Integrated Risk & Control @ FHLBC

Challenges of Success

Tom Harper
Executive Vice President and Chief Audit Executive
June 2018

FHLB Chicago | Federal Home Loan Bank of Chicago

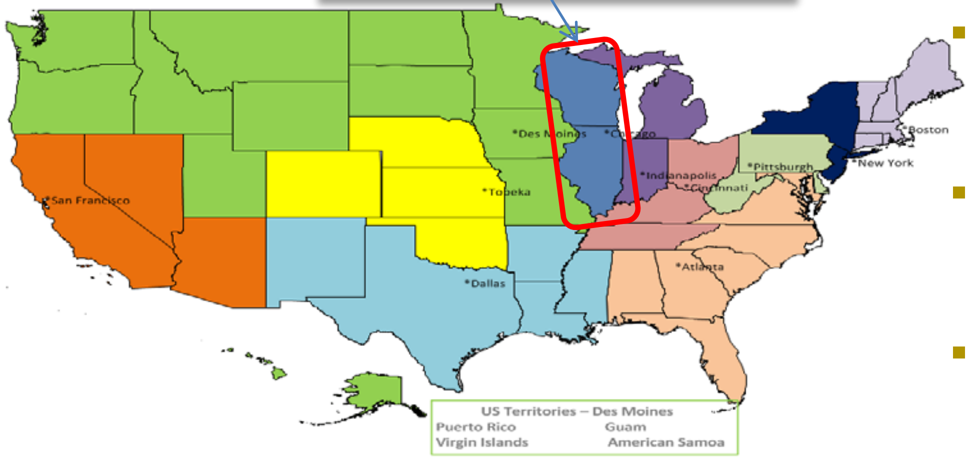
Objectives

- Understand why integrated risk management is valuable especially in the environment
- Understand the roles individuals play in the program
- Provide context to the way our program is designed
- Demonstrate how governance and risk management today requires that our processes are intuitive and embedded in our business rather than being a stand alone objectives
- Understand the challenges as a successful GRC program matures

The Federal Home Loan Bank (FHLB) System

FHLB Overview

FHLB Chicago
- **Includes IL and WI**



Members include banks, thrifts, credit unions and insurance companies

- Each FHLB is an SEC-registered, privately managed cooperative owned by members* in its district
- Each FHLB is governed by a separate board of directors, but regulated by a single regulator, Federal Housing Finance Agency
- The 11 Home Loan Banks comprising the FHLB System provide liquidity and funding solutions to nearly 7,500 members
- FHLBs are significant contributors to affordable housing and economic development initiatives across the nation
- As a Government Sponsored Enterprise, the FHLB System has good access to capital markets which provides competitively priced funding

FHLB-Chicago Overview

$70 billion wholesale bank

Over 740 members in Illinois and Wisconsin

Our members are our shareholders

Value Proposition:

Reliable Low-cost funding and liquidity

Secondary mortgage market products

Grant programs to support community investment

FHLBC is a cooperative that partners with our member shareholders to provide products and solutions that support their business growth

Escalating regulatory expectations

Increased market complexity and performance needs necessitate further advancement in risk management

United States			International	
Federal Reserve Enhanced Prudential Standards	OCC Heightened Standards	CCAR – Greater focus on internal controls	CRD IV	BCBS Principles on bank corporate governance

- Financial Institutions will have to demonstrate not just technical compliance, but also that their boards are capable of effectively challenging management decisions
- These regulations have increased both director responsibility and potential liability
- Elevated responsibility may have some unintended consequences:
  - **80 percent** of financial sector nonexecutive directors surveyed[1] said the risk committee is the most challenging.
  - Three possible explanations: broad range of responsibilities, forward-looking nature of job, and technical nature of regulatory compliance[2]

[1,2] Sir Howard Davies, "Audit is no longer the chore the board dreads most," *Financial Times,* July 28, 2014

Outline

- Genesis & Challenges
- Framework & Methodology
- Solution
- FHLB-Chicago Risk Management Environment
- Accomplishments

Genesis and Challenges

Supervision
- Increased supervision
- Increased pressure on regulators and auditors
- Need for better documentation and framework

Overhead
- Cost of infrastructure
- Multiple Risk, oversight organizations
- Multiple impact on business leaders
- Large number of people

Regulation
- Increased regulatory burden
- Hard to focus on ‘Risk’ rather than on ‘Compliance’

Business Change
- New business activities
- SEC registration
- Flexibility to incorporate business changes
- Changing external risks

Genesis and Challenges

- Provide greater transparency and consistency to the risk and governance process across the organization but particularly to managers, executives and the Board
- Move the organizational culture from a solely compliance focused organization to an integrated ‘Risk Management’ culture
- Evangelized a philosophy of ownership and accountability for risk and control to line management
- Provide a cost effective infrastructure that integrated the governance framework of the organization
- Improve risk management practices across the organization
- **Implement a coordinated, efficient and effective framework for risk & compliance management across the enterprise**

