Crowe Horwath

Smart decisions. Lasting value.™

Indiana Bankers Association Internal Audit Seminar

October 11 & 12, 2016

Agenda

- Introduction
- Auditing the Lending Function
- Auditing Mortgage Banking Functions
- ERM and Bank Risk Management Issues
- Auditing Corporate Governance
- Model Risk Management
- Auditing the Accounting Function
- Recent Trends in Financial Institution Fraud

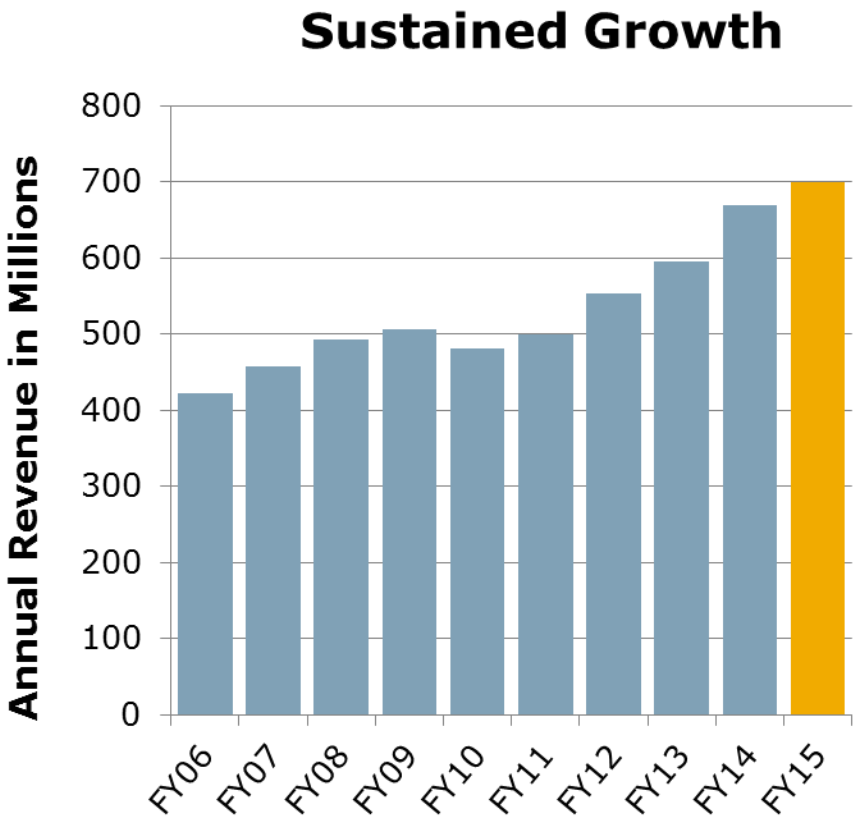
Introduction

A Little About the Class

- **Name**
- Bank/Company/Regulatory Agency
- Asset Size/Client Base
- Years in Banking
- Years in Auditing/Security/Compliance
- **Your Objective for Class**
- Something FUN about YOU
- Favorite Food
- Favorite Book/Movie
- **Birthday (Month and Day)**

Sustained Growth and Stability

- Founded in 1942, Crowe is celebrating more than 70 years of stability, growth, and innovation.
- Crowe ranks as the eighth largest **national** firm based on U.S. net revenue.*
- Crowe Horwath International ranks as the ninth largest **international** network.

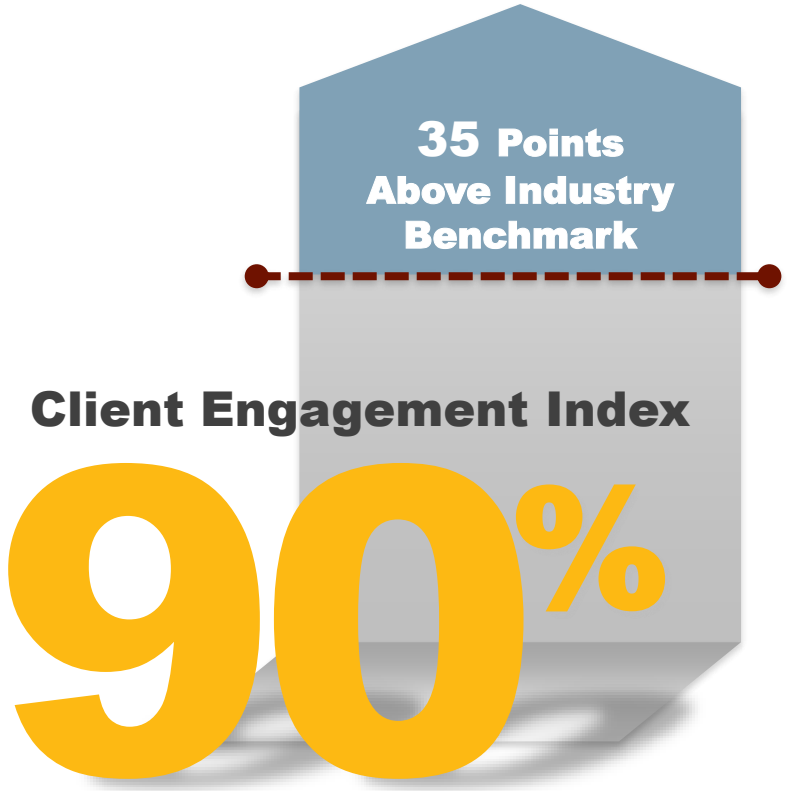


accountingTODAY 2015 TOP 100 FIRMS

* The 2014 Accounting Today Top 100 Firms

Exceptional Client Experience

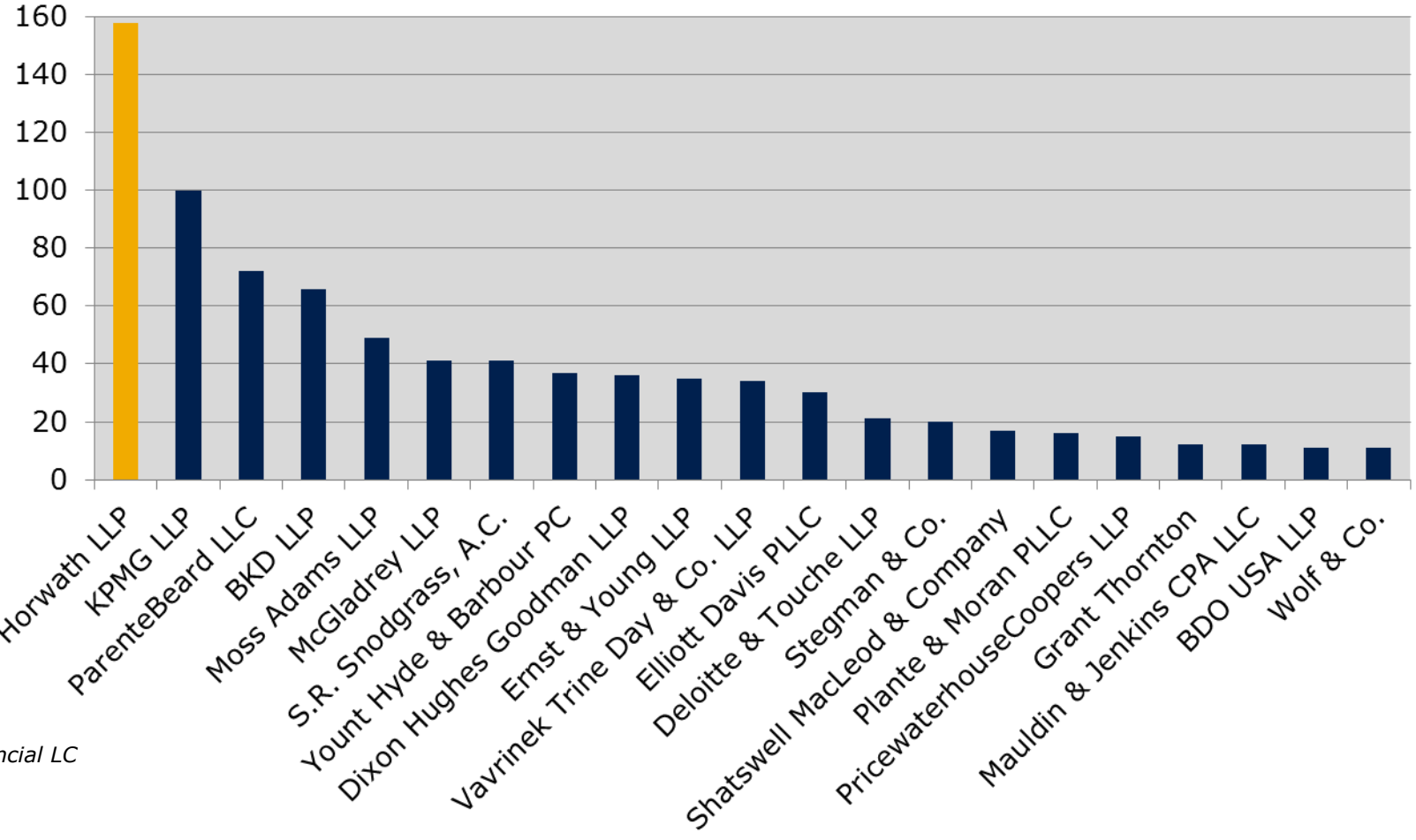
- Annually, we work with independent researchers to survey clients to help us understand how we can improve our client experience and earn their trust and recommendations.
- Crowe has achieved a **90 percent client engagement index, outperforming the accounting industry benchmark by 35 points.***
- An engaged client is one who:
  - Really likes working with Crowe
  - Will recommend Crowe
  - Would go out of my way to keep working with Crowe
  - Will continue to use Crowe



* "Most Engaged Customers" Business to Business Survey, Accounting and Tax, PeopleMetrics Inc. 2013

Financial Industry Specialization

- Crowe ranks No. 1 nationally in the number of audits for publicly traded financial institutions.*



** Source: SNL Financial LC 2012*

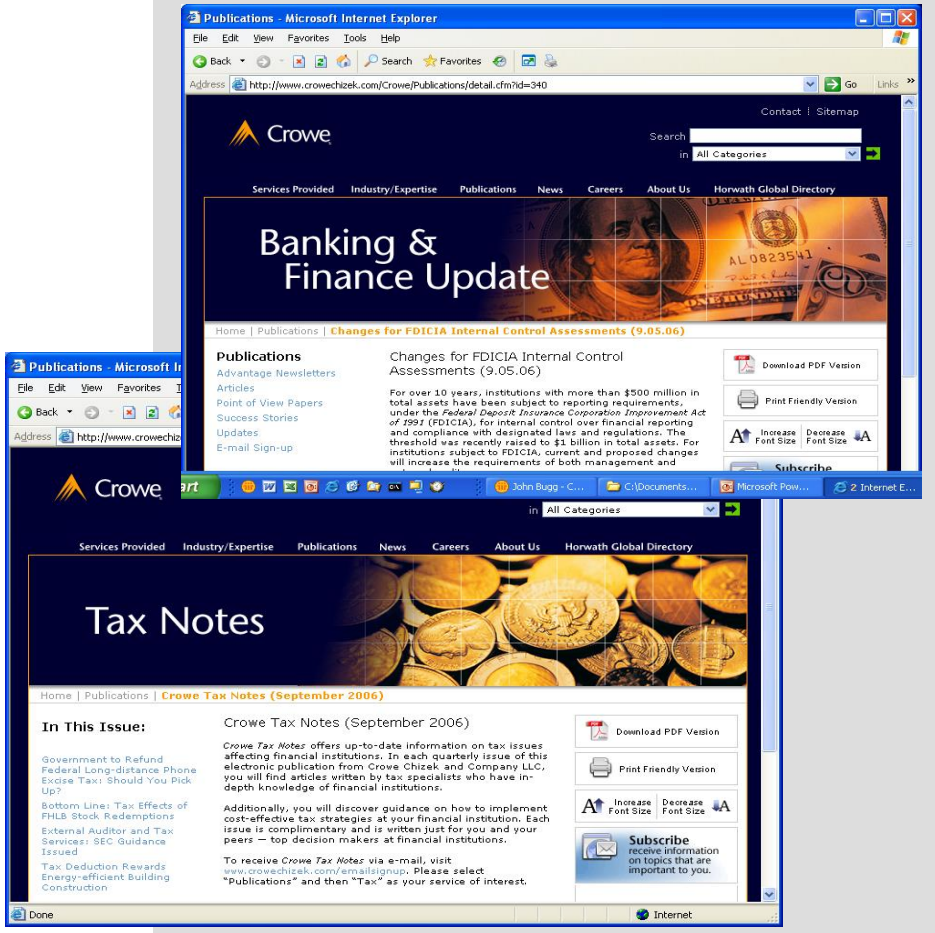
Crowe Horwath Financial Institutions Group

- By serving over 1,800 Financial Institutions across the country, Crowe has in-depth knowledge and experience in banking.
  - We have built strong relationships with federal and state regulators
  - We actively support national and state trade associations and provide thought leaders for speaking and publishing
  - Our thought leaders hold leadership positions and serve on boards of national accounting and banking organizations
  - We publish timely industry updates and papers on emerging issues such as accounting, tax, compliance, benefits and performance
  - We offer the most comprehensive list of services of any U.S. firm

Crowe Horwath Financial Institutions Group

- Crowe publishes timely industry information on critical topics such as accounting issues, tax updates, compliance and bank performance
- Visit www.crowehorwath.com/emailSignup to register for banking e-communications
- Crowe sends periodic invitations for online learning events
- Crowe's Annual Financial Institution Client Conference
- We also provide a number of online resource centers for areas of special interest such as AML/BSA

Crowe's e-Communications



Crowe Horwath Financial Institutions Group

- Crowe's Financial Institution Group works 100% of its time with financial institutions
  - Outstanding customer service is critical to your industry –

    Crowe reflects your commitment by helping clients succeed
  - Our project management focused audit approach
  - Our use of technology to streamline the audit
  - Our Client Service Standards set high expectations for our audit teams to deliver client satisfaction
  - Our commitment to complete our work on time
  - We audit our performance by asking for your feedback through our Client Engagement Survey and other processes

Assurance and Financial Advisory Services

We audit over 500 financial institutions throughout the United States and Puerto Rico, including approximately 125 SEC registrants and nearly 50 with assets greater than $1 billion.

- Audits, reviews and compilations
- Agreed-upon procedures
- Forecasts and projections
- SEC compliance and reporting
- Public securities registration and offerings
- Trust
- Information technology
- Brokerage
- Mortgage banking
- Third-party service reviews
- Loan review
- Fiduciary requirements

Risk Consulting

We help our 800+ financial institutions risk clients implement effective solutions to manage the full spectrum of risks.

Risk Management Services

- Internal audit: outsourcing and co-sourcing
- Information Technology audits
- Credit risk consulting
- Enterprise risk management
- Corporate governance

Contingency Planning Services

- Business resumption
- Disaster recovery
- Incident response

Internal Controls

- Sarbanes-Oxley
- AT 501 design and testing

Compliance Improvement Services

- Consumer compliance
- Bank Secrecy Act
- Enterprise compliance risk management

Anti-Money Laundering Services

We provide strategies to derive long-lasting value from Bank Secrecy Act (BSA), Anti-Money Laundering (AML) and Counter Terror Financing (CTF) expenditures.

- Governance and Enterprise-wide Program Oversight and Compliance Integration
- BSA/AML/OFAC Risk Assessments
- Independent BSA Audit / Compliance Review
- Risk-Based Customer Due Diligence including KYC, CDD and Customer Risk Rating
- Policy and Procedure, Guidance, Standards and Development
- Customer Single View
- Data Quality and Integration
- Transaction Monitoring Systems Implementation and Post Implementation Tuning
- Financial Intelligence Unit (FIU) formation and Business-as-Usual optimization
- Forensic / 3rd-Party Look-backs
- Investigations Outsourcing
- AML Program Assessment and Future State Roadmap
- Exam Preparation and Management
- Global sanctions filtering

Endorsed by the American Bankers Association

Credit Services: outsourced credit review, managing commercial real estate concentrations, credit administration process reviews, ALLL consulting, exam preparation and more.

Internal Audit Services: internal audit outsourcing, Sarbanes-Oxley Act section 404 and FDICIA related testing, audit committee assessment / training and enterprise risk management.

Information Technology Services: IT risk assessments, general controls review in accordance with Federal Financial Institutions Examination Council guidance, security architecture assessment, Gramm-Leach-Bliley Act 501(b) assessment, business continuity planning, ATM pin security (TG3) and more.

BSA / AML Compliance: BSA audits, risk assessments (AML/BSA/Office of Foreign Assets Control), compliance reviews, exam preparation and management, customer risk rating and customer due diligence, Forensic/third party look-backs, board of directors and senior management training and awareness and more.

Regulatory Compliance Services: Regulatory compliance risk assessments, consumer compliance testing, consulting and training, and enterprise-wide compliance risk management, trust operations and administrative reviews, exam preparation and more.

Tax Consulting

We provide federal and state tax services to nearly 700 financial services companies. Our goal is to identify opportunities that can provide an immediate return on investment through minimization of the tax burden.

Federal Tax Consulting Services

- Tax credits
- Mergers and acquisitions
- IRS practices and procedures, including tax controversies

State and Local Tax Consulting (SALT) Services

- Nexus studies
- Income and franchise faxes
- Sales and use taxes
- Property taxes
- Business incentives
- Tax audit and advocacy

Tax Compliance Services

- Assistance with analysis and documentation mandated by Section 404 of Sarbanes-Oxley
- Guidance regarding FIN 48 documentation requirements
- Complete tax department outsourcing

International Tax Services

- Minimization of worldwide effective rate
- Assistance with entity choice and domicile location

Performance Consulting

Our ideas help make branches more productive, compensation more effective, and operations more efficient.

Performance Assessment Services

- Benchmarking
- Expenses
- Performance

Comparative surveys and reports

- Branch performance
- Compensation

Payment solutions for small business customers

- Business Payment Connection™ (BPC)

Performance Consulting Services

- Merger and acquisition (M&A) integration
- Vendor selection
- Policies & procedures
- Compensation
- Market potential
- Branch strategy

Additional Services

In addition to assurance, tax, risk management, consulting and AML services, Crowe is nationally recognized for excellence in the following areas:

Financial Advisory Services

- Due Diligence
- Mergers & Acquisitions
- Valuation
- Investment Banking
- DeNovo Services

Forensic Services

- Litigation Services
- Fraud Services
- Alternative Dispute Resolution

Benefit Plan Services

- Benefit Plan Audit
- Employee Stock Ownership Plan (ESOP) Services
- Retirement Plan Services

Auditing the Lending Function

Lending Audit Objectives

- Disbursement Authorization and Funding and Documentation Exceptions
- Collateral Valuation, Control and Security
- Loan Payment Processing
- System Input and File Maintenance Changes
- Loan Accounting and System Reconciliations
- Loan Income Recognition
- Employee Loan Monitoring
- Financial Statement Disclosures

Lending Audit Objectives/Risk Factors

- Disbursement Authorization and Funding and Documentation Exceptions

  - Authorization
    - Loan proceeds are disbursed without proper underwriting, complete documentation and/or approval
    - Loans may be of lower loan quality and/or documentation may not be adequate to secure the bank's rights to repayment
    - Complete loan documentation may not be obtained resulting in no legal rights to collect and/or inadequate collateral support in the event of default

Lending Audit Objectives/Risk Factors

- Disbursement Authorization and Funding and Documentation Exceptions
  - Access to Assets
    - Proceeds are disbursed on loans that are not properly documented or are disbursed to fictitious loan customers
    - Collateral is released without proper approval or is misappropriated
    - Loan proceeds are disbursed to fictitious borrowers
    - Information may be utilized to submit a fictitious loan.
    - Loan history may be misplaced/lost
    - Notes, the bank's legal right to collect, may be misplaced/lost
    - Complete loan documentation may not be obtained resulting in no legal rights to collect and/or inadequate collateral support in the event of default

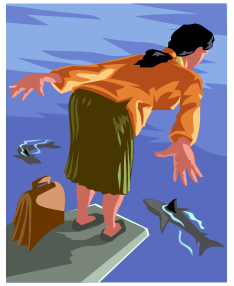
Lending Audit Objectives/Risk Factors

- Disbursement Authorization and Funding and Documentation Exceptions
  - Completeness and Accuracy
    - Loan proceeds are disbursed for incorrect amounts or to fictitious customers
    - Loan proceeds are disbursed without proper underwriting, complete documentation and/or approval
    - Loans may be of lower loan quality and/or documentation may not be adequate to secure the bank's rights to repayment
    - Complete loan documentation may not be obtained resulting in no legal rights to collect and/or inadequate collateral support in the event of default

Lending Audit Objectives/Risk Factors

- Collateral Valuation and Security
  - Authorization
    - Collateral securing loans may be inadequate, overvalued or inadequately secured resulting in inability to rely on collateral as a source of repayment in the event of default
    - Collateral may be released or misappropriated before the loan balance is fully paid off, resulting in lack of security for remaining balance
  - Access to Assets
    - Collateral securing loans may be lost or misappropriated, resulting in inability to rely on collateral as a source of repayment in the event of default
  - Completeness and Accuracy
    - Collateral securing loans may be lost or misappropriated, resulting in inability to rely on collateral as a source of repayment in the event of default
  - Evaluation of Balances
    - Collateral securing loans may be overvalued resulting in inability to rely on collateral as a source of repayment in the event of default

Lending Audit Objectives/Risk Factors



- Loan Payment Processing
  - Authorization
    - Payments are not recorded or are recorded incorrectly resulting in misstatement of loan and/or interest balance
  - Completeness and Accuracy
    - Payments received are not properly or timely recorded, resulting in misstatement of loan and/or interest balances
    - Payments are not recorded or are recorded incorrectly resulting in misstatement of loan and/or interest balance
    - Loan balances or accrued interest may be misstated due to errors in recording transactions or due to misappropriation of funds

Lending Audit Objectives/Risk Factors

- Loan Payment Processing
  - Substantiation of Balances
    - Loan balances or accrued interest may be misstated due to errors in recording transactions or due to misappropriation of funds
  - Access to Assets
    - Payments are not recorded or are recorded incorrectly resulting in misstatement of loan and/or interest balance

Lending Audit Objectives/Risk Factors

- System Input and File Maintenance Changes
  - Authorization
    - New account information/file maintenance may be recorded incorrectly or not recorded or a fictitious loan may be set up resulting in misstatement of loan and/or interest balance
  - Completeness and Accuracy
    - New account information/file maintenance is recorded incorrectly or not recorded resulting in misstatement of loan and/or interest balance
    - New account information/file maintenance may be altered or a fictitious loan may be set up resulting in misstatement of loan and/or interest balance
    - Information needed to properly classify and describe loans within the financial statement and monitor loan portfolio risk may be missing

Lending Audit Objectives/Risk Factors

- Loan Accounting and System Reconciliations
  - Authorization
    - Loan balances or accrued interest may be intentionally or unintentionally misstated due to errors and omissions in processing or defalcations
  - Substantiation of Balances
    - Loan accounts are not properly or timely reconciled allowing intentional or unintentional misstatements to go undetected
    - Loan commitments and guarantees may be made but not properly reported in the financial statements or properly monitored for credit or interest rate risk

Lending Audit Objectives/Risk Factors

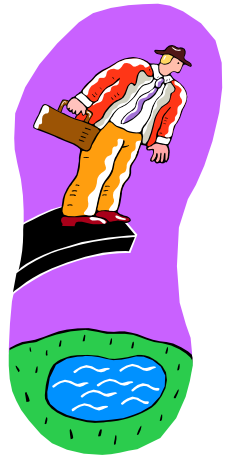
- Loan Income Recognition (Interest & Fees)
  - Completeness and Accuracy
    - Interest income or accrued interest may be intentionally or unintentionally misstated due to errors and omissions in processing or defalcations
    - Loan balances, interest income or accrued interest may be misstated due to capitalization of interest
    - Loan income may be intentionally or unintentionally misstated due to errors and omissions
    - Loan fees are not amortized in accordance with accounting principals

Lending Audit Objectives/Risk Factors

- Loan Income Recognition (Interest & Fees)
  - Authorization
    - Loan income is properly recognized and recorded
    - Loans are made with terms that are not in accordance with management's intent, resulting in the bank not being compensated adequately for lending-related risks
    - Interest income or accrued interest may be intentionally or unintentionally misstated due to errors and omissions in processing or defalcations
  - Substantiation of Balances
    - Interest income or accrued interest may be intentionally or unintentionally misstated due to errors and omissions in processing

Lending Audit Objectives/Risk Factors

- Employee Loan Monitoring
  - Authorization/Completeness and Accuracy
    - Loans are originated in an environment that results in poor quality loans, loans to fictitious borrowers, or loans that are not properly priced for the corresponding level of associated risk



Lending Audit Objectives/Risk Factors

- Financial Statement Disclosures
  - Completeness and Accuracy
    - Financial statement disclosures are inaccurate or incomplete
    - Individuals gathering financial disclosure data do not understand the data requirements or intentionally misrepresent the data causing the information gathered to be inaccurate or incomplete
    - Data gathered is inaccurate or incomplete due to errors during the data gathering process

Example Loan Set-up Controls

- Lending policy outlines approval procedures
- Reasonable loan officer lending limits established
- Loan proceeds disbursed by check or direct deposit
- Set-up information independently verified for accuracy
- New loan report prepared/reviewed
- New loans reviewed for proper documentation
- Loan files protected and organized
- Loans from general ledger reconciled to subsidiary ledger

Example Loan Set-up Testing

- Document controls over set-up of new loans
- Test a sample of new loans for proper set-up
- Test adequacy of loan file documentation
- Confirm sample of loans directly with customers
- Test new loan report for completeness
- Test disbursement of proceeds
- Test reconciliation of loan principal account
- Others??

Example Loan File Documentation Controls

- Checklist(s) used to assure documentation is complete
- Follow-up of incomplete items
- Effective tickler system used for insurance, financing statements and financial statements
- Credit analysis performed and documented in loan files
- Controls over lines of credit which require annual review and pay-out
- Controls to prevent draws in excess of line-of-credit

Example Loan File Documentation Testing

- Document controls over loan file documentation, tickler system follow up, and lines of credit
- Test sample of loans for proper documentation
- Review loans for current financial information and other critical documentation
- Review lines-of-credit for annual renewal and annual payout
- Test lines-of-credit for advances over approval limit
- Others??

Example Loan Payment Controls

- Receipt of payments restricted to loan tellers
- Payment tickets indicate person processing transaction
- Allocation of payment to principal and interest verified
- Special controls for extensions and renewals

Example Loan Payment Testing

- Document controls over loan payment receipt and posting
- Recalculate principal and interest for a sample of payments
- Verify payment ticket indicates employee who accepted payment
- Test assessment of late charges
- Others??

Example Master File Change Controls and Testing

- Controls
  - Segregation of duties
  - Accuracy of changes
- Testing
  - Review sample
    - Walkthrough process
    - Documentation of segregation
    - Documented support for changes

Example Interest Income Controls

- Rates are input correctly by % and type (fixed or variable)
- Daily accruals calculated automatically and consistently
- General ledger accrued interest is reconciled to the subsidiary ledger daily
- Accrual discontinued based on established delinquency criteria
- System established to change rates in accordance with variable rate agreement

Example Interest Income Testing

- Document controls over calculation of interest
- Recalculate accrued interest receivable

- Calculate general ledger yields and determine reasonableness
- Verify interest discontinued on loans meeting non-accrual criteria
- Verify rate changes on adjustable rate mortgages
- Recalculate deferred loan fees/costs recognized
- Others??

Example Employee Loan Controls

- Loans approved by senior management and/or Board of Directors
- Segregated on system
- Independent review of employee loan activity performed

Example Employee Loan Testing

- Document the process for approving and reviewing employee loans
- Review loan trial balance to determine that all loans are properly coded
- Trace employee loans to proper approval
- Review activity in employee loan accounts for unusual items
- Others??

Example Construction Loan Controls

- Controls are established to ensure draws do not exceed approved limits
- Disbursements are only made to authorized individuals
- Disbursements are only paid upon review of inspection reports, verbal title policy updates, and partial lien waivers from contractors or suppliers to substantiate collateral values and clear title
- Agreement terms as to refinancing and interest payments are followed
- Policies exist to ensure the exposure to "spec house" construction loans is limited

Example Construction Loan Testing

- Review a sample of construction loans and verify that balance on subsidiary does not exceed approved loan amount
- Confirm a sample of construction loans with borrowers, both disbursed and undisbursed balances
- Review a sample of construction loan files:
  - Vouch fund disbursements to properly signed and endorsed checks
  - Ascertain that prior to disbursements the loan officer obtained:
    - Inspection reports
    - Verbal title policy update
    - Partial lien waivers from contractors or suppliers.

  - Verify that principal and interest payments are being made in accordance with the agreement.
  - Ensure for "spec house" construction loans that no more than a set number of "spec houses" will be financed for one builder

Example Credit Card Controls

- All credit card loans are analyzed and underwritten in accordance with bank policies by authorized individuals.
- Over line credit card balances are identified and monitored.
- Credit card disputes are investigated by an individual independent of the credit card process and are resolved in a timely manner.
- Appropriate due diligence is performed before accepting credit card merchant processing accounts.

Example Credit Card Testing

- Assess the adequacy and completeness of the credit card department’s procedures.
- Review the credit card “over line” for any accounts in excess of bank policy.
- Select a sample of <X> recent credit card disputes and verify the adequacy and completeness of resolution procedures.
- Select a sample of <X> new merchant accounts and perform a review to determine whether the accounts were underwritten in accordance with policy and procedures and whether they were properly approved within the approver's authority.

Example Letters of Credit Controls and Testing

- Controls
  - Proper Approval
  - Collateral Perfection
  - Expiration Monitoring

- Testing
  - Review sample and test for:
    - Approval within officer limits
    - Collateral documentation in file or on suspense
    - Proper fee assessment and collection
    - Expiration monitoring

Example Indirect Lending Controls

- Dealers are accepted into the indirect lending program according to Bank policies and procedures.
- Dealer reserve transactions are executed and approved in accordance with Bank policy and procedures.
- Dealer reserve account balances are monitored for sufficiency.

Example Indirect Lending Testing

- Select a sample of <X> new Dealers and verify the Dealer Agreement has been properly signed and approved (including signed dealer reserve agreement); and, the Dealer has been appropriately approved by Senior Management and/or the BOD.
- Review the process of establishing and monitoring dealer reserve balances.
- Test <X> dealer reserve balances to ensure the balances maintained are per the agreement.

Example Floorplan Controls

- Management has established a formal, written floorplan loan policy.
- Management has established policies and procedures identifying documentation requirements for vehicles covered by floorplan loans.
- Floorplan audits are routinely conducted. Employees who conduct the audits are rotated. Discrepancies are resolved in a timely manner.

Example Floorplan Testing

- Obtain and review the loan policy and determine whether criteria has been established for the acceptance and on-going monitoring of floorplan dealers and loan relationships.
- Review <X> floorplan loan files for required documentation.
- Review documentation of <X> periodic floorplan audits conducted by management. Determine whether discrepancies were resolved, audits were conducted, and responsibility for audits was rotated among employees. Determine whether the floorplan audits met policy requirements.

Loan Loss Reserve, Collections and Recovery, and OREO/Repossessed Assets

- Process from the time a loan moves from current pay status to delinquent through the collection process to sale of asset
- Includes:
  - Delinquency
  - Foreclosed and Repossessed Assets
  - Charge-off and Recovery
  - Allowance for Loan Losses

Lending Control Objectives/Risk Factors

- Loan Delinquencies, Collections, ALLL, Charge-offs and Recoveries
  - Authorization
    - Collection efforts are not performed in accordance with management objectives, reducing potential for complete and timely repayments.
    - Problem loans are not properly monitored and recorded, increasing the potential for loss and misstatement of the loan and income related accounts.
    - An incorrect amount is charged-off or fictitious account is charged-off.
    - The established methodology for estimating the allowance for loan losses is flawed, not in accordance with accounting principles.
    - Accounting principles and significant assumptions in applying principles are not accurate or in accordance with management objectives.

Lending Control Objectives/Risk Factors

- Loan Delinquencies, Collections, ALLL, Charge-offs and Recoveries
  - Completeness and Accuracy
    - Loan balances or accrued interest may be intentionally or unintentionally misstated due to errors and omissions in processing or defalcation.
    - Past-due account information is not provided, reducing potential for complete and timely repayment.
    - Problem loans are not properly monitored and recorded, increasing the potential for loss and misstatement of the loan and income related accounts.
    - Problem loans are not recorded properly resulting in misstatement of the loan and income related accounts
    - Income is recognized improperly resulting in misstatement of AIP and income.
    - Records are not maintained of the actual principal balance owed by the borrower, reducing the potential for partial/complete collection.
    - An incorrect amount is charged-off or fictitious account is charged-off.
    - The methodology adopted for estimating the allowance for loan losses results in an inaccurate estimate.

Lending Control Objectives/Risk Factors

- Loan Delinquencies, Collections, ALLL, Charge-offs and Recoveries
  - Access to Assets
    - Cash/collateral is misappropriated.
    - An incorrect amount is charged-off or fictitious account is charged-off.
    - Inadequate collection procedures reduce the potential for partial/complete recovery.
    - The process for estimating the allowance for loan losses is biased resulting in an inaccurate estimate.
  - Substantiation of Balances
    - Loan accounts are not properly or timely reconciled allowing intentional or unintentional misstatements to go undetected.

Lending Control Objectives/Risk Factors

- Loan Delinquencies, Collections, ALLL, Charge-offs and Recoveries

  - Evaluation of Balances
    - Problem loans or fictitious loans exist without timely detection, increasing the potential for loss.
  - Evaluation of Balances/Completeness and Accuracy
    - The process for estimating the allowance for loan losses does not include all loans.
  - Evaluation of Balances/ Authorization
    - The process for estimating the allowance for loan losses is not performed timely and/or in accordance with the authorized methodology.

Example Delinquency Controls

- Loans are periodically (and timely) placed on nonaccrual status
- Renewals and extensions are adequately reported
- Policy over renewals and extensions includes limits and processes for approval
- Delinquent loans are adequately reported to management and the Board
- Bank has a watch or problem loan list that is updated periodically
- Delinquent loan report is prepared/ reviewed by someone without lending authority or collection responsibilities

Example Delinquent Loan Controls

- Delinquent loan report reviewed
- Delinquent report independently generated
- Established and consistent criteria for reporting loan as delinquent
- Past due notices mailed independently
- Collection efforts on individual loans reviewed

Example Delinquent Loan Testing

- Document controls over delinquent loans, including collections, past due notices, etc..
- Test delinquent loan report for accuracy and completeness
- Test loans that were 30+ days past due that were brought current before month-end (looking for loan interest capitalization)
- Test for extensions/renewals of delinquent loans (number of extensions, “evergreen loans”)
- Review collection process for independence
- Others??

Example Foreclosed/Repossessed Asset Controls

- Periodically analyzed to determine value of property
- Periodic appraisals/evaluations performed on all real estate owned
- Assets removed from loan trial balance when foreclosed/ repossessed
- Foreclosed/repossessed assets subsidiary is reconciled to general ledger at least monthly
- Subsequent sale - gain/loss is recorded appropriately
- Receipt of sales proceeds or rental income is adequately controlled - ensure return is maximized

Example Foreclosed/Repossessed Asset Tests

- Document controls over foreclosed/repossessed assets
- Test values of foreclosed/ repossessed assets to independent valuation
- Reconcile foreclosed/repossessed assets to subsidiary ledger
- Review assets to determine all deficient loan balances have been charged-off
- Vouch sales to supporting documents
- Review income from revenue-generating properties
- Others??

Example Charge-off and Recovery Controls

- The loan policy establishes criteria for when delinquent loans should be charged off (i.e., number of days delinquent)
- Appropriate individuals are assigned the authority and responsibility for determining which loans should be placed on non-accrual status or returned to accrual status, and approving charge-offs of uncollectible loans
- Status of collections are periodically reviewed by management and Board
- Charged off loan subsidiary ledgers are posted and balanced by an individual independent of approval, disbursement functions and the collection of loan payments or recoveries
- Charged off loan subsidiary records are reconciled to the general ledger allowance for loan losses account to ensure that subsidiary records have been updated
- Periodic progress reports are prepared and reviewed by an appropriate individual and the Board of Directors on all loans charged off on which collection efforts are continuing

Example Charge-off Recovery Testing

- Review loan policy to ensure charge off requirements (i.e., number of days delinquent)
- Review a sample of past due loans to ensure appropriate individuals authorized non-accrual status or return to accrual status
- Review a sample of charge-offs of uncollectible loans to ensure appropriate approval
- Review reports to the Board and management of loans in collection status. Ensure:
  - Accuracy and completeness of the report
  - That status of collections are periodically reviewed by management and Board
- Review the charged off loan subsidiary ledgers for:
  - accurate posting and balancing by an individual independent of approval, disbursement functions and the collection of loan payments or recoveries
  - reconciliation to the general ledger allowance for loan losses account to ensure that subsidiary records have been updated

Allowance Audit Approach

- Identify and document controls and procedures in place
- Design tests of the loan review system and the allowance system
- Consider trends, ratio analysis, peer comparison, concentrations, economic factors etc.

Example Controls For Allowance for Loan Losses

- Management has formal written procedures to determine the adequacy of the allowance.
- Procedures are updated to reflect current economic trends.
- Analysis is prepared by all loan officers, senior management or a loan review officer.
- Analysis includes a review of problem loans for potential loss exposure.
- Analysis includes allocations for loans not specifically evaluated.
- Analysis takes into consideration potential losses on unused loan commitments, standby letters of credit, overdrafts and accrued interest.

Example Allowance for Loan Losses Testing

- Document the process of completing the allowance calculation
- Test inclusion of potential problem loans in management's analysis
  - classified loan report
  - delinquent loan and nonaccrual loan report
  - watch list, inquiry of management, etc..

- Test accuracy of delinquent loan report used in the preparation of the ALLL
- Review a sample of delinquent loans to determine if they should be charged off or, if still accruing, be placed on nonaccrual status and accrued interest reversed
- Review supporting schedules for ALLL calculations
- Determine whether methodology changed to reflect changing conditions

Auditing Mortgage Banking Functions

Definition of Mortgage Banking and the Secondary Market

- Mortgage Banking is defined as: An organization that originates mortgages for resale to investors. Mortgage bankers derive their income much like merchant bankers – from the origination of fees and servicing income.

- Secondary Mortgage Market is defined as: A national market where residential mortgages are assembled into pools and sold to investors. The secondary market, which originated with FNMA, FHLMC, and GNMA supplies additional liquidity to mortgage lenders. Mortgages are sold through established conduits that assemble pools of loans for resale or through private placement of loans directly with an investor.

Auditing Mortgage Banking and Secondary Marketing- Written Agreements

- Investor agreements are on file and outline roles, responsibilities and the investor's requirements.
- Investor agreements are signed by authorized individuals.
- Written Policies and Procedures related to Investors should be in place.

Auditing Mortgage Banking and Secondary Marketing- Profitability Analysis

- Management has established a process that measures, monitors, and reports risks associated with the secondary market function.
- Management analyzes gains/losses on a periodic basis. The analysis includes gains/losses, pair-off fees paid, service released premiums received, mortgage servicing rights, purchase premiums paid, interest rate buy up/down, deferred loan fees.
- Gains/losses are compiled by an individual independent of the secondary market function.
- Gain/loss calculations are validated by a second individual independent of the secondary marketing function. Supporting documentation for the validation is retained.
- Gains/losses are reported to Senior Management on a periodic basis.

Auditing Mortgage Banking and Secondary Marketing-Quality Control

- An independent Quality Control review is performed on a periodic basis to test for compliance with investor requirements.
- The results of the Quality Control review are documented and reported to the investor and Senior Management on a timely basis (i.e. within 90 days of loan closing).
- Quality Control exceptions are researched and cleared in a timely manner by someone independent of the underwriting process.
- Responses to Quality Control exceptions are documented and reported to Senior Management.

Auditing Mortgage Banking and Secondary Marketing-Recourse Obligations

- Management tracks, monitors and reports its recourse obligations and repurchases.
- Management tracks and monitors loans rejected by investors. The results are reported to Senior Management on a periodic basis.

Auditing Mortgage Banking and Secondary Marketing- Loan Delivery

- Management tracks and monitors the delivery of loan file documents for timeliness (i.e. before the required delivery date), accuracy (i.e. correct loans and documents) and completeness (i.e. all sold loans).
- Management tracks and monitors holdbacks – funds withheld due to incomplete delivery of loan file documents.

Auditing Mortgage Banking and Secondary Marketing-Pipeline and Warehouse Management

- Sales are executed by an individual with BOD-approved trading authority.
- Sales/trade tickets are recorded and tracked (i.e. in a trade log) by an individual independent of the execution and approval.
- Trade confirmations are compared to recorded trade transactions by an individual independent of the trade execution.
- Unconfirmed trades are monitored and researched by an individual independent of the execution.
- Trade transactions (i.e. recording in the trade log, mortgages coded as sold) are checked for accuracy by an individual independent of the execution and recording.
- Sales are executed with BOD-approved investors, dealers, brokers.
- Loan sale proceeds are reconciled to trade tickets.
- Collection of proceeds from all sales is monitored by an individual independent of the trade execution and independent of the posting of proceeds.

Auditing Mortgage Banking and Secondary Marketing- Pipeline Management

- Pertinent loan commitment data is tracked via a pipeline system report: product type, interest rate, commitment date, and commitment (rate lock) expiration date.
- The pipeline report data is validated for completeness, timely data and accuracy by someone who is independent of the input/preparation.
- Management monitors its position of loan commitments on a frequent basis (i.e. daily).
- Management tracks and monitors fallout ratios by product type on a periodic basis (i.e. quarterly).
- Fallout ratios are compared to acceptable ratios established by Senior Management. Comparison results are reported to Senior Management.
- If the institution uses external funding, management has established a process to monitor its funding position on an ongoing basis.
- Management tracks and monitors pair-off activity.
- Authorized individuals have established and documented a pricing strategy that matches company objectives.

Auditing Mortgage Banking and Secondary Marketing-Warehouse Management

- Closed and unsold loans are tracked on a warehouse inventory report.
- Management monitors its position of closed and unsold loans (i.e. warehouse inventory) on a frequent basis (i.e. monthly) for turnover and aging.
- Management has established procedures for recording the change of loan status when closed loans are sold.
- Data on the warehouse inventory report is periodically validated against source documentation and periodically reconciled to the general ledger. The data is checked for accuracy and completeness by an individual independent of report preparation.
- Fees for Mortgages Held for Sale are deferred. For sold loans, deferred fees are fully amortized and recognized in the month of the sale.
- Loans classified as “held-for-sale” are periodically marked at the lower of cost or market by an individual independent of the secondary market function.
- Supporting documentation for the mark to market pricing is retained.

Foreclosure Work Program-General Steps

- Has the firm received any notices that they are ineligible to perform foreclosures for any other servicer or mortgage holder?
- Are records kept that support all aspects of the foreclosure activities for the appropriate period of time (in accordance with the agreement)? Using judgment, the auditor may decide to select a sample of recent cases and confirm key documents such as notice receipts, or affidavits are retained in the files. Inquire about the procedures in place for offsite storage of records, access, and destruction.

Foreclosure Work Program- Policies and Procedures

- What are the procedures for assigning attorneys and staff to foreclosures? Is there a process for issue escalation?
- Are any background checks performed on all new employees? Please note any exceptions. If full background checks are not performed on all new employees, are additional background checks performed for employees being transferred to a position working with U.S. Bank files?
- What is the firm's process for handling borrower or opposing counsel complaints?
- What is the firm's process for handling US Bank monies received from Borrowers?
- Does the law firm have a written information security policy endorsed by senior management?
- Does an IT Steering committee (or a similar group with similar purpose/roles) review and approve IT policies and procedures on an annual basis?
- Is any periodic testing performed or any other security related certification held (e.g. Penetration Assessments, ISO, etc..)? Please provide a copy of any reports.

Foreclosure Work Program- General Steps

- Are there any steps taken to identify if a mortgage holder has gone into bankruptcy? If so, what steps are taken once bankruptcy is discovered?
- What are notary procedures at the law firm? Is a notary log kept? Review a sample log. Interview a notary and identify any concerns with the storage of the notary stamp?
- From a financial standpoint, does the law firm currently meet U.S. Bank's policies?
- Does the firm have the appropriate levels of insurance required by the agreement?
- What incentives are in place for employees servicing U.S. Bank foreclosures? Do these incentives put quantity over quality or jeopardize compliance with legal process and regulations?
- Within the last twelve months, have there been any sanctions or fines against the firm for foreclosure related actions or other activities?

Foreclosure Work Program- Default Foreclosure Process

- What controls are in place to ensure that a state law requiring the borrower to be notified of mediation options or retention options has been complied with prior to the commencement of foreclosure?
- Are there controls in place to ensure that junior lien holders are properly identified and notified of a foreclosure and that the notification processes comply with the state law where the property is located?
- What controls exist to ensure that the commencement of the foreclosure process or the completion of the foreclosure sale does not occur prior to the allowed amount of time listed on either the mortgage or the note?
- Are there controls in place to ensure that all complaints are properly completed and filed with the court within the allowed time period provided by the state's civil procedure laws?
- Are there controls in place to ensure that all state foreclosure laws are complied with, in regards to the filing of summons, the court and ensuring that the summons contain all required information provided by the state's civil procedure laws?

Foreclosure Work Program- Default Foreclosure Process

- Are there controls in place to ensure that the service of process is done in a manner that is in compliance with the state civil procedure laws?
- Are there controls in place to ensure that all attorney fees charged or collected are permitted by: 1) the note and mortgage, 2) state's foreclosure law's.
- What controls are in place to ensure that a Motion for Default Judgment or Motion for Summary Judgment is completed in a manner that complies with state civil procedure laws?
- Are there controls in place to ensure the provisions within Judgment of Foreclosure are accurately followed?
- What controls are in place to ensure that all “Notice of Sale” documents are properly issued and comply with the foreclosure laws for the state where the property is located? US Bank to determine state requirements required by law firm.
- What controls are in place to ensure that a foreclosure sale does not occur until it has been verified that a borrower has not attempted to cure a default?
- Are there controls in place to ensure compliance with state laws that focus on rescission rights giving to a borrower?

Foreclosure Work Program- Training and Education

- Have the attorneys completed their continuing education or other training requirements?
- Does the law firm have an ethics and compliance policy and is it regularly communicated to employees?
- Does the law firm provide training to staff on the state specific aspects of foreclosure law and bank policy/database? Please describe and provide a list of dates and employees who received training.
- Are new employees provided with security training? Does this training take place before granting users access to any system with U.S. Bank information? Are users provided periodic/refresher training? Is training documented as users complete this training.
- Are new users provided with a copy of all user/employee IS policies (including Acceptable use, Privately Owned resource, and others) and required to sign all user policies to verify that they have read and understand the policy?
- Were all attorneys involved in US Bank files licensed in the state where they are processing foreclosures?

