

Fiduciary Risk – Range of Practice - April 2012

This RMA survey was intended to capture the current range of practice in fiduciary risk across a selection of member institutions.

The survey was conducted by RMA between March and April 2012. RMA analyzed responses from financial institutions covering various asset sizes, as presented below:

- Asset size below \$100 billion – 3
- Asset size \$100 billion to \$300 billion – 6
- Asset size \$301 billion to \$500 billion – 2
- Asset size \$501 billion to \$1 trillion – 1
- Asset size over \$1 trillion – 2

Background

More than 90% of the surveyed institutions have a Chief Risk Officer (CRO) function and nearly 65% of the CROs report to the CEO, with access to the Board of Directors. The majority of institutions apply separate frameworks to each of the risk types.

Findings

Our survey shows that all institutions consolidate risk information across risk types to provide a portfolio-wide view of firm risk. Each institution has a group responsible for consolidation efforts.

More than 70% of survey participants say their risk employees operate out of both a corporate function and individual business units. Institutions provided detailed overviews of how the risk management function is integrated into the business units and regional offices.

In the majority of cases, the following types of fiduciary businesses exist in the organizations: personal trust, institutional trust, asset management, and wealth management. Close to 70% of institutions participating in the survey have a risk group specifically designated for fiduciary risk. The number of full-time employees (FTE) dedicated to fiduciary risk ranges from one (1) to fourteen (14). Those individuals reside either at the corporate level or in individual business lines, or in both functions. For institutions that do not have staff dedicated solely to fiduciary risk, the responsibility for oversight and evaluation of fiduciary businesses and fiduciary risk issues falls into the operational risk area.

Close to 80% of respondents have a formal definition of fiduciary risk. In addition, those institutions have in place policies, statements of principles, etc. that relate to fiduciary obligations and the management of fiduciary risk. All of the institutions have

their fiduciary risk contemplated in their RCSAs and other established risk identification and assessment practices. To review the list and the extent of those practices, please see the detailed survey results.

Capital is held for fiduciary risk by 50% of participating institutions, and most of that capital is a component of operational risk.

In terms of fiduciary liability insurance, 70% use professional liability and 50% use fiduciary coverage.

About 65% of institutions provide either periodic or ongoing fiduciary awareness training to their employees. Institutions that provide training make it mandatory for their employees and try to track attendance. Training topics vary by institution.

Approximately 70% of survey participants have a monitoring and testing program for fiduciary activities. In most cases, compliance is responsible for this function. The reported frequency of program review varies greatly among those surveyed, as do the groups responsible for evaluating program results and the type of reporting presented.

All of the institutions report coordination among risk and other control functions (i.e., legal, compliance, audit) when handling fiduciary matters. Some institutions were able to provide examples of how fiduciary issues might be handled by their control functions.

Nearly 70% of the participants engage in scenario analysis relating to potential fiduciary exposure. Less than 50% were aware of their company holding capital for potential fiduciary exposures/events. However, approximately 70% of institutions have a fiduciary risk category to track losses. In less than 60% of cases, the risk function is part of the annual audit planning process.

The Board (or a committee of the Board) oversees fiduciary activities for 93% of the institutions. For 86%, the Board has delegated fiduciary oversight to a business level committee. The names for the committees vary, but the most common ones are: Fiduciary Risk Management Committee, Fiduciary Committee, and Fiduciary Risk Committee. There are between four (4) and twenty-four (24) members on the committees, who represent both the business and control areas of the organization. In about 50% of cases, this committee is not a subcommittee of the Board of Directors. Frequency of committee meetings varies as follows: 28% meet bi-monthly, 31% meet quarterly, and 21% meet monthly. The committee provides periodic reporting to the Board of Directors for 78% of respondents.

In all of the institutions, compliance monitors the regulatory landscape for potential changes to regulations covering fiduciaries. In 86% of cases, there are business-unit-specific fiduciary committees, 64 % of which provide periodic reporting to a corporate fiduciary committee. Approximately 57% of the institutions do not have a separate committee to oversee conflict issues.

Do you have a Chief Risk Officer (CRO)?

- Yes (13).
- No - Separate Chief Governance Risk & Market Risk Officers.

Does your CRO report to the CEO and have access to the Board of Directors?

- Yes (9).
- Yes - the Chief Risk Officer reports directly to the CEO and has direct access to the bank's Board of Directors.
- Yes - the CRO reports directly to the CEO. The CRO has access to the Board of Directors and individually meets with the Audit Committee at least six times per year.
- CRO is reporting to CEO and has access to the Board of Directors.
- Chief Governance Risk & Market Risk Officers both reporting to CEO.
- The Risk Officer reports to the Head of Trust & Asset Management and to the Chief Compliance Officer of the Bank. He reports to the Finance and Trust Committee of the Board of Directors Semi-Annually.

Do you have a separate framework that applies to each risk type - operational, credit, market? If so, please describe?