Solution Components

Process

STRATEGIC

Identified Key stakeholders → Identified core objectives → Evaluated alternative approaches OCEG, CoBit, COSO etc → Developed vision for the framework → Prioritized and set up multiple paths and a maturity model → Envisaged a multi-year initiative based on continuous refinement and priorities

TACTICAL

Develop conceptual framework → Implement individual domains based on business priorities → Implemented an enterprise issue management program → Implemented consistent reporting → Enhanced integration into the business process (outside of the compliance & governance organization)

People

CEO | CFO | COO | CCO | CRO | CAE

Operations | Finance | Risk | Compliance | Audit | External Audit

Technology

Eliminate EUC as a data repository and principle reporting mechanism

Deliver transparency at enterprise level and detailed level of the status of risk / control / compliance

Provide a robust infrastructure for governance and management of the overall GRC environment

MetricStream Enterprise GRC Platform

Components of our Environment

- Financial Reporting
- Regulations
- Control Environment
- Regulatory Reporting
- Business Process
- Operational Management

Risks

- market
- credit
- financial
- operational
- fraud
- legal & regulatory
- strategic

What builds up our INTEGRATED risk & control environment

Regulatory Compliance

- Compliance program
  - New regulations
- Financial Controls (SOx)
- Prudential Standards

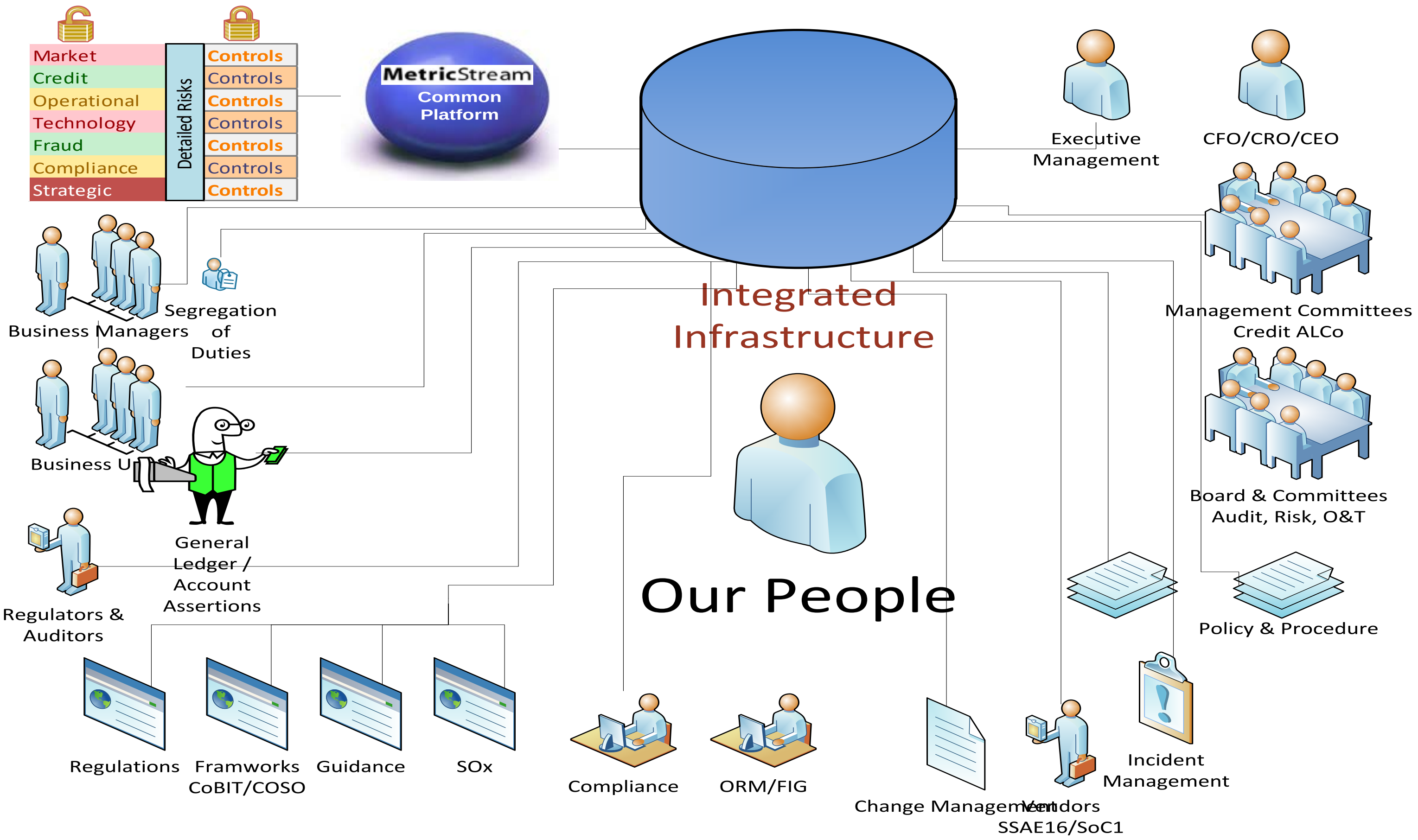
Operational Integrity

- Management Risk Assessments
- Fraud Reporting
- Event Reporting
  - Technology incidents
- Risk/Control Change Requests
- Business Resumption/Continuity

