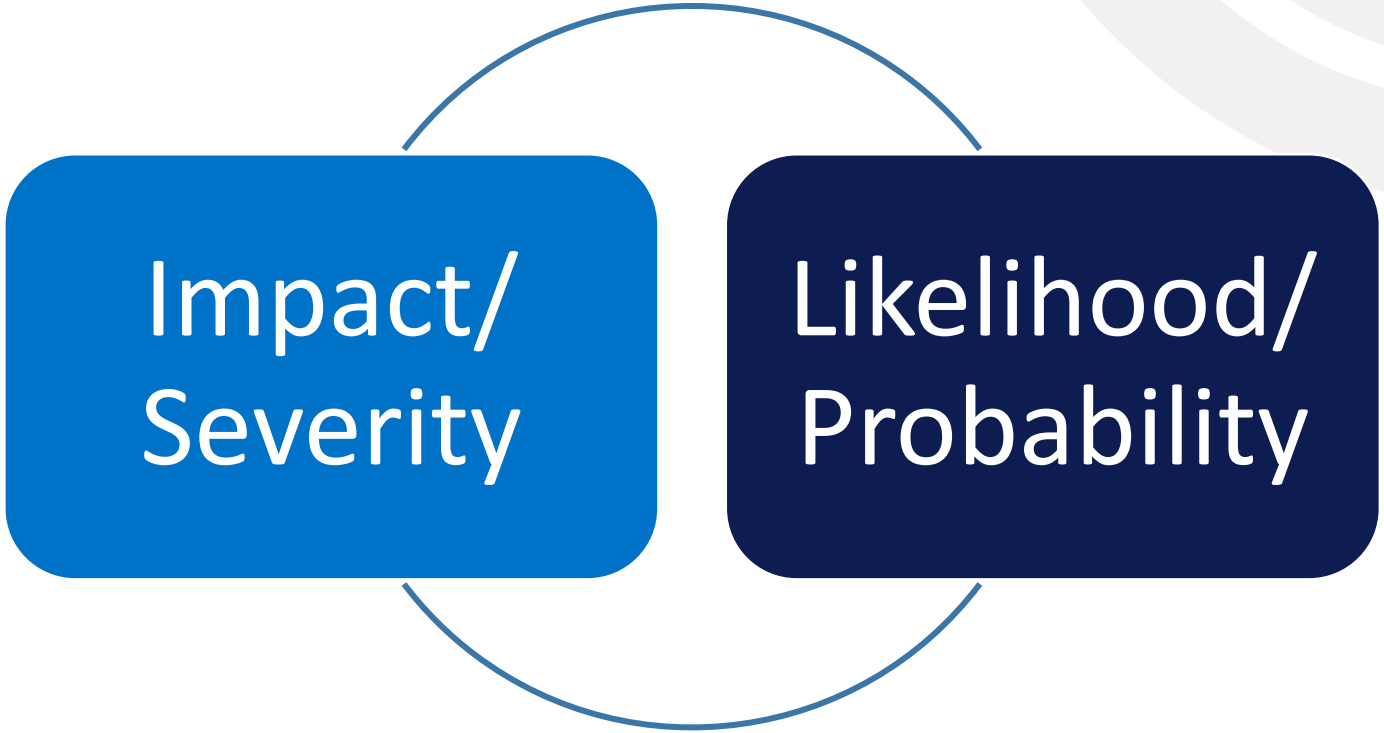
Business Area	Inherent Risk	Control Effectiveness	Residual Exposure
BSA/AML	High-Moderate	77.63%	Low
Customers	High-Moderate	77.58%	Low
Geography	High	78.41%	Low-Mod
Domestic	High	78.42%	Low-Mod
Foreign	High	78.40%	Low-Mod
OFAC	High-Moderate	75.98%	Low
Product/Service	High	77.89%	Low
ATM/Debit Cards	Low-Mod	78.40%	Low
Cash Management	High	78.40%	Low-Mod
Deposit Accounts	High	76.13%	Low
Lending Activities	High-Moderate	78.40%	Low
Monetary Instruments	High-Moderate	78.40%	Low
Online and Mobile Banking	High	78.40%	Low-Mod
Safe Deposit	Low-Mod	78.40%	Low
Wire Transfers	High	80.01%	Low-Mod