- Yes.
- Yes - we have a Chief Operational Risk Officer, a Chief Credit Risk Officer, and a Chief Market Risk Officer.
- Yes - separate frameworks exist for Operational Risk, Credit Risk, Market Risk, all reviewed and approved annually by CEO (and direct reports) and Board of Directors.
- We do have a separate framework that applies to the eight separate risks in the OCC's handbook.
- Yes - Credit, Market & Liquidity, Strategic, Fiduciary, Operational and Compliance.
- Yes - our framework had leaders by both business and for risks cutting across business.
- Yes - we have in place a well-understood Enterprise Risk Management Framework that serves to define our enterprise-wide risk approach for identifying, measuring, controlling and reporting on our significant risks. Individual risk specific frameworks are in place to manage key risks such as operational, credit, and market risks. Our bank considers Fiduciary Risk as a subset of legal risk within the broader operational risk category. Our Board committees approve the Enterprise Risk Framework and all supporting risk specific frameworks. In addition, we have a separate Risk Appetite Framework in place which defines the amount and type of risk that the bank is able and willing to accept in the pursuit of its business objectives.

- Yes - we have Operational, Credit and Market risk disciplines reporting up to the CRO.
- Yes - Risk management is a shared responsibility through a “three lines of defense” model: 1) Each business owns and is responsible for managing risks within its business. 2) Corporate risk, Compliance and Legal provide independent oversight delivered through corporate, business-aligned and regional personnel. 3) Corporate Audit provides independent assessment of the effectiveness of the first and second lines of defense in carrying out their responsibilities. Within the second line of defense, operational, credit and market risk are all viewed as separate disciplines, which are staffed independently and have senior management leadership. In addition, focused oversight—including corporate standards and policies on risks such as credit, sovereign, new products, compliance and ethics, operational, fiduciary, trading and market, model assessment and interest rate, and liquidity—is provided by corporate-level risk committees.
- Several of the major risk categories are governed through programs, policies, procedures and governance activities tailored for the management of the individual risk category. This includes credit, operational, compliance, market and liquidity risks. Strategic and reputation risks are governed through the ERM Program and Policy.
- Yes - all three risk disciplines have separate frameworks but come together from a governance perspective at the Risk Executive Committee level.
- No - single Group Risk Framework which categorizes and describes each risk type and management approach.
- No.

Do you consolidate risk information across risk type (operational, credit, market) to provide a portfolio wide view of firm risk?

- Yes (6).
- Yes, consolidated by Operating Group and by Risk Type.
- Yes, we aggregate risk according to quantity, quality and direction of risk according to the OCC handbook.
- Major data aggregation project underway to accomplish this objective.
- Yes, risk information is consolidated into an Enterprise Risk Report which is prepared on a quarterly basis to provide senior management and the Board with actionable forward-looking risk reporting on significant risk issues impacting our bank. It includes information on a broad range of risks facing the organization along with analysis of related issues and trends. In addition, the report provides an assessment of bank’s risk profile relative to its risk appetite and an overview of the economic and regulatory environment. Information on the capital required against risks and the capital available forms part of the report.
- Yes - but consistent definitions are still in need of further definition to truly aggregate info.
- The Enterprise Risk Management Program creates a framework for the holistic view and assessment of all risks, along with the understanding of risk interdependencies. A corporate level ERM Dashboard and Profile is compiled and

reported quarterly. The profile includes sections for each of the major risk categories and an executive summary provides an integrate view of corporate risks.

- Our Enterprise Risk Management group (ERM) is providing such reporting.
- Consolidation is done via Board level MI and reporting.

Do risk employees operate out of a corporate function or individual business units or both?

- Both (8).
- Both. There are employees in the line of business (first line of defense) who “own and manage” the risks. In the lines of business, we also have “RISC Offices” (Risk Information Security and Control) focused on controls, monitoring, operational risk, compliance risk and SOX in the business units. Employees in Risk Management (second line of defense) who provide risk oversight.
- All within a corporate function, some risk professionals are forward deployed into within the Operating Groups but still report into the Corporate Function
- We have a chief risk officer in the business who also consults with risk officers across the enterprise on a regularly scheduled basis.
- Corporate, but attached to a business.
- Risk employees operate out of both a corporate function as well as the individual business units. Bank’s philosophy on the management of risk is that responsibility for risk management is shared. Employees at all levels of the organization are responsible for managing the day-to-day risks that arise in the context of their roles. We apply the Three Lines of Defense model in our approach to the design of roles and responsibilities across the organization. The Business and Corporate Support segments are responsible for the informed management of risks which they actively manage, acting as the “First Line of Defense”. The “Second Line of Defense” is created by key oversight functions such as Global Compliance, Group Risk Management and Finance providing risk direction, oversight and partnership across the bank in areas of their subject matter expertise. These groups set and monitor policies, define work practices and oversee the business frontlines with regard to the effective operation of bank’s internal control framework. The Second Line also reviews the management of risk in relation to the risk appetite of the business including changes in the business environment for that particular risk type. Internal Audit Services, together with the Board of Directors and its committees and the external auditor, acts as the “Third Line of Defense” in ensuring that bank has the right processes and policies in place to manage significant risks.
- Corporate functions.

How is the risk management function integrated into the business units and regional offices?