Independent Reports

- Independent Security Officer Reviews
- Model Validations
- End User Computing
- Internal/External Audits
- FHFA Examinations

FHLBC Integrated Risks & Control Management Infrastructure

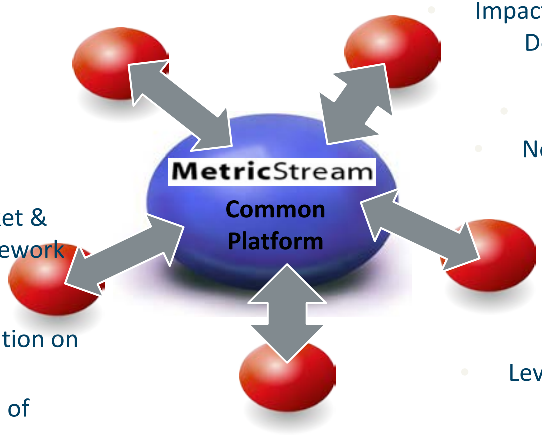


Solution

Creating a Single View into the Risk Organization

Defined Risk Geography

Improved Collaboration



Operational Risk

- Event assessments and loss statistics
- Control Changes
- Enterprise Risk Assessment
- New Products / Processes
- Changes in Market & Credit Risk Framework

Financial Reporting

- Key Control Changes
- Impact of Events and Control Deficiencies on Financial Reporting
- New Accounting Rules
- New Products/Processes

Compliance

- Provides information on New Regulations
- Evaluates impact of regulations
- Evaluates gaps identified in the control environment

External Audit / Regulator

- Best Practices
- Leverage Management and Internal Audit work
- Understand Enterprise Control Environment
- Directly access enterprise key control status

Internal Audit

- Uses Risk and Control information to design audit program
- Provides results of audit program to management to inform their risk assessment
- Provides feedback on proposed Control changes
- Evaluates and tracks significant issues and their resolution

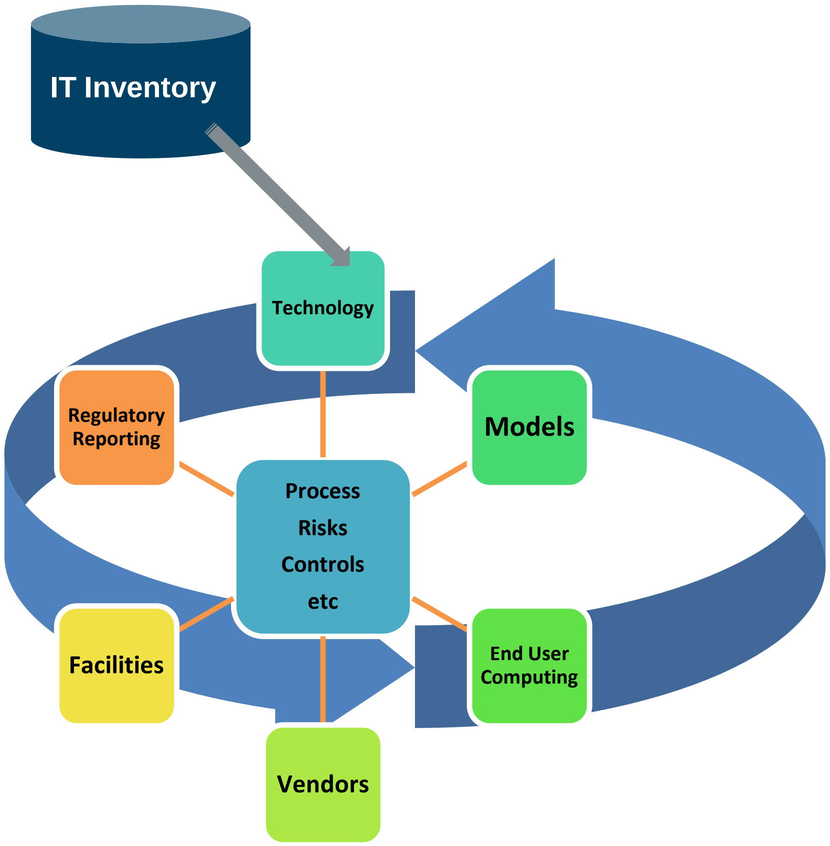
Where are we going

Mature Process	Recently Implemented	In implementation / Planned
Issue Management	Model Validation	EUC Object
Certification / Sox	EUC Validation	Model Object
Internal Audit	Event tracking and reporting	Other control frameworks
Continuous Monitoring	IT assets	
Continuous Audit	Regulatory Reporting	
Compliance Inventory	Business Continuity	