Escrow- Investor Serviced Loans

- Investor may have requirements regarding escrow activities - i.e. regarding overages, periodic analysis, cushion limitations, "force placed insurance", timeliness of payments, etc..

Escrow Testing- Disbursement Testing

- Objectives:
  - Transactions occur in accordance with management objectives and authorizations
  - Liabilities include all obligations of the company, and assets include all rights of the company.
- Test Steps
  - Select a sample of escrow disbursements. Trace to check/wire advice/ACH register and determine the following:
    - Escrow payments were made by the due date.
    - An appropriate tax and/or insurance invoice supports the payment amount and the receiving party.
    - The check/wire advice was signed by an authorized person.
  - If a third-party vendor is used for any part of escrow administration, determine that a written agreement or contract has been properly signed and executed. In addition, determine the institution is monitoring the vendor for compliance with the agreement

Escrow Testing- Delinquent Escrow Accounts & Escrow Balances for paid off loans

- Objectives:
  - Transactions occur in accordance with management objectives and authorizations
  - Information systems are sufficient to provide relevant and timely information
- Test Steps
  - Obtain management's system report utilized to monitor delinquent tax and insurance payments. Determine whether the report/reports are being reviewed by someone other than the person making the payments and if follow up is being performed to ensure timely resolution. If delinquent accounts exist, inquire with the report reviewer for reasons for the delinquencies and evaluate for reasonableness.
  - Obtain system reports identifying paid off loans with escrow balances. Determine whether the report/reports are being reviewed by someone other than the person making the payments and whether follow up is being performed to ensure timely resolution. If escrow balances exist for paid-off loans, inquire of the reviewer as to the reason for the balance and evaluate for reasonableness.

Escrow Testing- Escrow Analysis, Escrow Overage, and Shortage

- Objectives:
  - Transactions occur in accordance with management objectives and authorizations
  - Misstatements caused by error or fraud are prevented, or detected and corrected, in a timely manner
  - Information systems are sufficient to provide relevant and timely information
  - Sufficient financial and operational results are accurately and timely reported to internal and external parties
- Test Steps
  - For a sample of loans with escrow accounts, determine that
    - an escrow analysis was performed in the past 12 months according to the terms of the loan documents
    - the escrowed amount resulted in payments adequate to cover the anticipated bills
  - For a sample of escrow account overages as of the most recent escrow analysis, determine that funds were disbursed to the mortgagor.
    - Trace the payee name per the disbursement check to the mortgagor's name
    - Trace the dollar amount per the disbursement check to the overage amount in the escrow account
  - For a sample of escrow account shortages as of the most recent escrow analysis, determine that:
    - Funds have been received from the borrower to cover the shortage; or
    - The borrower's payment over the next 12 months was increased to cover the shortage.

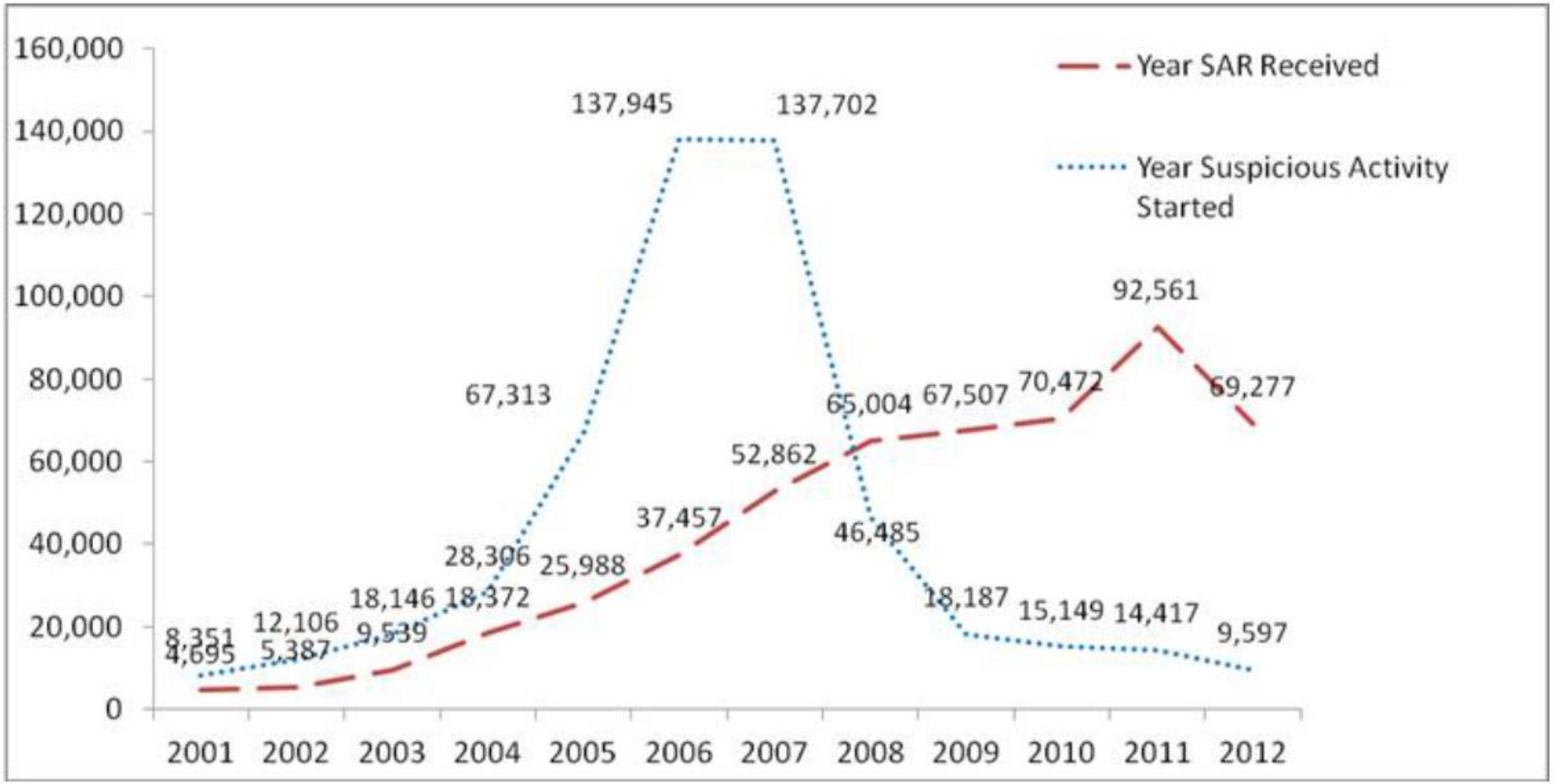
Mortgage Fraud- Defined

- Mortgage fraud is defined as the intentional misstatement, misrepresentation, or omission by an applicant or other interested parties, relied on by a lender or underwriter to provide funding for, to purchase, or to insure a mortgage loan.
- Mortgage fraud is a relatively low-risk, high-yield criminal activity that is accessible to many.
- Finance-related occupations, including accountants, mortgage brokers, and lenders were the most common suspect occupations associated with reported mortgage fraud.
- Perpetrators in mortgage industry occupations are familiar with the mortgage loan process and therefore know how to exploit vulnerabilities in the system.

Mortgage Fraud- Two Categories

- Mortgage loan fraud is divided into two categories: fraud for property and fraud for profit.
- Fraud for property/housing entails misrepresentations by the applicant for the purpose of purchasing a property for a primary residence. This scheme usually involves a single loan. Although applicants may embellish income and conceal debt, their intent is to repay the loan.
- Fraud for profit, however, often involves multiple loans and elaborate schemes perpetrated to gain illicit proceeds from property sales. It is this second category that is of most concern to law enforcement and the mortgage industry. Gross misrepresentations concerning appraisals and loan documents are common in fraud for profit schemes and participants are frequently paid for their participation.

Mortgage Fraud Trends- SAR Filings



Source: Financial Crimes Enforcement Network (FinCen)

Property or Land Flipping

- Property is purchased, falsely appraised at a higher value, and then quickly sold.
- The schemes typically involve one or more of the following: fraudulent appraisals, doctored loan documentation, inflating buyer income, etc..
- Kickbacks to buyers, property/loan brokers, appraisers, and title company employees are common in this scheme.

Legal Property Flip

Property → “Flipper” Acquires Property For a Low Price → “Flipper” Makes Repairs to Property → Appraiser Values “Repaired” Property → Buyer Acquires Property For a High Price → “Flipper” Pockets Difference Between Low & High Price

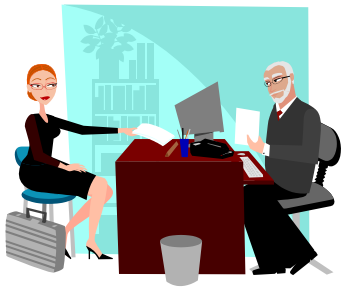
Illegal Property Flip

Nominee Loans/Straw Borrowers

- A nominee allows the borrower to use the nominee's name and credit history to apply for a loan, concealing the true borrower's identity.
- The nominee applies for credit in his own name and immediately remits the proceeds to the true beneficiary.
- The straw borrower may feel there is nothing wrong with this and fully believes that he is helping the third party.
- He expects the recipient of the loan proceeds to make the loan payments, either directly or indirectly.

Nominee Loans/ Straw Borrowers

Nominee agrees to borrow funds for another and is paid $500



The nominee applies for and receives credit for property purchase

Funds are used to buy property and nominee assumes fraudster will pay

The nominee must pay the debt when the fraudster defaults

Phantom Sale

- The fraud perpetrator identifies an apparently abandoned property and records a fictitious quitclaim deed to transfer the property into his name.
- The perpetrator then applies for and executes a loan.
- He pockets the loan proceeds and disappears.
- The financial institution is left with a mortgage loan that has no cash flow support and is collateralized by fraudulently obtained property.

Chunking

- Chunking is a variation of a land flip.
- The scheme begins with an unsophisticated borrower attending a seminar where a third party “teaches” a class on real estate investing.
- The third party cons the borrower and simultaneously submits loan applications on the borrower’s behalf.
- The scheme will usually involve a dishonest appraiser, broker, and/or a representative of a title company
- The third party acts as an agent for the borrower during closing and, unbeknown to the borrower, pockets the loan proceeds, as the true seller of the property.
- The unsophisticated borrower is left with the debt.

Chunking- News Article

USA Today, 9/26/2006

INDIANAPOLIS — The nation's largest home lender, Countrywide Financial, is suing an Indianapolis man for allegedly orchestrating a mortgage fraud scheme in which dozens of Virginia residents were tricked into buying homes in Indiana at inflated prices.

The company alleges that Robert Penn worked with relatives in Virginia and associates that included appraisers and mortgage companies to defraud the victims in a case that could total about $80 million in loans.

In a lawsuit filed in Marion County, where most of the Indianapolis-area properties are located, Countrywide claims the defendants duped their victims by inviting them to take part in either an "investment opportunity" or a "real estate investment club."

The lawsuit alleges the defendants obtained the properties for an average price of $50,000 but "sold" them to the unknowing victims for an average inflated price of $120,000 each, then pocketed the difference.

Multiple Selling

- Multiple selling is a scheme wherein a mortgage loan broker accepts a legitimate application, obtains legitimate documents from a buyer, and induces two or more financial institutions to each fully fund the loan.

- Since there is only one set of documents, one of the funding financial institutions is led to believe that the proper documentation will arrive any day.

- This scheme can be self-perpetuating with different loans being substituted for the ones with which documents cannot be provided. Essentially, the broker uses a "lapping scheme" to avoid detection.

Builder Bailout

- Builder bailout usually occurs when a builder has sold the majority of homes in a tract or subdivision, but is left with some unsold homes.

- To dispose of the remaining properties, the builder may utilize a variety of schemes that can include, but are not limited to, the use of a hidden seller with assisted financing as a front or the use of inflated property values.

Builder Bailout- Example

In a common scenario, the builder has difficulty selling property and offers an incentive of a mortgage with no down payment.

- A builder wishes to sell a property for $200,000. He inflates the value of the property to $240,000 and finds a buyer.
- The lender funds a mortgage loan of $200,000 believing that $40,000 was paid to the builder, thus creating home equity. However, the lender is actually funding 100 percent of the home's value.
- The builder acquires $200,000 from the sale of the home, pays off his building costs, forgives the buyer's $40,000 down payment, and keeps any profits.
- If the home forecloses, the lender has no equity in the home and must pay foreclosure expenses.

Equity Skimming

- An investor, using various documentation misrepresentations, receives a mortgage on a property.
- The investor rents the property to unsuspecting individuals, usually for a year at a discounted rate.
- The investor takes the proceeds and skips town.
- The investor makes no mortgage payments.
- The property is foreclosed on by the bank leaving the renters homeless and the lender with undervalued collateral.

Mortgage Warehousing

- Mortgage warehousing lines are used to temporarily “warehouse” individual mortgages until sold to an investor.
- A dishonest mortgage banker will attempt to warehouse the same mortgage loan on one or more credit lines.
- Similar to multiple selling, this scheme can be self-perpetuating with different loans being substituted for the ones with which documents cannot be provided.

Foreclosure Schemes

- The fraud perpetrator identifies a homeowner in or at risk of foreclosure.
- The fraud perpetrator misleads the homeowner into believing he can save his home in exchange for a transfer of the deed and upfront fees.
- The perpetrator profits from this scheme by re-mortgaging the property and/or pocketing the upfront fees.

Silent Second

- The buyer borrows the down payment from the seller through the issuances of a non-disclosed second mortgage.
- The primary lender is misled thinking the buyer is using his own money.
- The second mortgage may not be timely recorded to further conceal its status from the primary lender.
- This will affect the loan-to-value ratio and the debt level of the borrower.

Fraud Scheme Red Flags

- A much greater than normal increase in year-to-year income or an occupational income far higher than those of others in the same line of work.
- Applicant's reported Social Security and Medicare withholdings exceed the limits established by law.
- Borrowers purchasing property described as a "primary residence," but outside of their home states, or located an unreasonable commuting distance from their stated employer.
- Mortgage brokers or borrowers that always use the same appraiser.

Fraud Scheme Red Flags

- Borrower's signature does not match on all documents (identity theft).
- Multiple problematic loan applications containing the same parties working in conjunction with one another (i.e., numerous transactions involving the same mortgage broker, seller, appraiser, and settlement agency).

Fraud Scheme Prevention/ Detection Techniques

- Apply simple reasonability tests to detect fraudulent documents.
- Re-verify the information provided in the loan application.
- Close scrutiny by lenders of the loan settlement statement (frequently the Form HUD-1) where the loan funds are going could identify potential fraud prior to loan disbursement.

Fraud Scheme Prevention/ Detection Resources

- Pre-Employment Background Screening
- National Registry of Appraisers
- Building Cost Calculator
- Report Instances of Mortgage Fraud

Emerging Mortgage Fraud Trends

- There are four emerging scenarios to which the industry should be currently paying attention include:
  - Foreclosure prevention schemes
  - Elderly and immigrant identity fraud
  - Builder bail-out scams
  - Short sale fraud (“flopping”)

Foreclosure Prevention Schemes

- These generally involve fraudsters posing as professional, knowledgeable foreclosure specialists.
- Homeowners facing the threat of foreclosure and nearing eviction are contacted by these “foreclosure specialists” who promise to work out their loan problems or buy their home and offer the homeowners tenancy.
- Unfortunately for the homeowner, the fraudster has no intention of following through with these promises and instead will manipulate the homeowner into deeding the property to him.

Foreclosure Prevention Schemes

- Once the fraudster obtains the signed documents, a false lien release is generally filed or leveraged to secure funds from a fabricated sale or refinance on the property.
- In many cases, the homeowner is under the belief that he will rent the property for a period of time until he is in a better position to regain ownership rights.
- The fraudster continues to accept payments made by the homeowner while selling the property, absconding with the funds, and eventually evicting the homeowners.

Foreclosure Prevention Schemes

Case Study

- A dishonest "foreclosure prevention specialist" contacted troubled homeowners in the Washington, DC, area and convinced them to sign over their homes to "straw buyers" working for her company, supposedly so she could stabilize their mortgage and repair their credit.
- Instead, the fraudster used the straw buyers to take out loans against the homes' existing equity, which she pocketed before returning the deeds to her victims.

Foreclosure Prevention Schemes

Case Study

- Prosecutors estimate that the fraudsters and her associates bilked more than $35 million from her victims before she was caught.
- She used some of the money to finance her $800,000 wedding party, complete with a Porsche for one of her attendants.
- The fraudster plead guilty and faces 30 years in prison.

Foreclosure Prevention Schemes

Case Study 2

- Three men have been found guilty by a federal jury for their roles in a nationwide foreclosure-rescue scheme - Charles Head, Benjamin Budoff and Dominic McCarns .
- Head was the founder of several California companies, including Head Financial Services and Creative Loans, that allegedly defrauded homeowners of more than **$5.7 million** in equity between 2005 and 2006. Budoff and McCarns were employees of Head's companies.
- The companies allegedly promised distressed homeowners that they could stay in their homes and repair damaged credit by enrolling in a foreclosure-rescue program. The companies then paid straw buyers to replace the troubled homeowners on the titles and apply for mortgages to extract as much equity as possible from the homes.

Foreclosure Prevention Schemes

Case Study 2

- Meanwhile, troubled homeowners made monthly payments to the companies, mistakenly believing that the funds would go toward improving their credit scores.
- **The homeowners suffered at least $15 million in losses, according to the release.**
- The defendants preyed on the victims' fear of losing their homes and then took advantage of those victims' predicament to steal from them their last remaining equity in those homes. **Many homeowners were eventually "evicted and left destitute.**
- Head, Budoff and McCarns are scheduled for sentencing on March 19, 2014, and face up to **20 years in prison and a $250,000 fine for each count of mail fraud.**

Elderly and Immigrant Identity Fraud

- While not new, elderly and immigrant fraud is regaining popularity.
- In this predatory practice, elderly and non-English-speaking consumers are taken advantage of by fraudsters who steal their identities and use them in “straw buying” or other property transactions.
- This is currently happening in some reverse mortgage situations.
- Similarly, some immigrants who rent properties are discovering that their identities have been used on fabricated loan transactions.

Builder Bail-Out Scams

- This involves securing funds for condominium conversion or planned community development properties that, unbeknownst to the investor, will not be completed.
- The scams entail multiple purchases from would-be investors or false identities on fabricated loan transactions.
- Investors are lured by photos or inspections of a few converted units, used as models, with promises of further rehabilitation of remaining units.
- Once the contracts are in place, the fraud continues as the perpetrator secures funding for the contracts; however, no additional work is done and the investors and lenders are left with incomplete and, in some cases, uninhabitable dilapidated buildings.

Land Flipping vs. Land Flopping

Land Flipping

- Property is purchased, falsely appraised at a higher value, and then quickly sold.
- The schemes typically involve one or more of the following: fraudulent appraisals, doctored loan documentation, inflating buyer income, etc..
- Kickbacks to buyers, property/loan brokers, appraisers, and title company employees are common in this scheme.

Land Flipping vs. Land Flopping

Land Flopping (Short Sale Fraud)

- Mortgage loan is in default (this is intentional).
- Property is falsely appraised at a lower value.
- Borrower represents that someone is willing to assume the mortgage if the lender offers a concession.
- The original borrower “buys” the loan at a lessor value using straw borrowers or identity theft schemes.

Short Sale Fraud Example

- An Atlanta man was indicted by a federal grand jury on charges of aggravated identity theft and false statements to the FDIC.
- The man allegedly obtained several million dollars in loans in his name and the names of his family and friends from a bank before it was seized by the FDIC.
- After remaining delinquent on loan repayments and facing foreclosure, the man asked the FDIC to forgive $2.2 million dollars in loan payoffs on the properties and allow him to “short sale” them to new purchasers at reduced amounts.

Short Sale Fraud Example

- An investigation revealed the sales contracts and loan commitment letters provided by the man to the FDIC were fraudulent and the "new purchasers" were the victims of alleged identity theft.
- These cases are being investigated by the Special Agents of a Mortgage Fraud Task Force, comprised of representatives from the FBI and other investigative offices.

Future Consideration and Prevention

Borrowers:

- Verify their identity.
- Use “knowledge-based” authentication.
- Check OFAC Watch Lists.
- If a business, perform business credentialing and license credentialing.
- Perform appropriate due diligence.

Future Consideration and Prevention

Employees:

- Verify previous employment.
- Verify education references.
- Perform criminal background checks.
- Perform credit checks.
- Verify against Financial and Law Enforcement Sanctions databases.

Future Consideration and Prevention

Vendors:

- Perform business credentialing and license credentialing.
- Verify principal owner identification.
- Perform owner background check.
- Perform/review vendor employee screening.
- Verify references.
- Perform appropriate due diligence.

ERM and Bank Risk Management Issues

Agenda

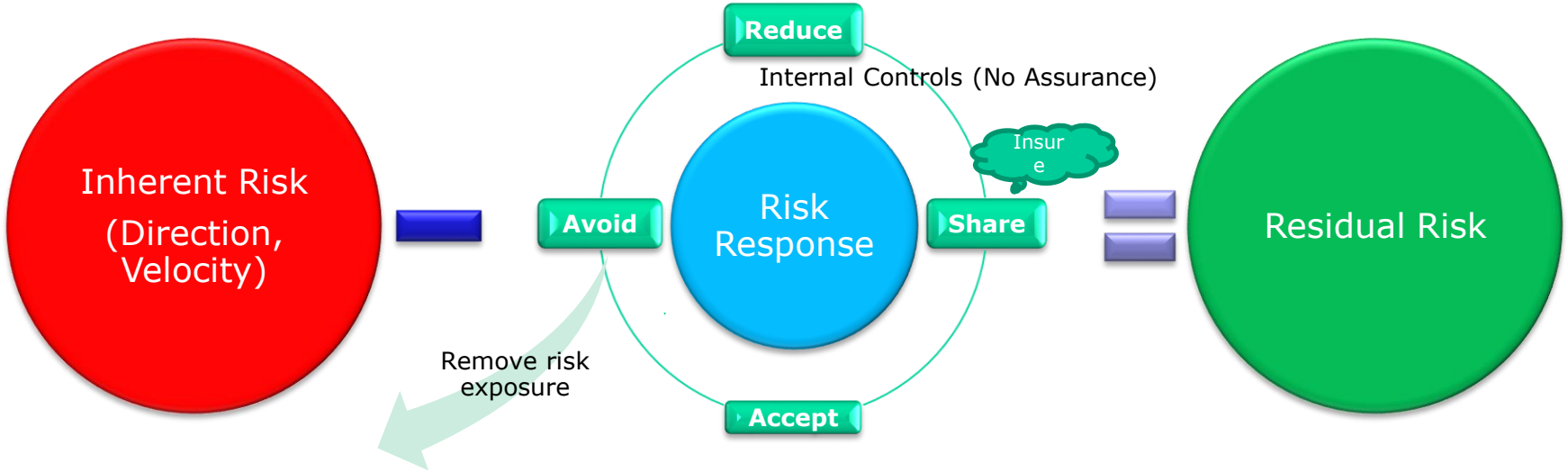
- Basics of Risk Management
  - Why risk management is important
  - Categories of risk
  - Role of Board in risk governance
  - What your regulators expect of you
- ERM and Risk Committees
  - Implementation strategy for ERM
  - Function and benefits of risk dashboards
  - Considerations for forming a Risk Committee
  - The position of Chief Risk Officer
  - Considerations regarding stress testing
- Other side of the Crisis
  - Lessons Learned
- A Practical Approach
  - Step-by-Step Process

Why Risk Management is Important

- Risk taking is inherent in banking
  - True with other industries as well
  - Risk is not good or bad
- Goal of Risk Management
  - Identify Risk
    - Understand risk taken (and potential rewards)
    - Likelihood, magnitude, frequency
  - Manage risk
    - Policies, procedures
    - Accept, avoid, reduce, share
- Risk management starts with the Board

Risk Response Decisions

- Accept risk
- Avoid risk
- Transfer or share risk
- Reduce/Mitigate risk



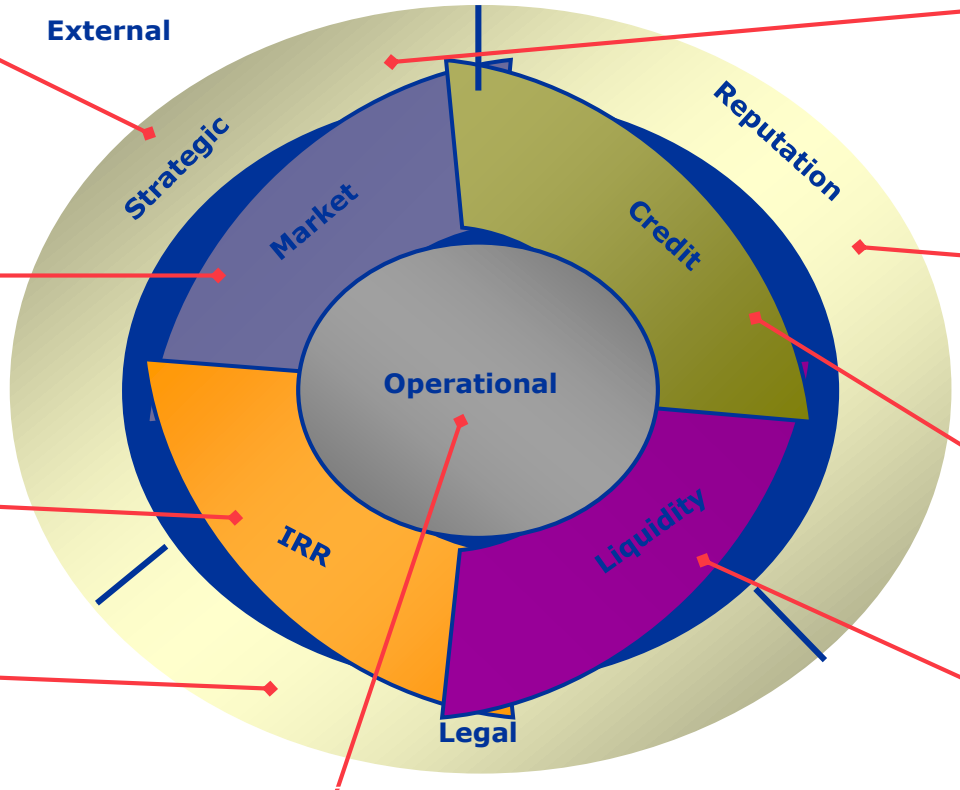
Risk Universe- Categories of Risk

External
Regulatory/Legal
Investor Relations
Competitor
Financial Markets
Catastrophic Loss
Sovereign/Political

Market
Valuation (on and off BS)
Foreign Exchange

Interest Rate Risk
Re-pricing
Yield Curve
Basis
Options

Legal
Compliance
Litigation
Contractual/Obligations
Fiduciary



Strategic
Corporate Governance
Leadership
Alignment
Planning
Communication

Reputation
Fraud
Ethics
Privacy

Credit
Traditional (Cash Flow)
Portfolio
Products
Geographies

Liquidity

Operational
Accounting
Technology

Member Loyalty/Retention
Performance Measurement
Budgeting and Planning

Financial Reporting
Product Development and Pricing
Human Resources

Third Party Relationships
Business Interruption
Policy/Procedure Compliance

Role of Board in Risk Governance

- Oversee risk management process
  - Policies
  - Procedures
  - Management execution
- Risk Appetite
  - Alignment with Strategy
- Monitoring Risk Management/Oversight
  - Dashboards
  - Committees
- Fiduciary responsibility to shareholders

Crowe Corporate Governance Framework

- Governance will determine the sustainability of activities and the enterprise as a whole,
- The Crowe Corporate Governance Framework™ links seven essential and interrelated components of corporate governance:

What your regulators expect of you

- Dodd –Frank Act of 2010
  - Independent directors
  - Risk committees
  - Stress Testing
- Risk management systems
  - Aligned to the complexity of the Bank
  - Systems should
    - Identify
    - Measure
    - Monitor
    - Control
- Enterprise Risk Management
  - Organization wide – across risk and operational silos
- Resources
  - The Director's Handbook - OCC

Enterprise Risk Management Defined

- Enterprise Risk Management (ERM) is a process designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

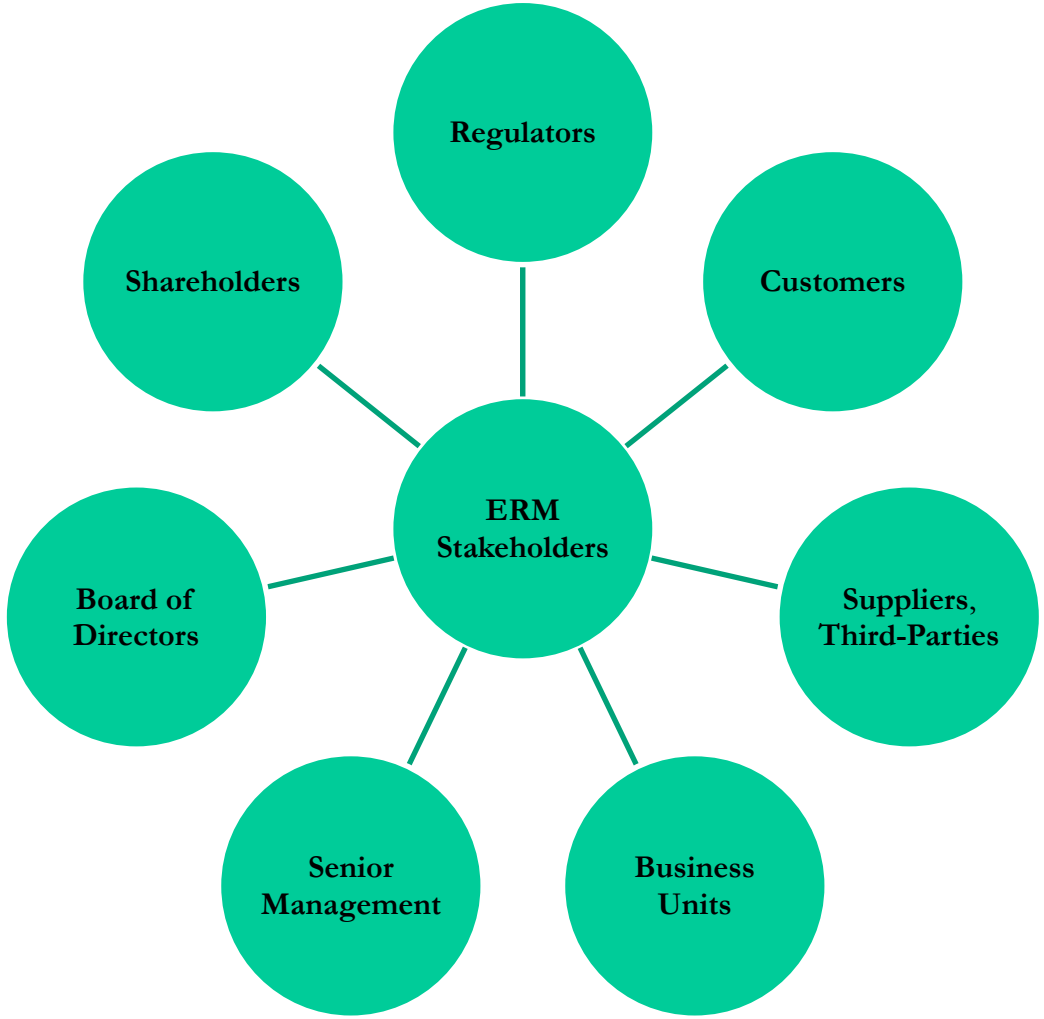
Key steps to build an effective ERM Program

- Understand that ERM is a journey – not an event
- Define the risk appetite and communicate it throughout the organization
- Create a documented, independent risk management structure
- Create a uniform risk language
  - Define and communicate risk-related roles and responsibilities
- Establish aggregation, escalation, and accountability
- Develop regular monitoring, analytics and reporting - Dashboard
- Maximize the use of technology and ensure complete, accurate, consistent and timely data
- Address risk in the strategic planning and decision-making process

ERM- Implementation Planning

- Define objective and scope
- Define timeline
- Identify executive sponsor
- Identify key stakeholders
- Define organizational structure
- Identify resources
- Identify framework
- Develop reporting plan

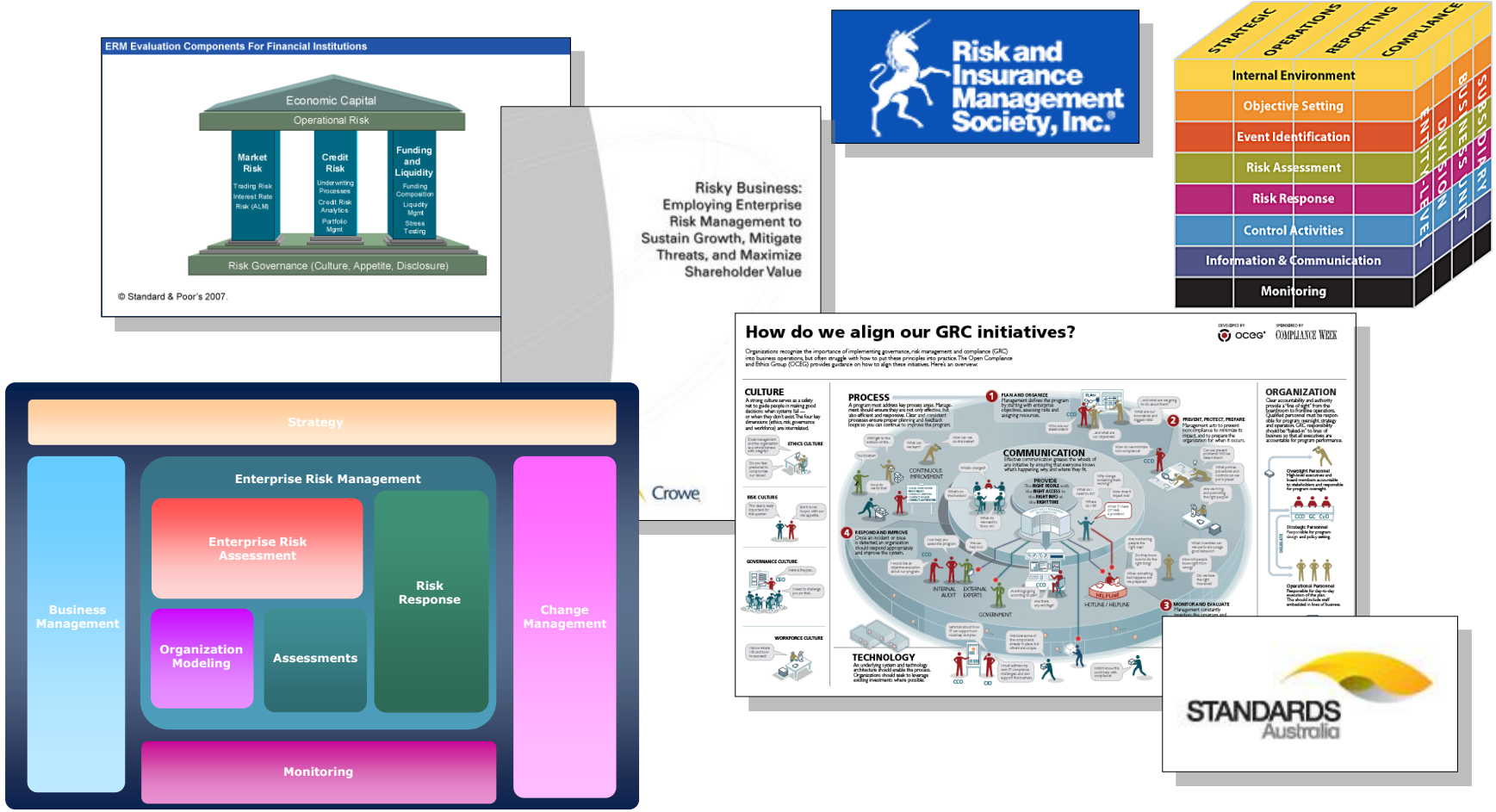
Identify Stakeholders



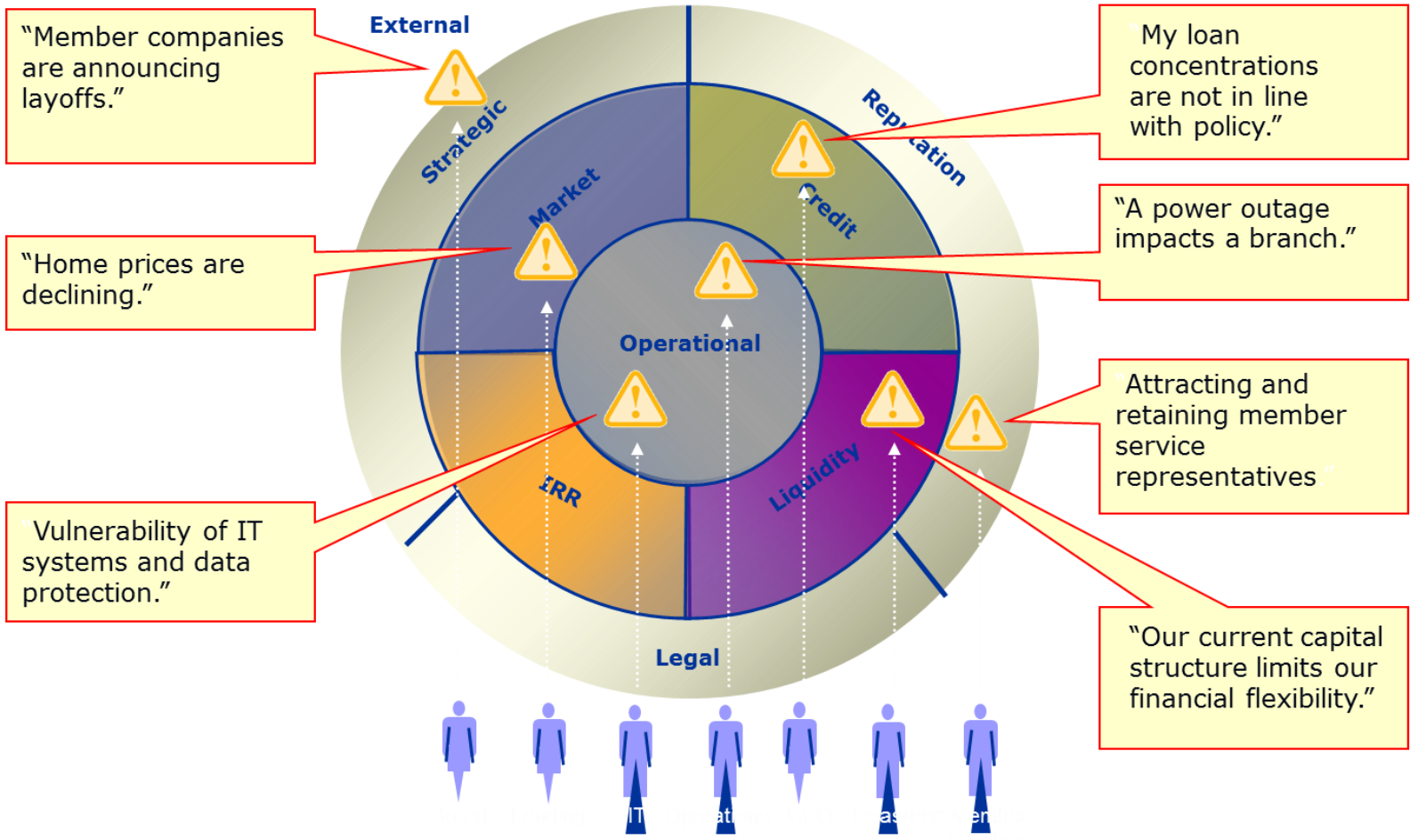
Identify Framework

- COSO
- AIRMIC (Association of Insurance and Risk Managers)
- FERMA (Federation of European Risk Management Associations)
- ISO 31000 (International Organization for Standardization)
- IRM (Institute of Risk Management)
- AS/NZ 4360:2004 (Australia/New Zealand)
- RIMS (Risk and Insurance Management Society)
- Etc.

Multiple Frameworks Available



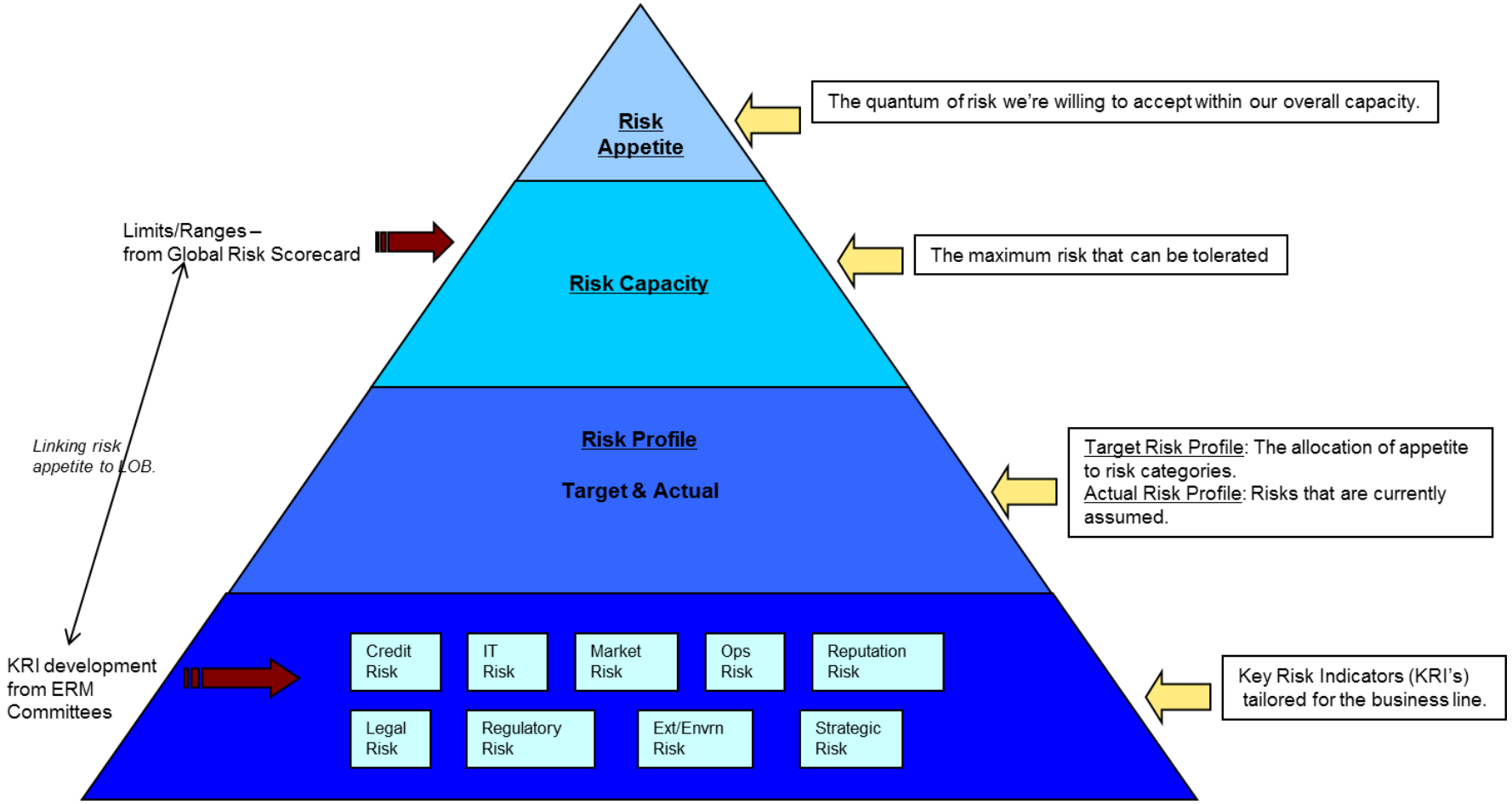
Defining Your Unique Enterprise Risk Universe



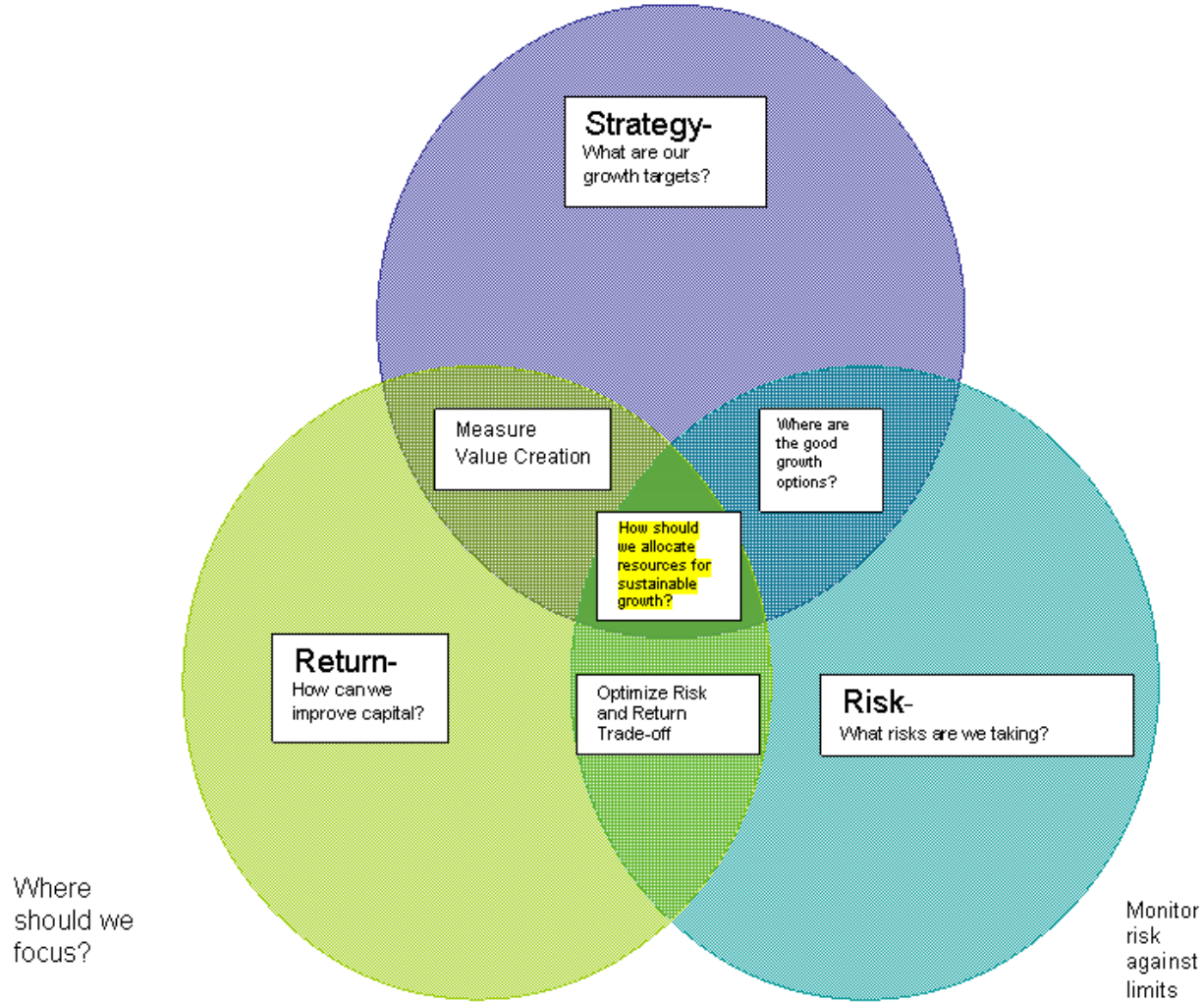
Define Risk Tolerance/ Appetite

- Risk appetite is the amount of risk - on a broad level - an entity is willing to accept in pursuit of value
- Risk Tolerance – "Acceptable variation relative to the achievement of an objective"
- Key Questions to determine risk appetite
  - What risks will the organization not accept?
  - What risks will the organization take on new initiatives?