- Various business units have Risk personnel and they report up to the Risk hierarchy.
- All within a corporate function, some risk professionals are forward deployed into within the Operating Groups but still report into the Corporate Function.
- Through corporate governance committees, policies and procedures.
- All ultimately report into Regional Office, some may be business unit specific others general - but all roll into Regional Office.
- Individual Business Unit Risk Teams and Performance Expectations required to have 10% weighted RM expectation.
- Have employees embedded in the units reporting up through a region head.
- Thru risk managers within the LOB's.
- The risk management function as part of the Second Line of Defense is comprised of GRM Relationship Management and Compliance groups which are aligned on a business segment and regional basis to provide risk/compliance direction, oversight, and challenge.
- Operational risk management team members report directly to the line of business and have dotted line reporting in to the top of the house risk management function.
- Staff within the Risk function is organized by risk type, business unit and geographic region. Consequently, within a particular business line, risk professionals from each of the three disciplines will be aligned with those business units and a risk manager aligned with the specific business unit will coordinate interaction between the business unit and the risk discipline. The business unit aligned risk manager will normally have expertise in the risk discipline that is most directly associated with that business unit (i.e., the risk manager for the trading businesses has a market risk background but also coordinates credit and operational risk personnel supporting that business unit. Similarly, on a regional basis, market, credit and operational risk professionals are located in and support the regional business and a regional risk manager supervises the overall alignment of the risk functions with the business units in the region. Focused oversight—including corporate standards and policies on risks such as credit, sovereign, new products, compliance and ethics, operational, fiduciary, trading and market, model assessment and interest rate, and liquidity—is provided by corporate-level risk committees.
- Risk Management, as the second line of defense, helps ensure that risk owners accept and manage risk at levels consistent with corporate risk philosophy and approved appetite. Risk Management also ensures that risk assessments are compiled, reviewed, challenged and aggregated for a holistic view of risk. There are collaborative interactions between the line of business and Risk Management through the course of business interactions. There are representatives from the first and second lines of defense participating as members of the risk governance committees.

- Both, corporate center OR functions as well as business unit OR functions have regional coverage. Where that is not the case local management is being leveraged.
- These are appropriate reporting lines into business units.
- Risk Partner's within each business unit and Divisional Risk Partners for each Division.

What are the types of fiduciary businesses that exist in your organization (e.g., discretionary trust services, asset management, personal trust, etc)?

- Asset Management, Wealth Management.
- Personal Trust, Institutional Trust, Asset Management.
- Personal Trust, Institutional Trust & Custody, Employee Benefit, Real Estate and Mineral Management, Investment Management.
- Discretion, non-discretion, advisory, alternative funds, 3rd party managed funds, Asset Management, Personal Trust, Corporate Trust.
- Discretionary Trust, Asset Management, Personal Trust.
- Wealth management (trust) and asset management.
- Traditional Personal Trust Business Custody Services Corporate Trust Asset Management.
- Fiduciary risk is a question of law that is guided by the types of products and services transacted with clients as well as the nature of the relationships we establish with those clients (i.e. degree of reliance on the bank, extent to which bank makes decisions on behalf of the client, consideration of the clients' best interests, etc.). The following is ordered from the highest to lowest level of perceived fiduciary risk that exists within various bank businesses today:
 - Fiduciary risk is inherent in both our Domestic and Global Trust Services business (Personal Trust / Discretionary Trust Services / Corporate Employee and Executive Services)
 - Some level of fiduciary risk occurs in our Wealth Management (Investment Advisory / Discretionary Portfolio Management/ Global Asset Management) and International Banking (Investment Advisory / Discretionary Portfolio Management) businesses.
 - Our Capital Markets, Mutual Fund Dealer, and Insurance (Agents and Advisors) businesses are unlikely (but still have the potential) to incur some level of fiduciary risk by virtue of the relationship established with certain clients and to the extent they recommend investment products to those clients.
- Wealth management, Corporate Trust and Institutional Trust accounts - all disciplines.
- Discretionary and directed trust services, institutional asset management and fiduciary services, director services, and management company services are examples of fiduciary businesses within the organization.
- All types of personal trust and employee benefit trust. No corporate trust services (bond trusteeship or shareholder services).

- Asset management, corporate trust, personal trust, private client.
- Custody and depositing, Corporate and private trusts, Asset Management.
- Limited asset management Insurance.

Does your organization have a risk group specifically dedicated to fiduciary risk?

- Yes (5).
- Yes - at the Corporate Level.
- Yes, in the line of business.
- There is one resource at the top of the house devoted to fiduciary risk, the rest of us are dedicated to a specific line of business.
- Responsibility for fiduciary risk oversight is shared between Risk and Legal. Within the Risk group, one person is dedicated to fiduciary risk and other senior members of Risk play a role in management of fiduciary risk. At the business unit level, fiduciary risk is incorporated into the operational risk framework. Corporate risk provides independent oversight delivered through corporate, business-aligned and regional operational personnel. 1 FTE at the corporate level. In addition, other senior managers within Risk support management of fiduciary risk and oversight of supervisory risk is a shared responsibility with Legal.
- No (3)
- No, it is embedded within Legal.
- Not specifically, however employees supporting certain businesses bear responsibility for monitoring and managing fiduciary risk. The extent of their involvement and degree of oversight naturally varies with the level of fiduciary risk that exists in those businesses.