Stakeholders growing
Requirements expanding
USE cases expanding
Data conflicts growing

Challenges - Data

- We have cross-referenced multiple data sources:
  - How do we update
  - Who maintains relationships
  - What is the definitive source of Data
    - Mostly standing / reference data
    - Currently supporting three models:
      - Primary record
      - Primary records + external enhanced data
      - Secondary records
  - Who develops and supports reporting
    - Subject Matter Experts



Challenges – Stakeholders & Communication

- GRC impacts multiple areas of the organization
  - 25% of the organization uses the system monthly
  - Business users have built their processes around the system
  - Monthly Steering Group – 20 key stakeholders
  - Smaller system stakeholder group

Principles and Discipline

- Minimize customization
- Maximize existing functionality
- Leverage proven solutions

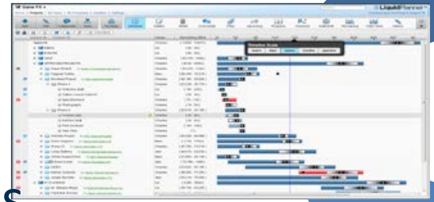
Challenges – Implementations

- Involving new business users
  - Devoting adequate resources to the task
  - Integrating into the culture of shared resource
  - Corporate GRC Philosophy
  - Vendor management
  - Regression testing
    - All units involved
  - Multiple project in parallel
  - New interfaces
  - Some Compromise!

- Principles and Discipline
  - Minimize customization
  - Maximize existing functionality
  - Leverage proven solutions

Challenges – Support

- Multiple reporting requirements
- Multiple macro & micro projects on-going at one time
- Vendor management
  - Production
  - Implementation teams
- Coordination of activities
- Consistency
- User provisioning automated



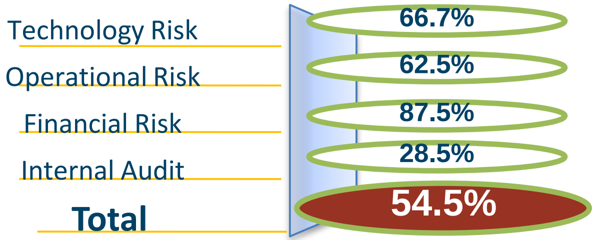
Accomplishments

Realized Benefits

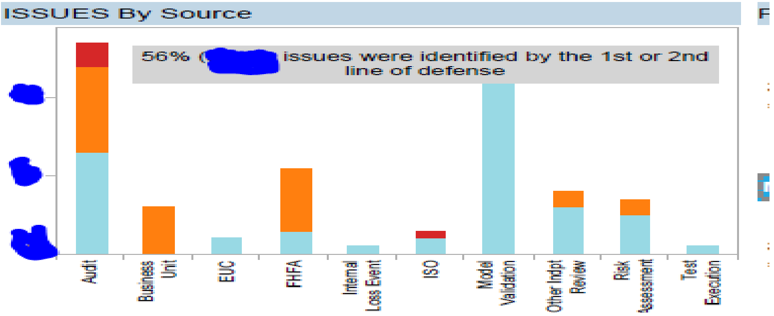
- Created consistent risk evaluation
- Implemented common definitions and standard frameworks
- Delivered critical independent but comparable risk reporting
- Eliminated end user computing based processes
- Delivered risk assessment, issue tracking and control interface to all employees
- Provided a long term ‘Risk’ organization to baseline risk and control metrics and track performance
- Reduced resolution time for critical risk and compliance related issues
- Reduced the number of open risk and compliance issues
- Reduced human capital cost for managing the audit risk and compliance infrastructure

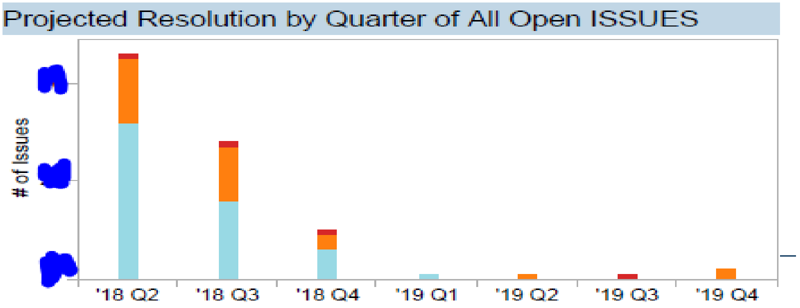
The Road Ahead

- Eliminate remaining majority of remaining end user computing in the operational aspects of control and risk evaluation
- Implement an evergreen risk assessment program
- Integrate continuous monitoring for significant portion of key controls for operational risk, compliance and SOx
- Implement continuous audit practices
- Integrate with management core technology for continuous exception reporting



54.5% Savings From Human Capital Costs





What is the downside?