Risk Appetite Pyramid



Risk Appetite: Aligning Strategy with Risk and Return



Risk Prioritization

- Dashboard/Heat Map
- Key risks/top risks
- Risk response

Risk Assessment			
Risk Rankings - Likelihood of Occurrence and Impact			
REF.	RISK NAME	LIKELIHOOD	IMPACT
R1	Improper Apportionment	HIGH	HIGH
R2	Incorrect Local Tax Distribution	HIGH	HIGH
R3	Statutory Tax Assessment Compliance	LOW	HIGH
R4	Electronic Payment and Refund Processing	LOW	MODERATE
R5	Refund Fraud	LOW	HIGH
R6	Audit Failure	LOW	MODERATE
R7	Integrated Tax System Functionality	MODERATE	HIGH
R8	Outside Economic Conditions	LOW	LOW

Broader Bank ERM Roles & Responsibilities

Board

- Sets the requirements for risk management measurement, monitoring and reporting as well as the organization's appetite for risk
- Encourage a culture of risk awareness and evaluate skills and resources dedicated to managing and monitoring risks within the organization
- Ultimate strategic oversight of risk within organization

Risk Committee

- Recommends risk policy and guidelines to senior management and monitors risks

Audit Committee

- Responsible for oversight of internal controls of an organization including oversight that appropriate risk management processes are in place

Senior Management

- Manages overall risk
- Approves risk tolerance (recommended by the CRO and Risk
- Committee)
- Takes action to mitigate risk
- Assures proper control environment is in place

ERM- Board Governance

Key questions Directors should focus on:

- What are the company's ***top risks (****and top emerging risks)*, how big are they and how often are they likely to occur? ***(Probability and magnitude)*** How often is the list of top risks updated?
- What is management doing about the top risks? ***Who owns key risks?***
- What size quarterly operating or cash loss has management and the board agreed is tolerable? ***Risk appetite.***
- Describe the staff responsible for risk management programs and their place in the organization chart. How do you measure the success of risk management activities? ***(Qualifications, empowerment, independence)***
- How would a loss from a key risk affect ***incentive compensation*** of top management and planning/budgeting?
- What discussions about risk management have taken place at the board level or among top management when strategic decisions were made in the past? ***Communication***

Risk Dashboards

- Snapshot of risk profile
- Comparison to risk parameters established by Board
- Identifies potential areas of concern
  - Leading indicators
- Frequency

Risk Committees- when are they specifically required?

- Risk management is the job of the Board of Directors
  - Committees support – but do not supplant responsibility

- Section 165(h) of the *Dodd-Frank Wall Street Reform and Consumers Protection Act*
  - First statutory requirement for a risk committee
  - Requires all publicly held bank holding companies with >$10 billion in assets to establish risk committees when deemed necessary or appropriate to promote sound risk management practices
  - Purpose is to document and oversee, enterprise wide, the risk management practices of the company's operations

Do you need a Risk Committee?

- For some – regulation will dictate
- For everyone else –
  - Weigh pros and cons of an additional board committee
  - Considerations
    - Complexity and maturity of enterprise risk management within the organization
      - Committee will demand assessment and reporting – is organization ready for that
    - Make up of Board and current level of risk management activities
      - Effectiveness of what currently happens at the board now
      - Evaluation if this will continue to be effective In the future
    - Would a risk committee be an important enhancement of overall risk management?
    - Current make-up and responsibilities of the audit committee?
      - Does audit committee already function as an audit and risk committee?
      - Is anything being shortchanges if audit committee is playing a dual role?
- Organizational structure
  - Complexity
  - HC committee or Bank board committee
- Not a one size fits all answer

Potential advantages of forming a Risk Committee

- Intentional, directed focus regarding managing the companies Risk
- Depending on complexity of operations and risk management – appropriate time and focus of select committee members
- Proactive, forward-looking view of organizational risk and risk management
- Strong correlation between effective governance and strong investment opportunities.
- Establishes the committee on your timetable and development pace
  - Before required by regulation
  - Before any “trickle down” or “best practices” requirements

Chief Risk Officer

- When needed
  - Growing trend – emerging best practice
  - Asset size or complexity?
- Officer function focused on risk management
- Supports ERM and Risk Committee functions
- Background

Chief Risk Officer- Roles

Chief Risk Officer

- Recommends risk management policy and tolerance for approval
- Ensures risks are identified
- Develops risk measurement methodologies and tools to quantify risk and assures such are utilized
- Conducts overall risk coordination
- Analyzes and reports on risk exposures
- Provides on-going risk training
- In some organizations, takes an active role in assisting line management in developing risk strategies

Business Units Risk Officer

- Assures that each unit's stated risk management tolerance is baked into each business unit's planning and budgeting processes
- Identifies and reports all risk exposures to CRO and CEO

Considerations Regarding Stress Testing

- Defined
  - Analysis of a bank's vulnerability to a variety of economic shocks through the use of simulated models set to a variety of scenarios.
- When required
  - >$10 Billion - annually
- Other considerations if not required
  - Use of models
  - Impact of adverse scenarios
    - Understanding magnitude of risk
  - Risk response – risk mitigation
  - Cost benefit

Other side of the crisis- lessons learned

- Concentration of risk
  - Credit concentrations
  - Market concentrations
- Strategic plans and understanding of risk
  - Strategy as a risk
- Risk Models
  - Only as good as assumptions
  - Modeling the downturns
- Operational risk consideration
  - Foreclosures
- Other

Structure of the Risk Committee

- Structure of Risk Committee
  - Chaired by an independent director
    - Independent director defined by SEC Regulation S-K
  - Include additional independent directors
  - One member with appropriate risk management expertise –
    - Commensurate with risk – capital structure, activities, size, complexity
    - Committee members should also have risk management experience commensurate with the complexity of the company
  - Understanding of:
    - Risk management principles and practices
    - Measuring and identifying risks
    - Monitoring and testing risk controls
  - Written charter
  - Meet regularly and as needed
  - Maintain records of proceedings, including risk management decisions

Role and Responsibilities of Risk Committee

- Document and oversee enterprise-wide risk management policies and practices
- Review and approve an appropriate risk management framework
  - Framework commensurate with the company's risks
  - Establishing risk limits (risk tolerance)
  - Policies and procedures related to risk management governance
  - Systems for identifying and reporting risks – including emerging risks
  - Monitoring compliance with risk limits
  - Monitor implementation of corrective actions related to risk management activities
- Work with the CRO

A Practical Approach

- ERM is a worthy goal for all businesses, regardless of size
- Risk-management activities need to be tied to strategy and ultimately built into everyday business processes
- The following five-step project plan enables organizations to identify and coordinate activities they already have begun, identify risks that are not adequately managed, and close gaps and move forward:
  - ✓ Organizing your team
  - ✓ Establishing a framework
  - ✓ Assessing risks
  - ✓ Inventorying current risk-response activities
  - ✓ Closing the gaps

A Practical Approach

Leveraging existing knowledge and programs will go a long way to help reduce the effort in getting started.

- Who
  - Internal Audit
  - The Compliance Officer
  - IT Security and Privacy or the Insurance Group
  - Chief Risk Officer
  - Safety
- What
  - Internal Audit Risk Assessment
  - Anti-Fraud Risk Assessment
  - Enterprise-Wide Compliance Risk Assessment
  - Insurance Risk Assessment
  - GLBA/IT Risk Assessment

Step 1: Organize the Effort

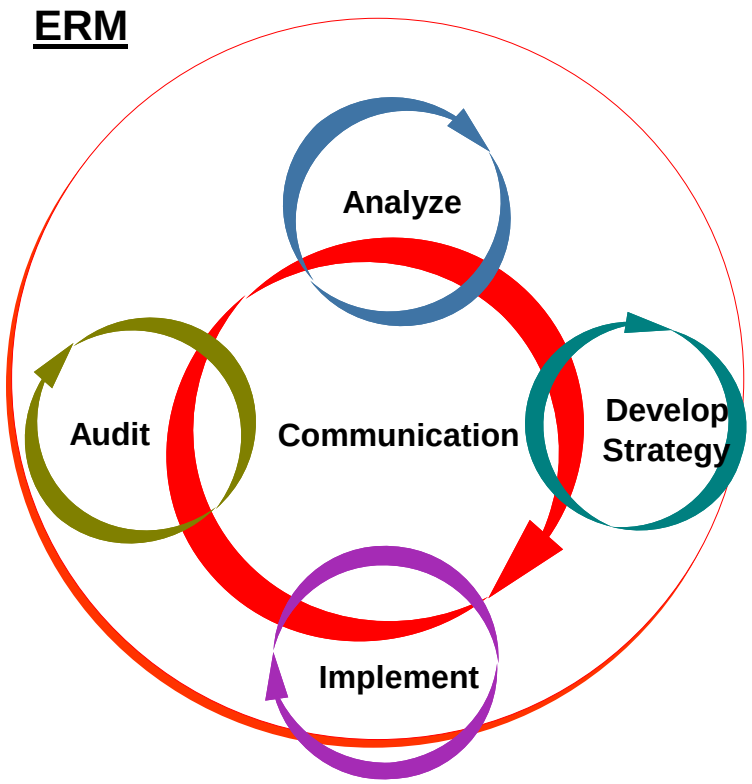
Assemble:

- Steering Committee
- Project Team
- Project Charter

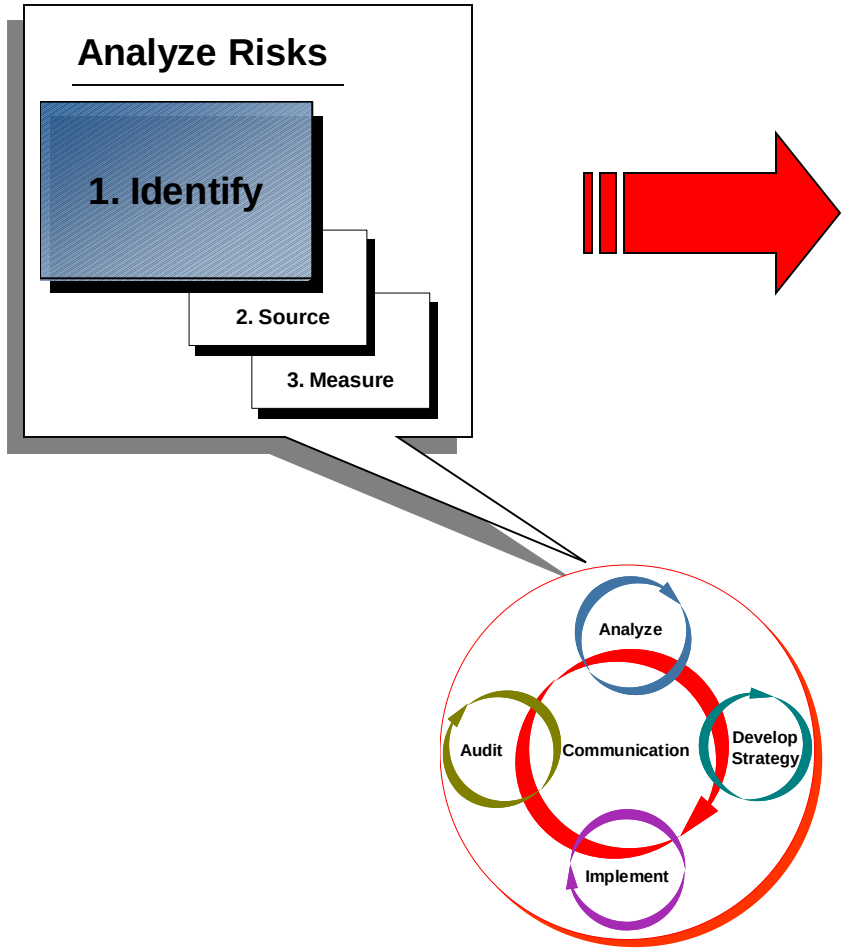
Step 2: Establish a Framework Around Risk

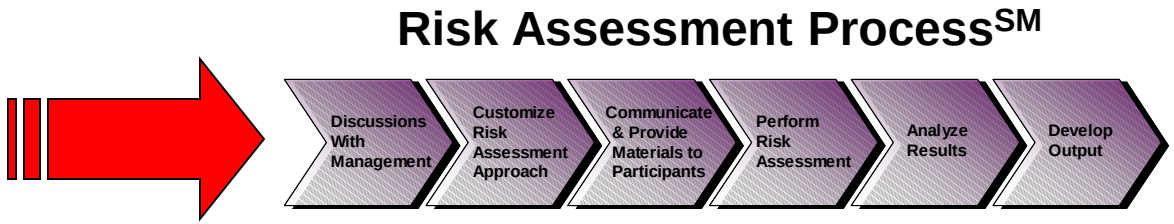
An ERM framework provides the context to develop specific ERM processes. For example, the framework may contain these five components:

- Analyze risks
- Develop risk strategies
- Implement risk strategies
- Audit risk strategies
- Communicate results



The “Analyze” Element of ERM





During the "Analyze" phase of ERM, risks are identified, sourced to a process or area (where the risks reside) and measured (based on impact and likelihood of risk).

Step 3: Risk Assessment- The Top 10- 15 Risks

- Identify key risks
- Identify where they reside
- Significance
- Where to draw the line

Likelihood Risk Ranking Table Description

Level	Descriptor	Likelihood of Occurrence
1	Rare	Very Low
2	Unlikely	Low
3	Possible	Moderate
4	Likely	High
5	Almost Certain	Very High

Impact Risk Ranking Table Description

Level	Descriptor	Impact of Occurrence
1	Insignificant	• Minimal loss of revenue • No regulatory or reporting impact
2	Minor	• 1-2 reportable incidents which may impact processing requirements
3	Moderate	• Several incidents which may impact processing or reporting requirements
4	Major	• Major reportable events to shareholders, or regulators
5	Catastrophic	• Multiple major reportable events to shareholders or regulators

Impact + Likelihood = Aggregate Inherent Risk

IMPACT

5. Catastrophic	5	6	7	8	9
4. Major	4	5	6	7	8
3. Moderate	3	4	5	6	7
2. Minor	2	3	4	5	6
1. Insignificant	1	2	3	4	5
	1. Rare	**2. Unlikely**	**3. Possible**	**4. Likely**	**5. Almost Certain**

LIKELIHOOD

3 Green = 12%	24%
3 Gold = 12%	
9 Yellow = 36%	
4 Purple = 16%	52%
6 Red = 24%	24%

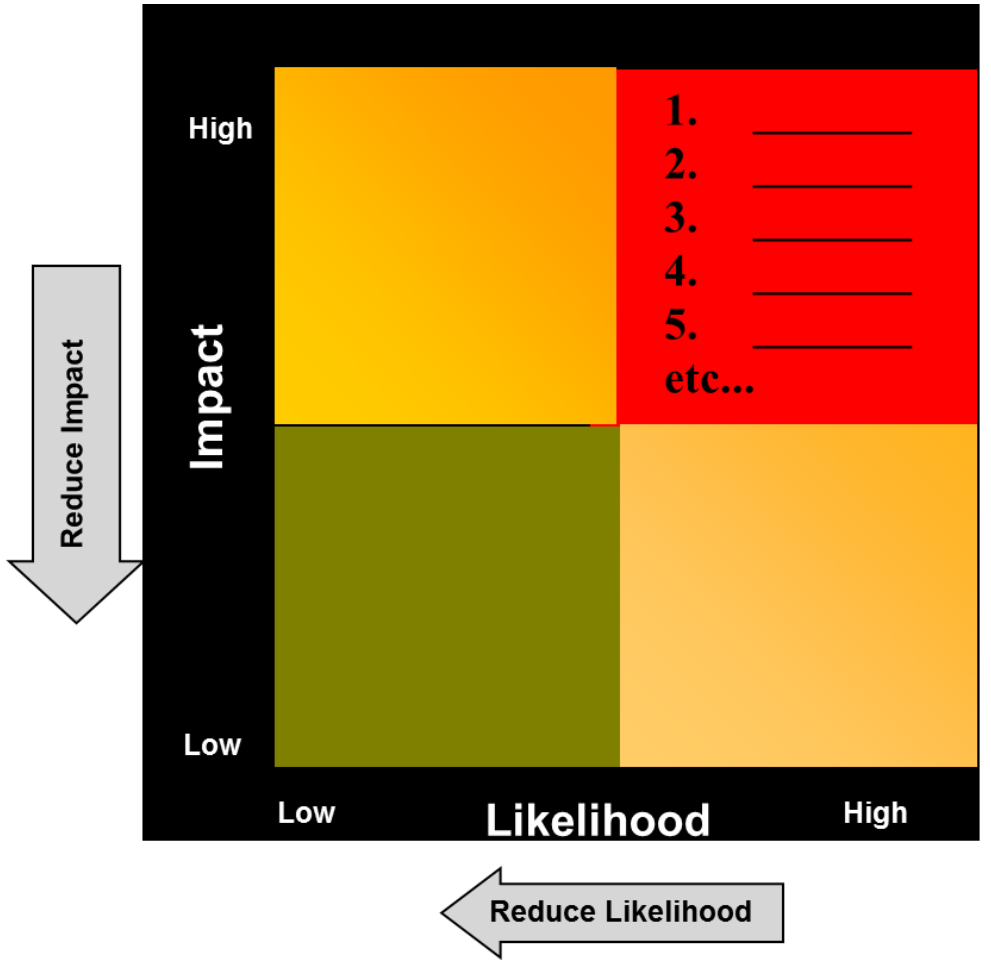
Risk Profiles Result from Risk Assessment

A risk profile summarizes key risks and allows organizations to focus risk management efforts.

Managing these risks will reduce the likelihood and significance over time, thus improving the organization's overall risk profile.

What is Your Organization's Risk Profile?

Which risks belong in the top-right quadrant?



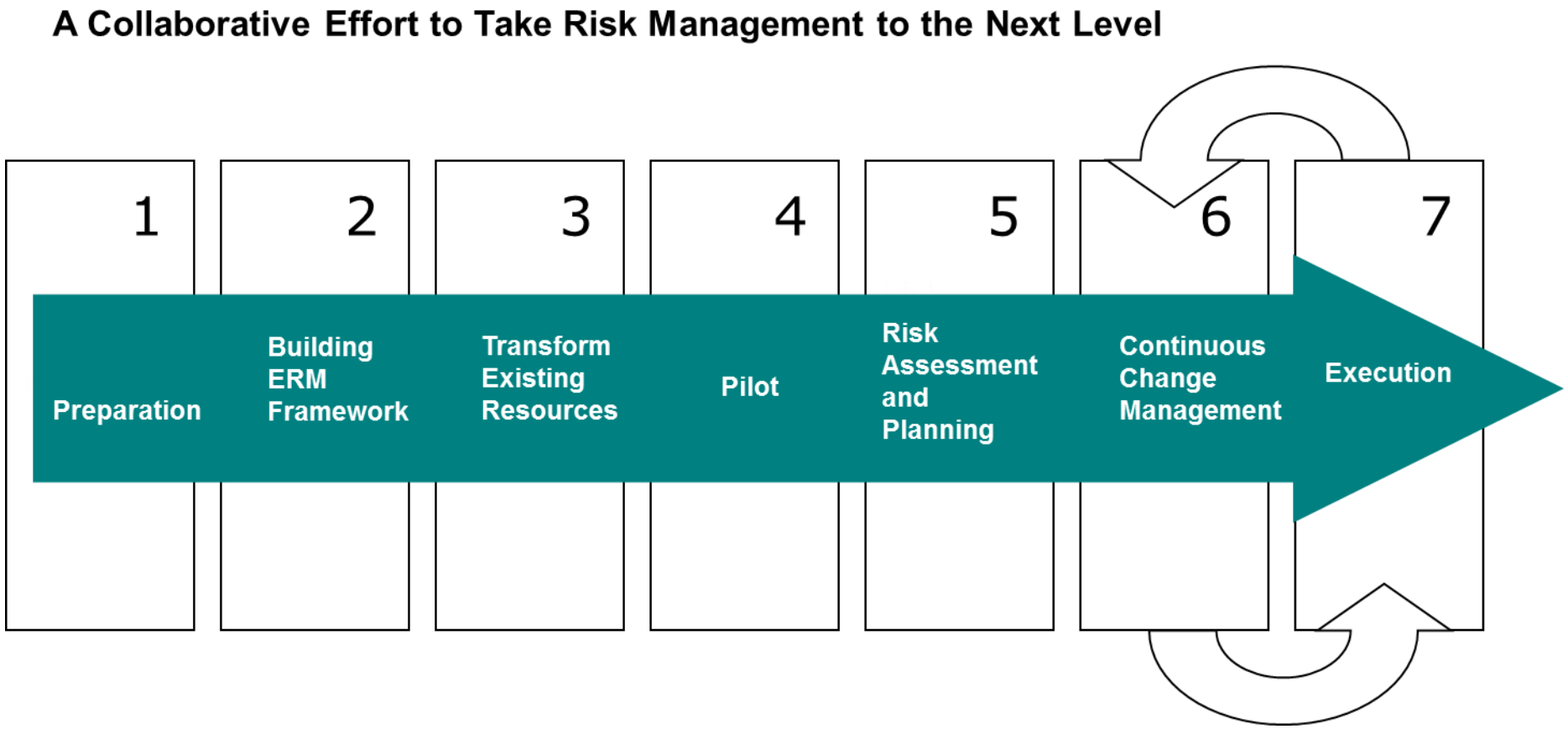
Step 4: Inventory Current Risk- Response Activities

- How do you think about risk?
- When someone says "risk," what do you think?
- Which risks are you responsible for responding to?
- How do you coordinate your risk mitigation or compliance activities with others in the organization?

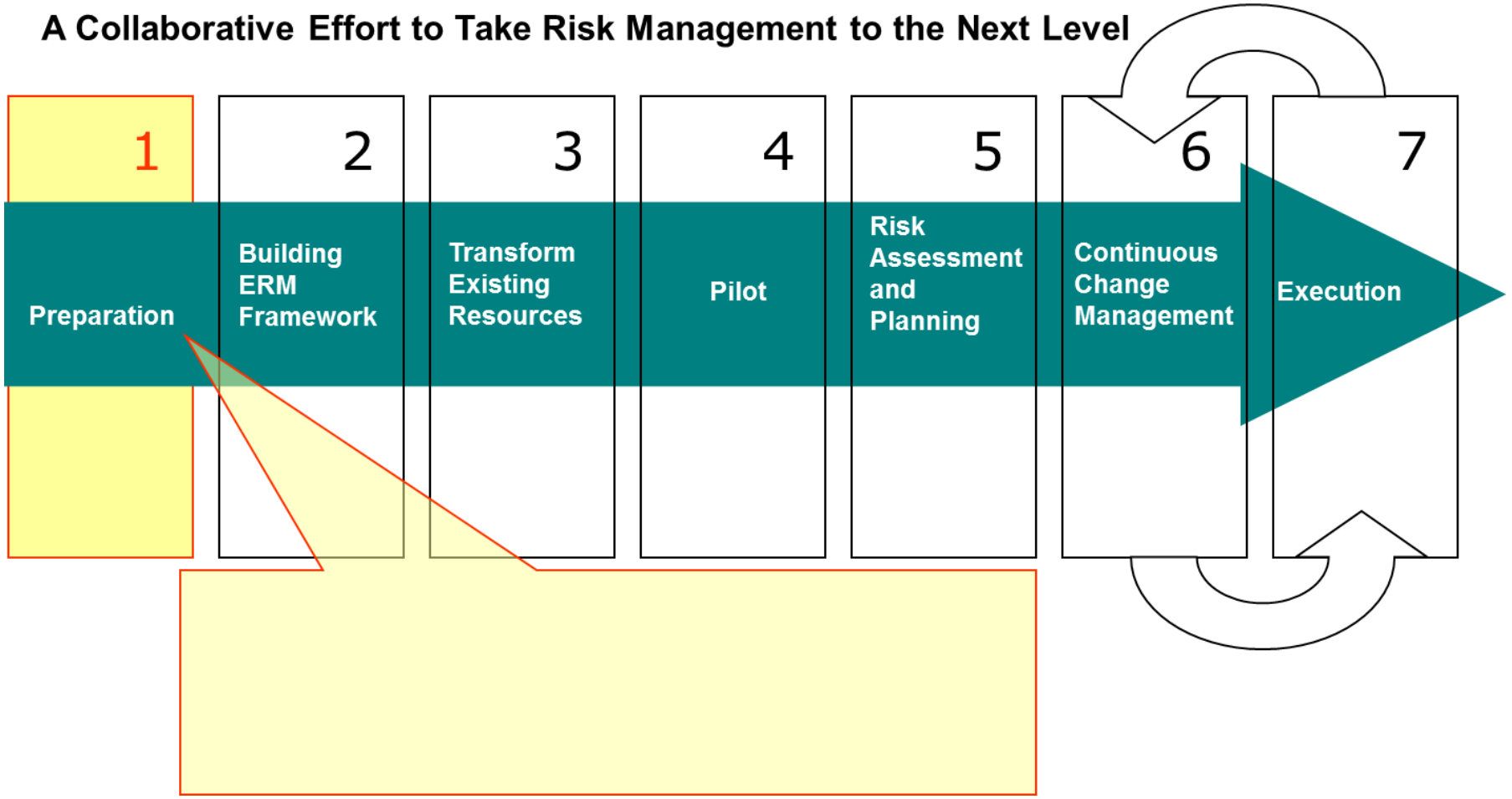
Step 5: Identify Gaps and Prioritize

- Recommendations
  - Guiding the organization to improve ongoing risk management processes
  - Decisions on how to best manage risks and where it should be managed

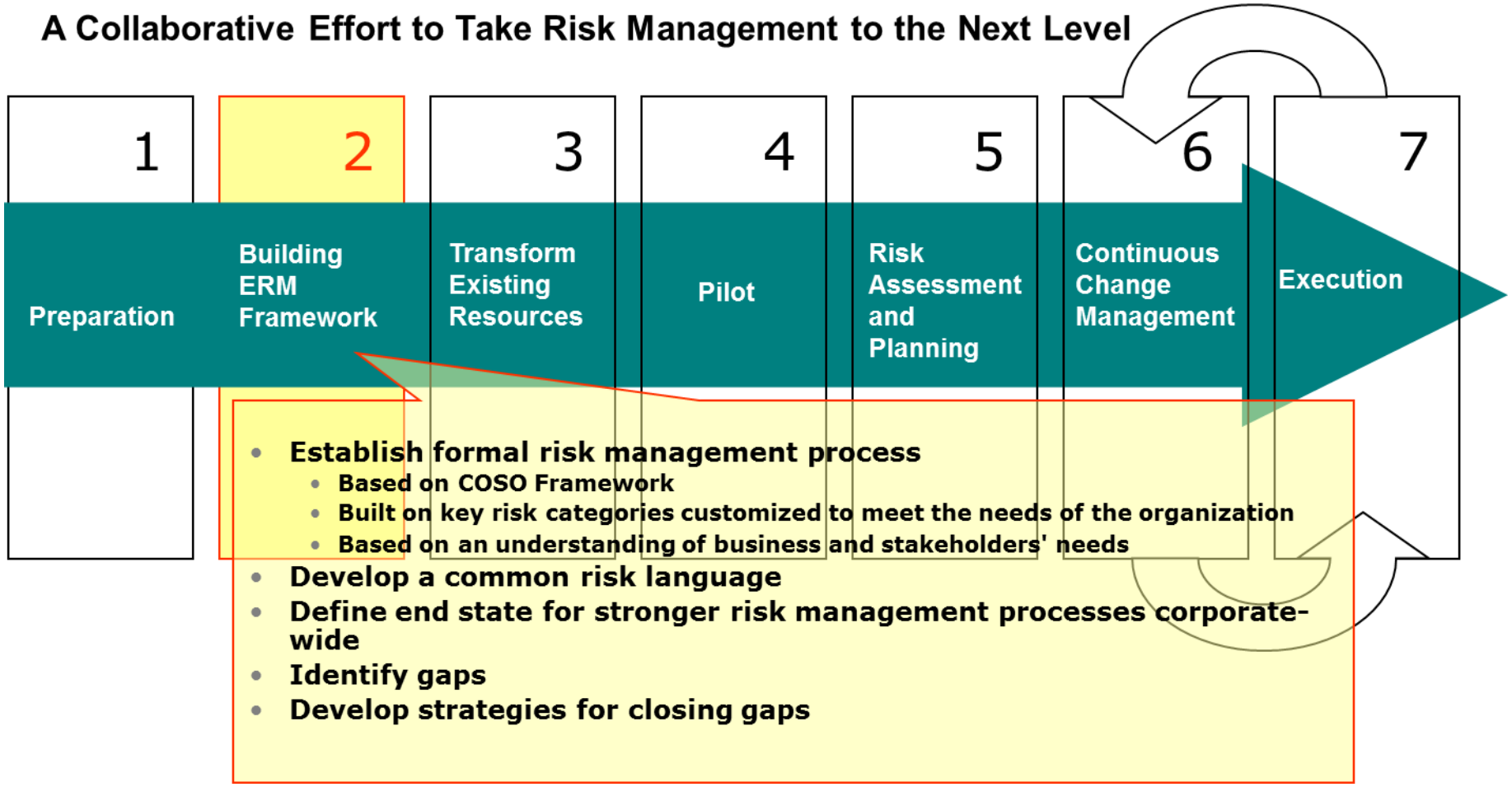
Transformation to Enterprise Risk Management



Transformation to Enterprise Risk Management (Continued)

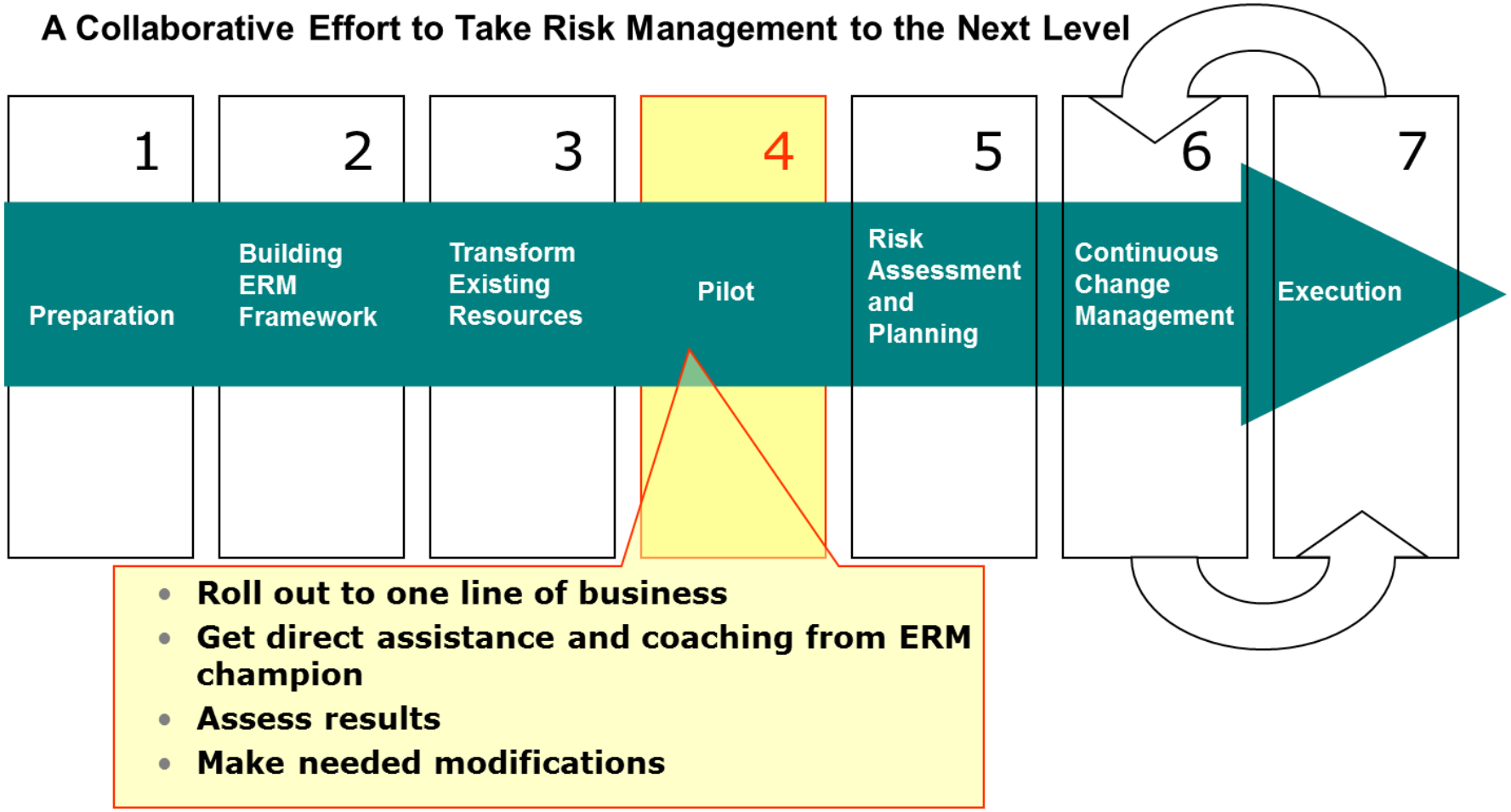


Transformation to Enterprise Risk Management (Continued)

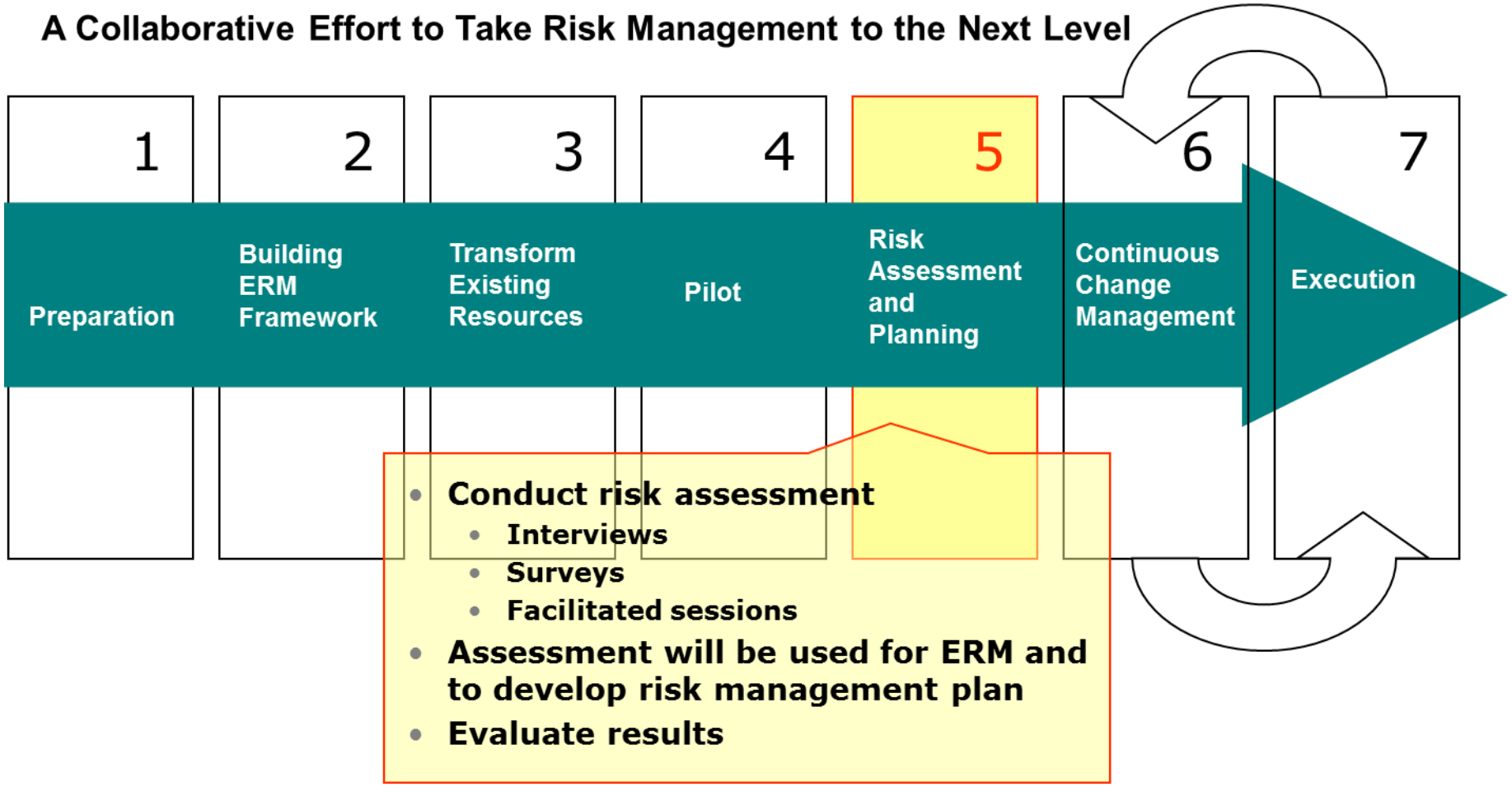


Transformation to Enterprise Risk Management (Continued)

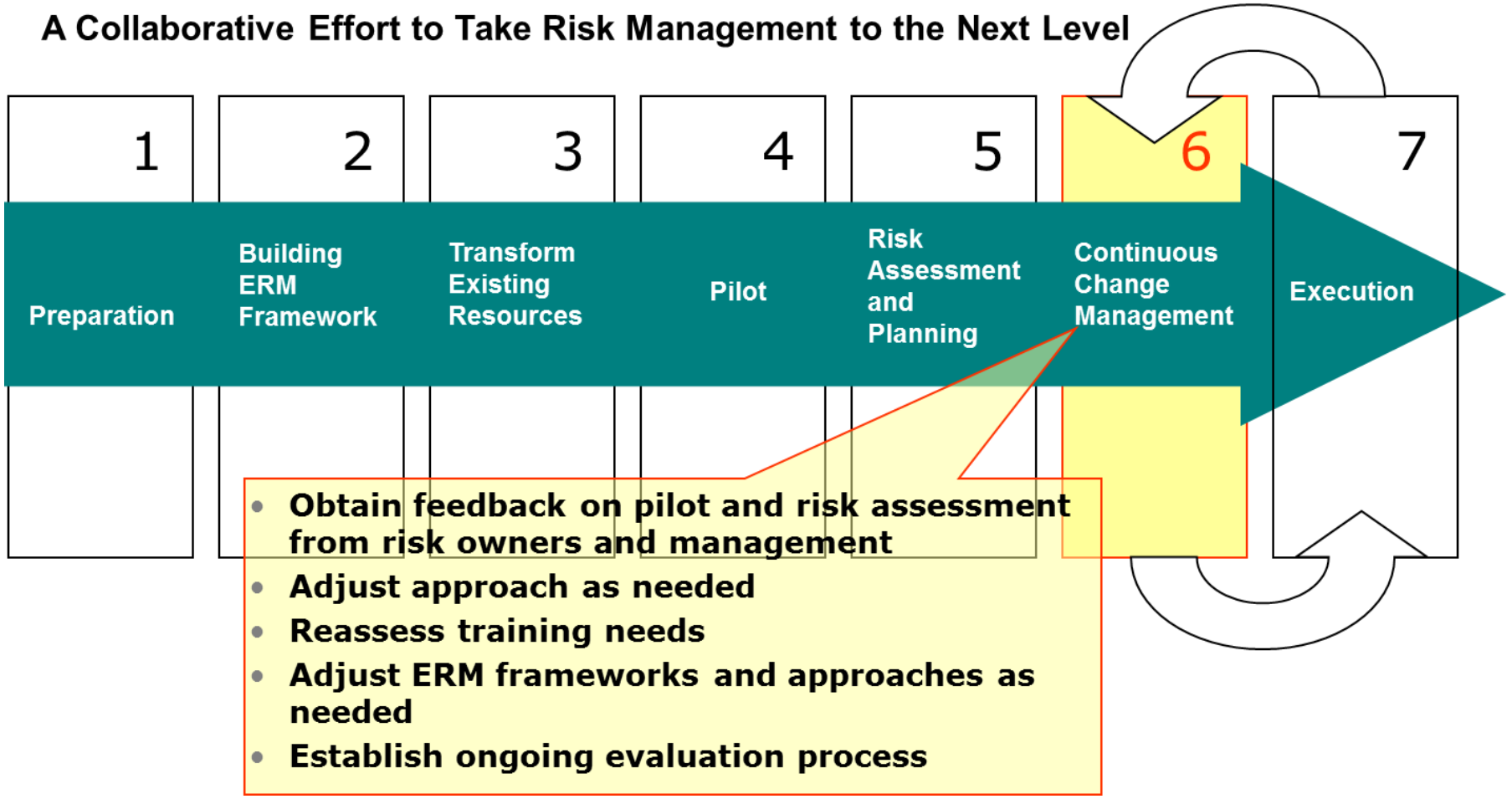
Transformation to Enterprise Risk Management (Continued)



Transformation to Enterprise Risk Management (Continued)



Transformation to Enterprise Risk Management (Continued)



Transformation to Enterprise Risk Management (Continued)

Characteristics of an Effective ERM Process

- Infrastructure to support ERM process, including:
  - Policy
  - Common risk language (customized risk model)
  - Defined roles and responsibilities
  - Tools to facilitate monitoring, updating, and reporting
- Framework to organize ERM activities
- Linkage to other management activities, e.g., strategic planning

ERM: Keys to Success

- Clearly articulated risk management goals that provide a foundation for ERM and for related training and communication
- Common risk language to enable individuals throughout the organization to conduct meaningful cross-functional discussions about risk
- Individuals clearly understand their roles in the assessment and risk management framework

ERM- Sample Risk Owners

	Business Process	Senior Executive
1	Accounting	Senior Manager
2	Funds Management (includes ALM, Cash Mgt., Securities, Borrowings & Repurchase Agreements)	Senior Manager
3	Bank Secrecy Act	Senior Manager
4	Branch Operations	Senior Manager
5	Lending (Credit Administration and Loan Operations)	Senior Manager
6	Special Assets/ALLL/Collections/Recovery	Senior Manager
7	Deposit Operations (includes Automated Clearing House, Remote Deposit Capture and Wire Transfer)	Senior Manager
8	Entity Level/Corporate Governance	Senior Manager
9	Human Resources and Payroll	Senior Manager
10	Information Technology	Senior Manager
11	Regulatory Compliance	Senior Manager

ERM- Risk Assessment Worksheets

- Send worksheets to each designated “Risk Owner”.
- The ERM worksheets will have the overall strategic goals for Sample Bank as a whole and will have some pre-populated objectives and risks based on the other risk assessments (e.g. the internal audit risk assessment).
- Risk Owners then add other objectives (strategic, reporting, operational, compliance) and their related risks to the worksheets.
- Sample Bank’s ERM coordinator and a Crowe representative will contact the Risk Owners to set-up one-on-one meetings to discuss the worksheets and finalize the information.

Risk Inventory

XYX Bank
Risk Assessment Summary
Working Draft
Date:

Line of Business:

Risk Owner:

Objectives - Document three to five key operational, reporting and/or compliance objectives of the line of business. (1)*

O1.	
O2.	
O3.	
O4.	
O5.	

Document the 1-3 most significant risks/risk events that could impact the line of business' ability to achieve each stated objective (2)*:

			Inherent Risk Assessment			Residual Risk Assessment			
Objective # (3)*	Risk/Event Description (4)*	Risk Category (5)	Likelihood (6)	Impact (7)	Aggregate (8)	Risk Response (9)	Effectiveness of Risk Response (10)	Residual Risk (11)	Direction (12)
			Moderate	High	High		Effective	M	S
			Low	High	Moderate		Effective	L	S

Risk Inventory (cont.)

(1) Document three to five key operational, reporting and/or compliance objectives of the line of business.
(2) Document the 1-3 most significant risks/risk events that could impact the line of business' ability to achieve each stated objective.
(3) Document the specific objective or objectives to which the individual risk relates
(4) Describe the nature of the risk or event that may impact the achievement of the objective(s)
(5) Document the specific category(s) of risk using the defined risk categories.
(6) Assess the likelihood that the risk/event will occur

Risk Inventory (cont.)

(7) Assess the impact on the organization/line of business should the risk/event occur using the scale on the attached schedule.

(8) Giving consideration to both likelihood and impact assess the aggregate inherent risk using the scale on the attached schedule - inherent risk is defined as the risk to an organization in the absence of any actions management might take to alter the risk's likelihood or impact.

(9) Describe the risk response(s) taken to address the identified risk/event. Risk responses may be controls in place or other actions taken to avoid, share or reduce the risk.

(10) Assess the effectiveness of the risk response in reducing the risk to a level that is within the organization's risk tolerance.

(11) Assess the residual risk - residual risk is defined as the remaining risk after management has taken action to alter the risk's likelihood or impact.