If yes, how many FTEs are dedicated to fiduciary risk?

- 1 (2).
- 2.
- 4.
- 8 (2).
- 12.
- 14.

If no, which area within your organization provides oversight and evaluation of fiduciary businesses and fiduciary risk issues (e.g., operational risk)?

- It is part of Operational Risk, with expertise from Legal department.
- The management of fiduciary risk is shared among compliance, legal, operational risk, and business teams. Compliance and risk management fulfill their oversight function by reviewing the management of risk in relation to the risk appetite of the business, including changes in the business environment for each particular risk type.
- Operational Risk (which includes regulatory compliance).

- Risk groups within the respective business lines are covering fiduciary risk.
- Operational Risk.
- Regulatory compliance and operational risk.
- N/A (2).

Do the individuals responsible for fiduciary risk operate out of a corporate function or individual business units or both?

- Corporate Function (4).
- Corporate function but embedded with the business.
- Individual Business Unit (2).
- Both (5).
- Both. The group dedicated to fiduciary risk is in the line of business. Risk oversight is through the operational risk function resident in Risk Management.
- As previously mentioned, bank’s approach follows a Three Lines of Defense model in which the business assumes responsibility for managing the day-to-day risks that arise in the context of their roles and across the various geographies in which we operate. Businesses are responsible for the informed and active management of these risks, acting as the “First Line of Defense”. Group Risk Management and other corporate support groups provide risk direction, oversight and partnership, acting as the “Second Line of Defense.” Internal Audit, together with bank’s Board of Directors and its committees and the external auditor, act as the “Third Line of Defense” in ensuring that bank has the right processes and policies in place to manage fiduciary risk.

What is the organizational reporting line for fiduciary risk (e.g., legal, compliance, enterprise risk)?

- Operational Risk (2).
- Fiduciary Risk reports up to Compliance and Risk.
- Legal and Enterprise Risk.
- Head of Business Unit and Compliance.
- Fiduciary risk dual reports to Operational risk and compliance risk.
- Up through the fiduciary risk officer.
- Compliance, then up to the CRO for the enterprise.
- Fiduciary risk issues are identified directly by the business, through self-monitoring processes conducted by oversight groups such as compliance, operational risk, or internal audit, or by external regulators. Results of monitoring programs or significant issues/exceptions are then reported up to the local Business Operating/legal entity Board Committees, with further escalation to bank’s Reputational Risk Oversight Committee and other members of senior management as appropriate.
- Solid reporting line to the business division and dotted line reporting to operational risk (enterprise).

- Responsibility for fiduciary risk oversight is shared between Risk and Legal with the dedicated named Fiduciary Officer reporting to the CRO.
- Enterprise Risk.
- Various - mostly business COO, some into Risk COO.
- Governance Risk incorporating regulatory, operational and legal.

Does your organization have a formal definition of fiduciary risk? If yes, would you be willing to share the definition with us?

- Yes - Fiduciary Risk is the Risk arising from not serving in the best interests of trust clients as trustee, executor, investment agent or guardian in accordance with governing documents, “prudent person” principles and applicable laws, rules and regulations. Fiduciary Risk is directly impacted by the management of other risk factors such as Market, Compliance and Transaction Risk.
- Yes - Fiduciary Risk is defined according to OCC Rules and guidelines.
- Yes - Similar to OCC definition
- Yes, The potential that an institution will breach its duty of care or its duty of loyalty.
- Yes - cannot share (5)
- Group Risk Management’s Risk Policy group maintains an Enterprise-Wide Fiduciary Risk Policy that defines fiduciary risk as “the risk of failing to faithfully fulfill bank’s obligations to a person to whom a duty is owed under applicable law within the jurisdiction when bank or the individual employee is acting in a fiduciary relationship, whether knowingly or unknowingly.
- A Fiduciary duty is defined as any duty where bank holds, manages, oversees or has responsibilities for assets for a third party that involves a legal and/or regulatory duty to act with the highest standard of care and with utmost good faith. A fiduciary must make decisions and act in the best interests of the third parties and must place the wants and needs of the client first, above the needs of the organization.
- No we do not have a formal written definition of fiduciary risk (3).
- Unknown.

Does your organization have policies, statements of principles, etc, that relate to fiduciary obligations and the management of fiduciary risk?

- Yes (8).
- Yes - our Enterprise-wide Fiduciary Risk Policy outlines the minimum requirements for the identification and management of Fiduciary Risk in bank’s businesses and applies to all bank’s business platforms, business units and subsidiaries. This enterprise policy requires supporting policies to be maintained at the local jurisdictional levels to manage fiduciary risks where required. Globally, the management of fiduciary risk and related obligations are embedded in compliance-specific policies that support the applicable businesses throughout

- the organization. Specific policies covering fiduciary risk are especially prevalent in our Domestic and Global Trust businesses.
- Yes - driven by each line of business.
 - The organization has a Statement of Conduct that all employees are required to adhere to. Individual business units have Codes of Ethics and policies and procedures in place to identify, assess and manage fiduciary risk and conflict issues.
 - Yes. We maintain Corporate Trust Policy Manual.
 - Policies and procedures are in place to address fiduciary activities.
 - No specific fiduciary policies as these are incorporated in codes of conduct and policies for insider trading rogue trading, conflicts of interest.