Business Area	Inherent Risk	Control Effectiveness	Residual Exposure
ATM Safety and Surcharge - Division 4 (included with Branches)	High-Moderate	78.40%	Low
Community Reinvestment Act (CRA)	High	72.28%	High-Moderate
Deposit Compliance	High	67.01%	Low-Mod
Regulation CC	High	76.36%	Low-Mod
Regulation DD	High	69.83%	Low-Mod
Regulation E	High	63.20%	High-Moderate
Elder Abuse - CA Welfare & Inst Code 15630	High	68.60%	High-Moderate
Information Privacy Act - Division 1.4	High-Moderate	78.40%	Low
Lending Compliance	High	56.08%	High-Moderate
California Division 1.7 for Covered Loans	High	78.40%	Low
Fair Debt Collection Practices Act (including Rosenthal Act)	High	58.57%	High-Moderate
FCRA	High	62.88%	High-Moderate
Flood	High	56.72%	High-Moderate
Home Mortgage Disclosure Act (HMDA)	High	74.32%	Low-Mod
Regulation B	High	55.00%	High-Moderate
Regulation O (Insider Loans)	High	78.40%	Low-Mod
Regulation X RESPA	High	42.15%	High-Moderate
Regulation Z TILA	High-Moderate	54.64%	Low-Mod
S.A.F.E Act	High-Moderate	78.40%	Low
TRID	High	54.56%	High-Moderate
UDAAP	High	65.00%	Low-Mod

DETERMINING MONITORING PLAN

KEY RISK MEASUREMENT TERMS

Inherent Risk



IMPACT

CONSIDER

- Reputation Risk
- Consumer Harm
- Regulatory Fines
- External Costs

DEFINE LEVELS OF IMPACT

High

Moderate High

Moderate

Low Moderate

Low

LIKELIHOOD

CONSIDER

- Findings
- Audit
- Examinations
- Awareness / Relevance
- Frequency of Transaction / Product Usage