(12) Assess the direction of risk as either (I)increasing, (S)table or (D)decreasing

ERM Project Timeline

Planning and Info Gathering

- Organize Team
- Project Planning
- Educate Stakeholders
- Establish Project Goals and Expectations
- Gather and Analyze Existing RM data
- Conduct on-site Interviews

Deliverables

- Project Plan and Timeline
- Education Materials

Assessment and Gap Analysis

- Evaluate Existing RM Structure
- Identify Gaps
- Develop Recommendations

Deliverables

- Crowe ERM Scorecard
- Recommendations

ERM Design

- Design ERM Structure
- Develop ERM Policy
- Define Roles and Responsibilities
- Design Tools and Templates
- Define ERM Process

Deliverables

- ERM Policy
- Sample Tools/Templates

Pilot and Implementation Plan

- Conduct Pilot
- Debrief Pilot
- Adjust ERM Process and Policy
- Develop Implementation Plan

Deliverables

- Pilot Results
- Implementation Plan

Auditing Corporate Governance

Agenda

- Overview of Corporate Governance
- COSO 2013 Internal Control Framework
- Audit Techniques and Strategies

Overview of Corporate Governance

Corporate Governance

Forbes reports that more details have emerged with regards to the list of the top corporate boards in America, as measured by JamesDruryPartners.

Forbes noted: "One surprise was finding that some prominent companies had fairly low governance capacity, while some of the smaller firms in the Fortune 500 were 'overboarded' **-- they had very impressive governance capacity and tended to outperform."**

CEO James Drury concluded, "I think **smaller mid-caps with high governance have a pulling effect over the long term,** and the large companies with low governance capacity have something of a drag on performance."

Corporate Governance

Corporate Governance is the systems and processes an organization has in place to protect the interests of its diverse stakeholder groups.

Good Corporate Governance Requires

- Establishing a culture of sound business practices and ethics
- Ensuring that management has a comprehensive understanding of how to manage risks
- The right processes for managing and monitoring risks are in place

Shareholder Returns Studies

University of Michigan Business School

"Firms with profitable investment opportunities and with more reliance on external financing have higher quality corporate governance, and firms with higher corporate governance ratings are valued higher."

McKinsey & Company

"An overwhelming majority of investors are prepared to pay a premium for companies exhibiting high governance standards. This applies to companies in every country of the world"

Business Week

"The stocks of companies with the best boards outperformed those with the worst boards by 2 to 1. But as the economy slowed...the Best Boards companies retained much more of their value, returning 51.7%, vs. –12.9% for the Worst Board companies."

Columbia Law Review

"... corporations with active and independent boards appear to have performed much better in the 1990's than those with passive, non-independent boards."

Journal of Economics

"We find that firms with stronger shareholder rights had higher firm value, higher profits, higher sales growth, lower capital expenditures, and made fewer corporate acquisitions."

Good Corporate Governance

- Good corporate governance is the “right thing to do”, but improved shareholder returns helps to justify the cost.
- Good corporate governance applies to all companies no matter where they are located.
- Good corporate governance needs to be principle based rather then rule based.

Compliant v. Good Corporate Governance

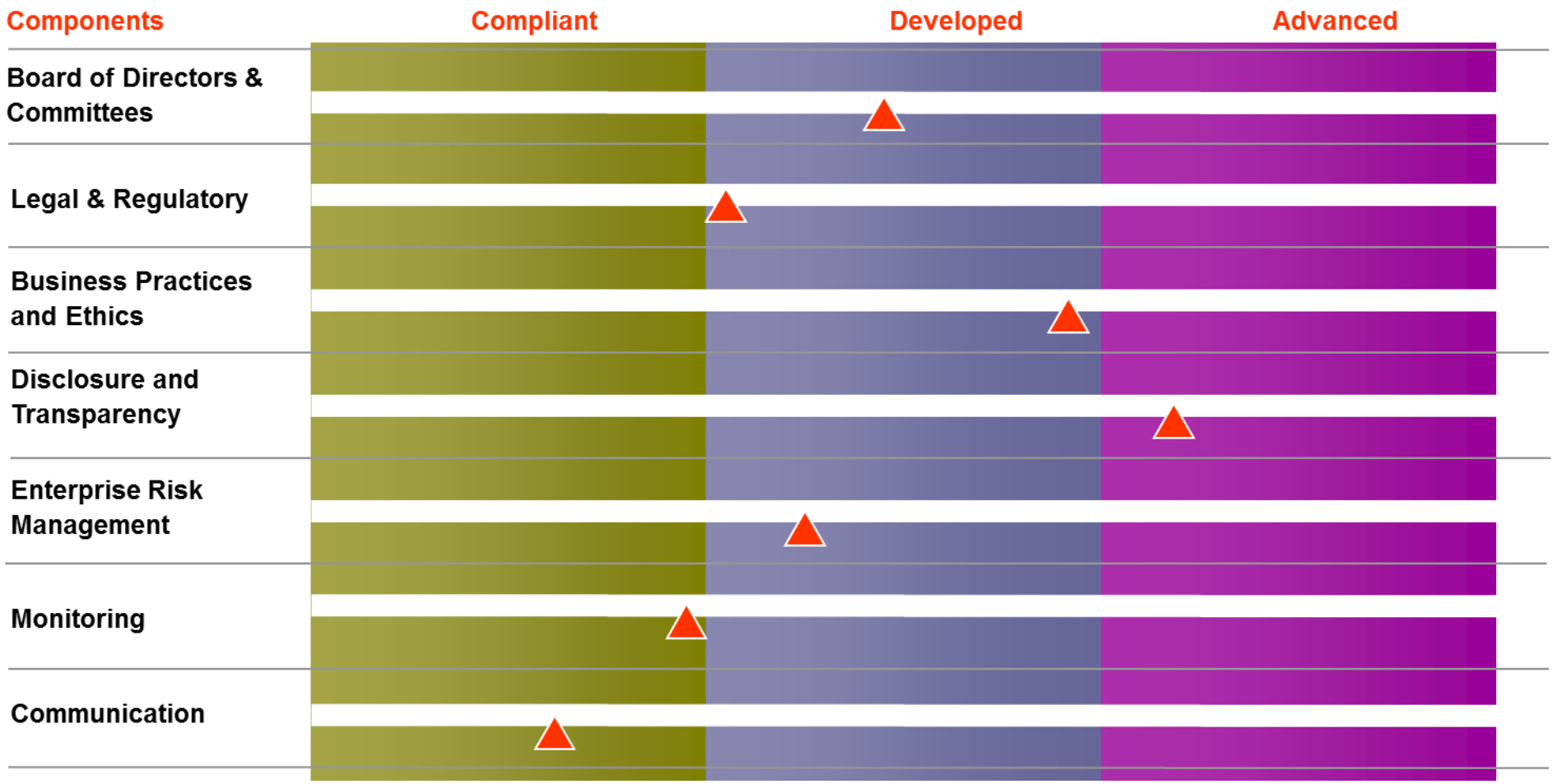
Good corporate governance requires more than focusing on legal and regulatory compliance. Good corporate governance that will withstand the test of time requires:

- Establishing a company-wide culture of sound business practices and ethics
- Ensuring that management has a comprehensive understanding of how to manage risks
- Implementing the right processes for managing and monitoring risks

Dynamics of Good Corporate Governance

Corporate governance is the systems and processes an organization has in place to protect the interests of its diverse stakeholder groups, i.e. shareholders, employees, customers, vendors, the community, etc..

Corporate Governance Scorecard



Sample Scorecard Assessment

Board of Directors and Committees:

Compliant

- Committees composed entirely of qualified outside directors
- Audit Committee members may only receive directors fees as compensation

Developed

- Board meets in executive sessions without CEO and other insiders
- Material portion of directors' pay is stock related

Advanced

- Only non-independent director is CEO
- Directors allowed to engage outside advisors at corporation's expense

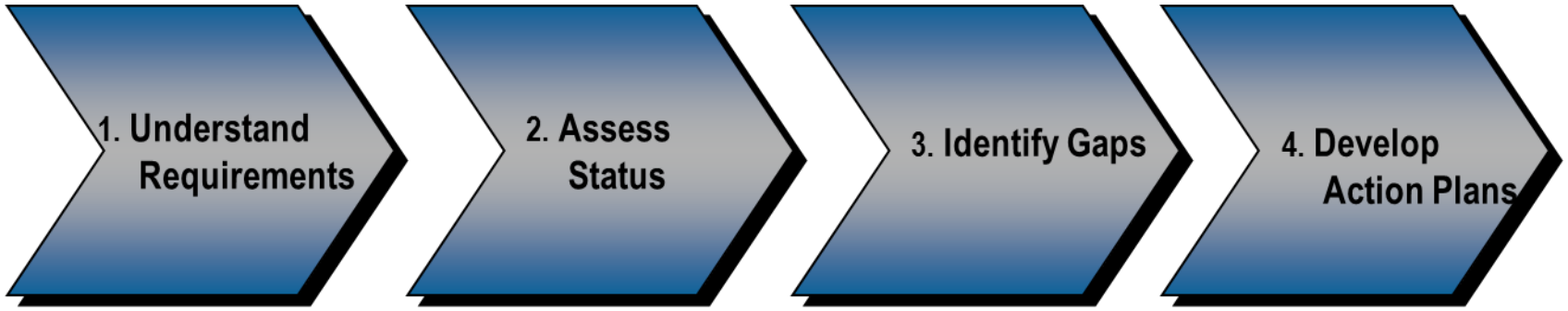
Corporate Governance Attributes

Attributes	Compliant	Developed	Advanced
Board of Directors & Committe	• Committees composed entirely of independent directors • Audit committee members may only receive director's fees as compensation	• Board meets in executive sessions without CEO and other insiders • Material portion of directors' pay is stock related	• Only non-independent director is CEO • Directors allowed to engage outside advisors at corporation's expense
Legal & Regulatory	• Minimal legal and regulatory requirements • Shareholders must be given the opportunity to vote on all equity-compensation plans	• Linkage of cost savings opportunities and compliance with new regulations	• Involvement in regulatory process to enhance governance requirements
Business Practices and Ethics	• Must adopt and disclose a code of business conduct and ethics • Disclose any change in or waiver of code of ethics for senior financial officer	• Annual review of code of conduct and ethics disclosed in annual report • Employee training concerning ethics, conflicts of interest and compliance standards required	• Status and action taken for each violation of the code of conduct and ethics published on company's web site • Board and senior mgmt visibly show strong support for ethical behavior
Disclosure and Transparency	• Minimum regulatory disclosures • Meet minimum GAAP requirements	• Periodic reports easily understood • Full disclosure or related parties and insider trading	• Reporting reflects business reality • Information timely, complete and easily accessible
Enterprise Risk Management	• Strategic planning and risk assessment are performed as separate activities with little integration • Internal audit involved in compliance role only	• Strategic planning incorporates the impact of each strategic alternative in light of the current and desired risk profile • Internal audit involved in review of risk policy, assessment and evaluation	• Strategic planning and enterprise risk management are fully integrated • Internal audit involved as a proactive, independent partner in monitoring enterprise achievement of all objectives.
Monitoring	• Internal audit reports are received, read and filed without appropriate follow-up	• Internal audit is an active partner with the board and senior management in areas of strategic importance	• Balanced scorecard of key metrics used to initiate action to move results within tolerable levels
Communication	• Website must include: corporate governance guidelines, charters of committees, and code of business conduct and ethics	• Key elements of corporate governance are embedded into new employee orientation and ongoing education and training programs	• Board approves press releases on all material matters, not just financial statement releases

Corporate Governance

- Sustainable governance requires all components.
- Let's look at three non-legal component, Disclosure and Transparency, Enterprise Risk Management and Business Practices and Ethics

Steps to Good Corporate Governance



- Understand the minimum requirements in each of the corporate governance categories
- Assess the organization's status by comparing current practices to minimum requirements
- Identify gaps between the organization's status and the minimum requirements and/or the desired state
- Develop action plans to address opportunities for improvement

Why Good Corporate Governance Makes Sense

Crowe Horwath Solution

- Educate the bank's Board and Senior Management on the attributes of good Corporate Governance
- Determine the bank's current Corporate Governance Score
- Assess the cost/benefit of moving the bank's score to the level that best fits the organizational needs
- Implement practical strategies to improve the bank's score to the desired level

COSO 2013 Internal Control Framework

Requirements for “Effective Internal Control”

- The Framework “does not” prescribe requirements of specific controls that must be selected, developed, and deployed for an effective system of internal control. That determination is a function of “management judgment” based on factors unique to each entity, such as:
  - Laws, rules, regulations, and standards to which the entity is subject
  - Nature of the entity’s business and the markets in which it operates
  - Scope and nature of the management operating model
  - Competency of the personnel responsible for internal control
  - The entity’s use and dependence on technology
  - Management’s response to assessed risks

Requirements for “Effective Internal Control” (continued)

- The phrase “present and functioning” is applied to components and principles:
  - “Present” refers to the determination that components and relevant principles exist in the design of the system of internal control.
  - “Functioning” refers to the determination that components and relevant principles continue to exist in the operation and conduct of the system of internal control.

- A component or relevant principle that is present and functioning implies that the organization:
  - Understands the intent of components and how relevant principles are being applied
  - Helps personnel understand and apply relevant principles across the entity
  - Views weakness in, or absence of a principle, as a situation that triggers management attention

Requirements for “Effective Internal Control” (continued)

- Senior Management and the Board of Directors must use judgment to assess whether each of the five components and relevant principles are present, functioning, and operating together in an integrated manner.

- When a component or relevant principle is deemed not present and functioning, or when components are deemed not operating in an integrated manner, a “major deficiency” exists. The PCAOB will need to determine if this classification will replace “significant deficiency” or “material weakness.”

- When a major deficiency exists, the entity cannot conclude that it has met the requirements for effective internal control.

COSO's Codification of Framework Principles

Control Environment	1. Demonstrates commitment to integrity and ethical values. 2. Exercises oversight responsibility. 3. Establishes structure, authority, and responsibility. 4. Demonstrates commitment to competence. 5. Enforces accountability.
Risk Assessment	6. Specifies suitable objectives. 7. Identifies and analyzes risk. 8. Assesses fraud risk. 9. Identifies and analyzes significant changes.
Control Activities	10. Selects and develops control activities. 11. Selects and develops general controls over technology. 12. Deploys through policies and procedures.
Information and Communication	13. Uses relevant information. 14. Communicates internally. 15. Communicates externally.
Monitoring Activities	16. Conducts ongoing and/or separate evaluations. 17. Evaluates and communicates deficiencies.

Note: Companies will need to link their internal controls to the 17 principles.

Principles and Attributes Related to the Control Environment Component

1. The organization demonstrates a commitment to integrity and ethical values.
   - Sets the tone at the top
   - Establishes standards of conduct
   - Evaluates adherence to standards of conduct
   - Addresses deviations in a timely manner

2. The board of directors demonstrates independence of management and exercises oversight for the development and performance of internal control.
   - Establishes board of directors oversight responsibilities
   - Retains or delegates oversight responsibilities
   - Operates independently
   - Provides oversight

3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
   - Considers all structures of the entity
   - Establishes reporting lines
   - Defines, assigns, and limits authorities and responsibilities

Principles and Attributes Related to the Control Environment Component (continued)

4. The organization demonstrates a commitment to attract, develop, and retain competent individuals.
   - Establishes policies, procedures, and practices
   - Evaluates competence and addresses shortcomings
   - Plans and prepares for succession

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
   - Enforces accountability through structures, authorities, and responsibilities
   - Establishes performance measures, incentives, and rewards
   - Evaluates performance measures, incentives, and rewards for ongoing relevance
   - Evaluates performance and rewards or disciplines individuals

Principles and Attributes Related to the Risk Assessment Component

6. The organization specifies with sufficient clarity to enable the identification and assessment of risks relating to objectives (the chart below depicts attributes applicable to each objective category).

	OPERATIONS	REPORTING			COMPLIANCE
		INTERNAL	EXTERNAL NON-FINANCIAL	EXTERNAL FINANCIAL	
a. Considers Tolerance for Risk/Required Level of Precision/Materiality	✓	✓	✓	✓	✓
b. Complies with Externally Established Standards and Frameworks/Complies with Applicable Accounting Standards/ Reflects External Laws and Regulations			✓	✓	✓
c. Reflects Management's Choices	✓	✓			
d. Reflects Entity Activities		✓	✓	✓	
e. Includes Operations and Financial Performance Goals	✓				
f. Forms Basis for Committing of Resources	✓				

Principles and Attributes Related to the Risk Assessment Component (continued)

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes its risks as a basis for determining how risks should be managed.
   - Involves appropriate levels of management
   - Includes entity, subsidiary, division, operating unit, and functional levels
   - Analyzes internal and external factors
   - Estimates significance of risks identified
   - Determines how to respond to risks

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
   - Considers the various ways that frauds can occur
   - Assesses incentives and pressures, opportunities, attitudes, and rationalizations

9. The organization identifies and analyzes changes that could significantly affect the system of internal control.
   - Analyzes changes in the external environment, changes in the business model, and changes in leadership

Principles and Attributes Related to the Control Activities Component

10. The organization selects and develops control activities that contribute to the mitigation of risks to acceptable levels.
    - Determines relevant business processes
    - Considers entity-specific factors
    - Evaluates a mix of control activities and types
    - Considers at what level activities are applied
    - Addresses segregation of duties

11. The organization selects and develops general control activities over technology to support the achievement of objectives.
    - Determines dependency between the use of technology in business processes and technology general controls
    - Establishes relevant technology infrastructure control activities
    - Establishes relevant security management control activities
    - Establishes relevant technology acquisition, development, and maintenance control activities

Principles and Attributes Related to the Control Activities Component (continued)

12. The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.
    - Establishes policies and procedures to support deployment of management directives
    - Establishes responsibility and accountability for executing policies and procedures
    - Performs procedures using competent personnel
    - Performs procedures in a timely manner
    - Takes corrective action
    - Reassess policies and procedures

Principles and Attributes Related to the Information and Communication Component

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal controls.
    - Identifies information requirements
    - Captures internal and external sources of data
    - Processes relevant data into information
    - Maintains quality throughout processing
    - Considers costs and benefits

14. The organization communicates information with internal parties, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
    - Communicates internal control information with personnel and the board of directors
    - Provides separate communication lines and selects relevant methods of communication

15. The organization communicates information with external parties about matters affecting the functioning of components of internal control.
    - Communicates to external parties and with the board of directors
    - Provides separate communication lines and selects relevant methods of communication

Principles and Attributes Related to the Monitoring Activities Component

16. The organization selects, develops, and performs ongoing and/or separate evaluations to determine whether the components of internal control are present and functioning.
    - Considers a mix of ongoing and separate evaluations
    - Establishes a baseline understanding
    - Considers the rate of change
    - Uses knowledgeable personnel
    - Integrates with business processes
    - Objectively evaluates
    - Adjusts scope and frequency

17. The organization evaluates and communicates internal control deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
    - Assesses results
    - Communicates deficiencies to management
    - Reports deficiencies to senior management and the board of directors
    - Monitors corrective actions

Audit Techniques and Strategies

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- The Board acts independently from management influence.
- The Board has sufficient information and meeting frequency to fulfill its fiduciary duties.

PROGRAM STEPS

- Obtain a listing of members of the Board of Directors. Determine if board minutes indicate the Board has concluded that a majority of directors are independent.
- Review Board and Board Committee minutes and packages from a sample of quarters to determine whether members receive detailed reports regarding significant issues (financial performance, fraudulent activities and related losses, employee misconduct, personnel, economic forecasts, regulatory requirements, committee issues, etc.).

- **COSO Principle #2**

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- The Board has sufficient information and meeting frequency to fulfill its fiduciary duties.
- Salary and benefits of executive officers are determined without collusion or inappropriate influence.

PROGRAM STEPS

- Review the Board meeting minutes from the current audit cycle and determine if meetings are being held at least quarterly.
- Through review of a listing of the Compensation Committee (or similar committee) members, determine whether it consists of Board members that are not also executive officers. Review minutes of the Compensation Committee (or similar committee) meetings for evidence to support that they have oversight in the compensation and employment of the executive officers.

- **COSO Principle #2**

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- The Audit Committee is sufficiently independent and competent in the financial matters of the institution.

PROGRAM STEPS

- Determine whether the Board of Directors has established an Audit Committee that meets the requirements of independence and financial literacy and that membership in the Audit Committee is evaluated and approved by the Board annually. Determine whether portions of the Audit Committee meetings are conducted with auditors without members of management present.

- **COSO Principle #2**

Corporate Governance- Board of Director and Audit Committee

ESSENTIAL CONTROL POINTS

- The Audit Committee is sufficiently independent and competent in the financial matters of the institution.

PROGRAM STEPS

- Determine the individual(s) on the Audit Committee that has been designated as a financial expert. Review the criteria used by the Board to determine the designation and determine if it considers whether the individual(s) has through education and experience as a public accountant, auditor, principal financial officer, controller, or principal accounting officer obtained the following:

  1) An understanding of generally accepted accounting principles and financial statements;
  2) Experience applying such generally accepted accounting principles in connection with the accounting for estimates, accruals, and reserves that are generally comparable to the estimates, accruals and reserves, if any, used in the institution's financial statements;
  3) Experience preparing or auditing financial statements that present accounting issues that are generally comparable to those raised by the institution's financial statements;
  4) Experience with internal controls and procedures for financial reporting; and
  5) An understanding of audit committee functions.

- **COSO Principle #2**

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- The Board has sufficient information and meeting frequency to fulfill its fiduciary duties.

PROGRAM STEPS

- Determine whether the Board of Directors or a committee therof reviews all related party transactions at least annually and that the Board or committee specifically reviews for the following:

  1) Transactions are being pursued in accordance with all understandings and commitments made at the time previously approved, and transactions are still desired;
  2) Newly proposed transactions are being reviewed;
  3) Proper documentation exists for all related transactions; and
  4) Insider transactions are proper.

- **COSO Principle #13, 14 and 15**

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- The Audit Committee's Charter is sufficient in scope and authority to allow the committee to fulfill its fiduciary duties.

PROGRAM STEPS

- Review the institution's Audit Committee Charter and determine that, at a minimum, it includes:

1) Details of the scope of the committee's responsibilities and how they are to be accomplished;
2) Requirement that the independent auditor is to be ultimately accountable to the Audit Committee and Board;
3) Requirement that the Audit Committee has the ultimate authority/responsibility to select, evaluate, and replace the independent auditor; and
4) Requirement that the Audit Committee is responsible for determining that the auditor submits a statement regarding relationships and services, which may affect independence.

- **COSO Principle #16 and 17**

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- The Audit Committee's Charter is sufficient in scope and authority to allow the committee to fulfill its fiduciary duties.

PROGRAM STEPS

- Through reviewing Audit Committee meeting minutes, determine that the Audit Committee has reviewed and assessed the adequacy of and compliance with the Audit Committee Charter.

- **COSO Principle #16 and 17**

Corporate Governance- Board of Directors and Audit Committee

ESSENTIAL CONTROL POINTS

- Instances of inappropriate activity on the part of the institution's management is brought to the attention of the Audit Committee and appropriate action taken.
- Executive management has established a whistleblower policy and hotline.

PROGRAM STEPS

- Observe evidence to support that the institution's Audit Committee has sufficient written procedures in place to receive, retain and treat internal and external complaints and handle whistleblower information regarding questionable accounting/auditing practices.
- Review reports of internal and external complaints and whistleblower potential violations (or a report indicating there were no reported complaints or potential violations) and test a sample of individual instances for investigation by competent management or Board members independent of the related problems.

- **COSO Principle #16 and 17**

Corporate Governance- Fraud Response Plan

ESSENTIAL CONTROL POINTS

- Management has implemented a fraud response plan that is used when suspected or known fraud incidents are detected.

PROGRAM STEPS

- Determine if a response plan has been devised to handle suspected or known fraud. Document the process and obtain the plan to determine if the following is considered:

  1) Commitment to the application of consistent and hard-line treatment of fraudsters;
  2) Who will lead the investigation;
  3) Roles played by internal resources (Human Resources and Internal Audit), Audit Committee, legal counsel, and external fraud specialist;
  4) How and when suspect(s) will be confronted;
  5) How evidence will be secured;
  6) When to involve law enforcement and/or regulatory agencies; and
  7) How to mitigate the effects of the fraud internally and externally.

- **COSO Principle #8**

Corporate Governance- Fraud Response Plan

ESSENTIAL CONTROL POINTS

- Management evaluates and adjusts, if necessary, the related internal controls and operational processes when fraudulent activity is detected.
- Management has established fraud training programs.

PROGRAM STEPS

- Determine the process in place to evaluate the relevant internal controls and operational processes that should be assessed and improved, if necessary, after a fraudulent activity is detected. Document the process and comment on whether the process in place is effective.
- Determine the type of communication and training that occurs after a fraud is detected to reinforce the institutions values, code of ethics, policies, and expectations. Document the process and comment on whether the process in place is effective.

- **COSO Principle #16 and 17**

Corporate Governance- Hiring and Promotion Practices

ESSENTIAL CONTROL POINTS

- Management defines and measures required competencies in key employee positions.

PROGRAM STEPS

- Discuss with management processes in place for defining and measuring required competence levels for members of senior management or key employees in positions of responsibility in the areas of finance and accounting. Document the process and determine whether there are clear definitions of competence requirements, and comment on whether the process is effective.

- **COSO Principle #3, 4 and 5**

Corporate Governance- Hiring and Promotion Practices

ESSENTIAL CONTROL POINTS

- The institution hires and promotes ethical and qualified people.

PROGRAM STEPS

- Determine the screening process for hiring or promoting members of senior management or key employees into positions of trust, such as the areas of finance, accounting, wire transfer, ACH, and information systems. Screening practices should include:

  a) background checks
  b) verification of references
  c) credit checks
  d) educational verifications
  e) employment history

- **COSO Principle #3, 4 and 5**

Corporate Governance- Hiring and Promotion Practices

ESSENTIAL CONTROL POINTS

- The institution hires and promotes ethical and qualified people.

PROGRAM STEPS

- Select a sample of members of senior management or key employees in positions of trust, such as the areas of finance, accounting, wire transfer, ACH, and information systems to determine that documentation exists for the following actions:

  a) background check
  b) verification of references
  c) credit checks
  d) educational verifications
  e) employment history

- **COSO Principle #3, 4 and 5**

Corporate Governance- Hiring and Promotion Practices

ESSENTIAL CONTROL POINTS

- Personnel are aware of issues (positive and negative) affecting their job performance

PROGRAM STEPS

- Discuss with management and document the process for personnel (regardless of organizational status) to receive periodic (at least annual) performance reviews and for the results to be documented. Determine if performance reviews incorporate an evaluation of how the individual has contributed to creating an appropriate workplace environment in line with the institutions values and code of conduct.
- Also, determine if "360-degree" personnel evaluations are utilized for key managers and review and document the process.
- Comment on whether the process is effective.
- **COSO Principle #3, 4 and 5**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management and other personnel follow established codes of conduct

PROGRAM STEPS

- Discuss whether the institution has a formal code of ethics (may be referred to as code of conduct) that reflects the core values of the entity and guides employees in an understandable fashion. Document the process for ensuring employees are aware of and have access to the most current version of the document and comment on the effectiveness of the process.

- **COSO Principle #1**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management and other personnel follow established codes of conduct

PROGRAM STEPS

- Select a sample of employees hired (to include members of senior management if possible) and determine that there is documentation that they have received the code of ethics

- **COSO Principle #1**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Compensation programs and financial incentives for employees encourage ethical behavior

PROGRAM STEPS

- Determine the compensation, promotion and recognition programs for management, and personnel in finance, information technology, lending, sales and marketing, and procurement. Document the process and comment on whether the programs are clearly communicated to employees and whether they are designed to encourage ethical behaviors. Determine the following:

1) If the program appears to suggest unrealistic performance targets (particularly for short-term results);
2) To what extent the compensation, promotion and recognition of senior management is based on achieving performance targets; and
3) Whether the program and performance targets have been reviewed by a committee comprised of independent Board members.

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Senior management responds promptly and effectively to events that may damage the institution’s reputation for integrity

PROGRAM STEPS

- Determine the process for senior management to respond to events that may damage the institution's reputation. Document the process and comment on whether written procedures exist within the code of ethics or in a separate document that clearly define the process for responding to such events. Comment on whether the process is effective.

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Senior management and employees in the accounting/finance function, as well as others in controls sensitive areas, periodically certify they are aware of and in compliance with the institution's code of conduct.

PROGRAM STEPS

- Select a sample of employees in control sensitive areas (including members of senior management and employees in the accounting/finance function) that have been with the institution for over one year to determine that they periodically certify (at least annually) that they are aware of and are in compliance with the institution's code of ethics.

- **COSO Principle #1**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management and other personnel follow established codes of conduct
- Senior management responds promptly and effectively to events that may damage the institution’s reputation for integrity

PROGRAM STEPS

- Review a sample of board minutes to determine whether the code of ethics is followed and enforced and for documentation of actions taken by senior management on events with potential to damage the institution's reputation.

- **COSO Principle #1**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management creates an environment in which employees believe that deviations from legal and ethical standards are not acceptable and that dishonest acts are not tolerated, and will be detected and punished.

PROGRAM STEPS

- Discuss with management steps taken to (1) create an environment in which employees believe that dishonest acts will be detected, are not tolerated, and punished and (2) communicate that deviations from legal and ethical standards are not accepted. Document the process and comment on whether the process in place is effective.

- **COSO Principle #5**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management and other personnel follow an established fraud policy.

PROGRAM STEPS

- Discuss with management whether the institution has a formal fraud policy (may be included as part of the code of ethics) that clarifies what the institution considers to be a fraudulent act, misconduct, and dishonesty; establishes an expectation for everyone working within and with the institution to behave honestly and with integrity; and provides consistent standards for dealing with improprieties.

- Document the process for ensuring that employees are aware of and have access to the most current version of the document and comment on the effectiveness of the process.

- **COSO Principle #8**

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management and other personnel follow an established conflict of interest policy.

PROGRAM STEPS

- Discuss with management whether the institution has a conflict of interest policy (may be included as part of the code of ethics) that addresses areas such as "self-dealing" (directing institution resources for personal gain), business relationships with customers and vendors (serving on boards, business ventures, etc), and acceptance of gifts and gratuities.

- Document the process for ensuring that employees are aware of and have access to the most current version of the document and comment on the effectiveness of the process.

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management has established a whistleblower policy and hotline.

PROGRAM STEPS

- Determine if a whistleblower policy and related hotline are in place and the process for communicating the presence to employees. Document the process for ensuring that employees are aware of and have access to the most current version of the document and comment on the effectiveness of the process. Determine if communications regarding the policy and hotline are initiated from the CEO in order to provide proper emphasis and importance.

Corporate Governance- Integrity and Ethical Values

ESSENTIAL CONTROL POINTS

- Executive management has established a whistleblower policy and hotline.
- Executive management and other personnel follow an established fraud policy.
- Executive management and other personnel follow an established conflict of interest policy.

PROGRAM STEPS

- Determine if vendors and customers are informed of whistleblower hotline and policy on gifts and gratuities. Document the process and comment on whether the process in place is effective.

- **COSO Principle #8**

Corporate Governance- Organizational Structure

ESSENTIAL CONTROL POINTS

- The organizational structure fits the institution's business objectives and strategies and its risk profile.

PROGRAM STEPS

- Through observation and review of Board of Directors meeting minutes determine the following:

  1) The Board of Directors assesses the appropriateness of the organizational structure in light of the nature and size of the institution, the complexity of its operations and the industry in which it operates; and

  2) The Organizational Chart defines the internal reporting structure for all line of business management.

- **COSO Principle #3, 4 and 5**

Corporate Governance- Organizational Structure

ESSENTIAL CONTROL POINTS

- Business continuity plans are established.

PROGRAM STEPS

- Determine that there is an adequate management succession plan established for all senior management positions and that the Board or a designated committee reviews the plan(s) at least annually.

- **COSO Principle #11**

Information and Communication- Communication

ESSENTIAL CONTROL POINTS

- Management communicates internal control and reporting responsibilities to employees effectively.
- Management communicates internal control and reporting responsibilities to employees effectively.

PROGRAM STEPS

- Discuss with management the process of communicating internal control and reporting responsibilities. Document the process and comment on whether the process is designed effectively.
- Test a sample of employee job descriptions from various business units to determine that internal control and reporting responsibilities are documented.

- **COSO Principle #14**

Information and Communication- Communication

ESSENTIAL CONTROL POINTS

- Processes exist to facilitate communication across the institution between people and functions that are critical to internal control and financial reporting.

PROGRAM STEPS

- Discuss with management the process of implementing new corporate initiatives. Specifically, discuss how these new initiatives are communicated to employees for adequate and timely changes. Comment on the effectiveness of the process.

- **COSO Principle #14**

Information and Communication- Communication

ESSENTIAL CONTROL POINTS

- Management responds promptly and effectively to communications received from regulators, customers, shareholders and other stakeholders.

PROGRAM STEPS

- Discuss with management the process of responding to feedback from key stakeholders. Obtain and review recent Board meeting minutes to determine that the Board is involved in any responses made to key stakeholders. Through review of the process obtain an understanding of who is authorized to communicate with external parties and determine that this is clearly defined. Comment on whether the processes in place are effective.

- **COSO Principle #15**

Information and Communication- Communication

ESSENTIAL CONTROL POINTS

- The institution's strategic plan and objectives are communicated to employees.
- Management has established fraud training programs.

PROGRAM STEPS

- Discuss with management the process for communicating the institution's strategic plan and entity level objectives to employees. Document the process and comment on whether the process is designed and operating effectively.
- Determine if fraud awareness training programs are in place and cover topics such as:
  1) Code of Ethics;
  2) Fraud Red Flags - at both a high level and specific to employees daily responsibilities; and
  3) Duty to communicate certain matters and examples of types of matters (actual or suspected fraud, misconduct, etc) and how to communicate these matters (whistleblower hotline)
- **COSO Principle #8 and #14**

Corporate Governance- Obtaining and Maintaining Relevant Information

ESSENTIAL CONTROL POINTS

- Institution senior management has adequate information about external business conditions and internal operations.
- Key managers and employees have adequate information to carry out their control and reporting responsibilities.

PROGRAM STEPS

- Discuss with senior management information they consistently obtain about external business conditions and internal operations. Document the types of information received, the frequency, and how it is used in decision making processes. Comment on whether the process is effective.
- Discuss with management the process of communicating information to key managers and employees so that they can carry out their control and reporting responsibilities. Document the process and comment on whether it is effective.

- **COSO Principle #15**

Monitoring- Budgeting and Analysis

ESSENTIAL CONTROL POINTS

- Future performance is adequately planned to ensure financial stability and viability.

PROGRAM STEPS

- Discuss with management how budgets are prepared and approved. Document the process and determine that the budget is approved at the appropriate level by obtaining a copy of the Board meeting minutes and determine that the budget was part of the discussion during the correct month. Document whether strategic and entity level objectives are considered as part of the budgeting process.

- **COSO Principle #6, #7, and #9**

Corporate Governance- Enterprise Wide Risk Assessment

ESSENTIAL CONTROL POINTS

- Risks are identified, understood and evaluated.

PROGRAM STEPS

- Determine how risk factors are identified. Document the process and comment on whether the process in operation is effective. Obtain a sample of Board meeting minutes and determine that risk assessments performed are being reviewed.

- **COSO Principle #6 and #7**

Risk Assessment- Enterprise Wide Risk Assessment

ESSENTIAL CONTROL POINTS

- Fraud risks are identified, understood and evaluated.

PROGRAM STEPS

- Determine how fraud risk factors are identified. Consider the following:

  1) Is a fraud risk assessment for institution and all related subsidiaries completed?
  2) What is management's role in assessing the institutions fraud risks?
  3) What is management's role in establishing and monitoring all aspects of the fraud risk assessment and prevention activities?

- Document the process and comment on whether the process in operation is effective. Obtain a sample of Board meeting minutes and determine that the fraud risk assessment performed is being reviewed.

- **COSO Principle #8**

Risk Assessment- Enterprise Wide Risk Assessment

ESSENTIAL CONTROL POINTS

- Fraud risks are identified, understood and evaluated.

PROGRAM STEPS

- Determine how the institution and related subsidiaries are structured/managed from an overall entity level to combat fraud. Consider how "tone at the top," institution-wide policies and procedures, and internal and external factors are considered. Document the process and comment on whether the process in operation is effective.

- Determine how the institution and related subsidiaries are structured/managed from specific business units to combat fraud. Document the process and comment on whether the process in operation is effective.

- **COSO Principle #8**

Risk Assessment- Enterprise Wide Risk Assessment

ESSENTIAL CONTROL POINTS

- Fraud risks are identified, understood and evaluated.

PROGRAM STEPS

- Determine how the institution and related subsidiaries are structured/managed from an overall entity level to combat fraud. Consider how "tone at the top," institution-wide policies and procedures, and internal and external factors are considered. Document the process and comment on whether the process in operation is effective.

- Determine how the institution and related subsidiaries are structured/managed from specific business units to combat fraud. Document the process and comment on whether the process in operation is effective.

- **COSO Principle #8**

Risk Assessment- Strategic Planning

ESSENTIAL CONTROL POINTS

- Risks are included in the strategic plan.
- The institution has a complete and timely strategic plan that ensures financial stability and viability.

PROGRAM STEPS

- Discuss with management the process of strategic planning and whether risks are included in the strategic planning process. Document the process and comment on whether it is effective.
- Obtain and review the current strategic plan to determine that the institution's objectives and plans are included and that risks are considered.

- **COSO Principle #7**

Model Risk Management

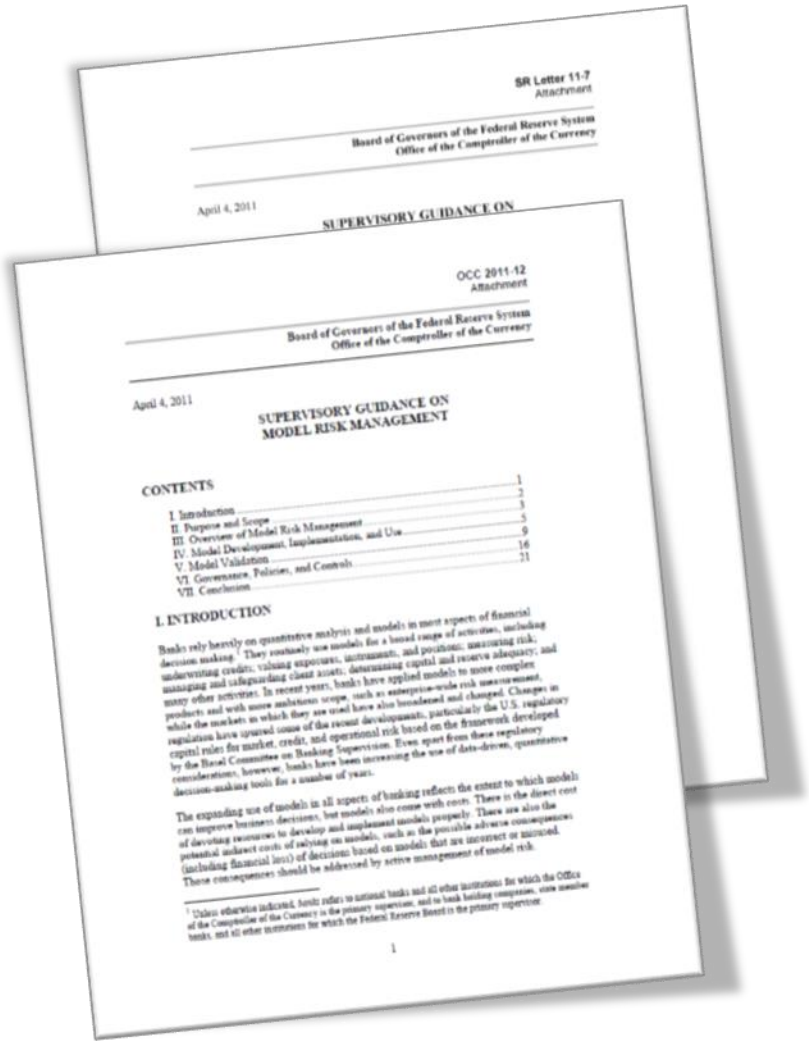
Agenda

- Overview of regulatory requirements
- Discussion of evolving expectations and industry perspectives
- Identification of the critical components of managing an effective model risk program
- Application of prescriptive approaches to model management

Regulatory Guidance on Model Risk Management

OCC and Federal Reserve published Supervisory Guidance on Model Risk Management in April of 2011 (OCC 2011-12, SR 11-7)

- The guidance articulates the elements of a sound program for effective management of risks that arise when using quantitative models in bank decision making.
- Models can improve business decisions, but they also impose costs, including the potential for adverse consequences from decisions based on models that are either incorrect or misused.
- The potential for poor business and strategic decisions, financial losses, or damage to a bank's reputation when models play a material role is the essence of "model risk."



SR Letter 11-7
Attachment

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency

April 4, 2011

SUPERVISORY GUIDANCE ON

OCC 2011-12
Attachment

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency

April 4, 2011

SUPERVISORY GUIDANCE ON
MODEL RISK MANAGEMENT

CONTENTS

I. INTRODUCTION

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making.[1] They routinely use models for a broad range of activities, including underwriting credit, valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement, while the markets in which they are used have also broadened and changed. Changes in regulation have spurred some of the recent developments, particularly the U.S. regulatory capital rules for market, credit, and operational risk based on the framework developed by the Basel Committee on Banking Supervision. Even apart from these regulatory considerations, however, banks have been increasing the use of data-driven, quantitative decision-making tools for a number of years.

The expanding use of models in all aspects of banking reflects the extent to which models can improve business decisions, but models also come with costs. There is the direct cost of devoting resources to develop and implement models properly. There are also the potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused. These consequences should be addressed by active management of model risk.

[1] Unless otherwise indicated, *banks* refers to national banks and all other institutions for which the Office of the Comptroller of the Currency is the primary supervisor, and to bank holding companies, state member banks, and all other institutions for which the Federal Reserve Board is the primary supervisor.

1

Guidance Mandates Three Primary Areas of Focus

Model Development, Implementation, and Use

- Design, theory, and logic of the model should be well documented and supported.
- Model methodologies and processing components should be explained in detail.
- Data integrity and testing are integral to model development and implementation.
- Model use must act as a productive source of feedback.

Model Validation

- Set of processes and activities intended to verify the model is performing as expected.
- It’s performed by independent staff with appropriate incentives, competence, and influence.
- All components, including input, processing, and reporting, are subject to validation.
- Validation activities should continue on an ongoing basis after a model goes into use.

Guidance Mandates Three Primary Areas of Focus (Continued)

Governance, Policies, and Controls

- Bank management should establish a strong model risk management framework.
- Formal policies and procedures should be documented to implement the framework.
- BUs generally are responsible for the model risk associated with their business strategies.
- Audit findings related to models should be documented and reported to the board.

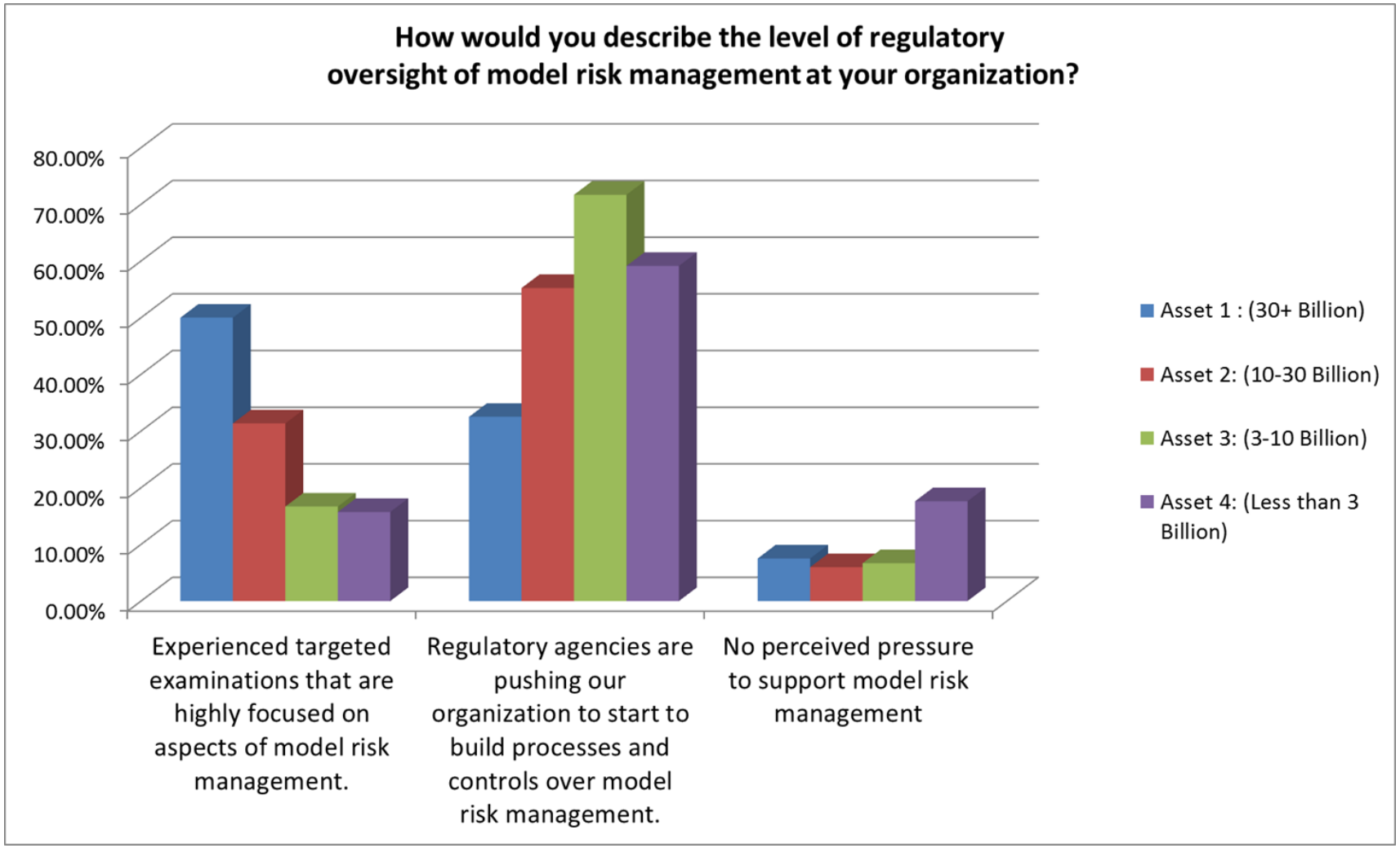
Typical Defined Models

- Allowance for loan losses: Impairment models, historical loss calculation models, migration models, probability of default models, loss given default models, qualitative factor models
- Mortgage servicing rights: Fair value estimation models
- Securities: Fair value estimation models
- Purchase accounting: Fair value models and cash flow estimation models
- Budgeting/forecasting models
- Loan stress-testing models
- Capital stress-testing models
- Loan pricing models
- Asset/liability and interest-rate risk management models
- Liquidity models and contingency funding models
- Fair Lending
- AML

Regulatory and Business Landscape

- Regulators' expectations for strong and effective model risk management programs continue to increase.
- Interpretation of Supervisory Guidance varies significantly.
- Regulatory agencies have shifted resources and attention to assessing how institutions manage models.
- Increased attention is being placed on operational models as opposed to only credit and financial models.
- There are fairly immature model risk management programs within large and small organizations.