What is your organization's risk appetite for the fiduciary risk (type and level)?

- Conservative appetite for fiduciary risk with respect to line of business and account type.
- We have one - but not answering.
- Low to moderate.
- Low at the current time.
- We consider fiduciary risk within the scope of operational risk. Within our Enterprise Risk Appetite, we have a defined appetite for operational risk events and use risk metrics to manage this appetite.
- Not specified by fiduciary risk alone - but by operational risk.
- A specific risk appetite for fiduciary risk has not been established. An overall risk appetite using a quantitative approach has been established for operational risk of which fiduciary risk is a component.
- The Policy defines the type and level of fiduciary risk we will manage. We do not have a formal risk appetite defined for fiduciary risk as part of the corporate risk appetite statement.
- Manage our business in prudent manner to minimize losses.
- Being defined.

What is your firm's framework for managing fiduciary risk?

- It is embedded in the Legal Risk Framework.
- Strong corporate governance model driven by various formal committees along with formally approved policies and procedures. The company also conducts a continuous audit of the business's fiduciary activities.
- Same risk framework as any other Operational Risk.
- Utilization of existing Risk Control Assessment tools, KRIs, Compliance testing, etc.
- Fiduciary Risk Management Committee reporting up to Risk & Capital Committee and then to Board Risk Committee.

- The framework for managing fiduciary risk is set out in bank’s Enterprise-wide Fiduciary Risk Policy. This policy outlines the responsibility of each business platform (including all business units and subsidiaries) in their various local jurisdictions to identify, assess, manage and mitigate any Fiduciary Risk inherent in its business and operations or arising from its specific activities and client relationships.
- 1) Each business owns and is responsible for managing risks within its business.
2) Corporate risk, Compliance and Legal provide independent oversight delivered through corporate, business-aligned and regional personnel 3) Corporate Audit provides independent assessment of the effectiveness of the first and second lines of defense in carrying out their responsibilities.
- Fiduciary risks for our bank will be identified, monitored, and managed by senior fiduciary management in conjunction with our Private Bank RISC Office. This will include completion of the annual Risk and Control Self-Assessment and periodic testing of control effectiveness through the Governance Risk and Compliance application. Control gaps identified in the Self-Assessment, ineffective controls identified in periodic testing, and issues identified in Risk Review reports will be remediated by management.
- Firm considers all aspects of operational, credit and market risk when managing day to day operations, i.e. through a committee structure.
- Principally, fiduciary risks must only be run in designated business lines.
- No specific framework.

Is your fiduciary risk contemplated in your RCSAs and other established risk identification and assessment practices? If yes, please list which ones and to what extent.

- Yes (2).
- Yes - part of all wealth related RCSAs.
- Yes - our entire risk and control self assessment is designed, at a core level, to identify and manage fiduciary risk. The categories of risk evaluated include the eight categories identified in the OCC’s handbook (i.e. operational, compliance, legal, credit, liquidity, reputational, financial, market).
- Yes - Self Assessments, KRIs, Losses, Risk Maps.
- Yes - in the operational risk assessment, the compliance assessment and the legal entity assessment.
- Yes - new product, vendor, business continuity, business processes
- Yes - through a combination of ongoing Risk and Control Assessments (RCAs) facilitated by the Operational Risk Heads in each business platform and product specific risk reviews and approvals. The business operational risk group performs regular Risk Control Assessments with a full review of the private client business where fiduciary risk is most prevalent.
- Yes - Fiduciary risk is identified as a separate risk category in RCSAs and other risk management assessment processes.

- Yes - it is very comprehensive and thorough with categorization of Risk Owner, Control Owner, Reviewer and Approver. This is the first year of our full end to end implementation of RCSA.
- Yes - through operational risk RCSA process.
- Yes - in RCAs and Top Risk Scenarios.
- Not explicitly

Do you hold capital for fiduciary risk? If yes, where is it being captured, and to what extent?

- Yes - it is a component of operational risk (3).
- Yes - Operational risk capital is allocated based on the size of assets under management. The capital is not specific to fiduciary risk under operational risk. It is not quantified or a separate line item.
- Yes - For Basel capital purposes, fiduciary risk is a subset of operational risk for which we hold capital.
- Yes, under TSA Operational Risk is a % of revenue; Under AMA it would be covered using loss driven approach
- Yes - captured by parent.
- Generally not specific to fiduciary risk.
- No, not specifically, however there is capital held for operational risk and by definition this may include fiduciary losses.
- Not at the business level.
- Not directly.

What kind of fiduciary liability insurance does your company have in place?

- Professional liability (10)
- Fiduciary coverage (7)
- Umbrella policy for real estate (1)

Does your organization provide periodic/ongoing fiduciary awareness training to employees?