- Costs – we have people and systems dedicated to maintain this infrastructure
- All business units have to participate in contributing to the infrastructure
- There is a level of administration associated with the programs
  - We have less people dedicated than most organizations and FHLBanks
  - We are more efficient and integrated than many organizations
- Documentation matters in the current environment
  - If it’s not written down, it probably does not exist! (for regulators and external auditors)

Where are we going

- Integrating business continuity management
  - Planned
- Integrating vendor risk evaluation management
  - Done
- Integrating model risk management & review
  - Completed
- Integrated ‘inventory management’
  - Applications
  - EUC, Models
  - Regulations, Reporting Requirements
  - More about the data model / geography
  - Not necessarily systematically integrated
  - That is a goal

Why does this matter?

- Having a Robust and Well executed infrastructure for managing governance, compliance and risk management matters:
  - It gives us confidence to try new things
  - It gives regulators and the board confidence to let is try new things
  - It frees up resources to allow us to try new things
  - It makes sure that the things we do well today....we continue to do well tomorrow
  - When the world changes we can be nimble and adapt without stopping everything we are doing

“Integrated Risk & Control Re-engineering”

Thank You

Tom Harper

Executive Vice President & Chief Audit Executive

FHLB - Chicago

APPENDIX

Risk Model: Definitions

Key Risk:

- A Business Risk or a Regulatory Risk that is directly associated with a critical business objective and may cause significant and/or material financial, strategic or operational losses, as well as legal liability to the Bank if the Bank does not have adequate processes and procedures in place to mitigate the impact of the risk to the Bank

Key Control:

- Business control necessary to manage a Key Risk directly associated with a critical business objective. A Key Control must adequately describe the steps undertaken by the Bank to ensure a Key Risk to the Bank is effectively mitigated, such as by indicating "who does what and when" as well as identifying the applicable policies and procedures, if any.

Regulatory Risk:

- a risk to the Bank that may jeopardize the Bank's legal standing with its regulator, may open the Bank to legal liability such as by causing its regulator to initiate enforcement proceedings against the Bank or make adverse findings during yearly examinations, or may be a violation of regulation or law. Synonymous with "compliance point.

Risk Model: What do controls & risks look like?

Key Risk	
The Bank does not follow procedures for wire transfers	*(The bank suffers loss because of)* unauthorized wire disbursements
Key Control	
There are procedures in place for wire transfers	The wire transfer system ensures that all wire transfers are input and verified by two separate authorized individuals
Regulatory Control	
The bank complies with OFAC regulations	Money transfers systems all incorporate up-to-date filters designed to identify potential OFAC violations and procedures are in place to address these if they occur.

Risk Model: Definitions

Inherent Risk:

- The magnitude of existing risk absent any related controls. Inherent risk attributes include but are not limited to high value, high volume, complexity, change, price volatility, subjective processes, skills and human dependencies, and external factors

Risk Management Practices:

- Existing programs are within the business processes that control risks associated with the business and measures the adequacy of the internal control system. Risk measurement attributes include, but are not limited to historic trends, prior audit/examination results, management's assessments, people trends, automation, and stability

Residual Risk:

- The risk remaining after the controls put in place to mitigate the inherent risk. Residual risk should be evaluated to determine if it is within the a tolerable range.

Overall Rating:

- A summary of the risk evaluation based on management's assessments of the risk management practices within the seven risk dimensions of the business process