Regulatory and Business Landscape



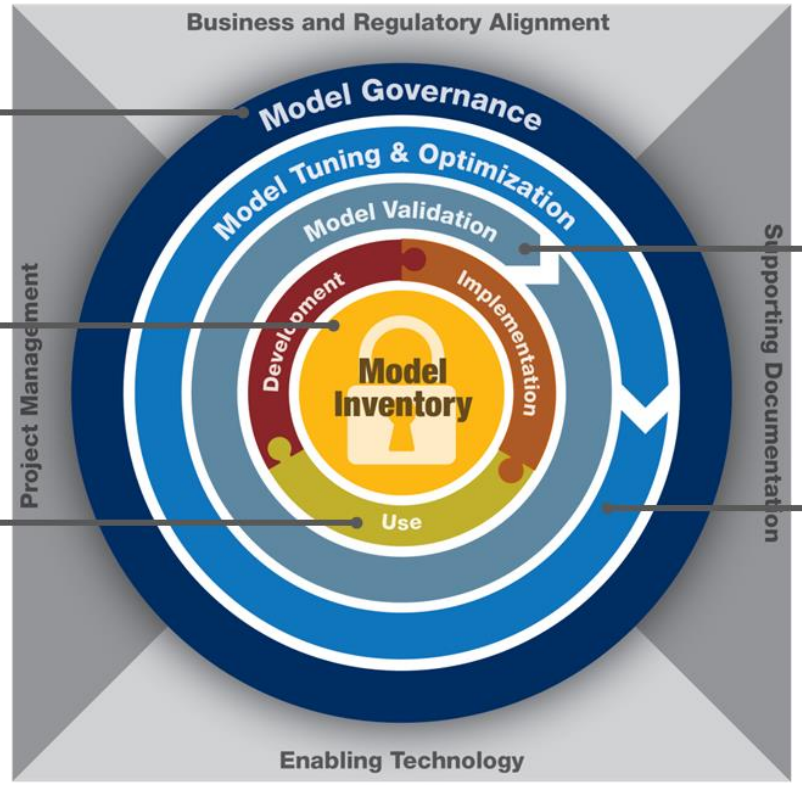
The Crowe Model Risk Management Framework

The rings of the Crowe Model Risk Management Framework capture the core requirements of the Supervisory Guidance and expand on key principals.

Prevailing internal controls are required to govern the model life cycle with the bank's board of directors providing oversight.

Model inventory provides a central repository to store all the information related to various models.

Model requirements, design, implementation plan, business purpose, and use need to be clearly documented and executed according to sound practices.

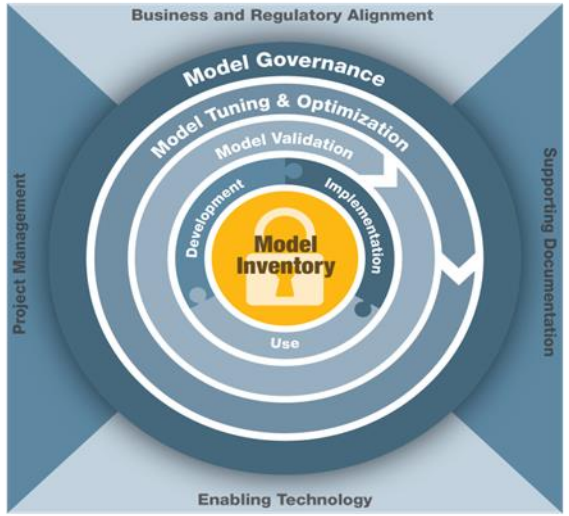


Model validation is essential to verify the accuracy and effectiveness against a standard model or any available benchmarks.

A prescriptive model tuning methodology and model analysis are necessary to optimize the overall efficiency of the models.

Model Inventory

- Three Principal Elements to Model Inventory
  - Enterprise identification
    - Establish definition of a model
    - Purpose and products
    - Policies, procedures, reports, control, and systems
    - Inputs and outputs and intended use
  - Accountability
    - Process/system ownership
    - Internal controls
    - Model compliance
  - Risk assessment
    - Perform a risk assessment of the model.
    - Establish criteria of factors to assist with arriving at a risk rating.
    - Validate risk assessment through testing.



Model Inventory

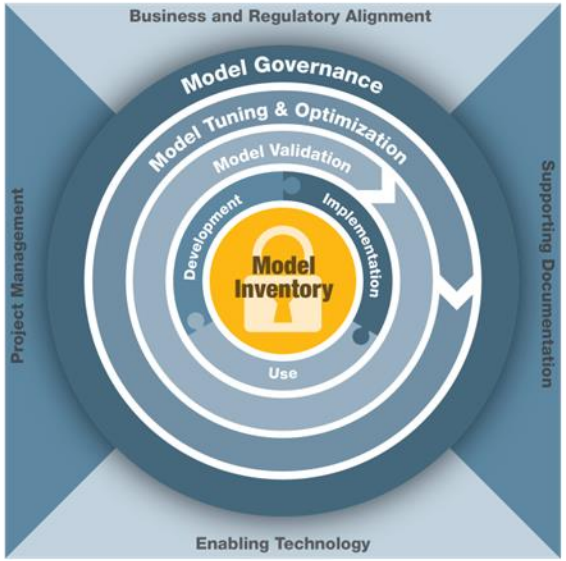
- What Constitutes a Model?

  Guidance definition:

  - The term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.
  - Models are simplified representations of real-world relationships among observed characteristics, values, and events.

  Three components to a model:

  - *Information input component*: delivers assumptions and data to the model
  - *Processing component*: transforms inputs into estimates
  - *Reporting component*: translates estimates into useful business information



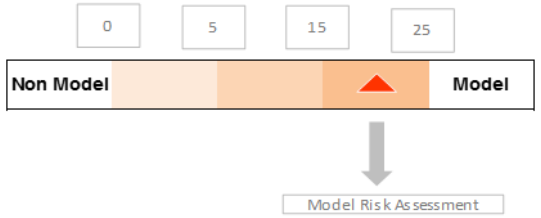
Model Inventory

Scenario 1

Decision Matrix

Prospective Model: Asset Liability Management (Interest Rate Risk)

		Response		
		Yes	No	Score
Question 1	Is it used to calculate or process various inputs transforming them into estimates to assess the potential impact to key strategic factors including but not limited to capital, net interest income, allowance for loan losses, etc.?	✓		5
Question 2	Are there assumptions or key data inputs (prepayment speed, decay rates) used to process data into quantitative estimates?	✓		5
Question 3	Does it assist management in the decision making process, i.e. pricing, asset strategies, liability strategies?	✓		5
Question 4	Does it produce output or results that materially impact other systems or applications?		✓	0
Question 5	Its is vendor support where unknown variables, estimates, or caculations are used?	✓		5
			Total	**20**

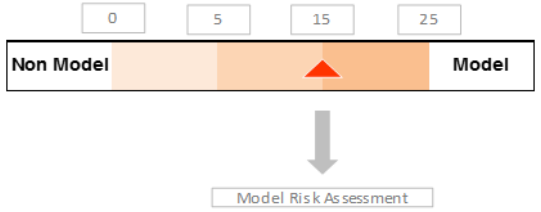


Scenario 2

Decision Matrix

Prospective Model: AML Transaction Monitoring System

		Response		
		Yes	No	Score
Question 1	Is it used to calculate or process various inputs transforming them into estimates to assess the potential impact to key strategic factors including but not limited to capital, net interest income, allowance for loan losses, etc.?		✓	0
Question 1 (a)	Is it used to for calculating or estimating the potential impact to key strategic factors including but not limited to capital, net interest income, allowance for loan losses, etc.?		✓	0
Question 2	Are there assumptions or key data inputs (prepayment speed, decay rates) used to process data into quantitative estimates?		✓	0
Question 2 (a)	Are the assumptions or key inputs (prepayment speed, decay rates) used to calculate or factored into results?	✓		3
Question 3	Does it assist management in the decision making process, i.e. pricing, asset strategies, liability strategies?		✓	0
Question 3 (a)	Is it used to materiallly comply with laws and implementing regulations?	✓		5
Question 4	Does it produce output or results that materially impact other systems or applications?		✓	0
Question 5	Its is vendor support where unknown variables, estimates, or caculations are used?	✓		5
			Total	**15**



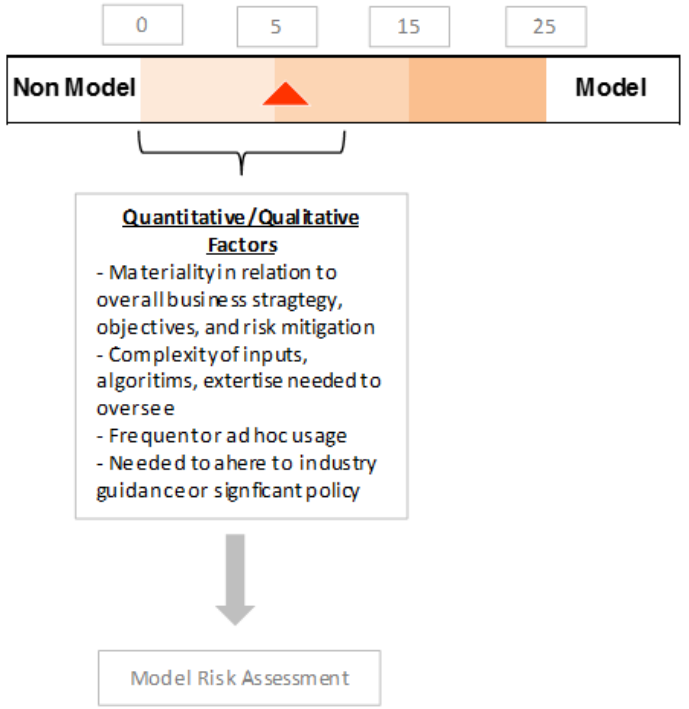
Model Inventory

Scenario 3

Decision Matrix

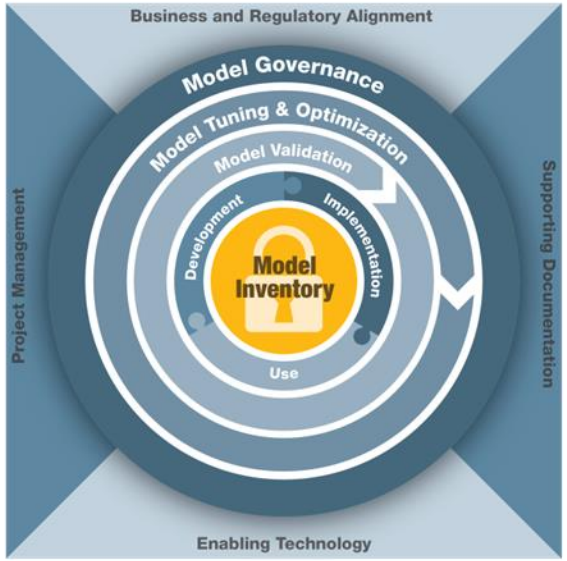
Prospective Model: Internal Cost Budgeting Model

		Response		
		Yes	No	Score
Question 1	Is it used to calculate or process various inputs transforming them into estimates to assess the potential impact to key strategic factors including but not limited to capital, net interest income, allowance for loan losses, etc.?		✓	0
Question 1 (a)	Is it used to for calculating or estimating the potential impact to key strategic factors including but not limited to capital, net interest income, allowance for loan losses, etc.?		✓	0
Question 2	Are there assumptions or key data inputs (prepayment speed, decay rates) used to process data into quantitative estimates?		✓	0
Question 2 (a)	Are the assumptions or key inputs (prepayment speed, decay rates) used to calculate or factored into results?	✓		3
Question 3	Does it assist management in the decision making process, i.e. pricing, asset strategies, liability strategies?	✓		3
Question 3 (a)	Is it used to materiallly comply with laws and implementing regulations?		✓	0
Question 4	Does it produce output or results that materially impact other systems or applications?		✓	0
Question 5	Its is vendor support where unknown variables, estimates, or caculations are used?		✓	0
			Total	**6**

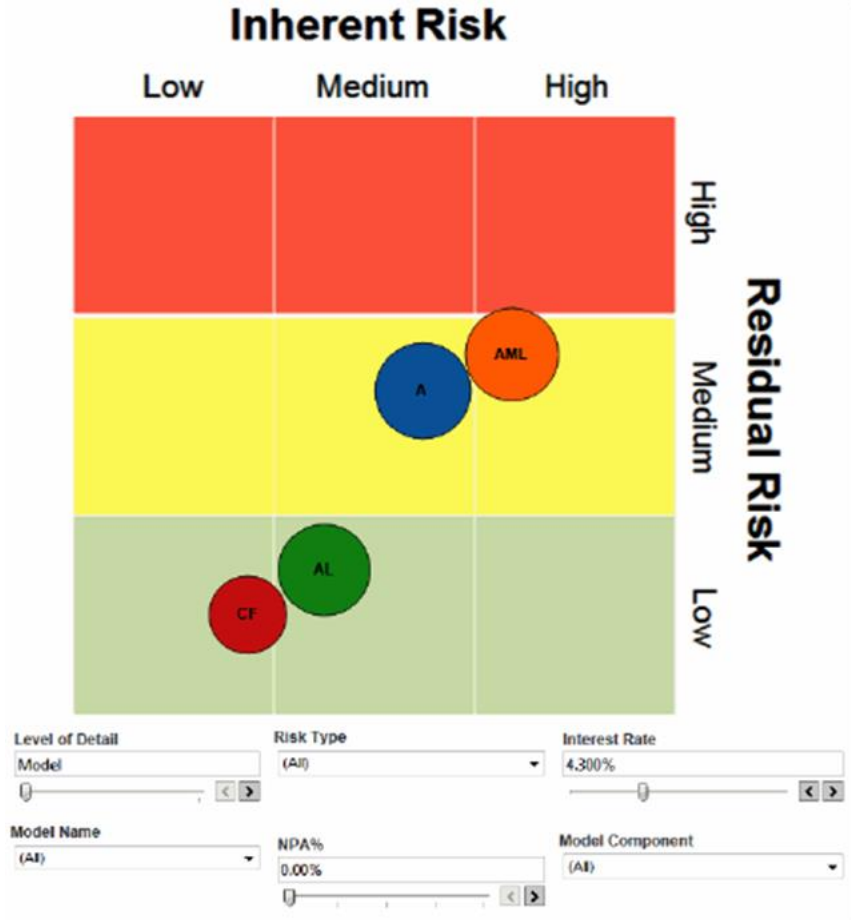


Model Inventory

- Model Risk Assessments
  - For each model, identify individual risk descriptions, for example, “What could go wrong?”
  - Categorize the risk description by risk type.
    - Compliance, operational, credit
  - Evaluate individual risks from the perspective of impact and likelihood and conclude on overall inherent risk.
    - Establish definitions or guidelines to assist in the rating of individual risks: Low, moderate, high
  - Evaluate controls that would mitigate the potential impact and likelihood of a risk event occurring.
    - Assess the controls’ mitigation effectiveness.
      - Inadequate, needs improvement, adequate, strong
  - Assess overall residual risk.

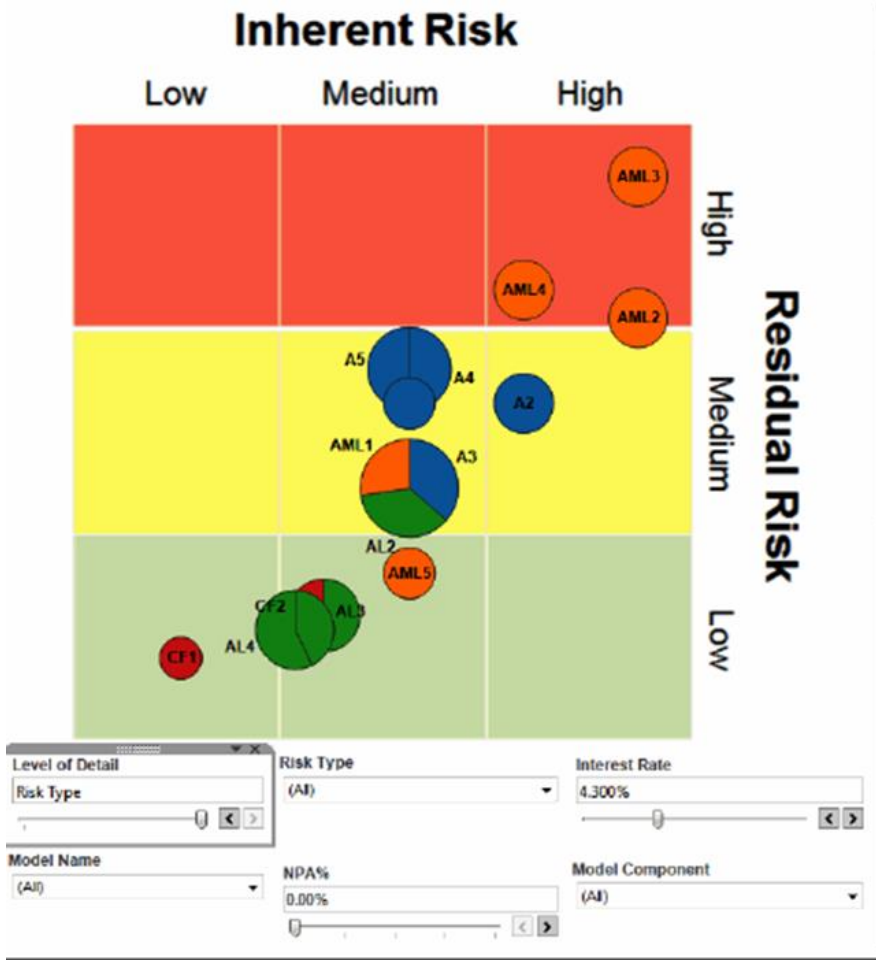


Model Inventory



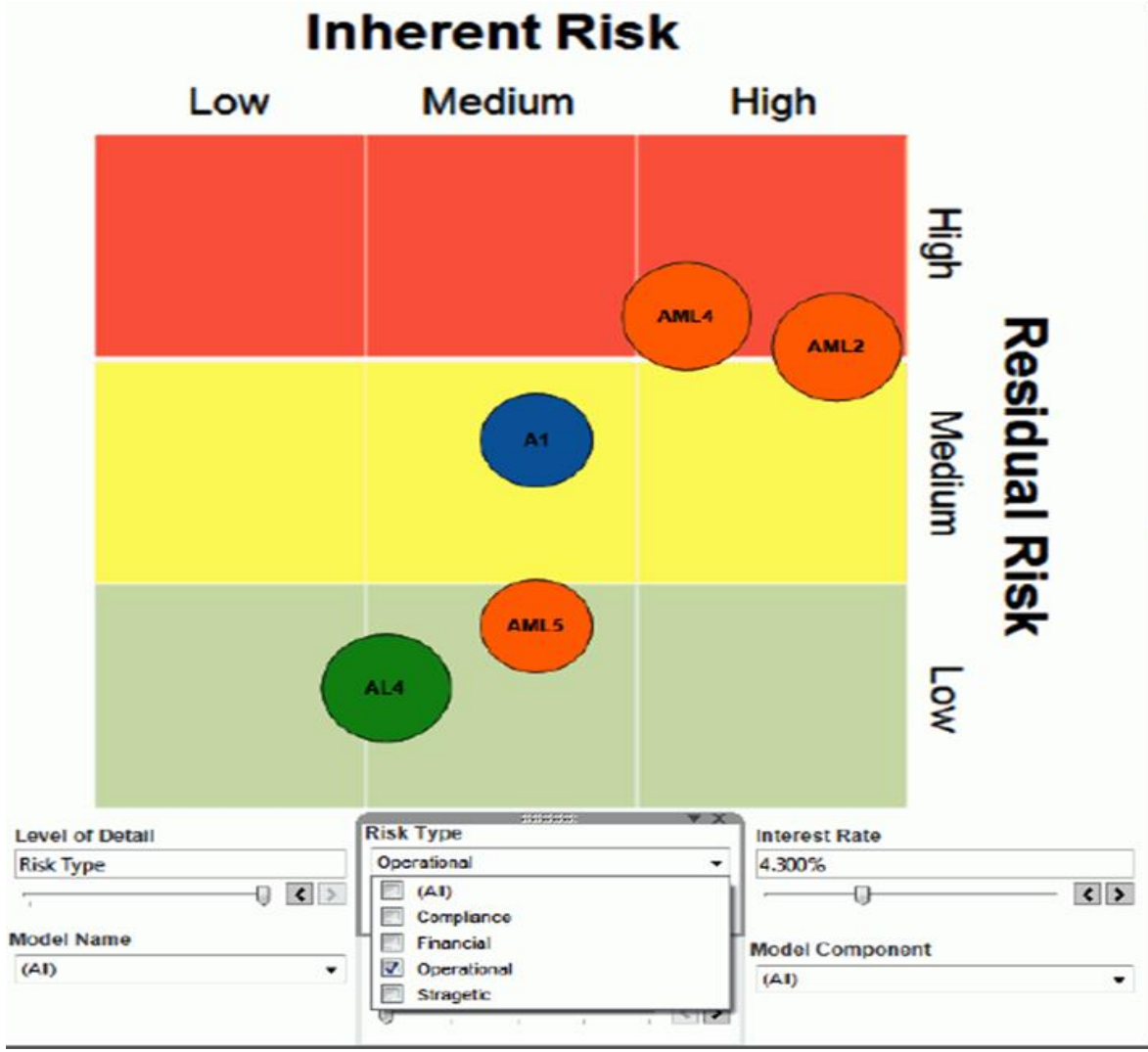
Model Name	Risk#	Risk Description	Impact	Likelihood	Inherent Risk	Control	Mitigation Effectivness	Residual Risk
Allowance	A1	Written procedures have not been established outlining the various steps for obtaining and running the model on a quarterly basis	Moderate	Remote	12	Procedures have not yet been formalized capturing the use of the model.	Needs Improvement	12
	A2	The allowance for loan loss calculation may be inaccurate and loans may not be evaluated for impairment resulting in inaccurate presentation and disclosure	Significant	Likley	16	The model data important reconciliation to the core loan system is performed by the Loan Administrator administrator and approved by the VP of Credit.	Adequate	12
	A3	Significant quantity of variables, segments, equations, and lines of code utilized	Significant	Moderate	12	Variables and the various inputs to the model are evaluated as to reasonables by the Credit Committee. Further, inputs to the model are validated for accuracy by an individual independent of the input.	Adequate	9
	A4	Incomplete inputs to the model may result in reporting that is inaccurate which may mask potential loan impairment issues.	Significant	Moderate	12	Management has not yet designed a control to validate data from the core processing system has been uploaded accurately.	Inadequate	13.2
	A5	Inputs to the model for calculating the general reserve are not verified by a second individual and as a result errors may not be caught which may impact the overall Allowance.	Significant	Moderate	12	Management has not yet designed a control to validate data from the core processing system has been uploaded accurately.	Inadequate	13.2
Anti Money Laundering	AML1	Output from model is not reviewed within appropriate timeframe to respond to regulatory prescribed timeframes	Moderate	Likley	12	5 FTEs are tasked with monitoring output from the model on a daily basis. Output is monitored daily and subject to quality assurance processes.	Adequate	9
	AML2	Data Mapping and Integregation Errors	Significant	Almost Certain	20	Data mapping and integeration was subject to rigorous independent validation. Ongoing processes administered to balance soruce data to system	Adequate	15
	AML3	Model inappropriatley configured to identify trends and patterns in money laundering	Significant	Almost Certain	20	Model settings were configured upon the inception of the model but have are not subject to regulator review or modification.	Needs Improvement	20
	AML4	Sensitive data maintained within the model is accessible to unathorized parties	Significant	Likley	16	User permissions were established upon implementation of system but have not since been reviewed.	Needs Improvement	16
	AML5	Modifications are applied to model without appopriate level of review and approval	Moderate	Likley	12	Change management policies and procedures limit modifications to one administrator who does not maintain day to day AML	Strong	6

Model Inventory



Model Name	Risk#	Risk Description	Impact	Likelihood	Inherent Risk	Control	Mitigation Effectivness	Residual Risk
Allowance	A1	Written procedures have not been established outlining the various steps for obtaining and running the model on a quarterly basis	Moderate	Remote	12	Procedures have not yet been formalized capturing the use of the model.	Needs Improvement	12
	A2	The allowance for loan loss calculation may be inaccurate and loans may not be evaluated for impairment resulting in inaccurate presentation and disclosure	Significant	Likley	16	The model data important reconciliation to the core loan system is performed by the Loan Administrastr administrator and approved by the VP of Credit.	Adequate	12
	A3	Significant quantity of variables, segments, equations, and lines of code utilized	Significant	Moderate	12	Variables and the various inputs to the model are evaluated as to reasonables by the Credit Committee. Further, inputs to the model are validated for accuracy by an individual independent of the input.	Adequate	9
	A4	Incomplete inputs to the model may result in reporting that is inaccurate which may mask potential loan impairment issues.	Significant	Moderate	12	Management has not yet designed a control to validate data from the core processing system has been uploaded accurately.	Inadequate	13.2
	A5	Inputs to the model for calculating the general reserve are not verified by a second individual and as a result errors may not be caught which may impact the overall Allowance.	Significant	Moderate	12	Management has not yet designed a control to validate data from the core processing system has been uploaded accurately.	Inadequate	13.2
Anti Money Laundering	AML1	Output from model is not reviewed within appropriate timeframe to respond to regulatory prescribed timeframes	Moderate	Likley	12	5 FTEs are tasked with monitoring output from the model on a daily basis. Output is monitored daily and subject to quality assurance processes.	Adequate	9
	AML2	Data Mapping and Integregation Errors	Significant	Almost Certain	20	Data mapping and integeration was subject to rigorous independent validation. Ongoing processes administered to balance soruce data to system.	Adequate	15
	AML3	Model inappropriatley configured to identify trends and patterns in money laundering	Significant	Almost Certain	20	Model settings were configured upon the inception of the model but have are not subjec to regulator review or modification.	Needs Improvement	20
	AML4	Sensitive data maintained within the model is accessible to unathorized parties	Significant	Likley	16	User permissions were established upon implementaiton of system but have not since been reviewed.	Needs Improvement	16
	AML5	Modifications are applied to model without appopriate level of review and approval	Moderate	Likley	12	Change management policies and procedures limit modifications to one administrator who does not maintain day to day AML	Strong	6

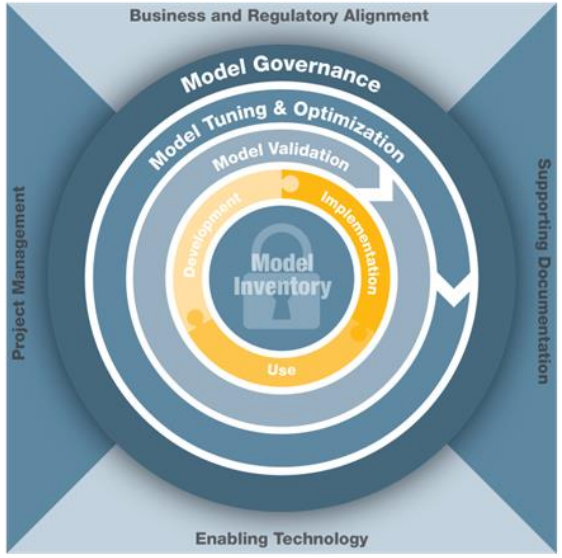
Model Inventory



Model Name	Risk#	Risk Description
Allowance	A1	Written procedures have not been established outlining the various steps for obtaining and running the model on a quarterly basis
Anti Money Laundering	AML2	Data Mapping and Integregation Errors
	AML4	Sensitive data maintained within the model is accessible to unathorized parties
	AML5	Modifications are applied to model without appopriate level of review and approval
Asset Liability	AL4	ALCO and the Board of Directors may not be provided the management information reports required to monitor interest rate risk and liquidity risk in a timely manner or the reports may be prepared by an individual with insuffic..

Model Development, Implementation, and Use

- **Model Development and Implementation**
  - **Model definition and requirements** contain well- documented requirements, theory, and logic of the model supported by published research and sound industry practices.
  - **Model design** is primarily driven by the model business requirements and specifications.
  - **Data management** includes data extraction, data massaging, data standardization, and application of the model along with transformations and calculations.
- **Model Use**
  - The process for **analyzing results** needs to be well- defined and documented.
  - **Continuous feedback** and improvement are established to confirm that the model is performing as expected as well as to identify opportunities for optimization and improvement.

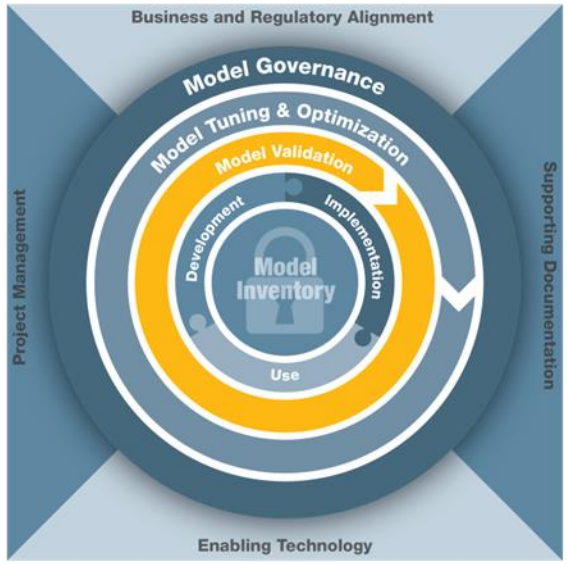


Model Development, Implementation, and Use

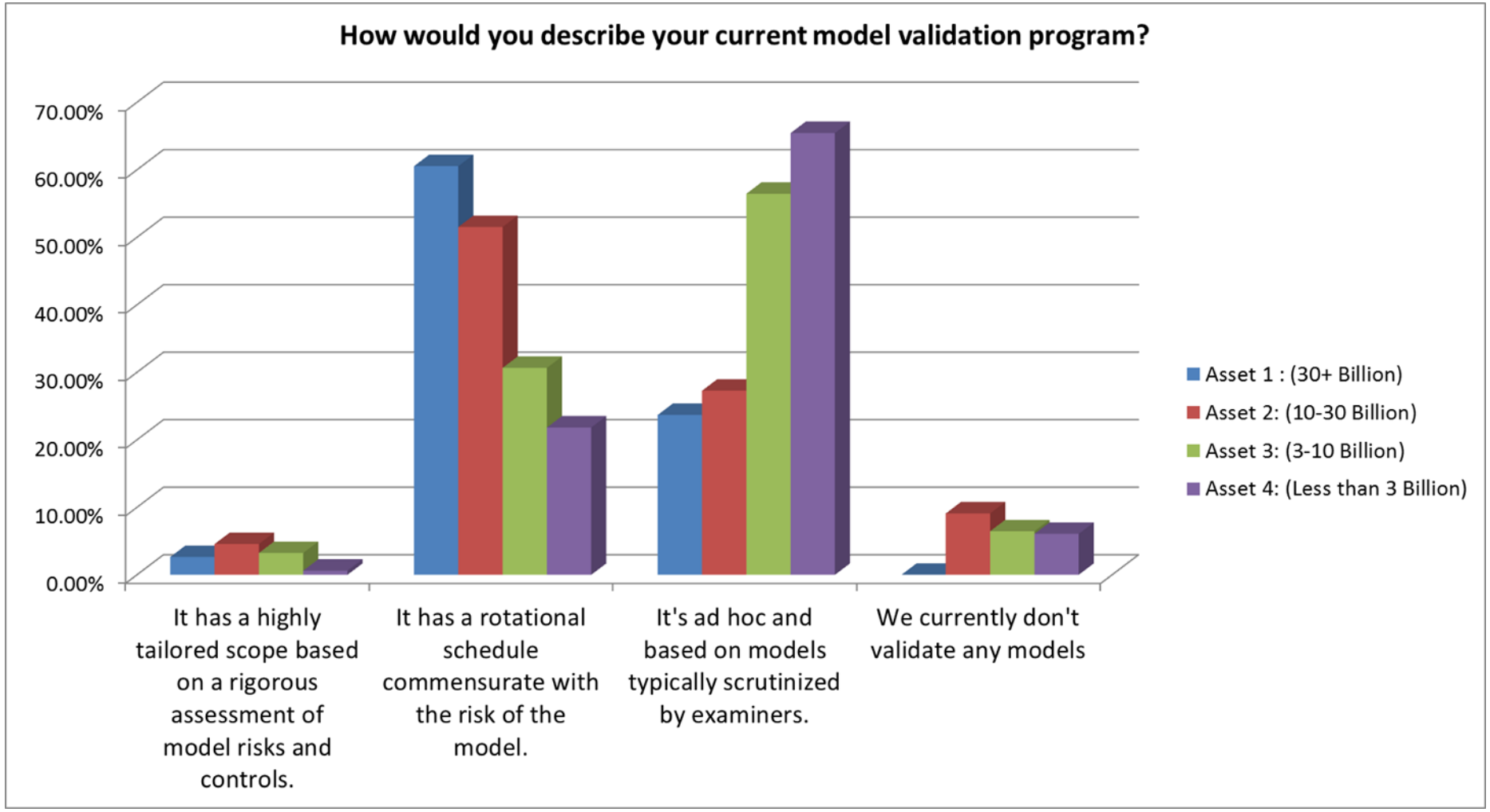
- Consider documentation that would enable an experienced modeler to recreate results.
- Summarize data integration and mapping with particular focus on data fields and any exclusions which may have been applied.
- Define the organization's documentation standards for legacy models.
- Assess the need to support summary- and executive-level documentation supporting model development and implementation.
- Consider how documentation will be updated and retained throughout the life cycle of a model.
- Solicit and retain documentation related to vendor-supported models.
- Formalize means to solicit model feedback.

Model Validation

- **Evaluation of conceptual design:** Evaluating the conceptual design and capabilities of the pertinent business processes
- **System validation:** Validating that the systems are properly designed to execute on the model
- **Data validation:** Validating that accurate and complete information is captured by a system to execute models
- **Process validation:** Assessing the adequate design and ongoing sustainability surrounding the processes and administration of the system and model



Model Validation



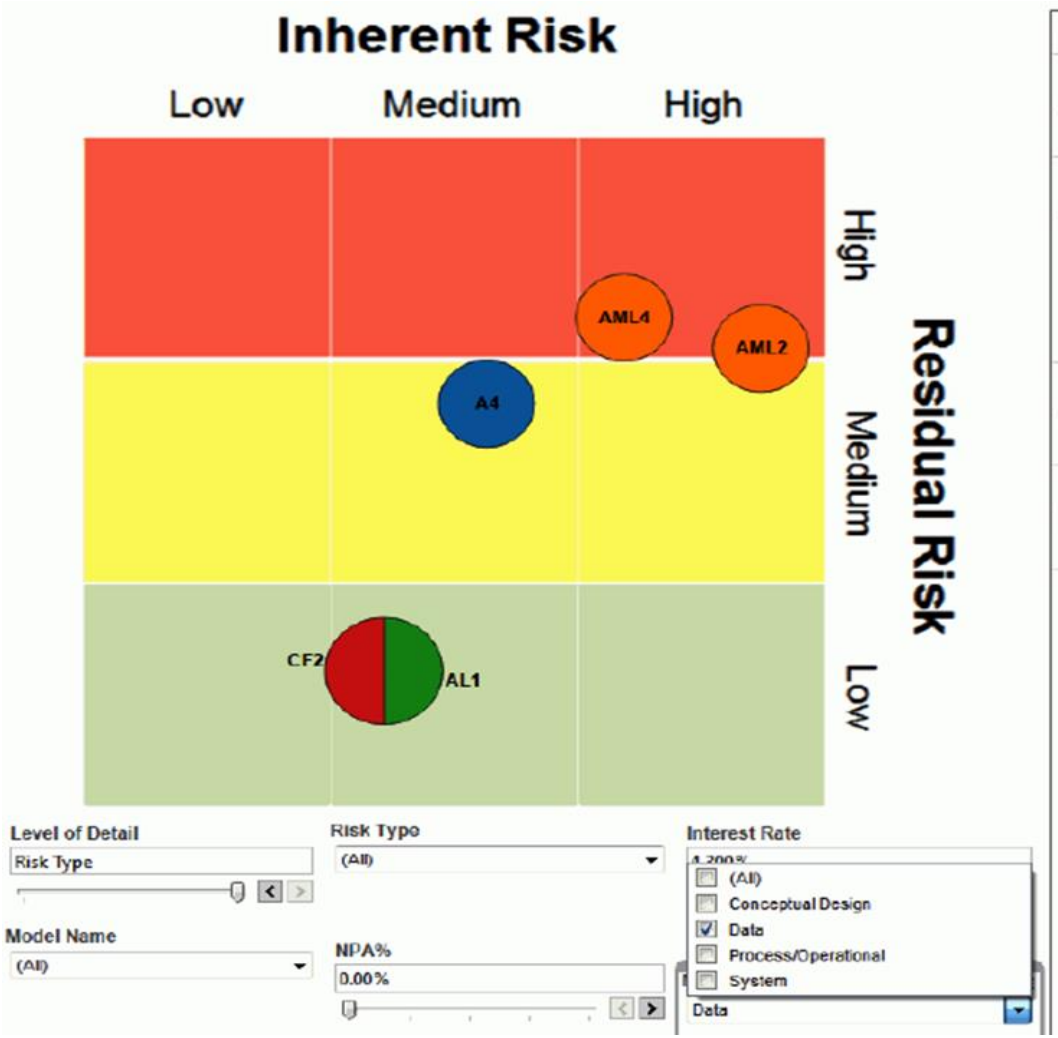
Model Validation- A Risk-Based Approach

	Conceptual Design	System Validation	Data Validation	Process Validation
High	▪ Challenge rationalization of the model theory ▪ Test validity of assumptions	▪ Verify key assumptions through stress testing and independent back testing	▪ Test input sensitivity ▪ Test completeness or recreate results	▪ Rigorously test model output, management decisioning, change control
Moderate	▪ Assess appropriateness of model assumptions, including consistency with market practices	▪ Challenge model owner tuning and optimization processes	▪ Sample field mapping of core systems and models	▪ Challenge and test operational effectiveness of established model procedures
Low	▪ Assess controls and processes governing model development and secondary review	▪ Assess vendor assurance reports	▪ Assess balancing controls and processes	▪ Evaluate design effectiveness of established model procedures

Frequency

Events

Model Validation



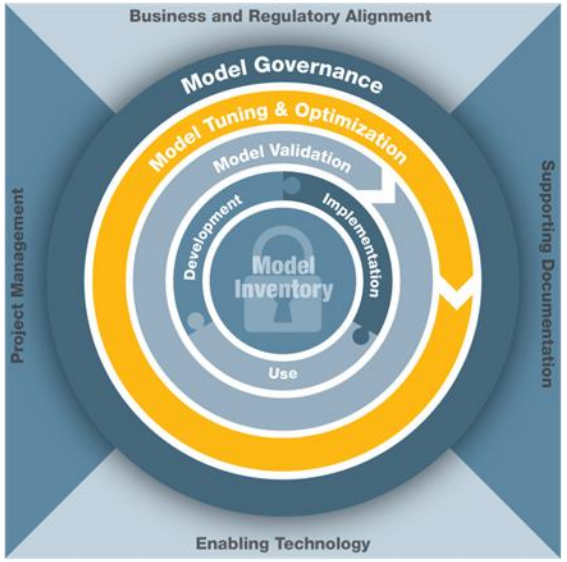
Model Name	Risk#	Risk Description	Impact
Allowance	A4	Incomplete Inputs to the model may result in reporting that is inaccurate which may mask potential loan impairment issues.	Signficant
Anti Money Laundering	AML2	Data Mapping and Integregation Errors	Signficant
	AML4	Sensitive data maintained within the model is accessible to unathorized parties	Signficant
Asset Liability	AL1	Incomplete Inputs to the model may result in reporting that is inaccurate which may mask potential interest rate risk.	Moderate
Contingency Funding	CF2	Incomplete Inputs to the model may result in reporting that is inaccurate which may mask potential funding needs in certain scenarios.	Moderate

Model Validation Perspectives and Strategies

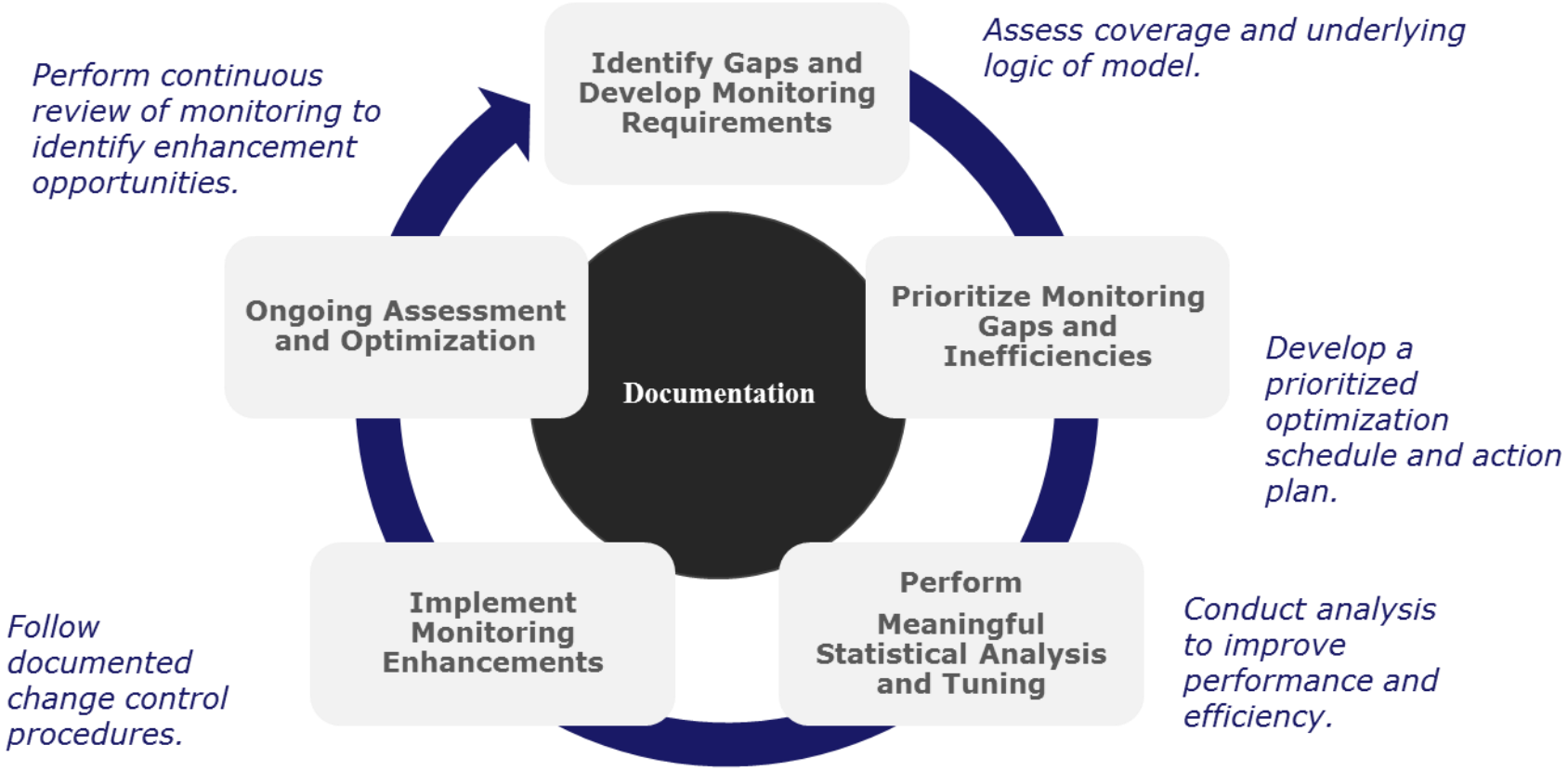
- Define model validation standards, documentation standards, and required elements of reporting and supporting documentation.
- Determine methods and criteria when assessing model results and model limitations.
- Actively track model limitations/gaps and related remediation efforts.
- Incorporate model limitations and gaps to the model risk assessment process.
- Determine how model limitations and gaps are reported and to whom they will be reported.
- Assess your internal capabilities to effectively execute model validation activities.