DEFINE LEVELS OF IMPACT

High

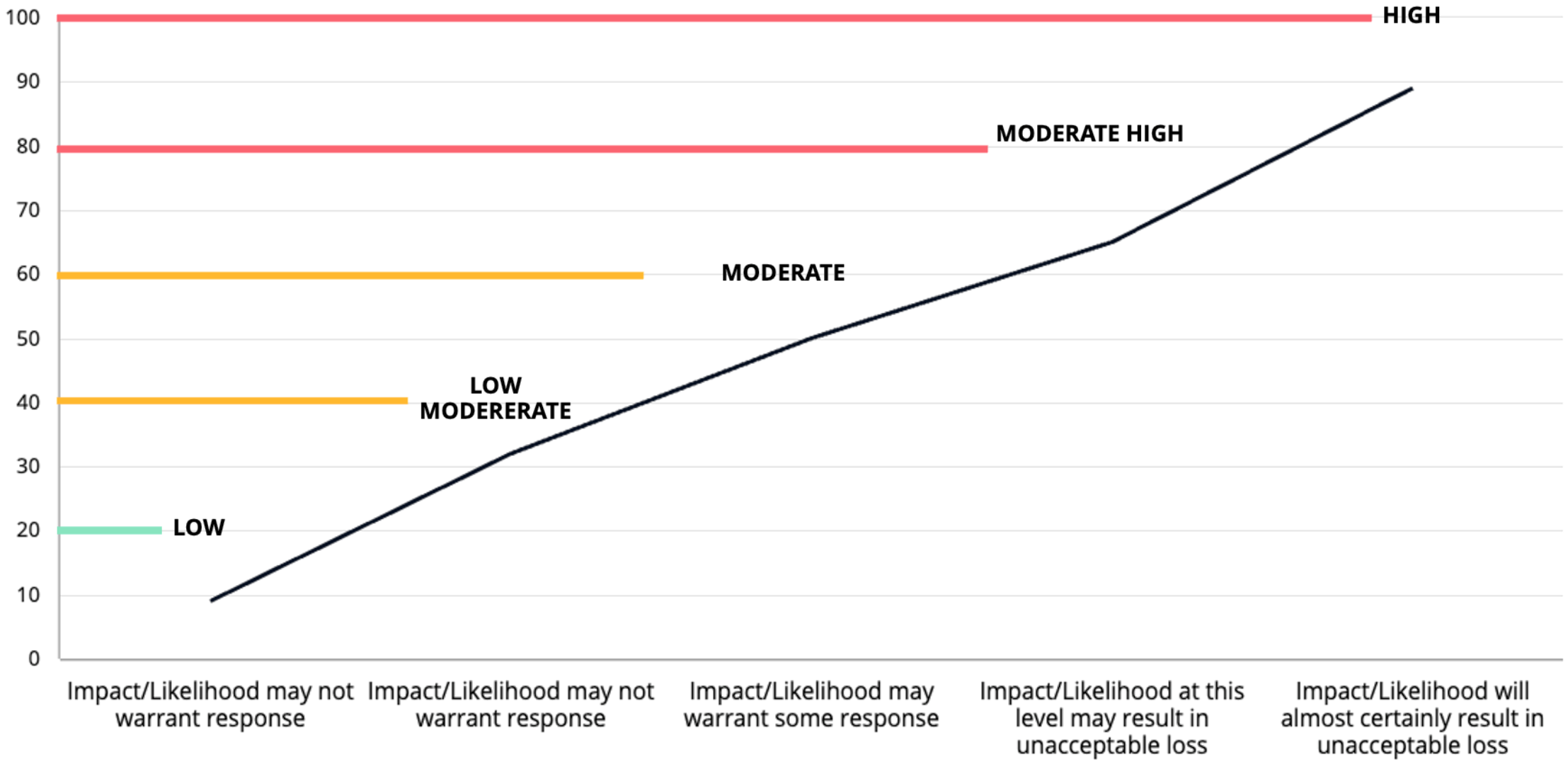
Moderate High

Moderate

Low Moderate

Low

IDENTIFY INHERENT RISK LEVEL



IDENTIFY INHERENT RISK LEVEL

Impact

(0 – 100)