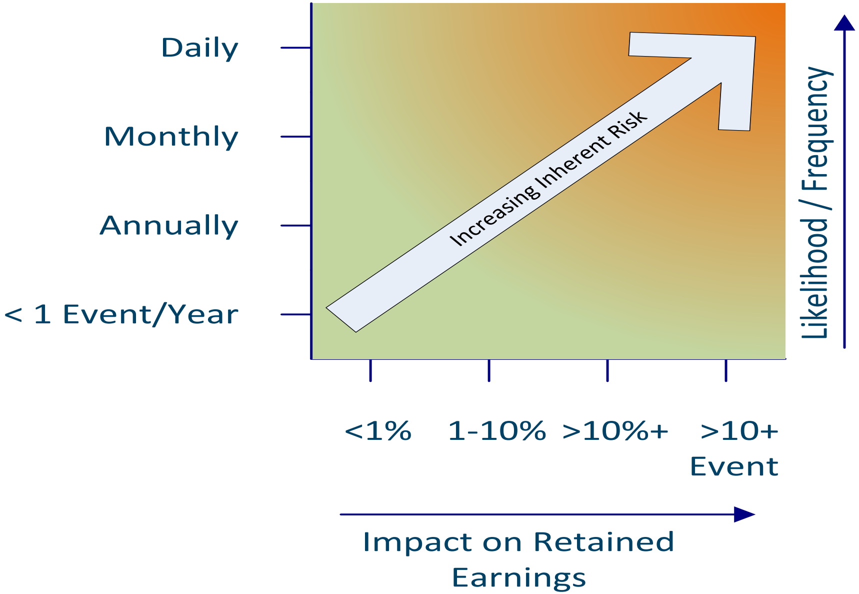
Inherent Risk - Concept and Application

- Inherent Risk is the risk within a business process or, in the case of a governance process, the risk overseen – absent the controls provided by the business.
- Inherent risk evaluation assumes that fundamental business strategy continues
- Inherent Risk incorporates an evaluation of the probability and impact of a loss event
- Our risk model is a prioritization based model however it is useful to have some baseline examples to facilitate the evaluation of relative inherent risk:
  - Example – Assumes that advance customers will be regulated financial institutions
  - Example – Assumes bank failures occur with a finite probability

Inherent Risk - Concept and Application

Uniform risk model

- Simple
- Easily related to by managers
- Applicable to a wide variety of assessments



Likelihood	Very High	Events that could occur on a frequency of Daily or more, very high volume of transactions or dynamic external environment that requires active management
	High	Events that could occur on a frequency of Monthly or more, high volume of transactions or dynamic external environment
	Moderate	Events that could occur on an annual frequency, moderate volume of transactions or recalibration and adjustment of risk management required infrequently
	Low	Rare events that occur less frequently than annually and require ad hoc or infrequent adjustments to risk management
Impact	Very High	Single managed event could impact 10%+ of retained earnings per year
	High	Cumulative mismanaged events could impact 10%+ of retained earnings per year
	Moderate	Cumulative mismanaged events could impact 1%+ of retained earnings per year
	4Low	Cumulative mismanaged events could impact less than 1% of retained earnings per year

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Market	Risk that changes in the value of assets or liabilities may adversely impact business goals and objectives. Includes: • Risk associated with trends in long term interest rate management commonly known as Asset & Liability Management • Risks associated with the management of all assets and liabilities where valuation is a critical aspect of business management or financial reporting • Risks associated Liquidity and Funding • Includes off balance sheet and Fair Value attributes	• Low volatility • Liquid organized and regulated market • Standardized instruments • Pricing transparent and quoted by multiple sources • Adequate price validation mechanisms • No synthetic pricing requirement • Instruments are traded regularly for cash • Minimal size of positions • Automated tools to manage and report risks and positions • Minimal reliance on key individuals • Includes areas where Market Risk is purely nominal i.e. cash • Very low likelihood of high impact possible adverse events which would threaten the organization	• Some degree of volatility in the market • Few positions in thinly traded or illiquid markets • Minimal model derived pricing • Few customized / OTC instruments • Synthetic pricing very well understood and transparent • Actual realization of model derived pricing • Moderate to large size of positions • Generally adequate automated tools to manage and report risks and positions • Minimal degree of reliance on key individuals	• Highly volatile market • Some positions in thinly traded or illiquid markets • Some model derived pricing • Some customized / OTC instruments • Synthetic pricing well understood and transparent • Actual realization of model derived pricing • Moderate to large size of positions • Generally adequate automated tools to manage and report risks and positions • Some degree of reliance on key individuals	• Highly volatile market • Thinly traded or illiquid market • Model derived pricing or insufficient price validation mechanisms • Customized instruments • Multiple inputs to synthetic pricing • Minimal actual realization of model derived pricing • Significant size of positions • Ineffective / Lack of automated tools to manage and report risks and positions • High degree of reliance on key individuals • Low frequency of high impact possible adverse events or high frequency of low impact events which in the aggregate pose potential catastrophic conditions

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Credit	Risk that the obligor of an instrument or loan does not repay interest, principal or fees. Includes: • Risks associated with managing risk mitigants such as collateral and other pledged assets • Risk associated with replacing transactions with new transactions to meet businesses goals • Risk associated with failure of a party to a complete a transaction, settlement exposure. • Risk associated with Cash Management credit • Risk associated with Vendor Performance ◦ Key suppliers ◦ Depositories / Correspondents	• Minimal or zero perceived risk of default by customers or counterparties • Size of total obligations low • Collateral held in house • Minimal reliance on borrowers to report financial position • Collateral of high quality and liquidity – valuation transparent • Obligations very short term • Borrowers of very high credit quality and operational capacity	• Size of total obligations high • Collateral held in house • Minimal reliance on borrowers to report financial position • Collateral of high quality and liquidity – valuation transparent • Obligations short term • Borrowers of high credit quality and operational capacity	• Size of total obligations high • Collateral diversified • Some reliance on borrowers to report financial position • Collateral of high quality and liquidity – valuation transparent • Obligations medium to long term • Borrowers of moderate credit quality and operational capacity	• Significant exposure to obligors and repayment. (before risk mitigants) • Significant reliance on third party managed collateral to secure positions • Significant reliance on obligors to maintain / report compliance with borrowing requirements • Valuation of liabilities and or collateral is challenging • Long term lending • Borrowers of low credit quality and operational capacity