Model Tuning and Optimization

- **Gap analysis:** To identify areas within the organization that currently do not have the necessary coverage required for risk mitigation
- **Prescriptive methodology:** To verify that a consistent methodology is followed across the organization and a documented approach and meaningful analysis, including statistical analysis, are conducted on an ongoing basis
- **Documentary evidence:** To confirm that the developmental evidence as well as other components are thoroughly documented throughout the life cycle of the process



Model Tuning and Optimization

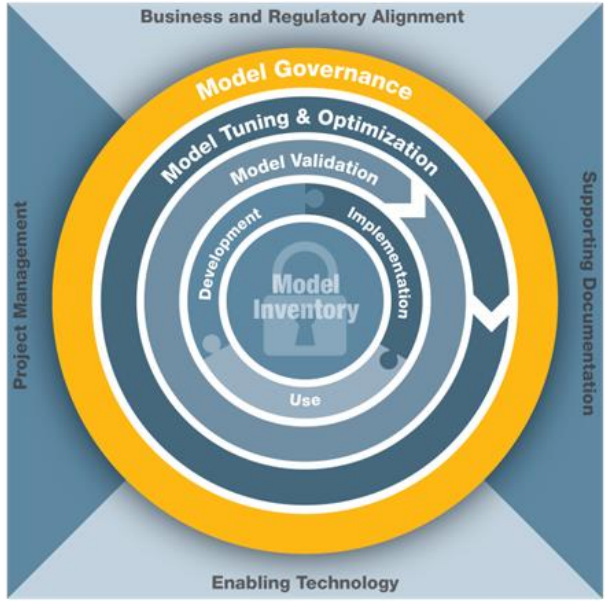


Model Tuning and Optimization Perspectives and Strategies

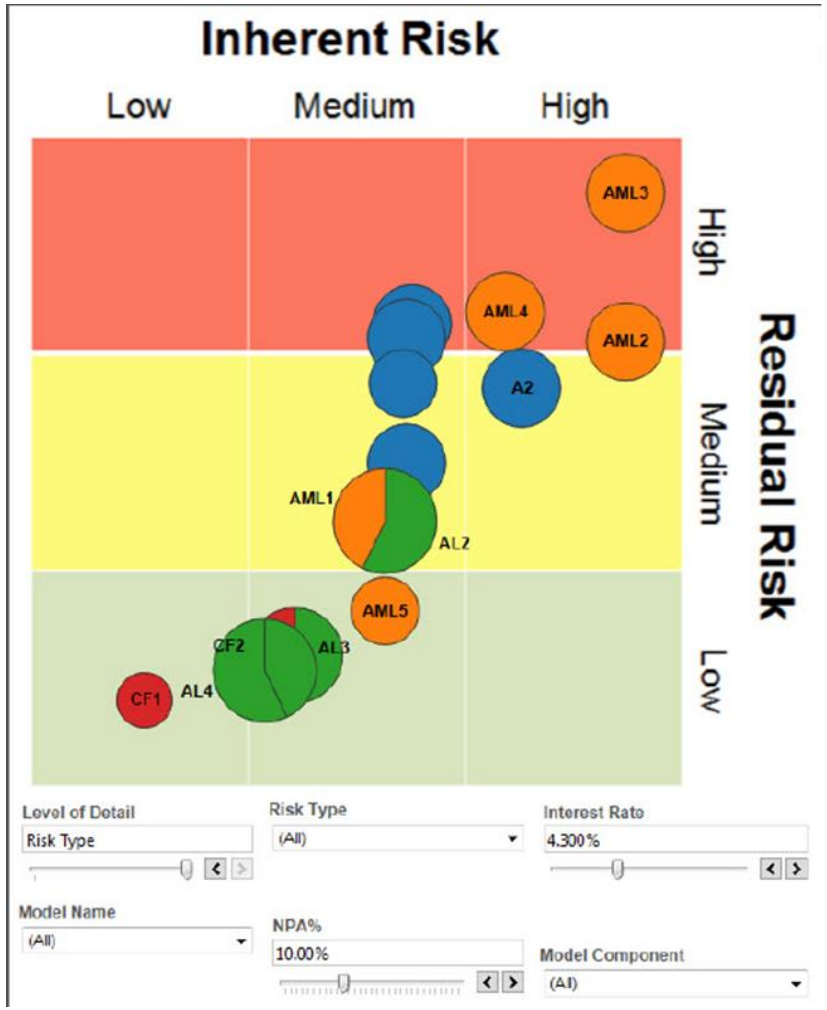
- Effective and perspective tuning and optimization processes and strategies limit scope and effort of model validation and reduce model risk.
- Deploy tuning and optimization methodologies that are statistically valid and limit adjustments based on “rules of thumb.”
- Oversee strong change control documentation that provides reasonable documentation supporting the rationale for change and allows for the appropriate segregation of duties.
- Consider the application of event-based tuning and optimization that actively monitors events and risks that impact a model’s performance.

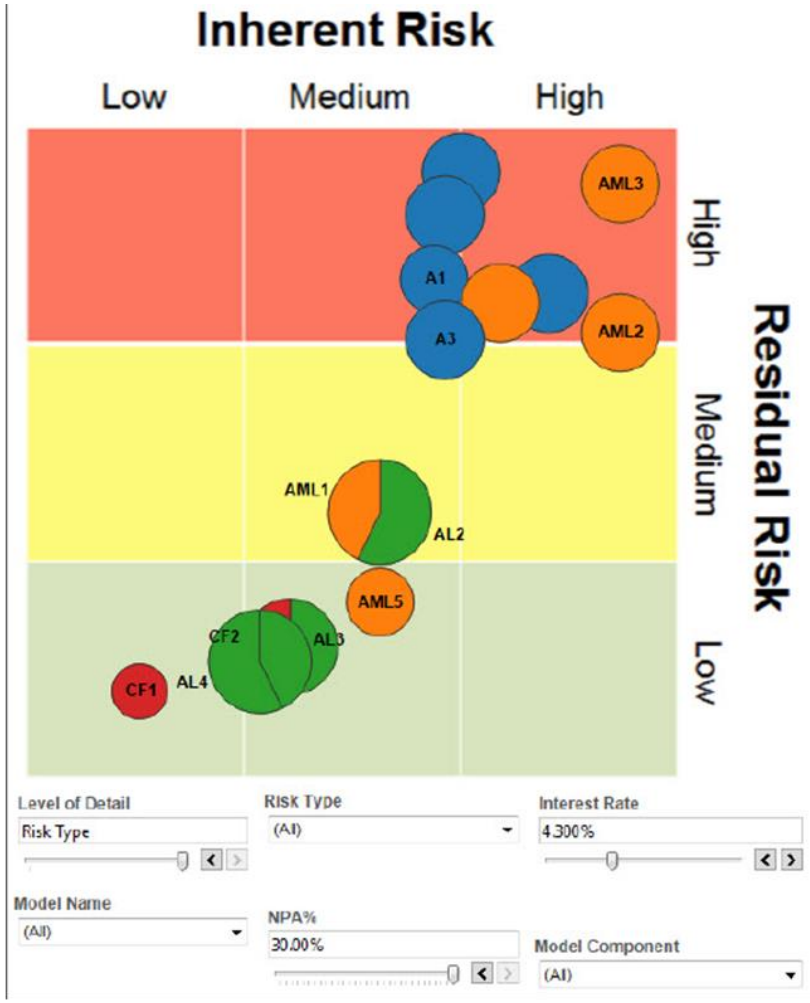
Model Governance

- Five Key Elements to Model Governance
  - Senior management and board involvement
  - Policies and procedures
  - Roles and responsibilities
  - Enterprisewide risk management
  - Independent audit and testing



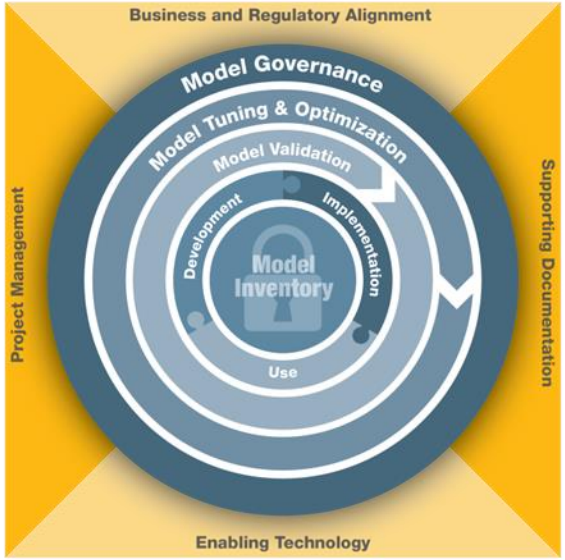
Model Governance





Model Foundation

- **Enabling technology:** Appropriate technology and systems need to be leveraged to support various models and the model risk management process.
- **Business and regulatory alignment:** Each model must have a purpose and needs to align with the strategic business objectives and regulatory guidance.
- **Project management:** Model risk management initiatives require a formal project management structure to support efficiency, accuracy, and completeness.
- **Supporting documentation:** Comprehensive and consistent documentation needs to be maintained to support that complete documental evidence exists for every component and phase within the process.



Auditing the Accounting Function

Agenda

- General Accounting
- Financial Reporting
- Regulatory Reporting

General Accounting

General Accounting

- Accounts Payable
- General Ledger
- Internal DDA
- Fixed Assets

General Accounting- Accounts Payable

ESSENTIAL CONTROL POINTS

- An individual independent of the approval process enters the payment into the accounts payable system based on original, approved invoice / documentation.
- Segregation of duties exists over invoice approval, check drafting, check signing, general ledger expense categorization approval and check comparison to original invoice.
- The accounts payable system can detect or prevent duplicate payments of vendor invoices or expense checks
- Disbursement checks are mailed by someone independent of the approval and recording of the expenses.

PROGRAM STEPS

- Discuss the following with management:

  - Accounts payable process from authorization, including verification of receipt of goods and/or services, through recording the transaction to the subsidiary and general ledgers in the correct time period and the subsequent mailing of disbursement checks to the vendors.

  - Monitoring process including avoiding and detecting duplicate payments, issuance of checks in sequential order and voided checks.

  - Safeguarding process, including signature plates and/or cartridges, if electronic signatures are utilized.

  - Employee expenditure reimbursement process, including the review of supporting documentation through recording the transaction to the subsidiary and general ledgers and the subsequent disbursement of funds. For institutions that issue credit cards to employees for institutional purposes, review the process of reimbursing employee credit card expenditures.

General Accounting- Accounts Payable

PROGRAM STEPS (CONT.)

- Document the process, considering the essential controls. Comment on whether the controls are designed effectively and in operation.

- Select an entry posted to the disbursement journal during the current audit cycle. Walk through the process to substantiate your understanding. Documentation obtained or observation should include the following:
  - Purchase authorization and/or purchase order.
  - Documentation of receipt of goods/services (if a vendor invoice).
  - Invoice receipt and approval.
  - Expense recording to appropriate general ledger account.
  - Expense recording within correct time period.
  - Disbursement check signed by authorized individual.

- Assess the following related to procedures in the area:
  1. Existence: Do written procedures exist for this process? If not, should the institution have them?
  2. Current: Are the written procedures a reflection of the current practice and controls?
  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?
- The focus of this assessment is not on whether the technical aspects (e.g. screenshots) of the process are included, but whether the controls and processes are accurately and completely described.

General Accounting- Accounts Payable

ESSENTIAL CONTROL POINTS

- Payment of vender invoices and related disbursements are approved according to the institution's procedures. Invoices are marked as paid.
- An individual independent of the approval process enters the payment into the accounts payable system based on original, approved invoice / documentation.
- Segregation of duties exists over invoice approval, check drafting, check signing, general ledger expense categorization approval and check comparison to original invoice.
- An individual independent of the approval of invoices and drafting of checks receives the goods/services and compares the goods received/services rendered to the original invoice for accuracy.

- Obtain the accounts payable disbursement register and perform the following:
  - For a sample of paid invoices, test to determine:

    - the vendor invoice (original, not a copy) was approved for payment by an authorized individual

    - the invoice is supported by required documentation indicating that the goods were received or the services were performed

    - the invoice was posted to the appropriate general ledger account(s) within the correct period

    - the payee per the disbursement check agrees to the invoice

    - the check signer is authorized and independent of the individual approving the invoice and preparing the disbursement check.

General Accounting- Accounts Payable

ESSENTIAL CONTROL POINTS

- The accounts payable system can detect or prevent duplicate payments of vendor invoices or expense checks.
- Institution personnel issue and account for disbursement checks in sequential order as well as clearly identify voided checks.
- Segregation of duties exists over invoice approval, check drafting, check signing, general ledger expense categorization approval and check comparison to original invoice.
- Management or individuals responsible for processing accounts payable monitor invoices from each vendor for unusual patterns.

- Obtain check registers from the accounts payable system (or manually prepared check logs), and determine:

  1. If there are gaps in the sequential order of the checks issued. If gaps occur, obtain evidence of the disposition of any missing checks.
  2. Whether duplicate invoices have been paid. If so, determine if management identified the issue and received a subsequent credit from the vendor.
  3. If there are suspicious invoice numbers (i.e. same number on more than one invoice from the same vendor, consecutive invoice numbers from the same vendor over an extended period of time, or invoice numbers from the same vendor that do not appear to be in logical order over a period of time). If unusual patterns are identified, discuss with management and determine need to obtain and review original invoices.

General Accounting- Accounts Payable

ESSENTIAL CONTROL POINTS

- An authorized, independent, senior individual reviews and approves documentation of employee expenses for legitimacy of purpose and compliance with policy before reimbursement.

- Select a sample of reimbursed employee expenses from the current audit cycle. Include executive management reimbursements in the sample. For institutions that issue credit cards to employees for institutional purposes, include credit card reimbursements in the sample. Review for the following:
  - The expense was for a legitimate business purpose.
  - Documentation was submitted and retained to support the legitimacy of the expenditure.
  - Determine if the reimbursed items are in compliance with the institution's policy.
  - There is evidence of approval by an authorized individual who is in a supervisory capacity to the employee or of sufficiently high rank in order to prevent undue influence.

General Accounting- Accounts Payable

ESSENTIAL CONTROL POINTS

- Written procedures exist and describe critical processes and controls within this activity.

- Assess the following for the procedures related to this activity:

  1. Existence: Do procedures exist for this activity? If not, should the institution have them?
  2. Current: Are procedures a reflection of current practice and controls?
  3. Completeness: Are procedures complete with respect to critical elements of the activity and the critical control points?

General Accounting- General Ledger

ESSENTIAL CONTROL POINTS

- Management has a process in place to review journal entries for compliance with institution guidelines.
- Supporting documentation is maintained for journal entries.
- Journal entries are properly authorized prior to posting.

PROGRAM STEPS

- Discuss with management the processing of journal entries, including the preparation, approval, and processing of these entries. Include all types of entries such as automated, ticket, batch and online manual input. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Select a sample of journal entries. Determine if the entries were processed within the institution's guidelines

General Accounting- General Ledger

ESSENTIAL CONTROL POINTS

- Written procedures exist and describe the critical processes and controls for the area.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do procedures exist for this process? If not, should the institution have them?
  2. Current: Are procedures a reflection of current practice and controls?
  3. Completeness: Are procedures complete with respect to critical elements of the process and the critical control points?

General Accounting- General Ledger

ESSENTIAL CONTROL POINTS

- Master file changes are independently reviewed for accuracy by comparing the approval document to a system generated report. This review is documented.
- Master file changes are processed by someone independent of approval. The approval of the master file change is documented.

PROGRAM STEPS

- Discuss with management the general ledger maintenance process from authorization and recording general ledger maintenance to the review of the maintenance to the general ledgers. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain a system-generated report of general ledger maintenance (or masterfile changes). For sample of masterfile changes, trace masterfile changes to evidence of authorized approval. Test to supporting documentation that the maintenance was independently reviewed for accuracy and propriety.

General Accounting- General Ledger

ESSENTIAL CONTROL POINTS

- Management has established procedures for performing master file changes to the general ledger, which includes the addition, deletion, or modification of general ledger accounts.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do written procedures exist for this process? If not, should the institution have them?

  2. Current: Are the written procedures a reflection of the current practice and controls?

  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?

- The focus of this assessment is not on whether the technical aspects (e.g. screenshots) of the process are included, but whether the controls and processes are accurately and completely described.

General Accounting- General Ledger

ESSENTIAL CONTROL POINTS

- Management maintains a written responsibility listing that identifies individuals responsible for reconciling and reviewing of specific general ledger accounts. In addition, the listing indicates the general ledger account reconciliation frequency and timing of review.

PROGRAM STEPS

- Discuss with management the process used to determine all general ledger balance sheet accounts are reconciled. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain the general ledger account attestation or account listing and test the completeness of the attestation listing. Compare the report or listing to the general ledger to determine all balance sheet general ledger accounts are included.
  - In addition, determine that the listing identifies:
    - responsibilities for reconciling accounts
    - responsibilities for reviewing reconciliations
    - frequency in which the general ledger accounts should be reconciled and reviewed
- Review the completed general ledger reconciliation monitoring report for a sample of months to determine that the process is being used and that all general ledger accounts are reconciled. Select a sample of reconciliations and ask the client to provide documentation of the reconciliations.

General Accounting- Internal DDAs

ESSENTIAL CONTROL POINTS

- Internal deposit accounts are opened, closed, and/or modified by someone independent of approval. The approval of the internal deposit change is documented.

PROGRAM STEPS

- Discuss with management the process for setting-up internal DDA accounts. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain a system report of new internal deposit accounts. For a sample of internal DDAs originated during the audit cycle, test to determine:
  - the account was properly approved
  - the account was properly set-up on the system (account owner, tax identification, account type, and opening balance)
  - the account set-up was independently reviewed for accuracy and propriety
- Trace the source of funds from origination to final posting to the internal deposit account.

General Accounting- Internal DDAs

ESSENTIAL CONTROL POINTS

- Management has established procedures for opening and closing internal deposit accounts.
- Written procedures exist and describe the critical processes and controls within this activity.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do written procedures exist for this process? If not, should the institution have them?

  2. Current: Are the written procedures a reflection of the current practice and controls?

  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?

- The focus of this assessment is not on whether the technical aspects (e.g. screenshots) of the process are included, but whether the controls and processes are accurately and completely described.

General Accounting- Internal DDAs

ESSENTIAL CONTROL POINTS

- Management maintains an internal listing or other tracking document to determine that all internal deposit accounts are identified and reconciled

PROGRAM STEPS

- Discuss with management the process for monitoring and reconciling internal deposit accounts, including maintaining a reconciliation responsibility listing. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain a system-generated report of internal DDAs. For a sample of active internal DDAs, test to determine:
  - a reconciliation was prepared by someone independent of transaction approval.
  - a review was timely completed.
  - whether the use of an internal DDA seems appropriate for the purpose.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- Individuals and/or a designated committee of the Board have been assigned authority to approve acquisitions, transfers, disposals, or retirements of property and equipment.
- Management performs a periodic review to compare depreciation and repair expense balances to prior periods for reasonableness as well as reviewing the reasonableness of estimated useful lives.
- Management evaluates new or modified leases for operating versus capital lease decisions, including reviewing operating leases with rent escalation clauses to determine the appropriate method to use to record lease expense.
- Transactions recorded to the subsidiary ledger are supported by appropriate documentation and are independently reviewed.

PROGRAM STEPS

- Discuss with management the following regarding fixed assets:
  - The purchasing/sale/transfer/retirement process from authorization through recording the transaction to the subsidiary and general ledgers.
  - The lease process from entering into or renewing leases, including the classification of operating or capital and maintenance of inventory of leases outstanding, through recording to a subsidiary ledger.
  - The monitoring process for comparing depreciation expense to remaining useful lives and recording depreciation expense.
  - The safeguarding process to determine steps taken by management to ensure fixed assets are physically safeguarded and adequately insured.
- Document the processes above, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

General Accounting- Fixed Assets

PROGRAM STEPS (CONT.)

- Select a fixed asset purchased during the current audit cycle. Walk through the process to substantiate understanding. Documentation obtained from management should include the following:
  - supporting authorization for the purchase;
  - management's evaluation to determine capitalization versus expensing the purchase according to institution policy;
  - evidence of assigning the asset to an appropriate general ledger account;
  - evidence of funds disbursement;
  - subsidiary ledger that supports the original entry for the purchase; and
  - evidence of independent review of the fixed asset set-up.

- Select a fixed asset sold and/or retired during the current audit cycle. Walk through the process to substantiate understanding. Documentation obtained from management should include the following:
  - supporting authorization for the transaction;
  - calculation for the resulting gain/loss;
  - evidence of funds receipt; and
  - evidence of removal of the asset and related accumulated depreciation from the subledger.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- Management has established guidelines and procedures for capitalizing or expensing purchases of property for the financial institution.
- Management maintains procedures that address depreciation and amortization methods, useful lives, estimated salvage values, preventative maintenance, etc.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do written procedures exist for this process? If not, should the institution have them?

  2. Current: Are the written procedures a reflection of the current practice and controls?

  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?
- The focus of this assessment is not on whether the technical aspects (e.g. screenshots) of the process are included, but whether the controls and processes are accurately and completely described.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- Individuals and/or a designated committee of the Board have been assigned authority to approve acquisitions, transfers, disposals, or retirements of property and equipment.
- The subsidiary ledger has the capability of classifying each fixed asset and its related accumulated depreciation and accurately computes depreciation expense.
- Transactions recorded to the subsidiary ledger are supported by appropriate documentation and are independently reviewed.
- Management utilizes an established policy when determining whether to capitalize a purchase as a fixed asset or expense it.

PROGRAM STEPS

- Obtain a listing of fixed asset activity (purchases, transfers, sales, retirements, etc) and perform the following:
  - For a sample of fixed assets purchased, test to determine:
    - the purchase was approved according to established policy;
    - the original supporting invoice exists and agrees to the subsidiary ledger;
    - the subsidiary ledger was properly set-up according to established policy (asset classification, dollar amount, depreciation method, useful life, etc);
    - the purchase was assigned an appropriate general ledger account and posted correctly to the general ledger;
    - the purchase was appropriately capitalized versus being expensed at the time of purchase;
    - the funds were disbursed according to established policy; and
    - evidence of independent review of the fixed asset set-up.

General Accounting- Fixed Assets

PROGRAM STEPS (CONT.)

- For a sample of fixed assets sold or retired, test to determine:
  - the sale or retirement was approved according to established policy;
  - the gain/loss amount was accurately calculated; and
  - the sale was recorded to the subsidiary ledger and general ledger (gain or loss recognition and related balance sheet accounts) in the appropriate account and time period.

- For a sample of assets transferred between fixed asset categories, review for reasonableness of current classification.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- Management performs a periodic review to compare depreciation and repair expense balances to prior periods for reasonableness as well as reviewing the reasonableness of estimated useful lives.
- The subsidiary ledger has the capability of classifying each fixed asset and its related accumulated depreciation and accurately computes depreciation expense.

PROGRAM STEPS

- Obtain a schedule of fixed asset categories, original book balance, current book balance, service date, remaining depreciable lives, depreciation expense and accumulated deprecation and review the schedule to determine:
  1. Reasonableness of the fixed asset categories and depreciable life.
  2. Assets with a book value of zero, but are continuing to have a monthly depreciation expense.
  3. Construction in process items that are being depreciated.
  4. Any land that is not the site of an institution-owned building.
  5. Assets set up to depreciate which should have been expensed at the time of purchase in accordance with institution policy.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- The subsidiary ledger has the capability of classifying each fixed asset and its related accumulated depreciation and accurately computes depreciation expense.

PROGRAM STEPS

- For a sample of depreciable assets, recalculate the depreciation expense for one month and trace to posting in the appropriate general ledger account.

- For a sample of leases, obtain the lease agreement and trace the monthly expense amount per the lease agreement to the general ledger expense account for a sample of months.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- Management evaluates new or modified leases for operating versus capital lease decisions, including reviewing operating leases with rent escalation clauses to determine the appropriate method to use to record lease expense.

PROGRAM STEPS

- Obtain a schedule of leases and leasehold improvement to determine whether:
  1. Management has properly classified the lease as operating or capital according to GAAP.
  2. Leasehold improvements are properly depreciated according to GAAP.
  3. The lease expense recorded is timely adjusted for any operating leases that have an annual increase.

General Accounting- Fixed Assets

ESSENTIAL CONTROL POINTS

- Management has an established insurance coverage review process in place to determine sufficient coverage on property and equipment.

PROGRAM STEPS

- Obtain management's most recent review of property and equipment insurance coverage to determine completion of the review by the required parties and in compliance with annual timing requirements.
- For a sample of purchases and sales/retirements since the last audit, verify that the institution's insurance coverage was updated to reflect the asset addition or sale/retirement.

Financial Reporting

Financial Reporting

- Closing
- Management Certification
- Preparation and Review

Financial Reporting- Closing

ESSENTIAL CONTROL POINTS

- Management maintains a standard closing entry schedule for monthly, quarterly, and annual entries.
- Financial reporting personnel obtain documentation that all account reconciliations are completed as well as information regarding any stale dated reconciling items on the reconciliations.
- Management has an established process for monitoring period end cut-off and approving back-dated journal entries.

PROGRAM STEPS

- Discuss with management the following:

  - Financial reporting closing process, from determination that all accounts are reconciled to posting of closing and back-dated entries for all affiliated entities, including the process for updating the closing schedule each period, as needed.

  - Consolidation and review process, including receiving balance sheet and income statement information for all affiliated entities, identifying and processing elimination entries and preparing the consolidated financial statements.

- Document the processes, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Financial Reporting- Closing

ESSENTIAL CONTROL POINTS

- A standard closing entry schedule is maintained for monthly, quarterly, and annual entries.
- Written procedures exist for the close process governing the preparation and presentation of financial statements and disclosures.
- Financial reporting personnel obtain documentation from accounting personnel that all account reconciliations are completed.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do written procedures exist for this process? If not, should the institution have them?

  2. Current: Are the written procedures a reflection of the current practice and controls?

  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?

Financial Reporting- Closing

ESSENTIAL CONTROL POINTS

- Management maintains a standard closing entry schedule for monthly, quarterly, and annual entries.

PROGRAM STEPS

- For the most recent month, quarter and year end, select a sample of entries from the closing schedule and trace to posting on the general ledger as required. Include in the sample entries from all entry sources and entries for lower dollar amounts as well as larger dollar amounts.

Financial Reporting- Closing

ESSENTIAL CONTROL POINTS

- Financial reporting personnel obtain documentation that all account reconciliations are completed as well as information regarding any stale dated reconciling items on the reconciliations.

PROGRAM STEPS

- Based on the discussion with management concerning the financial reporting closing process, obtain evidence that management received documentation confirming reconciliation of all balance sheet accounts for the most recent reporting period end. Review documentation for completeness and timeliness of reporting.
- Determine also if the listing identifies dated reconciling items. If so, review the nature of the items to determine if a related adjusting entry is necessary.

Financial Reporting- Closing

ESSENTIAL CONTROL POINTS

- Management has an established process for monitoring period end cut-off and approving back-dated journal entries.

PROGRAM STEPS

- For a sample of disbursements (vendor payments and employee reimbursements) immediately preceding and immediately following the most recent reporting period end (i.e. quarter or year end), obtain the related invoice and determine if the expense was classified within the proper reporting period.

Financial Reporting- Closing

ESSENTIAL CONTROL POINTS

- Management has an established process for monitoring period end cut-off and approving back-dated journal entries.

PROGRAM STEPS

- For a sample of back-dated journal entries from the most recent period end, obtain supporting documentation for the entry. Determine if the entry was approved as required by institution policy and if the entry was recorded in the correct period.
- Obtain the balance sheet and income statement from the month-end following the most recent quarter end and compare them with the quarter end balance sheet and income statements. Review, inquire of management and obtain supporting documentation for unusual fluctuations that may indicate cut-off issues.

Financial Reporting- Management Certification

ESSENTIAL CONTROL POINTS

- Management has an established process for CEO/CFO certification and departmental back-up certification for interim and annual filings.

PROGRAM STEPS

- Discuss with management the 10Q and 10K management certification process, including any back-up certification by line of business managers. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain management's most recent 10-Q and 10-K certification files and review for evidence that supports management's representations of the process. Document the results.

Financial Reporting- Management Certification

ESSENTIAL CONTROL POINTS

- Management maintains documentation to support the certification of the interim and annual reports.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do written procedures exist for this process? If not, should the institution have them?

  2. Current: Are the written procedures a reflection of the current practice and controls?

  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- Significant accounting estimates are reviewed on at least a quarterly basis.
- Individuals responsible for preparing and reviewing financial statements participate in relevant training and maintain adequate knowledge of ongoing changes in requirements.
- Individuals responsible for preparing financial statements consistently communicate necessary supporting information to and verify such information received from other lines of business for accuracy and completeness.
- The Audit Committee and Disclosure Committee review and approve interim and annual filings.
- Individuals responsible for financial reporting utilize a current disclosure checklist (including SEC disclosures, if a public company) or other tool (such as sample financial statements) and monitor reporting requirements.

Financial Reporting- Preparation and Review

PROGRAM STEPS

- Discuss with management the following:

  - Process for reviewing significant estimates, critical accounting treatments and new GAAP/other reporting requirements for the current period, including reporting to the Audit Committee or Disclosure Committee.

  - Process for providing filings to the Audit Committee and/or Disclosure Committee for review and approval of the financial statements, including information the committees receive and if information is provided prior to meetings to allow adequate time for review.

  - Process for preparation and review of period end consolidation and financial statements both internally and by external parties such as external auditors and legal counsel, including control of the financial statement document throughout the review process to ensure changes made are appropriate.

  - Process for financial reporting personnel to remain current on reporting requirements, including training and utilization of a current disclosure checklist, as necessary. Also include discussion on how these individuals remain current with activities and transactions across the organization to ensure proper accounting and reporting treatment.

- Document the processes, considering each of the essential control points. Comment on whether the controls are designed effectively and are in operation.

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- Written procedures exist regarding the preparation and presentation of the financial statements and financial statement disclosures.

PROGRAM STEPS

- Assess the following related to procedures in the area:

  1. Existence: Do written procedures exist for this process? If not, should the institution have them?

  2. Current: Are the written procedures a reflection of the current practice and controls?

  3. Completeness: Are written procedures complete with respect to critical elements of the process and the critical control points?

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- The Audit Committee and Disclosure Committee review and approve interim and annual filings.

PROGRAM STEPS

- Review a sample of minutes or other evidence that the Audit Committee and/or Disclosure Committee reviews and approves the financial statements. Determine information the committees receive and the timing of receipt, and whether there is evidence of the level of review, types of questions, follow-up from management, etc.

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- Individuals responsible for financial reporting utilize a current disclosure checklist (including SEC disclosures, if a public company) or other tool (such as sample financial statements) and monitor reporting requirements.

PROGRAM STEPS

- Obtain the most recent sample financial statements and/or disclosure checklist used to assist in the completion of financial statements and disclosures. Determine where management obtained the information and review for evidence of periodic updating to current requirements.

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- Management maintains adequate documentation supporting the institution's consolidation, including individual entity general ledgers and consolidating and reclassifying entries.

PROGRAM STEPS

- Obtain the consolidations for the most recent and the immediately preceding reporting periods along with supporting documentation. Perform the following:

  - Agree consolidation amounts to supporting subsidiary general ledger support.

  - Compare general ledger line item groupings to prior period for consistency.

  - Observe evidence, such as supporting documentation, that eliminations are accurate.

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- Management maintains adequate documentation supporting the institution's consolidation, including individual entity general ledgers and consolidating and reclassifying entries.

PROGRAM STEPS

- Obtain the consolidations for the most recent and the immediately preceding reporting periods along with supporting documentation. Perform the following:

  - Agree consolidation amounts to supporting subsidiary general ledger support.

  - Compare general ledger line item groupings to prior period for consistency.

  - Observe evidence, such as supporting documentation, that eliminations are accurate.

Financial Reporting- Preparation and Review

ESSENTIAL CONTROL POINTS

- Individuals responsible for preparing and reviewing financial statements participate in relevant training and maintain adequate knowledge of ongoing changes in requirements.
- Individuals responsible for financial reporting utilize a current disclosure checklist (including SEC disclosures, if a public company) or other tool (such as sample financial statements) and monitor reporting requirements.

PROGRAM STEPS

- Discuss with management any problems they have had with the reporting process. Note if they have had any corrections to prior year financial statements or any disclosures new to the current year that should have been disclosed in the prior year. Consider the need to adjust the audit scope to address any issues identified

Regulatory Reporting

Regulatory Reporting

- Call Report

Regulatory Reporting- Call Report

ESSENTIAL CONTROL POINTS

- Data input to the regulatory reports are subject to review to ensure the data has been reported in compliance with current regulatory requirements.
- Data input to the regulatory reporting system includes all assets & liabilities, capital accounts, income and expense accounts, off balance sheet items, and other information required by the

PROGRAM STEPS

- Discuss with management the process from data input through regulatory report signature. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Assess the following related to written procedures for this process:

  1. Existence: Do procedures exits for this process? If not, should the institution have them?
  2. Current: Are procedures a reflection of current practice and controls?
  3. Completeness: Are procedures complete with respect to critical elements of the process and the critical control points.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC Balance Sheet - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total and/or other supporting Call Report Schedules (RC-A through RC-G and RC-M), as applicable. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Assets on this Call Report Schedule is consistent with other internal financial reports not utilized as a source of input for this item.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC-A Cash and Balances Due From Depository Institutions - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Cash and Balances Due From Depository Institutions on this Call Report Schedule is consistent with other internal financial reports not utilized as a source of input for this item.
- Schedule RC B Securities - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Securities on this Call Report Schedule is consistent with other internal financial reports not utilized as a source of input for this item.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC C Loans and Lease Financing Receivables - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Loans and Leases on this Call Report Schedule is consistent with other internal financial or loan/lease reports not utilized as a source of input for this item.
- Schedule RC D Trading Assets and Liabilities - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Trading Assets and Total Trading Liabilities on this Call Report Schedule are consistent with other internal financial reports not utilized as a source of input for this item.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC F&G Other Assets & Liabilities - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Ascertain that Other Asset and Other Liabilities detail has been reported based on parameters in regulatory instructions. Also determine Total Other Assets and Total Other Liabilities on this Call Report Schedule are consistent with other internal financial reports not utilized as a source of input for this item.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC K Quarterly Averages - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Average Assets is determined based on the cost basis for securities designated available-for-sale and any deferred tax asset related to available-for-sale securities accounting is excluded. Also, determine that Total Average Assets is not just the sum of the other average asset categories reported on this Schedule.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RI Report of Income - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total and/or other supporting Call Report Schedules (RI-A through RI-E), as applicable. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Net Income on this Call Report Schedule is consistent with other internal financial reports not utilized as a source of input for this item.
- Schedule RI Interest Income and Expense Reasonableness - Perform an analytical review of interest income and expense reported by computing a yield/cost based on average data reported in Schedule K for the current and prior periods covered by this Schedule RI, and determine that the yield/cost is consistent with other yield/cost data in other internal financial reports not utilized as a source of data input.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RI A-E Supplemental - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory instructions. Ascertain that Other Noninterest Income and Other Noninterest Expense detail has been reported on Schedule RI-E based on parameters in regulatory instructions. Also determine that beginning and ending period Total Capital on Schedule RI-A and Total Allowance for Loan and Lease Losses on Schedule RI-B is in agreement with Total Capital and Total Allowance for Loan and Lease Losses reported on Schedule RC at the applicable quarter end.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC L Derivatives and Other Off-Balance Sheet Items - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory instructions. Also determine Total Loan Commitments and Total Derivatives on this Call Report Schedule is consistent with other internal financial or loan reports not utilized as a source of input for this item.
- Schedule RC M Memo - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory instructions.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC N Past Due and Nonaccrual Loans, Leases and Other Assets - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine Total Past Dues and Nonaccruals on this Call Report Schedule is consistent with other internal financial or loan/lease reports not utilized as a source of input for this item.
- Schedule RC O Other Data for Deposit Insurance and FICO Assessments - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory instructions. Also determine that Total Deposits on this Call Report Schedule is in agreement with Total Deposits reported on Schedule RC.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC P Closed end 1-4 Family Residential Mortgage Banking Activities - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine activities on this Call Report Schedule is consistent with other internal financial or loan/lease reports not utilized as a source of input for this item.
- Schedule RC Q Financial Assets and Liabilities Measured at Fair Value - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC R Regulatory Capital - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory instructions. Also determine Total Assets before risk weighting on this Call Report Schedule is in agreement with Total Assets reported on Schedule RC and that the risk-weighted data in this Schedule is consistent with data reported in Call Report Schedules RC-A through RC-C, RC-F and RC-L, as applicable.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC S Servicing, Securitizations, and Asset Sales Activities - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory reporting instructions. Also determine activities on this Call Report Schedule is consistent with other internal financial or loan/lease reports not utilized as a source of input for this item.

Regulatory Reporting- Call Report

PROGRAM STEPS (CONT.)

- Schedule RC T Fiduciary and Related Services Income - Determine that each data input item on this Call Report Schedule agrees to a supporting detail workpaper/spreadsheet/other internal IT system report information grouping total. Review the supporting detail to determine that, based on the descriptions or nature of content of items making up the information grouping total, the data input item is reported in compliance with regulatory instructions. Also determine that Total Fiduciary and Related Services Income on this Call Report Schedule is in agreement with Total Fiduciary and Related Services Income reported on Schedule RI.

Regulatory Reporting- Call Report

ESSENTIAL CONTROL POINTS

- Data input to the regulatory reports are subject to review to ensure the data has been reported in compliance with current regulatory requirements.

PROGRAM STEPS

- Select a sample of regulatory capital data items reported on Schedule RC-R and determine that the capital data items in this Call Report Schedule are consistent with related capital data included in external financial reports such as SEC filings 10Q and 10K.

Recent Trends in Financial Institution Fraud

Agenda

- Fraud Statistics
- Internal Fraud Red Flags
- Recent Fraud Schemes

Fraud Statistics

Impact of Fraud on Financial Institutions

- Hard to measure
- No one universal definition of fraud = various interpretations
- No one agency that is responsible for investigating fraud

Additionally, many fraud losses are misreported.

Why does this occur? Because most institutions don’t recognize when a fraud has occurred and chalk it up to a bad underwriting decision or another form of operational expense.

Cost of Fraud

Other less-quantifiable costs of fraud to the organization:

- Reputation risk to financial institution
  - Customers trust us with one of their most significant possessions: their money
  - Reputation risk is difficult to quantify
- Increased regulatory focus
- Morale impact on employees

Suspicious Activity Reports

- The Bank Secrecy Act (BSA)

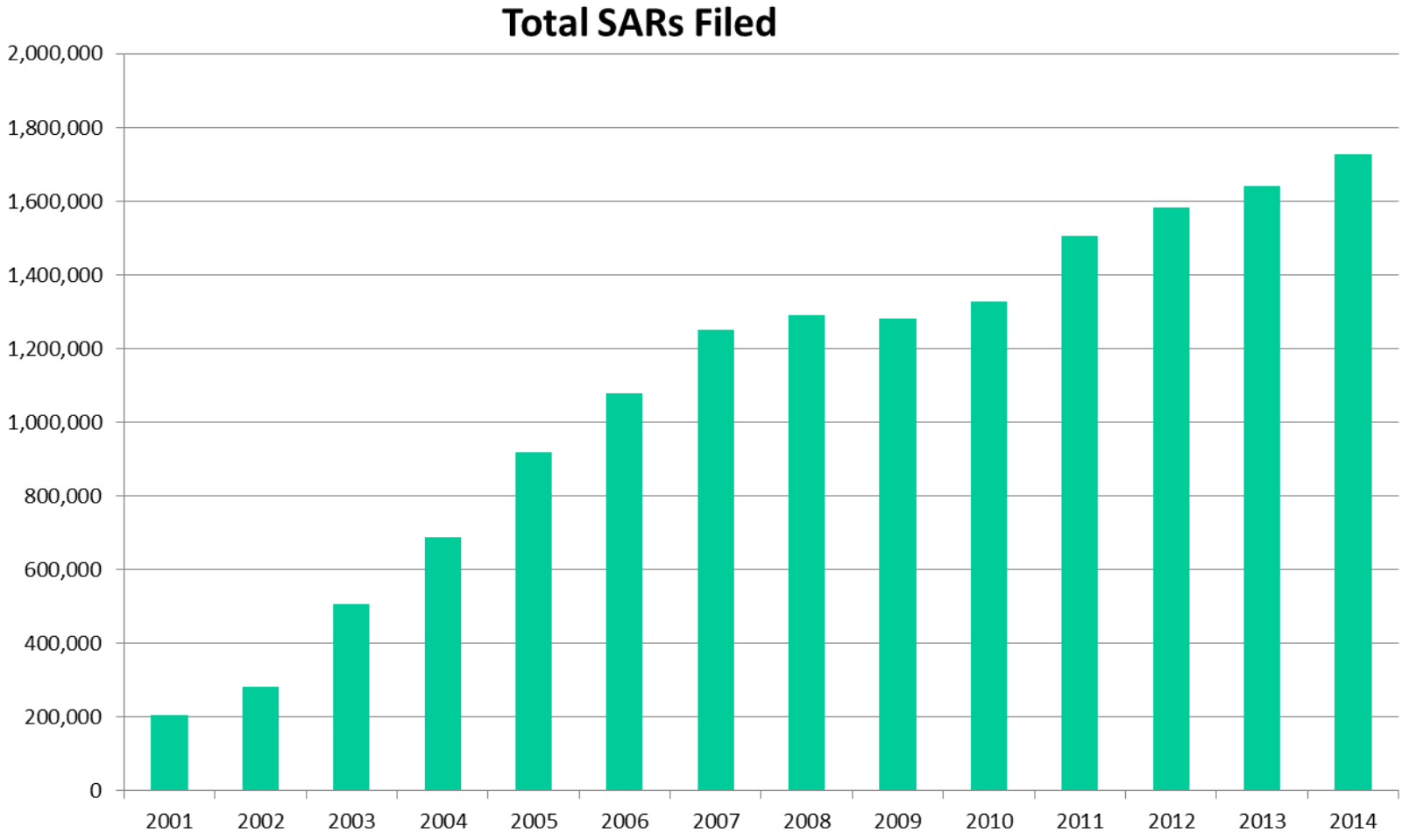
- Regulations require that financial institutions file Suspicious Activity Reports (SARs)
  - Report known or suspected violations of law or suspicious activity
  - Filed with the Department of Treasury's Financial Crimes Enforcement Network (FinCEN)

Suspicious Activity Reports

- FinCEN compiles statistics based on the filed SARs to identify trends and patterns for use by not only the financial institutions but also by law enforcement

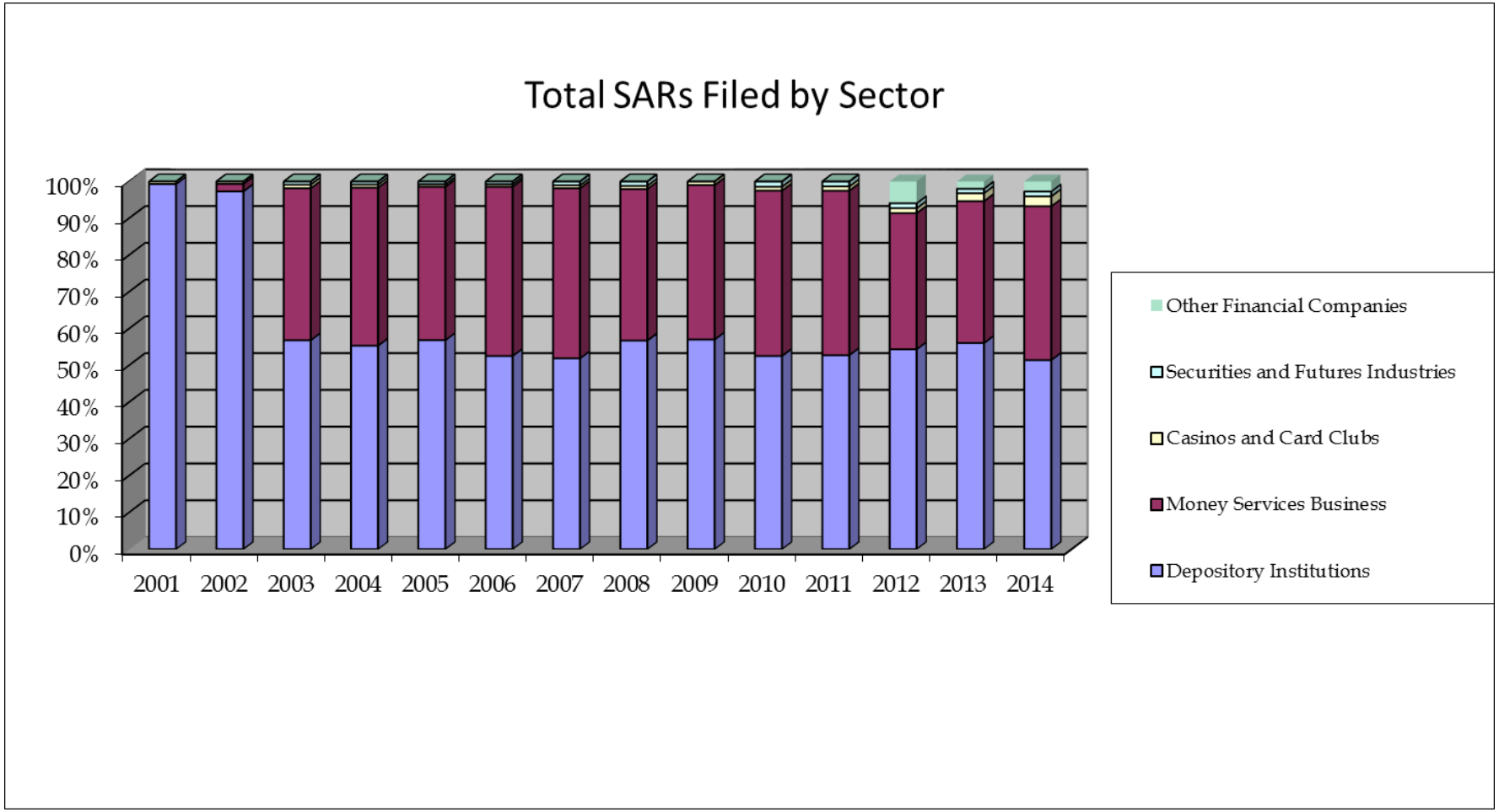
- Multiple types of financial institutions are required to file SARs:
  - Depository Institutions
  - Money Service Businesses
  - Securities Sector
  - Others

Suspicious Activity Reports



Source: Financial Crimes Enforcement Network (FinCen)

Suspicious Activity Reports



Source: Financial Crimes Enforcement Network (FinCen)

Suspicious Activity Reports

2014 Emerging Trends in Depository Institutions

Category	Suspicious Activity	2014	2013	Change
FRAUD	Tax Fraud	6,148	6,638	-7%
	Prepaid Card Fraud	2,705	3,999	-32%
	Deposit Fraud	2,435	2,188	11%
	Counterfeit Check	2,069	3,041	-32%
	Kiting (Unspecified)	1,704	1,705	0%
	Check Kiting	1,554	1,536	1%
	Online Banking	1,460	1,355	8%
	Credit Card Kiting	1,128	919	23%
	Due Diligence	1,064	643	65%
IDENTIFICATION	Social Security Number Fraud	48,851	21,399	128%
DOCUMENTATION	Insufficient Documentation Provided	1,010	869	16%

Source: Financial Crimes Enforcement Network (FinCen)

Suspicious Activity Reports

2014 Emerging Trends in Depository Institutions

Category	Suspicious Activity	2014	2013	Change
OTHER	Income Discrepancy	20,352	7,021	190%
SUSPICIOUS	Identity Fraud	9,755	2,229	338%
ACTIVITIES	Tax Fraud	6,841	6,663	3%
	Employment Discrepancy	2,577	1,017	153%
	Fraud Ring	2,376	3,066	-23%
	False Statement	1,850	835	122%
	Check Kiting	1,794	2,267	-21%
	Bust Out Scheme	1,074	936	15%
	Kiting (Unspecified)	1,028	1,202	-14%
	Suspicious Financial Activity	968	517	87%
	Excessive Cash Payments	964	1,575	-39%
	Rapid Utilization/Movement of Funds	890	1,434	-38%

Source: Financial Crimes Enforcement Network (FinCen)

Suspicious Activity Reports

2014 Emerging Trends in Depository Institutions

- Top trends in 2014 were for the most part consistent with prior years, with most noticeable increases being the following themes: **Fraudulent Use of a SSN, Suspicion Concerning the use of Funds, Income Discrepancy, Identity Fraud, and Employment Discrepancy**. References to each of these trends more than doubled in 2014 when compared to prior years.
- The standout trend for 2014 was the increase in references to **Funnel Account Activity**, which garnered almost 10,000 mentions within the category of Money Laundering.
- **False Identity Theft Claim (Mortgage Fraud), False Statement (Other Suspicious Activities), and Circumventing Chinese Currency Regulations (Structuring)** were also key activities trending higher.