- Yes (9)
- No (5)

What types of topics are covered in the training?

- Regulatory, Policy and Procedures, Insider Trading, Ethics, Document retention, BSA-AML, Information Security.
- Risk Management, Compliance, trust administration, etc.
- Overall guidance on what exactly a fiduciary is and how to execute one's duty.
- Fiduciary Conflicts of Interest, Insider information, Reg 9, duties of a fiduciary.

- Yes. Compliance-training covers fiduciary awareness to the extent applicable to a particular business structure/product offering. For certain businesses (domestic and global trust), training is delivered from within the business and focuses on fiduciary responsibilities for trustees as well as developments in legal and regulatory expectations. For other businesses such as Wealth Management, training is not specific in its focus on fiduciary elements, yet the concept of fiduciary risk is nevertheless embedded within both the product training and professional licensing requirements that are required for employees to sell investment products or services. Businesses also cross train one another on the concept, for instance, fiduciary concepts are included in the training that trustees provide to investment advisors as part of the planning for trust product/business opportunities.
- The training is aimed at broadening employee’s awareness of where fiduciary obligations exist, sources of fiduciary duty, consequences for breach of fiduciary duty and strategies aimed at mitigating fiduciary risk. More focused training is provided at the business unit level to understand the key roles and responsibilities of the bank as a service provider in a given area (e.g., investment management, trustee services).
- Topical fiduciary updates and risk/procedural reviews.
- Conflicts of interest Code of conduct.
- Not applicable.

Is training mandatory for employees?

- Yes (9).
- No (4).

Is attendance tracked?

- Yes (9).
- No (3).
- Not Sure (0).

What area(s) in your organization are responsible for identifying, assessing, measuring, monitoring and managing fiduciary risk?

- All business units and corporate function.
- Part of the Operating Group as first line of defense; Supported by Operational Risk and Legal.
- Risk & Compliance Groups.
- Fiduciary risk within Operational risk.
- Business Unit risk teams and corporate fiduciary risk management and compliance risk team.
- Business line management and operational risk team members.
- Dedicated risk management team.

- Trust & Investment Services Compliance LOB is responsible to own and manage Fiduciary Risk.
- As mentioned earlier, the Business, Compliance, Operational Risk, Group Risk Management, Internal Audit, as per the Three Lines of Defense model.
- (a) Each business owns and is responsible for managing risks within its business. (b) Corporate risk provides independent oversight delivered through corporate, business-aligned and regional personnel. (c) Corporate Audit provides independent assessment of the effectiveness of the first and second lines of defense in carrying out their responsibilities.
- Business units have ownership and self identify. The second line of defense provides risk oversight with timely identification, measurement, monitoring and management. The second line of defense conducts review and challenge of the business risk conclusions.
- Business COO and risk functions.
- Operational Risk.
- Monitoring by Risk Partners within Bus, Internal Audit, External Auditors.

What tools and processes does your organization utilize to identify, assess and monitor for fiduciary risk both at the corporate level and within individual business units (e.g., reports, dashboards, KRIs, self-assessments, audit process)?

- KRIs, Oversight Risk Personnel, LOB personnel, reports.
- Part of reporting broadly and within Risk Appetite and Key Risk Indicators.
- Enterprise Risk Management System.
- All the examples listed.
- Self assessments, KRIs, compliance testing, audit testing.
- Central reporting Dashboards, RCSAs, KRIs, continuous monitoring
- Metrics, reports, exams and audit, self testing and centralized QC testing of controls.
- Business Units monitor the completion of compliance certificates/checklists to support compliance with fiduciary-like regulatory obligations, as well as KRIs such as client complaints and loss event data. Individual compliance teams monitor and test for fiduciary risk as part of their oversight responsibilities. Testing differs across regions, regulated entities, and product types. For instance, wealth management businesses will be subject to a variety of monitoring for trade suitability, conflicts of interest management, portfolio allocation and fair execution, among others. In addition, Internal Audit reviews regional Global Compliance activities at least once every three years, which includes an assessment of compliance monitoring practices. Internal Audit also conducts continuous audit reviews as part of their quarterly monitoring process of certain businesses which includes a fiduciary risk element. The resulting dashboard metrics are reported up to Operational Risk. Finally, the bank Ombudsman is also involved through their monitoring of client complaints.
- (a) Incident/loss reporting, a risk dashboard, business unit level KRI reporting, RCSA and other self assessments as well as internal/external audit findings are all

inputs in the identification, assessment and monitoring of fiduciary risk across the enterprise. (b) At the corporate level, the fiduciary committee is charged with assisting and overseeing the businesses across the organization in the discharge of the Company's fiduciary responsibilities to our clients. Given its broad mandate and the breadth of the Company's business activities, the Committee receives input and support from the various levels of the organization. To this end, the fiduciary committee relies extensively on the network of business unit risk managers and compliance officers. (c) To discharge its oversight responsibilities, the Committee relies on a number of established risk management processes including annual risk self assessments. Fiduciary risk management is included as a separate topic in this process. The process requires that business units identify and assess the risks they take in their existing and new business activities and prepare a plan to address them. The results are reviewed by the businesses' senior management and executive management of the Corporation with input from corporate audit and corporate risk. (d) A monthly dashboard is provided to the Risk Committee of the Board of Directors that includes a section on fiduciary risk issues including both internal and external events (e) There is an annual certification by the head of each major business unit representing and confirming that adequate internal controls are maintained and that no material fiduciary breaches have been identified and gone unreported.