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Financial Reporting	Risk that financial statements and supporting ledgers are insufficiently detailed, inaccurate or misrepresent the financial condition of the organization. Includes: • Regulatory reporting • Filings • Notes and other disclosures in financial statements • Financially based Management Information • GAAP and other compliance • Potential unauthorized acquisition, use or disposition of assets	• No accounting issues • No elements of the statements require judgment or estimation • No historic issues or re-statement • Stable accounting practices • No new requirements • Transactions short term, minimal accruals or off-balance sheet activity	• No accounting issues • Some areas of the statements require judgment or estimation • No historic issues or re-statement • Stable accounting practices • No new requirements • Transactions longer term, minimal accruals or off-balance sheet activity	• Some issues known with accounting treatments • Some areas of the statements require judgment or estimation • No historic issues or re-statement • New requirements • Transactions longer term, substantial accruals or off-balance sheet activity	• Complex accounting issues • Significant judgmental accounting issues and estimates • Public filings and registrations • History of re-statement • New requirements • Off balance sheet and fair value treatments

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Operations & Technology including Vendor & Agency Risk	• Risk to the business caused by a failure to effectively operate routine business operations. Includes • Vendor Risks inherent in relying on a third party to provide business services (exclusive of credit factors) • Technology Risks associated with the technology supporting a business. Also covered under the relevant business risks • Business Continuity risks • Agency Risks associated with the provision of services to third parties (see also Fiduciary Risks)	• Standardized transactions • Low value / Volume • High degree of automation • Stable operating and technology environment • Stable and current technology platform • Business recovery requirement low >7 days • No services provided for outside parties • No processing performed by outside parties • No reliance on key individuals • Staff continuity	• Mostly Standardized transactions • Moderate value / Volume • Most processes incorporate a high degree of automation • Stable operating and technology environment • Stable and current technology platform • Business recovery requirement moderate >1 and <7 days • Minimal services provided for outside parties • Minimal processing performed by outside parties • Minimal reliance on key individuals • Low staff turnover	• Substantial non-standardized transactions • High value / Volume • Significant processes incorporate a minimal degree of automation • Some changes in operating and technology environment • Current technology platform • Business recovery requirement high <1 day • Significant services provided for outside parties • Significant processing performed by outside parties • Reliance on key individuals • Moderate staff turnover	• Mostly non-standardized transactions • High value / Volume • Significant processes incorporate a minimal degree of automation • Changing operating and technology environment • Niche/Ageing/Cutting Edge technology platform • Business recovery requirement high <1 day • Significant services provided for outside parties • Significant processing performed by outside parties • Reliance on key individuals

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Fraud	• Considers all aspects of fraud (see all other areas) including: • Misappropriation of business assets, including third party assets (eg. theft of assets or fraudulent expenditures) • Misrepresentation of results and financial records (eg. falsification of accounting records) • People risks including hiring practices and policies	• No fungible or convertible assets • Minimal linkage of compensation to financial results • Purchasing activity flows through other areas • Minimal impact on financial reporting	• Some fungible or convertible assets • Some linkage of compensation to financial results • Purchasing activity flows through other areas • Receives disbursements or custody of physical assets • Some impact on financial reporting	• Some fungible or convertible assets • Some linkage of compensation to financial results • Purchasing activity controlled within area • Receives disbursements or custody of physical assets • Significant impact on financial reporting	• Significant fungible or convertible assets • Significant linkage of compensation to financial results • Major Purchasing activity controlled within area • Receives disbursements or custody of physical assets • Material impact on financial reporting

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Compliance & Legal •Regulatory •Fiduciary •Contract •Reputation	• Risk of non-compliance with a regulation, law directives. Considers the entire legal dimension includes: • Reputation risk • Fiduciary Risk – liability of the organization to third parties (possibly general public) as a result of it's position of trust • Conflicts of Interest • Individual laws and regulations	• Minimal applicable regulation • No servicing of outside entities • Minimal customer impact • Minimal contractual relationships	• Some applicable regulation • Clear integration of Regulatory Risk in management processes • Robust Compliance function • Minimal servicing of customers • Minimal decision making on behalf of customers • Reliance on standardized contractual relationships	• Substantial regulatory burden • Some integration of regulation into management oversight • Minimal compliance function • Substantial provision of services to customers • Products / Services to customers require judgment • Overlap between entities business model and customers • Some reliance on complex contractual relationships	• Substantial regulatory burden • Minimal integration of regulation into management oversight • No effective compliance function • Substantial provision of services to customers • Products / Services to customers require significant judgment • Substantial overlap between entities business model and customers • High degree of reliance on complex contractual relationships