80 points

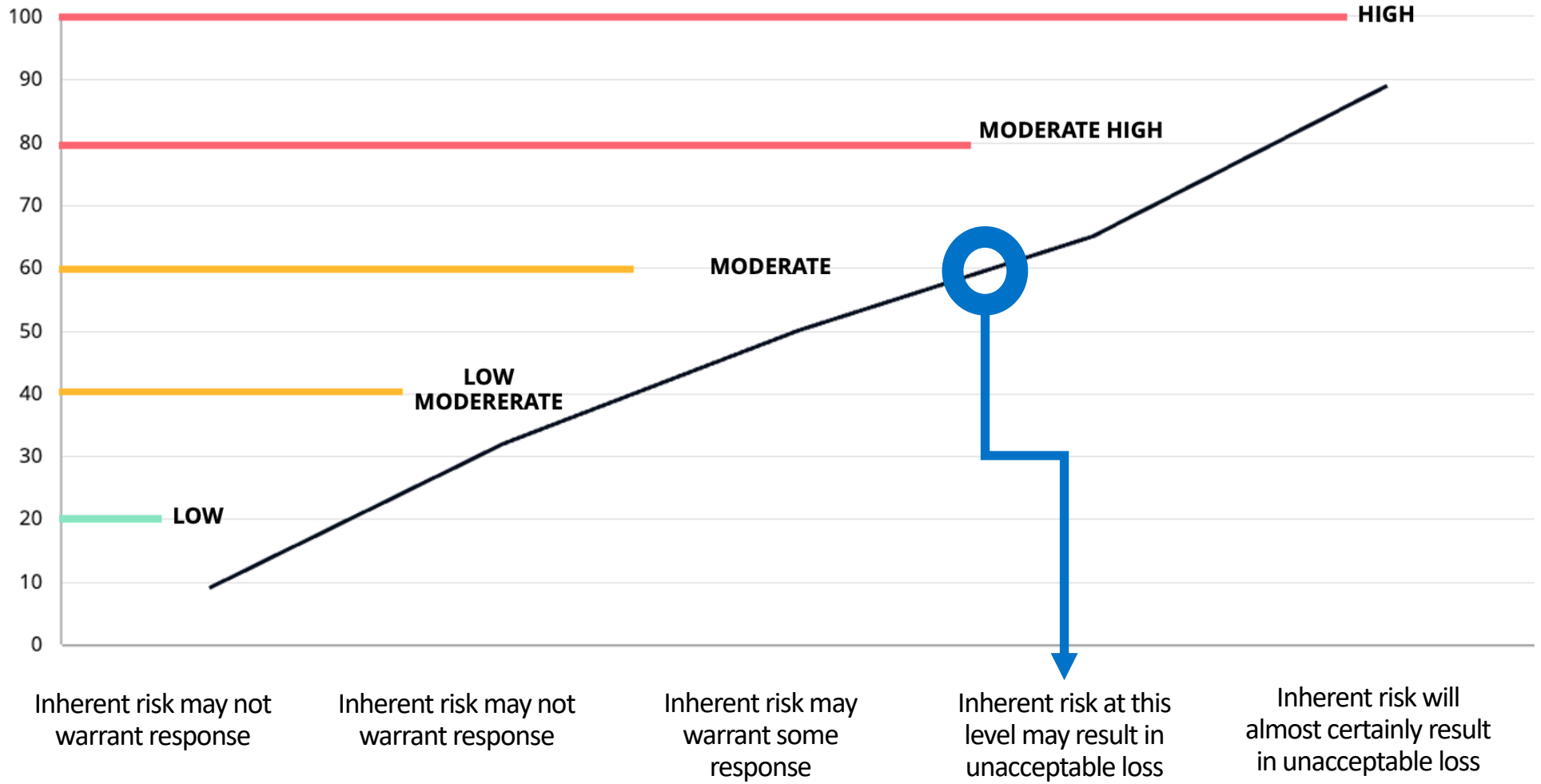
×

Likelihood

(0 – 100%)

80% = .80

=



RISK RESPONSE

1. Mitigate
   - Identify the Control
   - Assess the Weight
2. Accept
3. Transfer
4. Decline

Having defined risk tolerance and appetite makes it easier to suggest a course of action

MITIGATION

- Certain controls help mitigate more risk than others
- Type of Control
  - Preventative
  - Detective
  - Corrective
- Automated vs Manual

Inherent risk – Control(s) = Residual Risk

MONITORING

TRIGGERING EVENTS FOR RISK ASSESSMENT UPDATES:

Internal and external events like audit findings, regulatory change, agency priorities, new product, outdated training and policies

UPDATE:

- Impact (rare)
- Likelihood (potential)
- Control effectiveness (common)

HOT TOPICS AMPLIFYING COMPLIANCE RISK

- Fees
- Overdrafts
- AML/CFT
- AI/ML
- Fair Lending
- Lending Compliance
- CRA Modernization

- Identify heightened compliance risk via:
  - Common violations
  - Complaint data
  - Enforcements
  - Lawsuits
  - Audit and exam results