- Business level self assessments and risk profiles are utilized, as well as reference to audits by a centralized risk review group. Additionally, a detailed risk assessment is conducted each year with quarterly updates as needed. The risk assessment includes results from self-assessments, audits and exams. KRIs have not been formalized for fiduciary risks and we do not have immediate plans to develop these.
- RCSA, audit process, KRI/KPI, reports.
- RCSA, Top Risk Scenarios.
- Reports.

Does your organization have a monitoring and testing program for fiduciary activities?

- Yes (10).
- No (4).

If yes, who executes the program (e.g., compliance)?

- Compliance (4).
- Compliance for testing and committee structure for monitoring.
- Committee, business units, Fiduciary Risk Officer.
- Business lines, operational risk, audit.
- Operational risk (which includes regulatory compliance).
- Compliance - a dedicated fiduciary monitoring and testing program is not in place. Elements within the overall Compliance program of the company are used to supplement fiduciary oversight as noted below. • The compliance oversight

- program establishes a corporate-wide framework with standard procedures for inventory of regulatory obligations, assessing regulatory risks, determining an appropriate risk response, and remediating compliance issues. These procedures provide a comprehensive and consistent approach to managing regulatory risk. • A controls & testing program is one component of the overall compliance oversight program. During the risk assessment process, depending on a number of risk criteria, certain regulatory risks are flagged and an assessment of the design and/or operating effectiveness of controls will be performed.
- LOB Risk Reviewers Compliance Risk Review (internal audit).
 - A combination of the Business and Compliance. Fiduciary activities are monitored by virtue of the client relationships in place. For example, there are specific monitoring and testing programs in both our domestic and global trust businesses, while in our wealth management business, a variety of portfolio and suitability monitoring programs support the overall management of fiduciary risk.
 - Not applicable.

How often are topics under the program reviewed?

- Depends on topic, reviews are made on a monthly, quarterly or annual basis.
- Quarterly
- Based on calendar
- Certain aspects of our monitoring/testing programs occur daily, while others are weekly or less frequent. All are based on regulatory requirements/industry best practice and depend on both the scale of the business/level of perceived fiduciary risk.
- Regulatory risk assessment and risk response process is formally performed annually and updated periodically as new risks arise and change throughout the year. If risks are flagged as requiring testing, timing of testing is also determined by risk.
- On an annual basis as a minimum.
- Annually.
- Testing annually - monitoring ongoing.
- 1-3 years.
- Varies.
- Not applicable.

How are the results evaluated and by whom?

- Results are evaluated by Risk and Compliance and by the LOB through the Corporate Governance Committees.
- All Fiduciary business lines, Operational risk, audit.
- Evaluated through fiduciary risk governance, business unit risk and reported up through board.
- Compliance with business management.

- By the second line of defense compliance unit and the Chief Fiduciary Risk Officer of the enterprise.
- Compliance/Operational Risk and the relevant local business, Operating/legal entity, Board Committees.
- Operational risk team members.
- Senior compliance officers review all testing results. CCO, Management Committee, Board of Directors, and Examining and Audit Committee review material testing results.
- Trust Managers, LOB Executives, Chief Fiduciary Officer.
- Senior management / boards where applicable.
- N/A.

What type of reporting is produced?

- Exception reporting.
- Monthly and Quarterly Reports.
- Framework products and reports.
- Dashboard and summary reporting.
- Numerous, but a detailed overview on a quarterly basis to the senior management committee and the Board Risk Committee.
- Written reports to senior management with findings and recommendations.
- This depends upon the monitoring activity in question. Trade suitability reporting, conflicts reporting, portfolio allocation, and reporting around complaints and litigation are all used for different purposes by different groups within the organization. For instance, portfolio allocation reporting is used to identify and correct any deviations from established parameters. Exceptions are escalated through appropriate channels, significant issues/exceptions are reported to senior management and the Board (local or possibly also bank-level), as well as to regulatory agencies as required. Reporting can be transaction-based, conduct-based, or based on the overall effectiveness of our control monitoring processes.
- Formal compliance activity reports.
- KRI and KPI metrics included in compliance reporting. Material testing results included in formal board reporting packages.
- C-CAP and GRC. Archer platform provides aggregation of testing results. Any issues identified are discussed by Fiduciary Committee.
- Not sure.
- N/A.

Is there coordination among risk and other control functions (i.e., legal, compliance, audit) when handling fiduciary matters?

- Yes (12).
- Yes - Risk is the primary repository of OCC and other regulatory examination letters and reports. Risk then convenes Compliance and the Line of Business, and sometimes legal to discuss issues and prepare responses.

- Yes - including fraud, legal, compliance and op risk.