Source: Financial Crimes Enforcement Network (FinCen)

Suspicious Activity Reports

2014 Emerging Trends in Depository Institutions

- **Tax Fraud-related items** remained the most pervasively referenced type of activity, mentioned in multiple suspicious activity categories in Depository Institutions SARs. During 2014 approximately 14,000 tax-related free-text entries appeared within the combined categories of Fraud, Money Laundering, and Other Suspicious Activities.

Source: Financial Crimes Enforcement Network (FinCen)

Insider Fraud Continues to Rise

Kroll's Global Fraud Report 2015-2016 surveyed 768 senior executives from a broad range of industries worldwide noting:

- **75% of companies experienced a fraud** incident in the past year. **81% of companies affected by fraud reported insider perpetrators**. Whistleblowers responsible for exposing 41% of fraud incidents.
- Three quarters of companies (75%) have fallen victim to a fraud incident in the past year, **a rise of 14 percentage points in just three years**.
- The biggest fraud threat to companies **comes from within**. Of those companies where fraud occurred and the perpetrator was identified, **four in five (81%) suffered at the hands of at least one insider**, up from 72% in the previous survey.

Insider Fraud Continues to Rise

Kroll's Global Fraud Report 2015-2016:

- **Financial Services**
  - **70% of Financial Services companies reported being affected by fraud**
  - Financial Services companies reported an average loss of revenues from fraud of 0.5%
  - The Financial Services sector saw the third highest proportion of firms affected by regulatory or compliance breaches (17%)
  - The Financial Services sector saw the second highest for information loss (18%)
  - **The Financial Services sector saw the highest for management conflict of interest (17%).**
  - The Financial Services sector also reported theft of physical assets or stock at 18%
  - **82% of Financial Services companies have seen their exposure to fraud increase from the previous year**

Insider Fraud Continues to Rise

Kroll's Global Fraud Report 2015-2016:

- **Financial Services**
  - Among companies in the Financial Services sector where fraud was uncovered in the past year and where the perpetrator is known, **42% report that senior or middle management took a leading role** in at least one such crime, and a striking 58% say the same of junior employees.
    - These are the highest rates across all business sectors
  - Top Drivers of increased exposure for Financial Services companies
    - **High staff turnover** which affects the businesses of 49% of financial services respondents
      - Tied for the highest of all business sectors
    - **Entry into new, riskier markets**

Cost of Occupational Fraud

The ACFE's 2016 *Report to the Nations* reported the following:

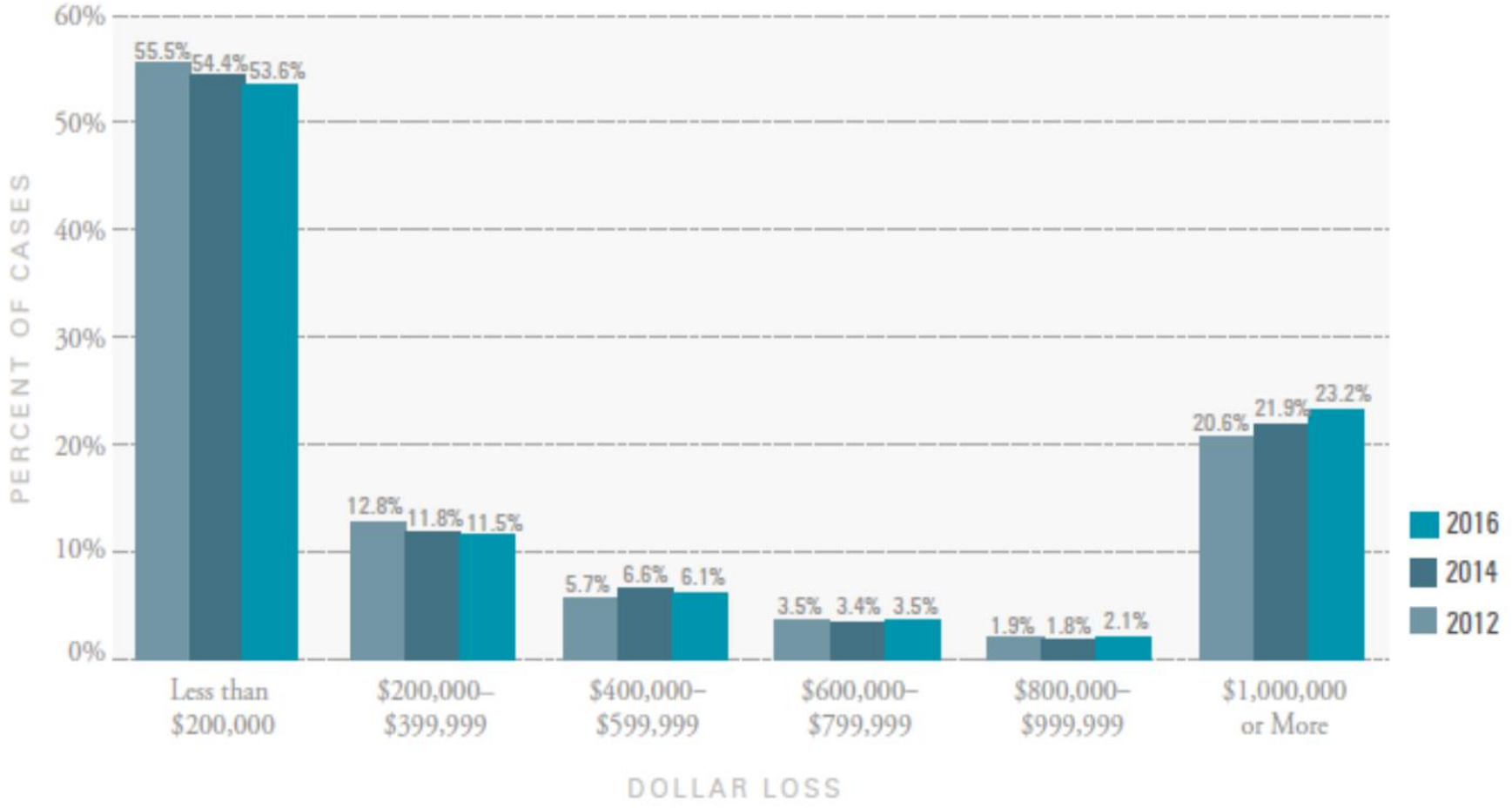
- The CFEs who participated in our survey estimated that the typical organization **loses 5% of revenues in a given year as a result of fraud.**
- The total loss caused by the cases in our study **exceeded $6.3 billion**, with an average loss per case of $2.7 million.
- The **median loss for all cases in our study was $150,000**, with 23.2% of cases causing losses of $1 million or more.

Cost of Occupational Fraud

The ACFE's 2016 *Report to the Nations* (continued):

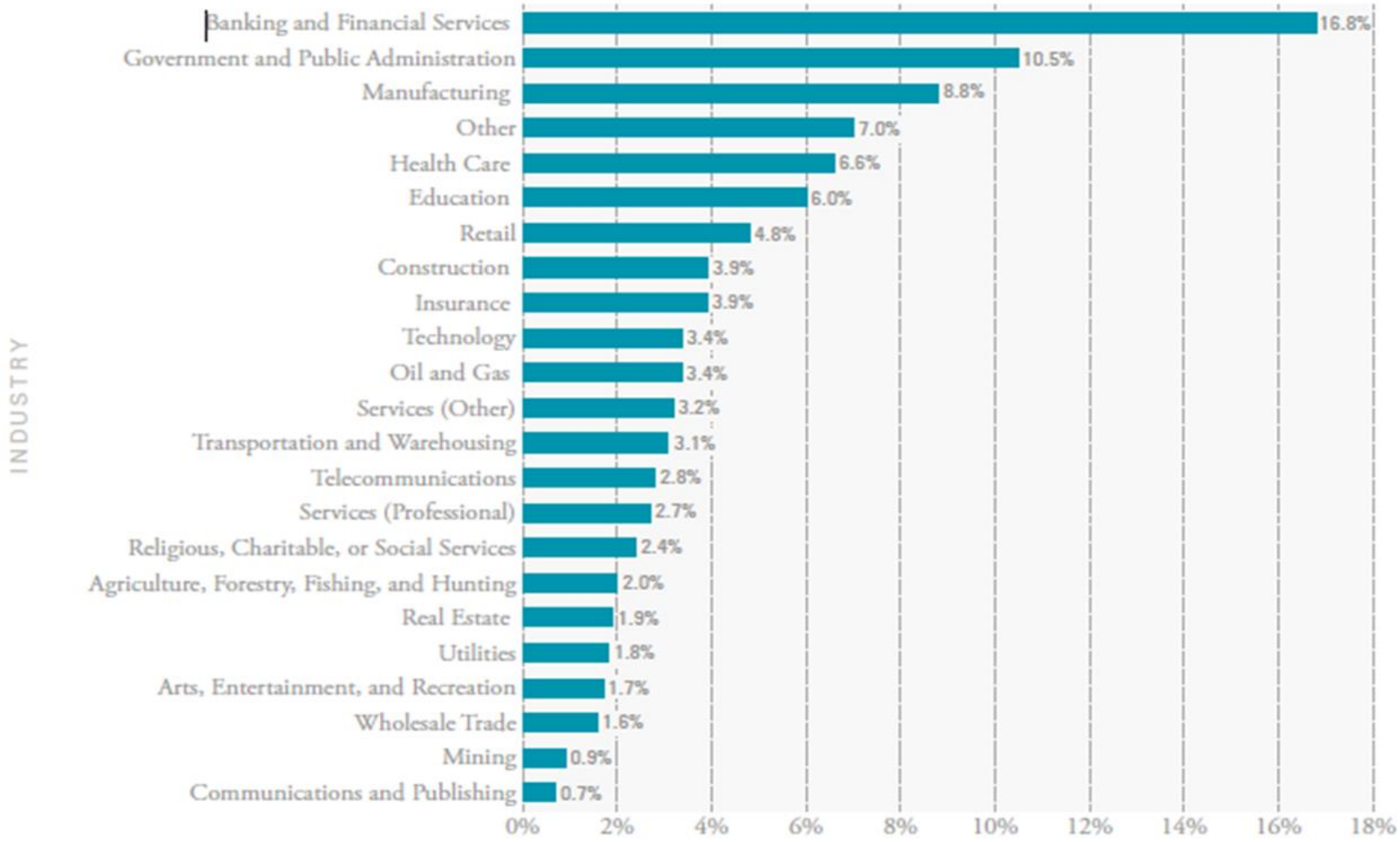
- In **94.5% of the cases in our study, the perpetrator took some efforts to conceal the fraud**. The most common concealment methods were creating and altering physical documents.
- The perpetrator's **level of authority was strongly correlated with the size of the fraud**. The median loss in a scheme committed by an **owner/executive was more than four times higher than the median loss caused by managers and nearly 11 times higher than the loss caused by employees.**

Distribution of Dollar Losses



Source: ACFE 2016 *Report to the Nations*

Fraud by Business Sector



Source: ACFE 2016 *Report to the Nations*

Change in Implementation Rates of Anti-Fraud Controls

Control	2010 Implementation Rate	2016 Implementation Rate	Change from 2010–2016
Hotline	51.2%	60.1%	8.9%
Fraud Training for Employees	44.0%	51.6%	7.6%
Anti-Fraud Policy	42.8%	49.6%	6.8%
Code of Conduct	74.8%	81.1%	6.3%
Management Review	58.8%	64.7%	5.9%
Surprise Audits	32.3%	37.8%	5.6%
Fraud Training for Managers/Executives	46.2%	51.3%	5.2%
Independent Audit Committee	58.4%	62.5%	4.1%
Management Certification of Financial Statements	67.9%	71.9%	4.0%
Rewards for Whistleblowers	8.6%	12.1%	3.5%
Job Rotation/ Mandatory Vacation	16.6%	19.4%	2.8%
External Audit of Internal Controls over Financial Reporting	65.4%	67.6%	2.2%
Employee Support Programs	54.6%	56.1%	1.5%
External Audit of Financial Statements	80.9%	81.7%	0.8%

Source: ACFE 2016 *Report to the Nations*

Median Loss Based on Presence of Anti-Fraud Controls

Control	Percent of Cases	Control in Place	Control Not in Place	Percent Reduction
Proactive Data Monitoring/Analysis	36.7%	$92,000	$200,000	54.0%
Management Review	64.7%	$100,000	$200,000	50.0%
Hotline	60.1%	$100,000	$200,000	50.0%
Management Certification of Financial Statements	71.9%	$104,000	$205,000	49.3%
Surprise Audits	37.8%	$100,000	$195,000	48.7%
Dedicated Fraud Department, Function, or Team	41.2%	$100,000	$192,000	47.9%
Job Rotation/Mandatory Vacation	19.4%	$89,000	$170,000	47.6%
External Audit of Internal Controls over Financial Reporting	67.6%	$105,000	$200,000	47.5%
Fraud Training for Managers/Executives	51.3%	$100,000	$190,000	47.4%
Fraud Training for Employees	51.6%	$100,000	$188,000	46.8%
Formal Fraud Risk Assessments	39.3%	$100,000	$187,000	46.5%
Employee Support Programs	56.1%	$100,000	$183,000	45.4%
Anti-Fraud Policy	49.6%	$100,000	$175,000	42.9%
Internal Audit Department	73.7%	$123,000	$215,000	42.8%
Code of Conduct	81.1%	$120,000	$200,000	40.0%
Rewards for Whistleblowers	12.1%	$100,000	$163,000	38.7%
Independent Audit Committee	62.5%	$114,000	$180,000	36.7%
External Audit of Financial Statements	81.7%	$150,000	$175,000	14.3%

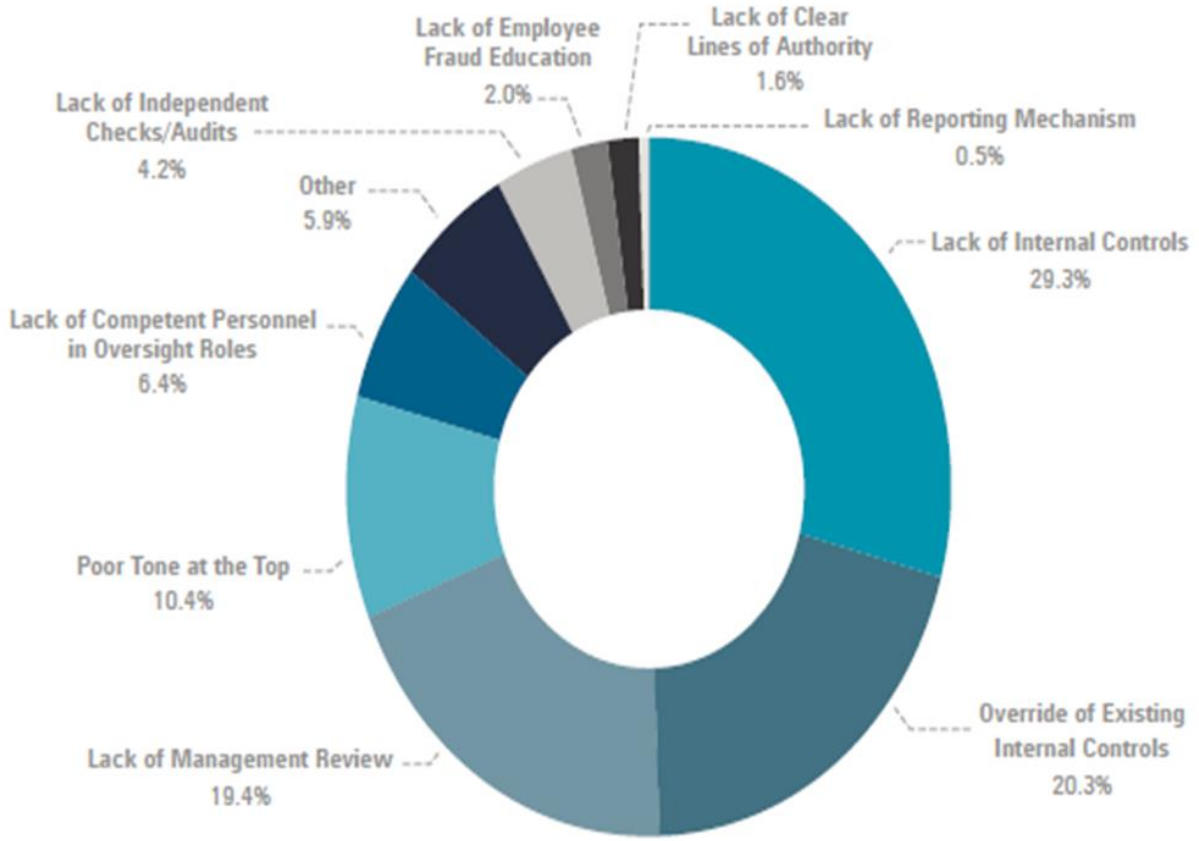
Source: ACFE 2016 *Report to the Nations*

Median Duration of Fraud Based on Presence of Anti-Fraud Controls

Control	Percent of Cases	Control in Place	Control Not in Place	Percent Reduction
Surprise Audits	37.8%	12 Months	24 Months	50.0%
Proactive Data Monitoring/Analysis	36.7%	12 Months	24 Months	50.0%
Dedicated Fraud Department, Function, or Team	41.2%	12 Months	24 Months	50.0%
Hotline	60.1%	12 Months	24 Months	50.0%
Formal Fraud Risk Assessments	39.3%	12 Months	24 Months	50.0%
Management Review	64.7%	12 Months	24 Months	50.0%
Independent Audit Committee	62.5%	12 Months	24 Months	50.0%
Internal Audit Department	73.7%	12 Months	24 Months	50.0%
External Audit of Internal Controls over Financial Reporting	67.6%	12 Months	24 Months	50.0%
Management Certification of Financial Statements	71.9%	12 Months	24 Months	50.0%
Code of Conduct	81.1%	13 Months	24 Months	45.8%
Job Rotation/Mandatory Vacation	19.4%	10 Months	18 Months	44.4%
Anti-Fraud Policy	49.6%	12 Months	21 Months	42.9%
Fraud Training for Employees	51.6%	12 Months	20 Months	40.0%
Fraud Training for Managers/Executives	51.3%	12 Months	20 Months	40.0%
Rewards for Whistleblowers	12.1%	11 Months	18 Months	38.9%
External Audit of Financial Statements	81.7%	15 Months	24 Months	37.5%
Employee Support Programs	56.1%	12 Months	18 Months	33.3%

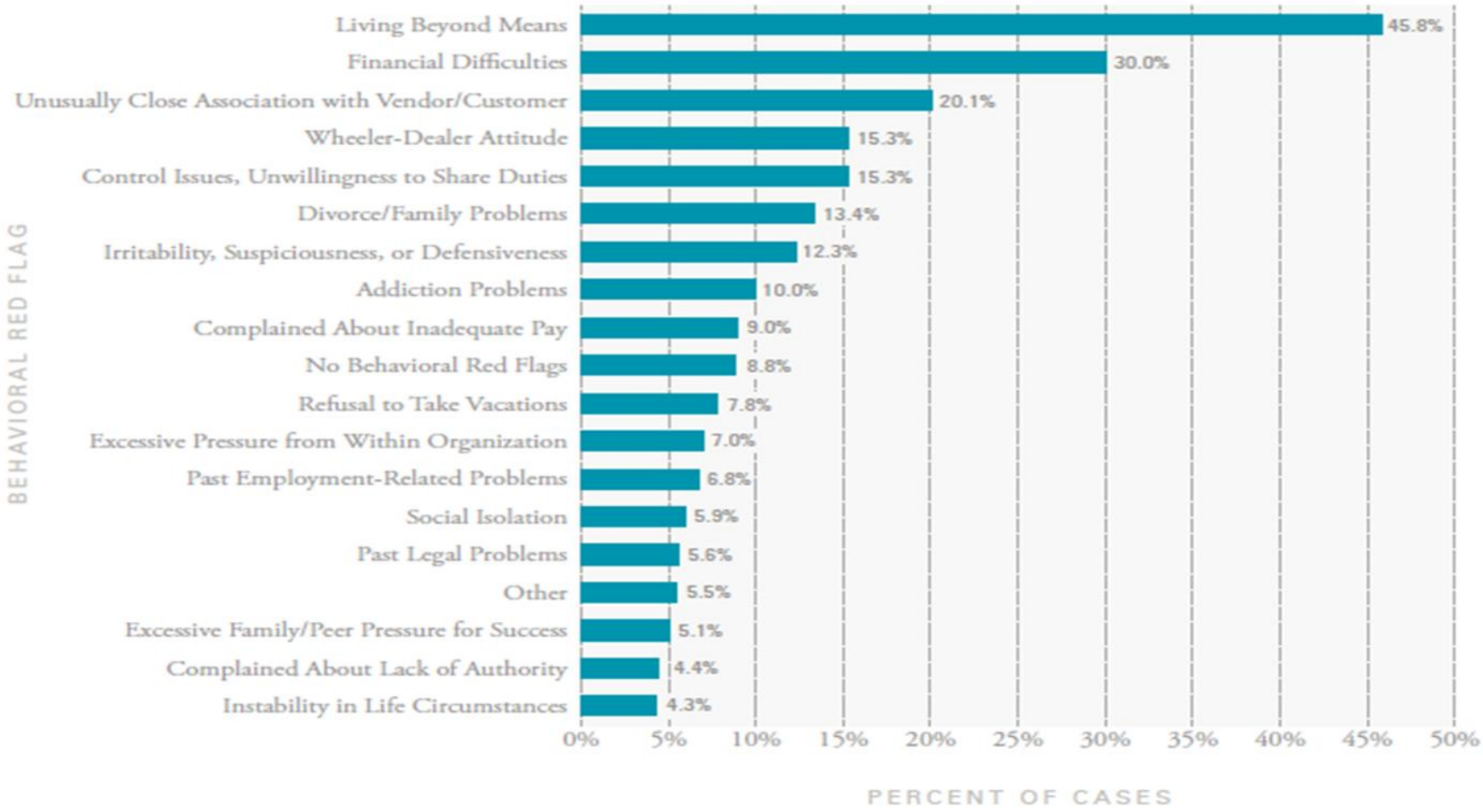
Source: ACFE 2016 *Report to the Nations*

Primary Internal Control Weakness Observed



Source: ACFE 2016 *Report to the Nations*

Behavioral Red Flags Displayed by Perpetrators



Source: ACFE 2016 *Report to the Nations*

2015 ABA Study on Deposit-Account Fraud

- The nation's banks **stopped more than $11 billion in fraudulent transactions in 2014**. Fraud against bank deposit accounts cost the industry **$1.9 billion in total losses, an increase from $1.7 billion** in 2012.
- Banks' sophisticated prevention systems and customer vigilance successfully **stopped 85 percent of fraud attempts in 2014**. The increase in fraud losses in 2014 was due to the number of **large-scale retailer data breaches**, which resulted in a significant increase in attempted debit card fraud.
- The survey -- which sampled 101 banks of varying sizes -- found that **debit card fraud accounted for 66 percent of industry loss**, with the majority of cases involving counterfeit cards, card-not-present transactions or lost or stolen cards. **Check fraud was the next most common fraud type at 32 percent**. Online banking and electronic transfers -- including wires and ACH -- accounted for 2 percent of industry loss.

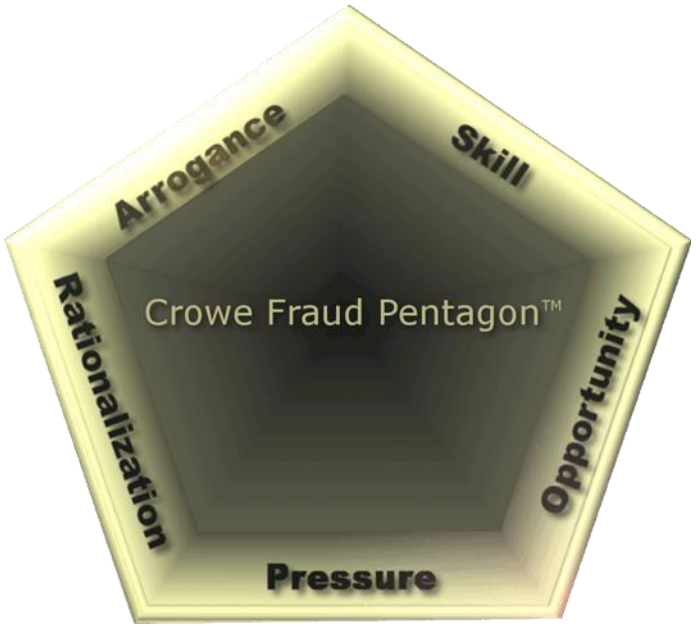
Internal Fraud Red Flags

Fraud Pentagon

Today's fraudster is clever, cunning, and operating in an environment ripe for criminal activity.

Economic unrest is making it easier for skilled employees to find ways to set fraud in motion--and they are finding cunning ways to do so.

Senior management has to take an offensive stance against fraud, and have a clear plan to minimize the impact when fraud does occur. The fraud triangle developed by Donald R. Cressey has now morphed into a Fraud Pentagon™.



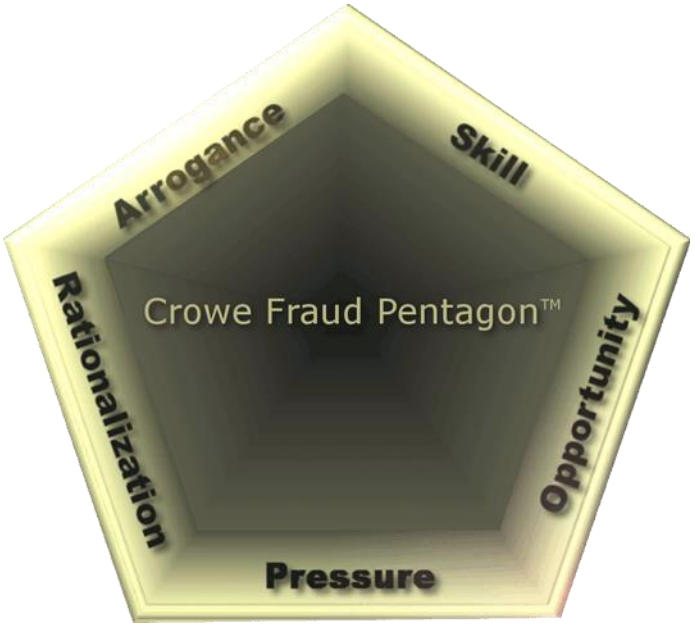
Five Elements of the Fraud Pentagon

- Knowing what may provoke an employee, even an otherwise lawful individual, to blur the line between legal and illegal activity is the key to effectively fighting fraud.
- Famed criminologist Donald R. Cressey first identified three elements - **opportunity, pressure (or motivation) and rationalization** - as the "fraud triangle" in the 1950s to explain why people commit fraud.
  - Fraud is more likely to occur when someone has an incentive (pressure or motive) to commit fraud, weak controls provide the opportunity for a person to commit fraud, and the person can rationalize the fraudulent behavior (attitude).

Five Elements of the Fraud Pentagon

In today's world, we have to expand the fraud triangle to a five-sided Fraud Pentagon™, where an employee's skill and arrogance must be factored into the conditions generally present when fraud occurs.

- Skill is an employee's ability to override internal controls, while arrogance is an attitude of superiority and entitlement that believes that the rules and controls do not apply.
- Talent and confidence play a major role in determining whether an employee today has what it takes to see fraud through.



Five Elements of the Fraud Pentagon

- Unchecked, these five elements—pressure, opportunity, rationalization, skill and arrogance—can provoke employees to commit fraud.

- Skilled staff with widespread access to bank information, a mindset of entitlement, and the confidence to pull it off compound the risk of fraud. Each of these drivers is present to some extent in banks at all times, but never more so than in the current pressure-filled economic environment.

Five Elements of the Fraud Pentagon

Arrogance Case Study

- A federal judge sentenced Edward J. Woodard Jr. (the head of failed Bank of the Commonwealth) to 23 years in prison.
- The former president and CEO of the Norfolk-based community bank was convicted at trial of 11 counts of bank fraud and related charges in a conspiracy that prosecutors said caused the bank to fail in 2011.
- The judge lectured Woodard before imposing the sentence, telling him he was **arrogant and indifferent as he ran "a continuing scheme of criminal conduct"** and had shown no remorse.

Five Elements of the Fraud Pentagon

Arrogance Case Study (Continued)

- "The court does not believe yet that you understand you committed crimes," Jackson told him. "None of us would be in this courtroom today if you had simply done the right thing."
- Woodard and former bank Executive Vice President Stephen Fields continued approving loans to developers and so-called "friends of the bank". Together, they caused $80 million in loan losses in the years before the bank failed.
- At the 10-week trial, a jury found that Woodard and Fields used a series of illegal banking practices to hide the true nature of the bank's losses from the board of directors, shareholders and regulators. The Federal Deposit Insurance Corp. has estimated the bank failure has cost it $334 million.

Characteristics In general, fraud perpetrators tend to be:

- In a position of trust
- Mostly high school educated
- Females versus males
- Have a family/children
- Involved in Community/Charity
- Motivated-often by some need
- Able to rationalize actions

Characteristics- Compared to other types of crime, white collar criminals are:

- A higher percentage of women than men
- More affluent
- Older
- More likely to be married
- Less likely to have used alcohol/drugs
- Had more children
- Heavier
- Completed more grades in school
- More likely to be church members

Source: "How to Detect and Prevent Business Fraud" Albrecht

Conditions Conducive to Fraud

- Weakness in the system of internal control -- segregation of duties and management overrides
- Independent and domineering individuals -- “nerves of steel”
- Weakness in management abilities of senior officers
- Poor maintenance of records in file storage areas
- Lack of effective internal audit
- Limited or no review of employee accounts
- Lack of Board involvement or weak Audit Committee
- Poor staff morale or high turnover
- Incomplete or missing documentation

Conditions Conducive to Fraud

- Unusual relationship between borrower and respective loan officer
- High levels of personal indebtedness by employee
- Accounts which do not balance, such as “suspense”, “official checks”, “cash items” or “clearings”
- Accounts which are force balanced and which have high volume of activity
- Decisions made by one dominant individual
- Out-of-area lending
- Frequent deviation from policies, procedures or common practices—lots of exceptions

Fraud “Red Flags”

- Unusually high personal debts
- Living beyond one’s means
- Excessive gambling habits
- Alcohol problems
- Drug problems
- Feeling of being underpaid
- Feeling of insufficient recognition for job performance
- Poor credit rating

Fraud “Red Flags”

- Consistent rationalization of poor performance
- Wheeler-dealer attitude
- Intellectual challenge to “beat the system”
- Criminal record
- Not taking vacations of more than two or three days
- A department that lacks competent personnel
- A department that does not enforce proper procedures for authorization of transactions
- No separation of duties between the accounting functions

Fraud “Red Flags”

- No explicit and uniform personnel policies
- Inadequate attention to details
- Placing too much trust in key employees
- Pay levels not commensurate with the level of responsibility assigned
- Failure to discipline violators of company policy
- Not adequately checking background before employment

Recent Fraud Schemes

Recent Fraud Schemes- FBI National Press Office- Fraudulent Electronic Funds Transfers

- Within the last several months, **the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials** belonging to small and medium businesses, municipal governments, and school districts.

- In a typical scenario, the targeted entity receives a **"spear phishing" e-mail which either contains an infected attachment,** or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware is installed on their computer. The malware contains a key logger which will harvest each recipient's business or corporate bank account login information.

- Shortly thereafter, the perpetrator **either creates another user account with the stolen login information or directly initiates funds** transfers by masquerading as the legitimate user. These transfers have occurred as both traditional **wire transfers and as ACH transfers.**

Fraudulent ACH Case Study

- A bank customer's laptop was hacked into.
- The person at the customer who inputs ACH transactions happened to look at her queue and noticed a $47,000 ACH for payroll that she had not input.
- She cancelled the transaction before it processed, so the fraud did not occur. The customer called the bank and was advised to have all of their computers scanned by their IT person.
- The customer did so and found numerous computers/laptops had viruses including the virus that copies password information (including answers to security questions). The customer has since cleaned their computers and installed virus protection software.

Fraudulent Wire Case Study

- A loan assistant received an email from a customer, responded to the email, but forgot to attach the document the customer requested.
- She called him and apologized for not attaching the information. The customer had no idea what she was talking about (i.e. he had not sent the email).
- A few days later, an email wire request for this customer came through. The loan assistant called the customer immediately to ask if he had made the request. He had not, so she did not process it.
- The email had the request and a facsimile signature saved in the signature matched the customer's identically.
- Somehow the fraudster had hacked into the customer's email and was able to send emails from their account as well as obtained bank employee names and email addresses.

Fraudulent Wire Case Study

- A bank suffered a $180,000 loss due to a wire fraud.
- The wire request was made over the phone to the Central Wire Desk and was covered by a Wire Agreement that includes unique PIN codes, Call-Back procedures, and recorded lines.
- The wire clerk followed all procedures correctly; however the fraudster had both **the unique PIN codes and had the call-back number re-routed (via the phone company) to his cell-phone**.
- The customer had lost their work laptop which included all the wire information (call-back number and PIN).

Fraudulent Electronic Funds Transfers- Prevention Techniques

- Basic Internal Controls:
  - Customer Verifications (ex. call-backs)
  - Scheduled Transfers

- There are several technology solutions that help banks determine when multiple parties are “on-line” at the same time. Also, “smart systems” are available to look at customer trends/patterns and will highlight unusual activity.

- Increased customer awareness and preventative techniques (security protocols, encryption, malware software, etc..).

Fraudulent Electronic Funds Transfers- Prevention Techniques

MEDIA RELEASE

Conference of State Bank Supervisors
United States Secret Service
Financial Services-Information Sharing and Analysis Center

State and Federal Authorities Combat Corporate Account Takeover

Corporate Account Takeover is a form of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts controlled by the thieves.

Sponsoring organizations created a Task Force aimed at mitigating the risks of Corporate Account Takeover. The Task Force developed **a list of nineteen processes and controls for reducing the risks of Corporate Account Takeovers**. These processes and controls expand upon a three-part risk management framework developed by the FS-ISAC, the US Secret Service, the Federal Bureau of Investigation, and the Internet Crime Complaint Center (IC3) . Fundamentally, a bank should implement processes and controls centered on three core elements: **Protect; Detect; and Respond**.

Fraudulent Electronic Funds Transfers- Prevention Techniques

PROTECT
Implement processes and controls to protect the financial institution and corporate customers.

P1. Expand the risk assessment to include corporate account takeover.
P2. Rate each customer (or type of customer) that performs online transactions.
P3. Outline to the Board of Directors the Corporate Account Takeover issues.
P4. Communicate basic online security practices for corporate online banking customers.
P5. Implement/Enhance customer security awareness education for retail and high risk business account holders.
P6. Establish bank controls to mitigate risks of corporate accounts being taken over.
P7. Review customer agreements.
P8. Contact your vendors to regularly receive information regarding reducing the risk of Corporate Account Takeovers.

Fraudulent Electronic Funds Transfers- Prevention Techniques

DETECT

Establish monitoring systems to detect electronic theft and educate employees and customers on how to detect a theft in progress.

D1. Establish automated or manual monitoring systems.
D2. Educate bank employees of warning signs that a theft may be in progress.
D3. Educate account holders of warning signs of potentially compromised computer systems.

Fraudulent Electronic Funds Transfers- Prevention Techniques

RESPOND

Prepare to respond to an incident as quickly as possible (measured in minutes, not hours) to increase the chance of recovering the money for your customer.

R1. Update incident response plans to include Corporate Account Takeover.

R2. Immediately verify if a suspicious transaction is fraudulent.

R3. Immediately attempt to reverse all suspected fraudulent transactions.

R4. Send a "Fraudulent File Alert" through FedLine.

R5. Immediately notify the receiving bank(s) of the fraudulent transactions and ask them to hold or return the funds.

R6. Implement a contingency plan to recover or suspend any systems suspected of being compromised.

R7. Contact law enforcement and regulatory agencies once the initial recovery efforts have concluded.

R8. Implement procedures for customer relations and documentation of recovery efforts.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 1

- A **former loan officer** at Colorado East Bank & Trust in Lamar, Colo., has admitted to his role in a **$1.2 million fraud scheme**.
- Christopher Tumbaga, 37, pleaded guilty to one count of bank fraud and one count of **receiving illegal kickbacks** in exchange for making loans,
- Tumbaga allegedly used his position as a loan officer at the $776 million-asset Colorado East to help his high school friend and co-defendant Brian Headle finance his real estate development business with fraudulently obtained credit.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 1 (continued)

- Prosecutors say that Tumbaga secured a $250,000 line of credit for Headle **based on false information along with more than 14 loans opened under multiple names.** In return, Tumbaga purportedly received more than $60,000 in kickbacks.
- "In order to get bank funds into Headle's hands, Tumbaga **submitted loan documents with falsified information, including fake financial statements** and documents identifying loan recipients as Headle's relatives, as a way to qualify the loans and skirt bank lending limits to single individuals,"

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 1 (continued)

- Tumbaga's misdeeds also allegedly include forging the bank president's signature in order to approve a loan and withdrawing $100,000 from a bank customer's line of credit so that Headle could pay down his bank debts, according to the release.
- Tumbaga's **faces up to 30 years** in federal prison for each of the two counts.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 2

- Citigroup Inc. said that it has discovered at least **$400 million in fraudulent loans** in its Mexico subsidiary and said employees may have been in on the crime.
- The bad loans were made to Mexican oil services company Oceanografia OCNGR.UL, a contractor for Mexican state-owned oil company Pemex PEMX.UL.
- Oceanografia borrowed from Citigroup's Mexican unit, Banco Nacional de Mexico, known as Banamex, using expected payments from Pemex as collateral.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 2 (continued)

- In recent weeks, Banamex learned that Oceanografia appeared to have falsified invoices to Pemex that were collateral for loans. The bank wrote down about $400 million of loans backed by the bogus invoices.
- Citigroup noted that a Banamex employee had processed the fraudulent invoices that appeared to be from Oceanografia, and said **that it is "not clear how many people were involved in the fraud."**

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 2 (continued)

- "I can assure you there will be accountability for those who perpetrated this despicable crime and any employee who enabled it, **either through lax supervision, circumvention of our controls or violating our code of conduct**," Citigroup's CFO stated.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 3

- Pennant Management, a Milwaukee investment firm, has said it invested $179 million, on behalf of clients, in securities backed by what turned out to be bogus USDA-guaranteed loans.
- This may be the largest loan fraud case in history.
- In a lawsuit, Pennant said it bought 26 fake loans from First Farmers Financial, a Florida firm that had been approved by the USDA to originate business-and industrial-loans through the agency's rural-development program.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 3 (Continued)

- Nikesh Patel, First Farmer's founder, allegedly forged the signatures of USDA officials to pass the fake loans off to Pennant.
- "We still feel that this is a full-faith-and-credit obligation, so we will continue to pursue the Department of Agriculture," said Mark Elste, Pennant's chief executive. "We have the best wishes of our clients in mind."
- Pennant's major complaint is that, unlike other government-backed loan programs, the USDA's programs have no central transfer agent or database to allow buyers to easily confirm that they're buying legitimate guaranteed loans.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 4

- A former loan officer at Wilmington Trust in Delaware is facing jail time after pleading guilty to bank fraud.
- Joseph Terranova conspired to extend credit to borrowers on terms that would not have been approved by the bank, the Justice Department charged in an indictment filed in April with the U.S. District Court in Wilmington.
- Terranova, who faces a maximum penalty of five years imprisonment and a $250,000 fine, also was accused of loaning money to customers to enable them to stay current on loans and caused the bank to misreport loans that were past due or troubled.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 4 (Continued)

- "We hope that in bringing these charges and securing a conviction, others will be deterred from engaging in similar conduct," U.S. Attorney Charles Oberly III said in a press release.
- Terranova "concealed the bank's true financial condition by engaging in 'extend and pretend' schemes to keep loans current and to hide past-due loans from regulators and investors," added Christy Romero, the special inspector general for Tarp.

Recent Fraud Schemes

Loan Documentation Fraud Prevention

- Direct Access to IRS Information
- Cross-Reference Disclosed Data
  - Name
  - Social Security number
  - Property Ownership
  - Tax Records
  - Employment History
- Strong Policies/Procedures
- No Policy Deviation, Without Approved Exception Documentation
- Effective Segregation of Duties/Responsibilities

Recent Fraud Schemes

Teller Cash Fraud

- A head teller stole over $7 million in cash from the cash vault at a $52-million credit union, forcing regulators to liquidate the 70-year-old institution.
- The teller confessed to stealing the money by walking out of work on a weekly basis with stacks of $100 bills, sometimes containing as much as $100,000.
- The teller was able to hide her thefts by making journal entries into the vault cash account whenever there was an audit or cash count by the credit union supervisory committee, and then making adjusted entries after those counts were completed.

Recent Fraud Schemes

Teller Cash Fraud (Updated)

- The teller was sentenced to eight years and eight months in prison and ordered to repay the stolen funds, but that is unlikely because she gambled them all away on Ohio River casino boats. She stole $7 million over 46 months, a total of about $150,000 every month, or about $37,000 every week.
- A bond company paid $2 million of the loss, but about $5 million had to be written off as an expense.
- The theft bankrupted the $52 million credit union, forcing it to merge with a larger credit union.

Teller Cash Fraud- Preventative Techniques

Surprise Cash Counts

- Include all cash supplies and cash items (returned checks, food stamps, redeemed bonds, etc..) assigned to the teller.
- Physically count each bill in the teller's possession. For Vault Tellers, physically count all loose bills and large bills ($50s and $100s); sample count strapped $20s, $10s, $5s and $1s ("fan" straps not counted). For any currency in "Fed wrapped" packages, open packages and "fan" bills to ensure legitimacy. For bagged shipments, either verify or control until pick-up and positively confirm with receiver. For bagged coin, "feel" contents (i.e. pennies are smaller than quarters) and verify on a sample basis.
- Balance cash counted back to the general ledger (i.e. the last time the teller actually balanced to the general ledger).

Teller Cash Fraud- Preventative Techniques (continued)

- If the teller was counted at any time subsequent to teller balancing (i.e., the teller balanced to the general ledger at 2pm, but the count was performed at 4pm), physically verify and control any post cut-off work (i.e. actual cash ins and cash outs). Do not rely on teller tape/machine totals, as these can be easily mis-represented.
- On the day following the cash count, ensure Teller Balancing did not make any adjustments to the teller's general ledger cash balance. If so, the individual responsible for performing the surprise cash count should investigate for propriety.
- On the day following the cash count, ensure there are no outstanding "Cash in Transit" on the general ledger for the teller. If there are, follow to ensure propriety

Recent Fraud Schemes

Certificates of Deposit Fraud

- A former branch manager for an Iowa Bank, pleaded guilty last week to selling **more than $4 million of phony certificates of deposit** to banks, credit unions and other entities, and now the buyers are trying to get their money back.
- A N.H. Credit Union, which bought a $99,000 CD it thought was issued by the Iowa Bank, is one of about **50 institutions victimized in the scam.** The credit union has filed a civil suit against the $890 million-asset Iowa Bank.
- The **former branch manager, who worked at the Iowa Bank for 28 years**, confessed to selling the phony CDs, then using two bank accounts in the names of deceased bank customers to launder the proceeds from the scam.

Recent Fraud Schemes

Certificates of Deposit Fraud

- Federal criminal charges were filed against a **47-year-old woman** who was charged with one count of embezzlement by a bank officer for allegedly **stealing hundreds of thousands of dollars from the CD accounts** of customers at a Marshall, Minnesota bank where she worked.
- The charges state that the bank officer embezzled the money for her personal use.
- If convicted, the bank officer faces a potential maximum penalty of 30 years in prison.

Recent Fraud Schemes

Certificates of Deposit Fraud

- A former Bank of America employee in Massachusetts has been sentenced to three to five years in state prison for **stealing more than $2 million from her clients.**
- Elaina Patterson, **54, used her position as a personal banker at a bank branch** in Reading, Mass., to swindle friends, family members and other customers
- She persuaded family members and friends to invest nearly $4.5 million in accounts that she claimed carried above-average interest rates of between 10% and 15%. After **issuing fake certificate of deposit receipts** and forms to convince her investors that the accounts were real, Patterson used their money to make payments to other investors and for her personal use.

Certificates of Deposit Fraud- Preventative Techniques

- Ensure the “vault supply” is maintained under dual control.
- Ensure the “working supply” is locked in the vault at night.
- Ensure the “working supply” is assigned to designated individual(s) for accountability. (Note: Normally, CSRs keep the working supply.)
- Someone independent of sales and custody (or dual control) daily/weekly verifies sold items from the working supply.
- For book entry certificates, controls should be in place to ensure that receipts given to customers for purchased certificates are compared to the deposit subsystem.

Recent Fraud Schemes

Fictitious General Ledger Entry

- A former assistant manager pleaded guilty Friday to stealing more than $525,000.
- The t**hirty-year-old** said she stole the funds by **creating fictitious accounts and false teller entries of unauthorized and fraudulent loans, deposits, check disbursements and transfers, in order to divert funds from customer accounts**.
- She also confessed to destroying records to conceal the scheme.

Recent Fraud Schemes

Fictitious General Ledger Entry

- The former **operations manager and head teller** were convicted of **stealing almost $600,000** by crediting their own accounts from general ledger funds.
- The 35-year-old former operations manager was sentenced to 12 months in prison and ordered to pay $395,000 in restitution.
- Earlier, the former head teller pleaded guilty to embezzling $185,000.
- Prosecutors said the employees had control over their own accounts and each woman stole the funds by **depositing money from general ledger accounts into their own checking accounts.**

Recent Fraud Schemes

Fictitious General Ledger Entry – Wire Transfer

- The former senior **VP and CFO** has been being charged with embezzling more than $339,000.
- Charges were filed against a **56 year old man**, who was accused of wiring money from the general account to a personal account in order to cover stock market losses, according to Jackson County prosecutors.
- If convicted, he could face 20 years in prison.

Recent Fraud Schemes

Fictitious Entry – Line of Credit

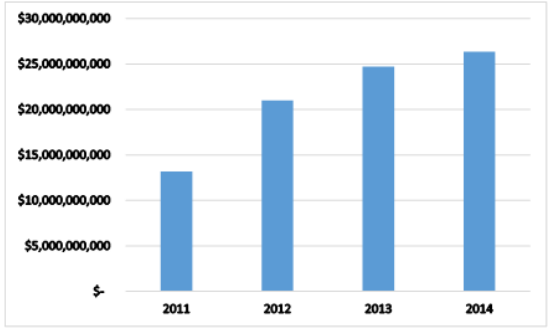
- A **vice president and branch manager** of a Laguna Hills branch was sentenced this afternoon to 41 months in federal prison and just over $1.8 million in restitution for **stealing nearly $2 million from a customer's account.**
- The branch manager **withdrew money from a line of credit** in the name of a trust that held an account at his bank. To cover up the scheme, he made interest payments on the money supposedly loaned to the trust.
- The branch manager "stole almost $2 million dollars from a client for **a personal venture where he was trying 'to hit it big,'"** according to a sentencing memo filed by prosecutors. "Much like gambling, [the branch manager] used the money on a start-up company that he was intimately involved in and where he could win or lose. Like most risky gambles, he ultimately lost it all."