LEVERAGING RISK ASSESSMENTS IN AUDIT PLANNING

DISCLAIMER

- The following section envisions a world where:
  - Financial institutions have access to the data they need to support risk-based decisions
  - Regulators fully support risk- based auditing

USING RISK ASSESSMENTS TO INFORM AUDIT SCOPES

- How should your compliance risk assessment help define scopes:
  - Helps prioritize areas of focus within the compliance program
  - Identifies where strong internal controls are warranted
  - Permits appropriate dedication of resources to areas that need them most
  - Assists in the development of the audit plan and compliance monitoring program
  - Meets regulator expectations

USING RISK ASSESSMENTS TO INFORM AUDIT SCOPE

Is your risk assessment detailed enough?

Does it reflect your current reality?

How are you coordinating with other risk areas?

BANK SECRECY ACT – REGULATORY REQUIREMENTS

Requirement	Regulatory Risks	Institutional Changes	Exposure Penalties	Regulatory Changes / Environment	Calculated Monitoring Frequency	Monitoring Frequency Override
There is a BSA Policy approved by the Board.	Low	Low	High	Low	Semi-Annually	Annually
The policy contains the 4 required elements (designated Bank Secrecy Act Officer, training, internal controls, independent testing)	Low	Low	High	Moderate	Semi-Annually	Annually
Training is conducted to ensure employee compliance with regulatory requirements (suggested at least annually).	Low	Low	High	Low	Semi-Annually	Semi-Annually
There are procedures for identifying reportable transactions and completing CTRs and CMIRs (FinCEN Form 105 for international transactions).	Low	Low	High	High	Quarterly	Quarterly
There are procedures to record required information relating to currency purchases of negotiable instruments from $3,000 to $10,000	High	High	High	Moderate	Monthly	Monthly
There are procedures to record required information relating to wire transfers exceeding $3,000.	Low	Low	High	Low	Semi-Annually	Semi-Annually
There are procedures for investigating and reporting suspicious activities, including accurate and timely completion of SARs, subsequent SARs and reporting SARs to the Board.	Low	High	High	High	Monthly	Monthly

PRIORITIZING AUDITS

IIA Practice Guide Developing a Risk Based Internal Audit Plan

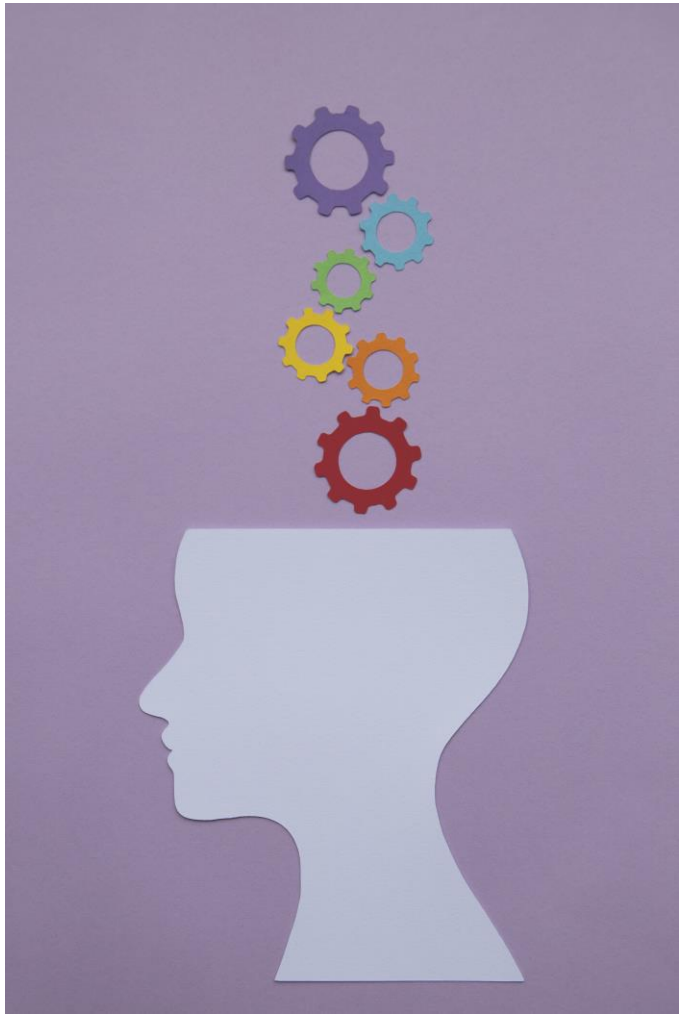
Figure 1: Internal Audit Plan Development Cycle