D Inherent Risk Evaluation

Risk Type	Definition	Low	Moderate	High	Very High
Strategy & Planning	• Considers the risk to the business from changing business strategies (or lack thereof) in response to internal and external factors. Also considers risks inherent in the management strategy and whether these are managed in an appropriate way • Sufficiency and skills of management • Risk attitude of management • Structure & Management organizational optimization • Conflicts of Interest • Tone at the top and corporate culture • Overall Management Policies and Processes • Management Information • Cost attribution & Pricing rationalization	• Clear alignment of business goals and risk control structure • Unit is characterized by a stable environment with little internal or external pressure. Vision and strategy not vital to success • Technology not vital to success of business plan • Staff and Management are sufficient and well qualified to undertake their roles • Staff turnover is moderate and there is no reliance on individual key members • Organizational structure is suitable and sustains a suitable control environment • Management has a open and effective culture of risk and control management • Management has a history of effectively identifying through existing management information control breakdowns and need for organizational change	• Alignment of most business goals and risk control structure • Unit is characterized by an environment with moderate internal or external pressure. Vision and strategy are more important vital to success • Technology supports success of business plan • Staff and Management are sufficient and well qualified to undertake their roles • Staff turnover is moderate and there is no reliance on individual key members • Organizational structure is suitable and sustains a suitable control environment • Management has a open and effective culture of risk and control management • Management has a history of effectively identifying through existing management information control breakdowns and need for organizational change	• Unclear alignment of business goals and risk control structure • Unit is characterized by an environment with a significant internal or external pressure. Vision and strategy are very important vital to success • Technology supports success of business plan • Staff and Management are mostly sufficient and well qualified to undertake their roles • Staff turnover is higher and there is some reliance on individual key members • Organizational structure is mostly suitable Management has a more reserved and less effective culture of risk and control management • Management has a history of not identifying issues through existing management information control breakdowns and need for organizational change	• Minimal alignment of business goals and risk control structure • Unit is characterized by an environment with a significant internal or external pressure. • Vision and strategy are very important vital to success • Technology vital to success of business plan • Staff and Management are in-sufficient or qualified to undertake their roles • Staff turnover is higher and there is much reliance on individual key members • Management has a more reserved and less effective culture of risk and control management • Management has a history of not identifying issues through existing management information control breakdowns and need for organizational change

Control Environment – Concept and Application

- Control Environment is the infrastructure, processes and procedures implemented by management to mitigate the inherent risk in the business to a level acceptable to management and stake holders
- The control environment is normally proportional to the inherent risk being managed – i.e. less risky areas demand less control infrastructure

D Control Environment

Risk Management Practices	Weak	Moderate	Acceptable
General Control Evaluations	• Minimal Metrics in place for management of Key Controls for all areas: – SOX – Risk – Compliance • Significant Exceptions in Historic Risk Assessments or Examinations • Minimal risk identification • No management QA process • Minimal risk management processes • Minimal organizational checks and balances • Un-clear organizational responsibilities • Little dedicated support infrastructure – Credit, Finance, Market, IT • Limited Integrated Automated systems • Limited Loss event history • Challenged by personnel capacity & skill set • Minimal provision for Business Continuity. Minimal testing of plans	• Some Metrics in place for management of Key Controls for all areas: – SOX – Risk – Compliance • Some Exceptions in Historic Risk Assessments or Examinations • Occasional Pro-active risk identification • Partial management QA process • Some risk management in processes • A few organizational checks and balances • Mostly clear organizational responsibilities • Some dedicated support infrastructure – Credit, Finance, Market, IT • Some Integrated Automated systems • Some Loss event history • Some challenges with personnel capacity & skill set • Some provision for Business Continuity. Some testing of plans	• Comprehensive Metrics in place for management of Key Controls for all areas: – SOX – Risk – Compliance • Minimal Exceptions in Historic Risk Assessments or Examinations • History of Pro-active risk identification • Effective management QA process • Embedded risk management in processes • Clear organizational checks and balances • Clear organizational responsibilities • Dedicated support infrastructure – Credit, Finance, Market, IT • Highly Integrated Automated systems • Minimal event history • Competent and adequate staff. Minimal reliance on key individuals. Cross training in place • Substantial provision for Business Continuity. Comprehensive testing of plans