Fictitious General Ledger Entry- Preventative Techniques

- Effective reconciliation of general ledger accounts:
  - All general ledger balance sheet accounts and in-house deposit accounts should be properly reconciled (the general ledger/in-house deposit account balance agreed to a subsidiary record, reconciling items adequately dated/described and followed to clearance, and the reconcilement form signed/dated by a preparer and approver) on a timely basis. In addition, reconciling items should clear the accounts timely and properly.
- Segregation of Duties
- Effective Supervision

Identity Theft- Statistics

Identity Theft / Fraud Statistics	Data
Average number of U.S. identity fraud victims annually	12,157,400
Percent of U.S. households that reported some type of identity fraud	7.5 %
Average financial loss per identity theft incident	$5,130
Total financial loss attributed to identity theft in 2014	**$26,350,000,000**
Total financial loss attributed to identity theft in 2013	$24,700,000,000
Total financial loss attributed to identity theft in 2012	$21,000,000,000
Total financial loss attributed to identity theft in 2010	$13,200,000,000



Percent of Reported Identity Thefts by Type of Fraud	Percent Reported
Misuse of Existing Credit Card	**64.1 %**
Misuse of Other Existing Bank Account	35 %
Misuse of Personal Information	14.2 %

Source: Statistic Brain Research Institute

Recent Fraud Schemes

Credit Card Identity Theft

- Six servers at several Washington-area high-end restaurants **stole credit card numbers from customers and ran up a $750,000 tab** at stores like Gucci and Barney's of New York.

- In New Orleans, a waitress was charged with **selling up to 50 customers' credit card information**. The waitress sold the numbers for **$220 apiece** to two men who provided her with a machine used to scan the credit cards.

- A Buffalo, N.Y., man was convicted of **hiring several cashiers at local restaurants and a department store to steal customers' credit card information.**

Recent Fraud Schemes

Credit Card Identity Theft – Case Study 1

- Barnes & Noble Inc. bookstores has informed federal law enforcement authorities that "a sophisticated criminal effort" has potentially exposed customers' credit and debit card information to **hackers who tampered with PIN pad devices at 63 of its stores.**

- The company's statement did not speculate on the number of potentially affected cardholders, but said it is working with issuers and payment card brands to identify accounts that may have been compromised to allow issuers to employ extra fraud security measures on potentially impacted accounts.

Recent Fraud Schemes

Credit Card Identity Theft - Case Study 2

- The FBI recently reported that it broke up a credit card gang for allegedly creating thousands of phony identities **to steal at least $200 million**.

- The fraudsters made **up more than 7,000 false identities** by creating fraudulent identification documents and credit profiles with the major credit bureaus, pumping up the credit of the false identities by providing false information to the credit bureaus about the identities' creditworthiness, running up large loans using the false identities and never paying back the loans. Of course, the higher the fraudulent credit scores, the larger the loans the fraudsters could obtain.

Recent Fraud Schemes

Credit Card Identity Theft - Case Study 2

- The fraudsters allegedly used **sham companies, complicit merchants and black-market businesses** to pull off their crimes.

- They purchased millions in gold, expensive cars, electronics and clothing. They set up bank accounts in Romania, China, Japan, Canada, the United Arab Emirates, India and Pakistan to wire millions of dollars.

- The U.S. Department of Justice (DOJ) charged 18 individual **between the ages of 31 and 74** with one count each of bank fraud. Each could be required to pay a $1 million fine and be sentenced up to 30 years in prison if found guilty.

Recent Fraud Schemes

Credit Card Identity Theft - Case Study 3

- The massive data heist at **Target stores** across the country was one of the largest security breaches of its kind, with at least 70 to 110 million customers being affected. Target said credit and debit card numbers were stolen, along with encrypted PINs for debit cards.
- Police in South Texas say account information stolen during the Target security breach **is now being divided up and sold off regionally** as evidenced by the arrest of two Mexican citizens in connection to 96 fraudulent credit cards.
- The computer network at **Neiman Marcus** was penetrated by hackers **as far back as July 2013**, and the breach was not fully contained until early January 2014.

Recent Fraud Schemes

Credit Card Identity Theft - Case Study 3

- According to a report released Friday by the cyber intelligence group IntelCrawler, **a 17-year-old Russian man**, username "ree4," appears to have been the author of the point-of-sale malware used for the Target, Neiman Marcus, and six other large U.S. retailers, maybe more.
- IntelCrawler says that ree4 sold his "BlackPOS" malware **to more than 60 Eastern European cybercriminals**, plus some in other regions.
- But ree4 doesn't seem to have personally taken part in the Target or Neiman Marcus hacks beyond writing and selling the malware.

Recent Fraud Schemes

Debit Card Identity Theft

- It took **13 hours for eight people to steal $2.4 million in New York City through 3,000 ATM withdrawals**. The DOJ charged them for belonging to a New York cell of an international operation that stole approximately **$45 million from two banks by using stolen prepaid debit card data**.
- The attackers are accused of breaching the card processors' networks, where they removed transaction limits from prepaid card accounts and then encoded numbers swiped from the banks onto magnetic-stripe cards. The people arrested in New York allegedly used the cloned prepaid cards at ATMs.

Recent Fraud Schemes

Rob Banks from the Inside
USA Today 2/17/2015

- Kaspershy Lab, a Moscow based security firm, released a report showing that a gang of international hackers stole approximately **$1 Billion from over 100 banks over 30 countries** by using malware to take over the banks' internal operations.
- The gang used **phishing and other social engineering techniques to infect bank employee computers**. Once a virus infected a single bank computer, it then spread throughout the bank's internal network giving the gang access to customer data and various areas of bank operation.
- One scheme was to use the gained access to **infiltrate the bank's ATM network and dispense cash remotely**. One bank lost up to $7.3 million this way.
- Losses per bank ranged from **$2.5 million to $10 million**.

Recent Fraud Schemes

Identity Theft – Counterfeit Check Fraud

- A group of 18 defendants were charged with operating an identity theft ring that used information obtained from tellers at New York City banks to generate counterfeit checks from hundreds of accounts.
- Prosecutors charged that **the ring collected personal and bank account information belonging to 500 people by paying off bank tellers** and also by buying copies of legitimate payroll checks. Thousands of counterfeit checks were manufactured with the information.
- From a Bronx apartment known as **"the Lab,"** the leaders of the ring used specialized computer software, scanners, printers, check stock, magnetic ink, and company logos found on the Internet to produce the fake checks, which were cashed by "soldiers" enlisted for the scheme.

Recent Fraud Schemes

Real Estate Broker Identity Theft - Case Study 1

- The settlement agent receives a message from the buyer's real estate agent **instructing them to release the earnest money** and deposit back to their client. The email gives wire instructions for the buyer's account.
- It later turns out that **the actual real estate agent did not send this message**, though it came from their email address, and even had other attachments relating to the transaction.
- The buyer's real estate agent's **email account had been "high jacked"** and a criminal was watching the email traffic in order to intervene at just the right moment and send their own message via the real estate agent's account. There is no way to distinguish that it is not really from the true real estate agent.

Recent Fraud Schemes

Real Estate Broker Identity Theft - Case Study 2

- The settlement agent sends the real estate agent **wire instructions for the buyer's earnest money** deposit and final funds to close.
- The criminal who has **hacked the email account** then sends amended wire instructions to the buyer from the real estate agent's email address, with a different bank account on it.
- Or, the settlement agent never sent wire instructions to the real estate agent, but the criminal watches the account and at just the right time, emails wire instructions from the real estate agent's account with a title company name on it, with a bank account that is not with any title company. The funds never make it to the settlement agent

Identity Theft- Preventative Techniques

- Enhanced customer awareness and training.
- Compliance with Section 114 (Red Flag Guidelines) and Section 315 (Reconciling Address Discrepancies) of the Fair and Accurate Credit Transaction Act (FACT Act). Including monitoring of 26 known "red flags", grouped as follows:
  - Alerts, Notifications or Warnings from a Consumer Reporting Agency
  - Suspicious Documents
  - Suspicious Personal Identifying Information
  - Unusual Use of, or Suspicious Activity Related to, the Covered Account
  - Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

Identity Theft- Preventative Techniques (continued)

- Multifactor Authentication - Using more than one of the following ways to confirm identity:
  - What you know (user ids, pin numbers, passwords)
  - What you have (card, token)
  - What you are (your fingerprint, retina pattern)
  - Shared Secret—Prompts a user to enter multiple pieces of information that only that user would know (e.g., mother's maiden name, last transaction amount, etc..) (Passmark [RSA], custom solutions)
  - GeoLocation—Confirming that the location from which the user authenticates is consistent with trends or other information on hand about the user
  - Related foot-printing techniques include checking time of day, computer or MAC Addresses, etc.. (Passmark, Cyota—both acquired by RSA in 2006)

Identity Theft- Preventative Techniques (continued)

HSBC Introduces New Security
For Online Banking

HSBC Bermuda is introducing a new security device to give Personal Internet Banking customers an extra layer of protection from fraudsters. The security device creates a unique security code every time the customer logs in to Personal Internet Banking.

Identity Theft- Preventative Techniques (continued)

Harland Clarke Redesigns Check Boxes for Security

Harland Clarke Corp. said that it **is replacing its brick-shaped check boxes with a new package that it says offers security and other advantages.**

Rather than stacking checks in a conspicuous and familiar package, Harland Clarke is shifting to a package it calls CheckFolio. The new folio design is "an 'outside-the-box' approach" to check packaging, said Gwen Cuffie, Harland Clarke's vice president of product solutions and marketing, in a press release.

The security benefits of the package are its tamper-evident wrapping and a shape that is more easily hidden in the home, such as by placing the folio among books on a bookshelf or among documents in a filing cabinet. This design change is in response to consumer requests for more secure packaging, the company says on its website.

Harland Clarke, of San Antonio, Texas, says it will transition its products to the new design over the course of the year. The company says CheckFolio is also a more environmentally friendly design because it uses less material than a standard check box does.

Phishing Scams

JPMorgan Victim to Email Phishing Scam (American Banker)

JPMorgan customers were targeted with a phishing scam earlier this week aimed at obtaining online banking credentials.

Security researchers from the email provider Proofpoint said the "Smash and Grab" phishing campaign tries to lure individuals to click on a malicious link in an email that looks like an authentic message from JPMorgan.

Even if customers do not proceed to sign into their JPMorgan bank account, the fraudsters try to automatically install the Dyre banking Trojan on their computers to steal passwords from other institutions.

JPMorgan Chase, which is the top U.S. bank with $2.5 trillion in total assets, has more than 50 million customers. The bank believes most of the spam was eliminated by fraud filters. Proofpoint reported that about 150,000 emails were sent on Tuesday.

Phishing Scams

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)

SUBJECT: Consumer Alert

Summary: *E-mails fraudulently claiming to be from the FDIC are attempting to get recipients to click on a link, which may ask them to provide sensitive personal information. These e-mails falsely indicate that FDIC deposit insurance is suspended until the requested customer information is provided.*

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports from consumers who received an e-mail **that has the appearance of being sent from the FDIC.** The e-mail informs the recipient that "in cooperation with the Department of Homeland Security, federal, state and local governments…" the FDIC has withdrawn deposit insurance from the recipient's account "due to account activity that violates the Patriot Act." It further states deposit insurance will remain suspended until identity and account information can be verified using a system called "IDVerify." If consumers go to the link provided in the e-mail, it is suspected they will be asked for personal or confidential information, or malicious software may be loaded onto the recipient's computer.

This e-mail is fraudulent. It was not sent by the FDIC. It is an attempt to obtain personal information from consumers. Financial institutions and consumers should NOT access the link provided within the body of the e-mail and should NOT under any circumstances provide any personal information through this media.

Phishing Scams

Dear Members:

Alert: Fraudulent "Phishing" Scam Email Designed to Look Like it is from AICPA

On Thursday, February 16, 2012, the AICPA became aware of a fraudulent email using an AICPA banner and referencing the recipient's possible involvement in an unlawful income tax refund activity that was sent to numerous individuals, CPAs, non-CPAs and members of the general public.

The fraudulent email is not from the AICPA. The AICPA and CPA2Biz have conducted an intense review of our internal IT systems and, based on our knowledge of this scheme, have concluded that **none of our systems have been compromised**.

Yesterday we posted an alert on AICPA.org and our social media properties. You may want to ensure that your company, employees and clients are aware of this "phishing" email scam. The Better Business Bureau has an overview of the issue on their website. Do not open any attachment or click on any link as the email may contain a virus. Delete it immediately.

While the exact source has not yet been determined, we are actively investigating the situation.

We will share any updates regarding this matter directly on our website.

If you wish to speak with an AICPA member service specialist, call 888.777.7077 and select option 1.

Phishing Scams

OCC Issues Alert on Fraudulent Letters

The Office of the Comptroller of the Currency issued an alert about fraudulent letters -- distributed via **email, fax, or postal mail** -- involving funds purportedly under the control of the OCC and other government entities.

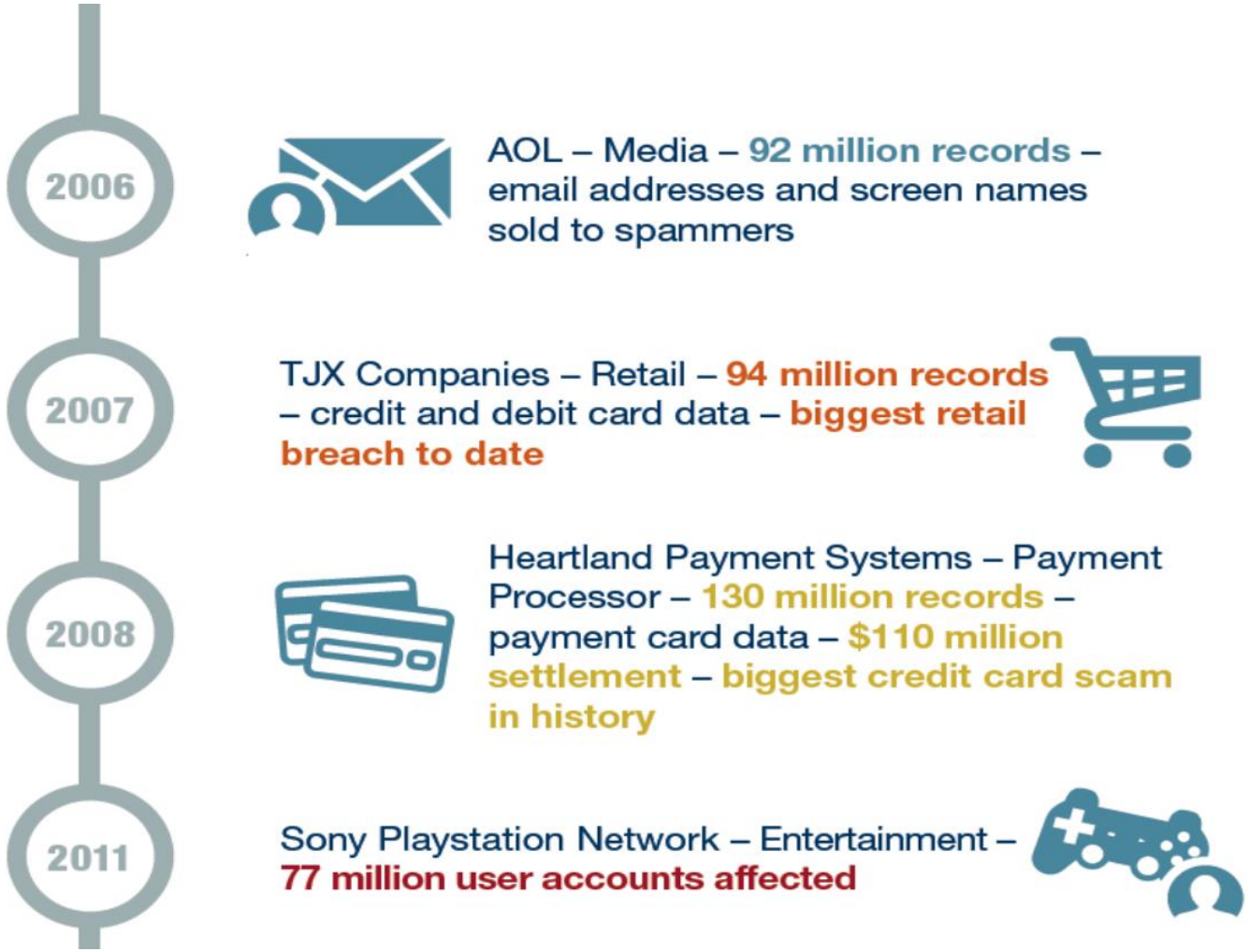
"The letters may indicate that funds are being held by the Halifax Bank, London, England, and that the recipient will be required to pay a mandatory express service charge to have the funds released," the OCC said. The letters are "being sent to consumers in an attempt to elicit funds from them and to gather personal information to be used in possible future identification theft."

The letters also contain forged signatures of former OCC officials and a fictitious email address. The agency emphasized that any document claiming that the OCC is involved in holding any funds for the benefit of an individual or entity is fraudulent. "The [agency] does not participate in the transfer of funds for, or on behalf of, individuals, business enterprises or governmental entities," the OCC said.

Phishing Scams- Preventative Techniques

- Never follow a link in an email and reveal personal data. Go to websites independent of the email.
- Use non-internet means (ex. a phone call) to verify a source. In doing so, do not accept a phone number in the email (use outside source).
- Ensure that email firewalls are current and frequently tested.
- Install automated email verification and email filters.
- Adopt user education and training, including periodic testing of employees.
- Cordon off or “sandbox” suspect emails.

CyberSecurity Threats- A History



CyberSecurity Threats- A History

2007
2013

Multiple companies including 7-Eleven and JCPenney – **160 million records** – credit and debit cards – **largest hacking scheme** ever prosecuted in the U.S.

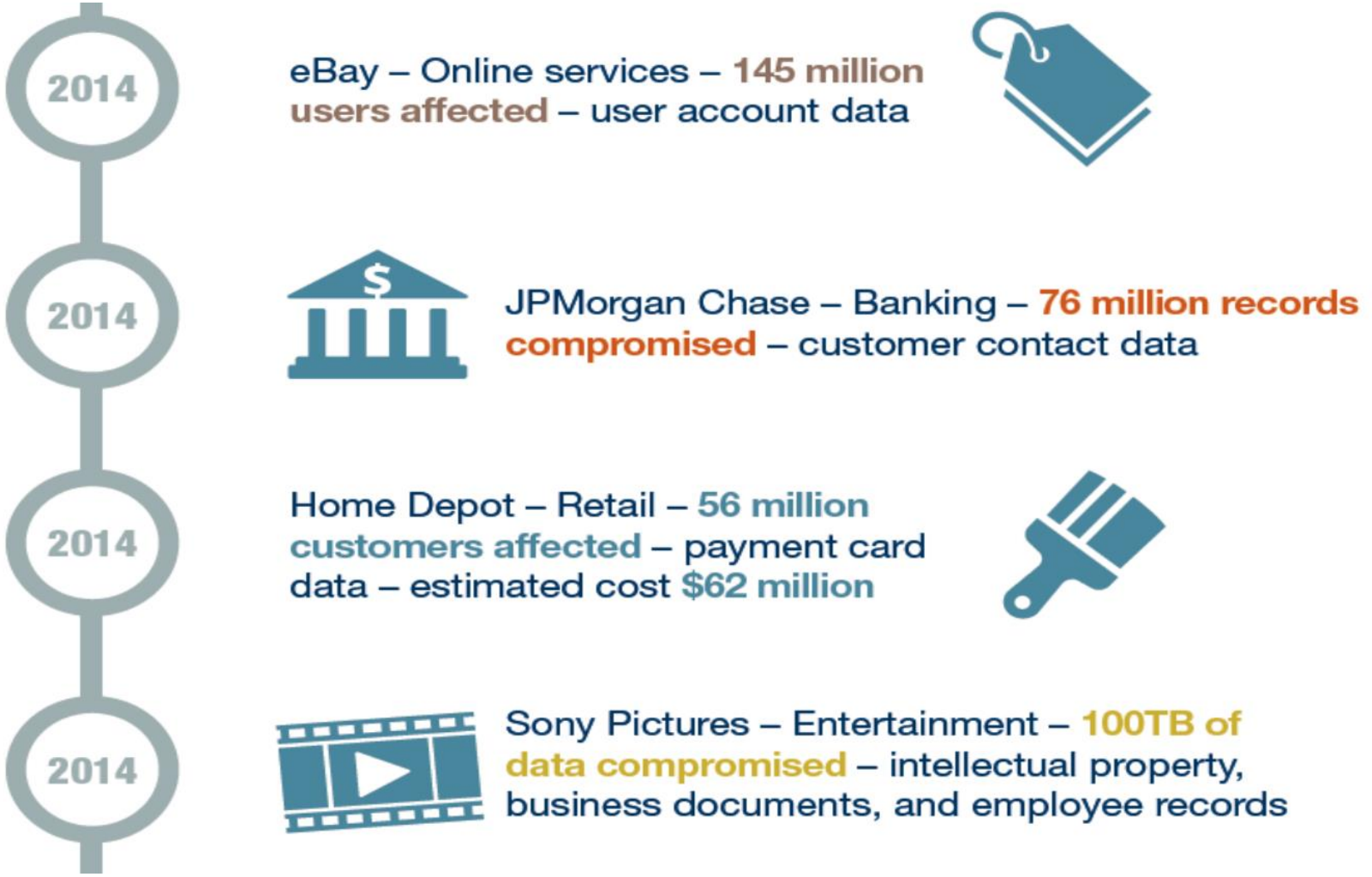
2013

Adobe Systems – Online services – **36 million customers affected** – credit and debit card data and user accounts

2013

Target – Retail – **at least 70 million customers** – customer payment and contact data compromised – **estimated cost $148 million**

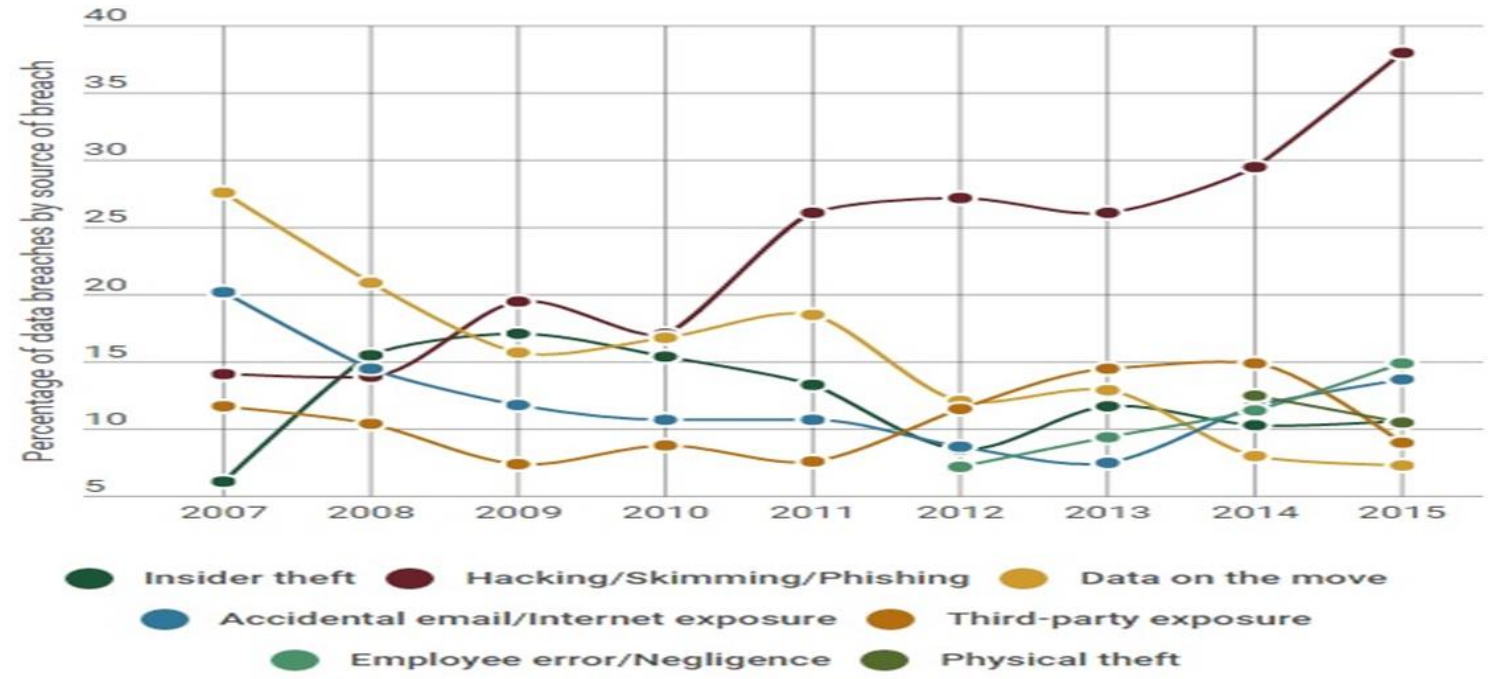
CyberSecurity Threats- A History



CyberSecurity Attack

Hack Attack

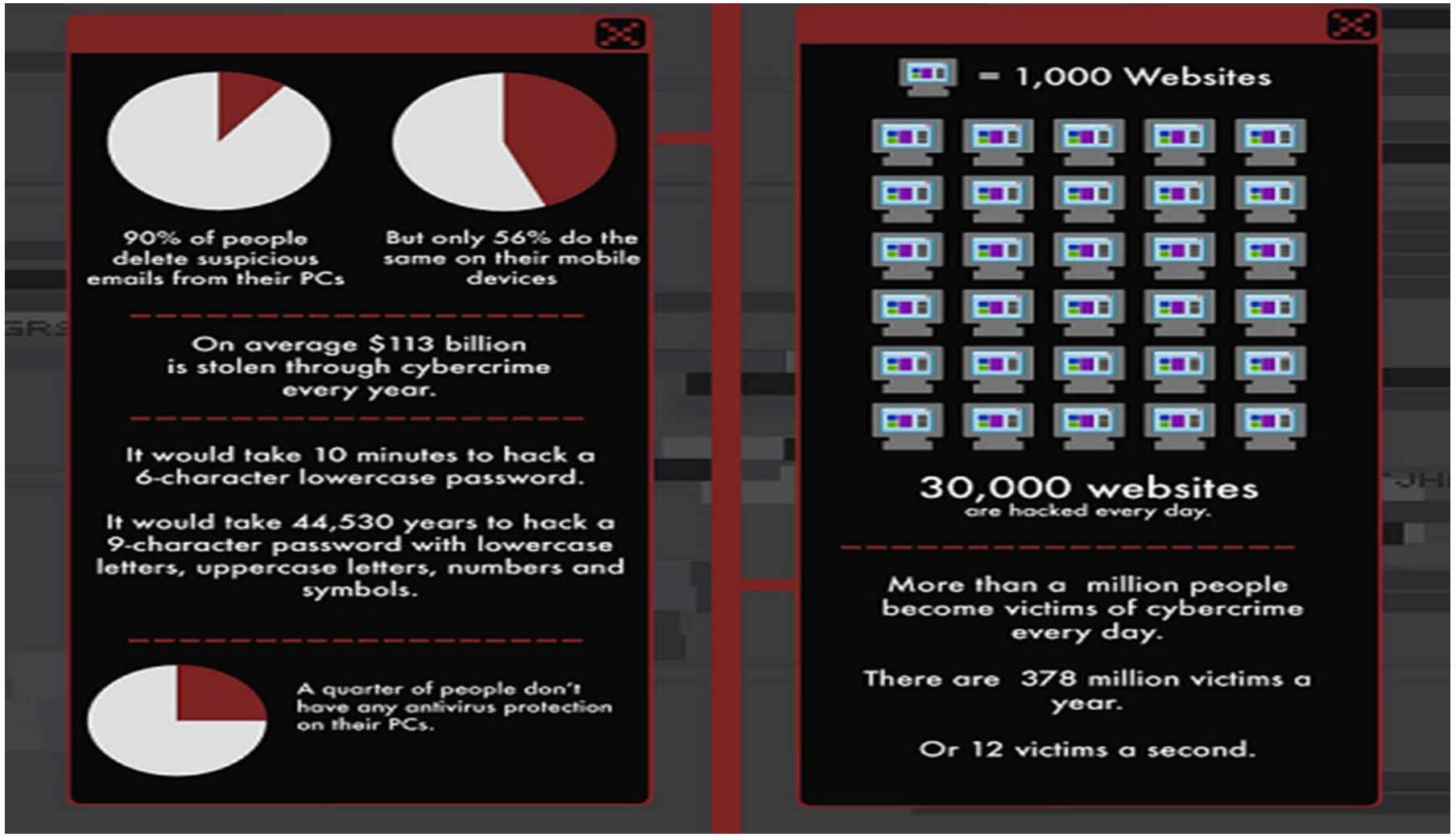
Hacking, phishing and skimming attacks account for a fast-growing share of all U.S. data breaches, amounting to nearly 300—nearly 4 in 10—in 2015.



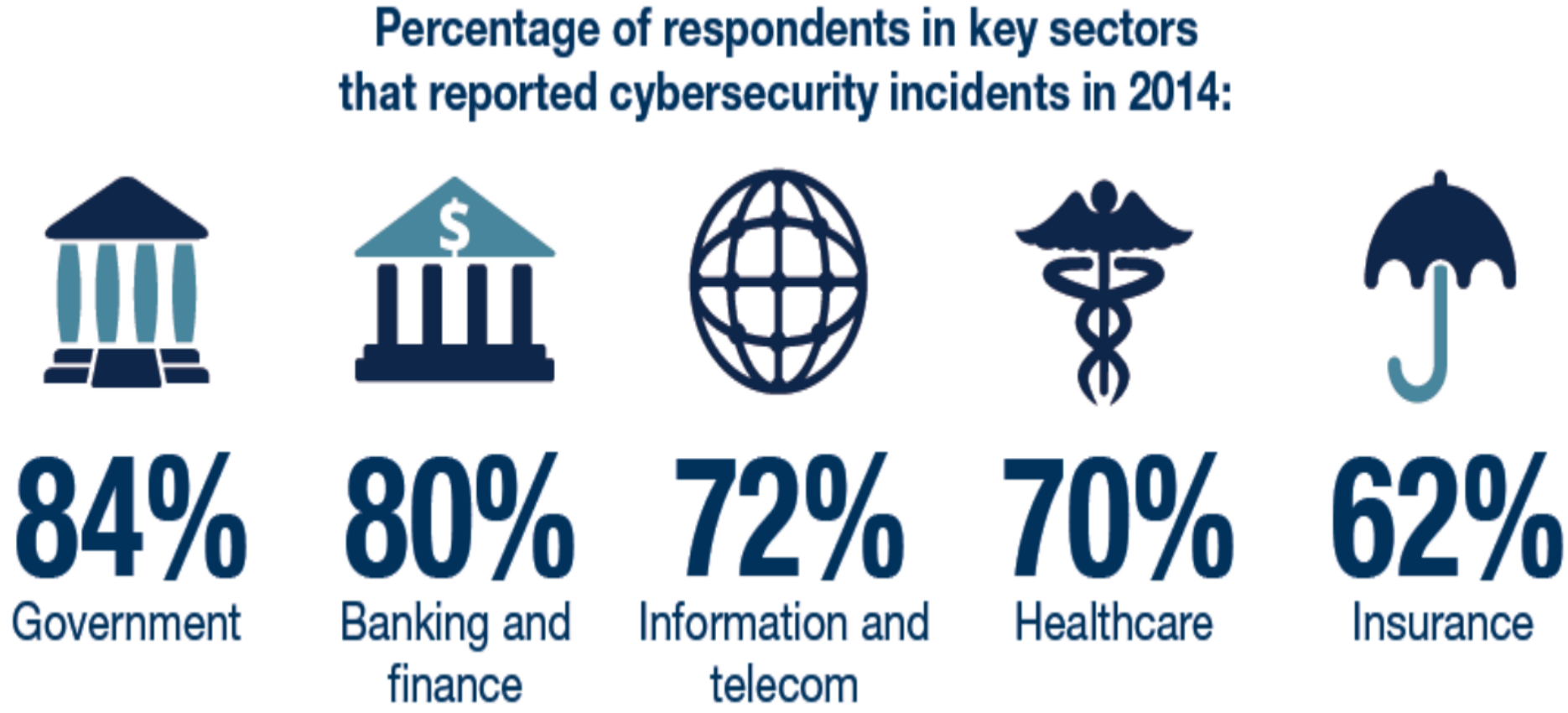
Source: Identity Theft Resource Center

ABA BANKING JOURNAL

CyberSecurity Threats Today



CyberSecurity Statistics

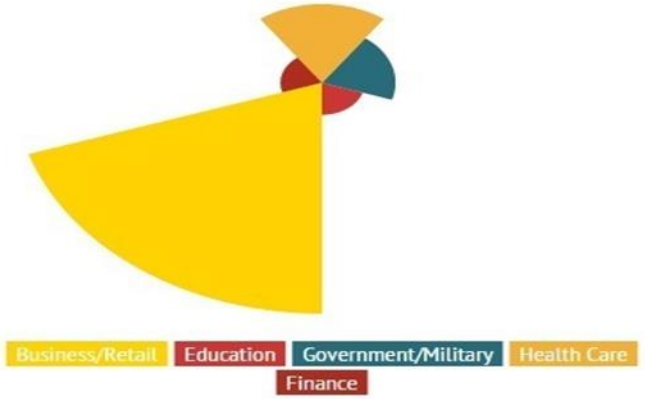


CyberSecurity- Statistics

Per the American Banker Association – November 2014

Retailers and other businesses have accounted for 32% of data breaches in 2014…

…but they have accounted for 82.6% of the total compromised customer records.



Source: Identity Theft Resource Center.

American Bankers Association

CyberSecurity Threats

Biggest Cyber Threats

- **Mobile Malware**: Studies show that more than 90% of malware is likely to be focused on Androids with a "high probability" of the first appearance of a mass "worm" spreading itself through text messages.
- **Medical Identity Theft**: The Ponemon Institute stated that 94% of Medical Organizations that reported in their recent study had a least one data breach in the last two years.
- **Targeted Attacks**: Also know as "Spear Phishing" or "Whaling" will continue to be on the rise. These are sophisticated attacks on "C Suite" and key operational personnel (ex. the Payroll Clerk).
- **Ransom Malware**: Malware designed to "capture" data from individuals and businesses and hold it hostage until a fee is paid.
- **Intercepting Text Messages**: Using malware that can read text messages of others, like authentication codes sent by banks to verify on-line transactions.
- **Hacktivism**: Vigilantly data or disruption of service attacks.
- **Cloud Attacks**: Attacks to stored data via cloud technology. This would be "hyper jacking" since thousands of users could be affected.

CyberSecurity Threats

Cyber Attacks Involving Extortion

- The FFIEC recently issued a statement to notify financial institutions of the **increasing frequency and severity of cyber attacks involving extortion**.
- Financial institutions should develop and implement effective programs to ensure the institutions are able to identify, protect, detect, respond to, and recover from these types of attacks.
- Cyber criminals and activists use a variety of tactics, such as **ransomware, denial of service (DoS), and theft of sensitive business and customer information to extort payment** or other concessions from victims.
- In some cases, these attacks have caused significant impacts on businesses' access to data and ability to provide services. Other businesses have incurred serious damage through the release of sensitive information.

Recent Fraud Schemes

Hacktivists Threaten Five Banks with More Cyberattacks

- Hacktivists who claim responsibility for a series of cyberattacks on at least ten banks worldwide are vowing to reprise the electronic assaults on five of them in the coming days.
- The al Qassam Cyber Fighters Group said late Monday it would target JPMorgan Chase (JPM), Bank of America (BCA), U.S. Bank (USB), PNC Financial (PNC) and SunTrust (STI) as part of a second phase of its operation.
- The group added that if the "film is going to be eliminated from the Internet, the...attacks also will be stopped."
- For its part, YouTube told American Banker in November the trailer comports with the company's content guidelines.
- The attacks would constitute a repeat assault on the banks, which all saw their websites slow during a string of so-called denial of service attacks in September that U.S. officials called unprecedented in their scale and speed.
- Other banks that have endured the assaults include Wells Fargo (WFC), BB&T (BBT), HSBC (HBC), Capital One (COF) and Regions Financial (RF).

Recent Fraud Schemes

N.Y. Fed Points Finger at Swift in $80 Million Cybertheft (American Banker)

- **Hackers broke into the Central Bank of Bangladesh's servers and stole its credentials for Swift payment transfers**. The hackers used those credentials **to wire $80 million from the bank's account at the New York Fed** to accounts in the Philippines and Sri Lanka, Agence France-Press reported. The Fed says the Society for Worldwide Interbank Financial Telecommunication is to blame
- "To date, there is no evidence of any attempt to penetrate Federal Reserve systems in connection with the payments in question, and **there is no evidence that any Fed systems were compromised**," a spokesperson said. "The payment instructions in question **were fully authenticated by the Swift messaging system** in accordance with standard authentication protocols. The Fed has been working with the central bank since the incident occurred, and will continue to provide assistance as appropriate."

Recent Fraud Schemes

N.Y. Fed Points Finger at Swift in $80 Million Cybertheft (American Banker)

- Sending a message through the Swift system generally requires an identification number, an account number, and a password. Swift reviews and verifies the message for completeness**. If no second factor of authentication was required for the Central Bank of Bangladesh's transactions, then the hackers could meet Swift's requirements by using the information they stole from the Bangladesh bank.**
- The **New York Fed did see signs of unusual activity after the fact** — Bangladeshi officials told Reuters that the unusually high number of payment instructions and the transfer requests to private entities, rather than other banks, **made the Fed suspicious and that it alerted the Bangladesh bank. But its fraud detection systems did not catch the transactions before they went through.**
- While four requests to transfer a total of $81 million to the Philippines went through, **a fifth, for $20 million, to a Sri Lankan nonprofit organization, got held up because the hackers misspelled the name of the organization**, Reuters reported. Instead of "foundation," the hackers typed "fandation." This prompted a routing bank, Deutsche Bank, to seek clarification from the Bangladesh central bank, which stopped the transaction.

Breaches By the Numbers

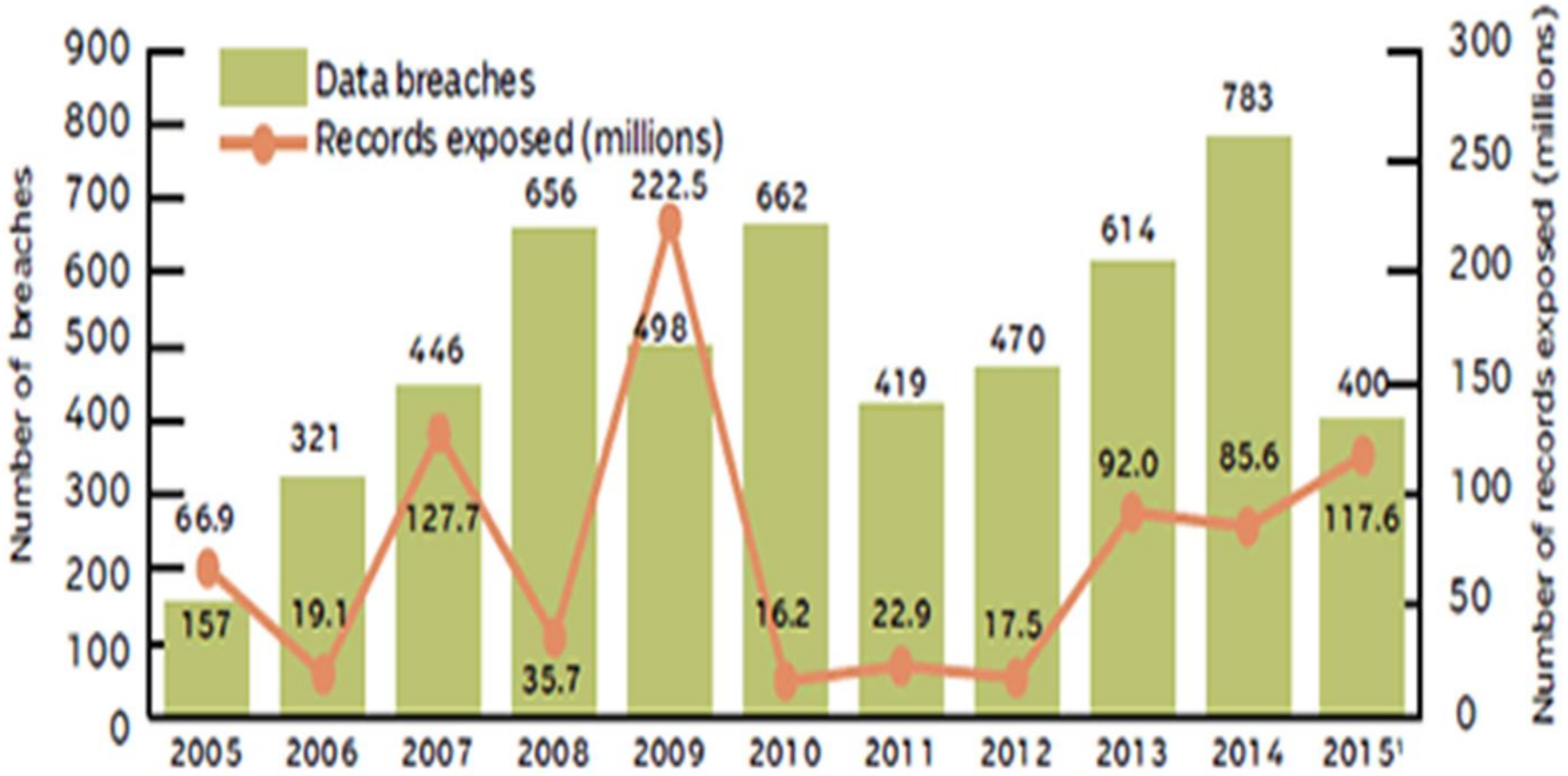
- 43% of companies had a data breach in the past year (of 567 surveyed)
- Only 15% of all breaches that occur, make the media
- 600-700 breaches reported nationally on an average year

Data Breach Costs

- Average cost per record lost in 2015 = $145

Figure 9. Impact of eight factors on the per capita cost of data breach

Data Breach- Statistics



(1) As of June 30, 2015.
Source: Identity Theft Resource Center.

Recent Fraud Schemes

Data Breach

- Heartland Payment Systems Inc. said that cyber criminals compromised its computer network, gaining access to customer information associated with the 100 million card transactions it handles each month.
- The company said it couldn't estimate how many customer records may have been improperly accessed, but said the data compromised include the information on a card's magnetic strip — card number, expiration date and some internal bank codes — that could be used to duplicate a card.
- Heartland processes transactions for more than 250,000 businesses nationwide, including restaurants and smaller retailers.
- Avivah Litan, an analyst at research company Gartner, called it the largest card-data breach ever, based on her conversations with industry executives.

Recent Fraud Schemes

Data Breach Response

- Forcht Bank said that it had been informed of the breach by its debit card processor, Heartland Payment Systems . The breach would allow the hackers to create duplicate debit cards.
- About 8,500 of Forcht's cards could potentially be impacted, but the bank said no fraudulent activity on the cards has been reported.
- The bank said it will issue new cards and is notifying all affected customers by mail and phone calls.
- A spokesman for Forcht said it had been told that other banks were likely involved, but Forcht wanted to be "out in front" in informing its customers.

Recent Fraud Schemes

Data Breach Response

- Heartland Payment Systems Inc. has begun commercial testing of its end-to-end encryption system for card transactions.

- "Our fully encrypted end-to-end terminal solution is currently being-beta tested at 10 merchant locations," Robert O. Carr, Heartland's chairman and chief executive officer, said during a conference call to discuss the Princeton, N.J., transaction processor's second-quarter results. "We expect to be offering merchants our new 'E3' product with what we believe **will be the highest level of data security in the market** in the near term."

Recent Fraud Schemes

Data Breach Update

- Heartland Payment Systems has reported it suffered another data breach last month.
- A May 8 incident in its Santa Ana, Calif., office that may have compromised customers' personal information, including social security numbers and bank account information.
- Heartland did not indicate the size or scope of the breach.
- **Password protected company computers were stolen**, but Heartland claims it sees no evidence to suggest the data stored on them were or will be used.
- The company is working with the risk mitigation services company Kroll to offer customers identity theft protection **for a year at no cost.**

CyberSecurity- Preventative Techniques

- Implement a formal and up-to-date cybersecurity program.
- Designate a cybersecurity leader with appropriate authority and resources.
- Inventory, assess, and prioritize IT systems, data stores, vendors and suppliers, and potential cybersecurity risks.
- Employ procedures to detect and contain cyberattacks – not just to prevent them.
- Create and maintain a plan for responding to cybersecurity incidents.
- Use testing, assessments, and continuous improvement as core elements of your cybersecurity plan.

CyberSecurity- Preventative Techniques

- Institute a cybersecurity culture, coming from the Board down, and integrate cybersecurity into your enterprise risk management (ERM) program.
- Improve education and training across the organization.
- Keep pace with cyber threats; banks must stay aware and inform employees of new threats.
- Prioritize areas in order to allocate the appropriate resources to mitigate the largest risks.
- Explore cybersecurity insurance.
- Evaluate whether employees should be permitted to use personal devices to connect to the network, as this may inadvertently open the Bank to additional risks.
- Utilize the Federal Financial Institutions Examination Council (FFEIC) assessment tool.

CyberSecurity- Preventative Techniques

- Compliance with all aspects of the Gramm-Leach-Bliley Act (GLBA).
- If a breach occurs, follow FFIEC Guidance—Security Breaches:
  - "Assess the nature and scope of an incident and identify what customer information systems and types of customer information have been accessed or misused"
  - "Notify its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information."
  - "File a timely Suspicious Activity Report (SAR), and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities."
  - "Notify customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it."

Questions?

Matthew G. Davis, CIA
Crowe Horwath LLP
matthew.davis@crowehorwath.com
Mobile: 864.630.8357
Direct: 404.442.1630

Joseph Garcia, CPA
Crowe Horwath LLP
Joseph.Garcia@crowehorwath.com
Main 630-574-7878
Direct 630-575-4343