FRAMEWORK FOR PRIORITIZING AUDITS

- Continuous Risk Assessment Methodology
- Predetermined Audit Frequency

- Either Method must include
  - Regulatory Required Audits
  - Mission-critical engagements

OTHER CONSIDERATION POINTS



MANAGEMENT AND BOARD REQUESTS

CHANGES TO OPERATIONS

CHANGES TO REGULATION

CHANGES IN REGULATORY FOCUS

CHALLENGES WITH REGULATORY REQUIREMENTS

- Targeted scopes
- Extended timeframes
- Leveraging all work performed

TOOLS AND TECHNIQUES FOR AUDIT PLANNING

Technology Enabled	Tried and True
• Data Capture • Data Analytics • Continuous Monitoring	• Self Assessment • Planning Process • Leveraging Monitoring

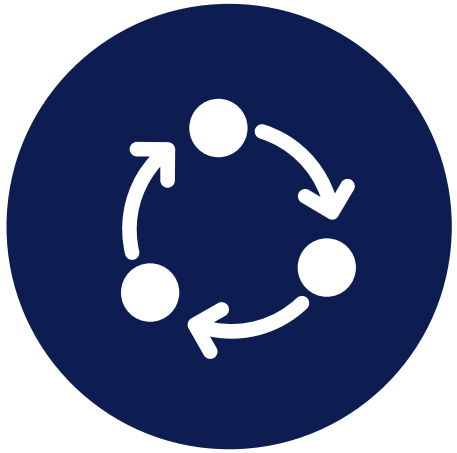
REMEDIATION & CORRECTIVE ACTION

BE PROACTIVE

- Audits and compliance testing allow the bank to initiative self-corrective action
- Remediation program should address root cause and determine the severity, duration, and perverseness of the violation

EFFECTIVE FOLLOW-UP ON CORRECTIVE ACTIONS

Prevent repeat violations through:



A Systematic Process

Monitoring and Testing

Deploying audit resources to areas of concern and heightened risk

KEY TAKEAWAYS

- Go back to foundational risk management principes and ensure there are objective methods to assess risk
- Continually monitor for change and make changes to your risk assessments to reflect current realities
- Balance risk assessment with real world data to construct a tailored audit plan
- Ensure root cause analysis and systematic remediation to prevent repeat violations and issues

Q&A

THANK YOU!

California Bankers Association (CBA) makes no representations or warranties about the accuracy or suitability of any information in the webinars and related materials (such as presentation documents and recordings); all such content is provided to webinar registrants on an “as is” basis. WB HEREBY DISCLAIMS ALL WARRANTIES and Conditions Express Implied Statutory or Otherwise REGARDING THE CONTENTS OF THESE MATERIALS, INCLUDING WITHOUT LIMITATION ALL WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. WB is not liable for any claims, losses, or damages of any kind arising out of or in any way related to this information provided by presenters of these webinars. CBA hereby disclaims all liability for any claims, losses, or damages of any kind in connection with use or application of these materials. The information contained in these webinars and related materials is not intended to constitute legal advice or the rendering of legal, consulting, or other professional services of any kind. Users of these materials should not in any manner rely upon or construe the information or resource materials in these materials as legal, or other professional advice and should not act or fail to act based upon the information in these materials without seeking the services of a competent legal or other professional.