Can you provide us with any examples of how fiduciary issues might be handled among your organization’s control functions (e.g., steering committee process)?

- Fiduciary Risk Mgmt Committee overlooks fiduciary risks - committee is comprised of Legal, Audit, Risk, Business Risk Officers.
- Compliance & Risk identify issues and then bring those issues to the appropriate line of business committees for evaluation and resolution.
- Quarterly Fiduciary Management Committee with sub-Fiduciary risk committees within each Fiduciary business line rolling up to it.
- Chief Fiduciary Risk Officer.
- As an example, our global trust businesses follow defined escalation criteria and escalation procedures against which all fiduciary-based risk decisions must be assessed. Any issues/exceptions are reported first to the Global Trust Advisory Board - a committee made up of senior leaders from the business and control functions, who, as an example, may be asked to advise on the acceptance or rejection of a particular client relationship. Significant/unresolved issues are then escalated to bank’s Reputational Risk Oversight Committee.
- Senior committees are traditionally staffed with senior control function personnel. Issues identified or escalated to senior control committees may be referred to a cross-functional team or committee for further review and remediation.
- Fiduciary issues are first addressed by the Fiduciary Committee, which has representatives from Legal and Compliance as members and people from Risk and Audit as ex officio members.
- Escalation process to the appropriate committee or control function.
- At operational risk committee level.
- Reporting on near misses.
- No.

Does your organization engage in scenario analysis relating to potential fiduciary exposures/events? If so, please provide a general description of the process.

- Yes (2)
- Yes - as part of our Risk Analysis, we consider potential direction of the business within the next 6 to 12 months.
- Yes - incorporated in scenario testing for those business lines having Fiduciary Risk.
- Yes - as part of the overall Scenario Analysis process for all risk categories.
- Yes - annual process where various risks are assessed including events specific to fiduciary risk.
- Yes - we employ a structured workshop-based approach to scenario analysis. Workshops are organized along a combination of event type and business line dimension. Fiduciary risk is covered as an event type within each of the primary fiduciary businesses. Senior executives are invited to participate in these

workshops. Pre-read materials are provided to the executives in advance of the workshop, and consist of internal and industry data related to the event type being discussed. During the workshop, executives identify and validate scenarios, agree on a set of scenarios to be developed and assessed, and discuss incremental mitigation strategies.

- General OR scenario analysis process for the firm but not necessarily specific to fiduciary risk.
- Via the Operational Risk Top Risk Scenarios.
- No (2).
- No, the scenario program does not explicitly identify fiduciary events as a specific scenario, however, the potential impact where fiduciary duties are breached, are considered.

Does your firm hold capital for potential fiduciary exposures/events?

- Yes (6).
- No (3).
- Not Sure (4).

Does your organization have a fiduciary risk category to categorized and track losses?

- Yes (9).
- No (2).
- Not Sure (2).

Does the risk function participate in the annual audit planning process?

- Yes (8).
- No (5).
- Not Sure (1).

Are you focused on or aware of any industry trends that you would be willing to share with us?

- Yes (4).
- No (6).

Please explain here:

- Dodd Frank has resulted in a number of new rules that have application to our business, (i.e., Pay to Play, ADV Part 2, Large Trader, etc.)
- Legislation introduced in July 2010 as part of the U.S. Dodd-Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank”) includes a proposal to change the standard of conduct and supervision of U.S. broker-dealers based on

an SEC review of the standards that are in place under the U.S. Investment Advisors Act of 1940 for Investment Advisors who provide personalized investment advice about securities to retail customers. The SEC has not issued any proposed regulation to date.

- (a) Increased global regulatory and client pressure on custodial banks to assume a more “fiduciary-like” standard of care. (b) Department of Labor initiatives to expand the definition of a fiduciary.
- Increased focus on fiduciary risks and extreme exposures - hence our framework remains under development.

What is the governance framework for overseeing fiduciary activities and material fiduciary matters?

- Fiduciary Risk Management Committee reports to Senior Risk Committee.
- Fiduciary Oversight Committee and all other committees roll up to this committee.
- Board and Operational Risk at highest levels with Fiduciary Committees and sub-committees rolling up to them, pulled together by the Fiduciary Risk Officer.
- FULL governance with reporting up through a subcommittee of the board of directors.
- Central and reported through the board.
- Formal fiduciary committee structure with specialized committees where needed.
- The management of fiduciary risk is embedded within the governance structure that is in place for each business line and legal entity. The degree to which fiduciary risk is reflected in the established policies, procedures, and control processes (monitoring, detection, reporting, and escalation) depend upon the extent to which fiduciary risk exists in those businesses. For instance, there are specific policies and procedures, and targeted monitoring of fiduciary risk in place in our domestic and global trust businesses, while a more general, integrated focus on fiduciary risk as an element of overall risk is in place for our wealth management businesses.
- We have an overarching Trust Oversight Committee to bridge all lines of business across the company.
- The Board has established a Risk Committee which has responsibility for all areas of risk oversight, including fiduciary risk. This committee has delegated responsibility for fiduciary oversight to the Fiduciary Committee, a corporate committee comprised of senior and executive representatives from business units, Risk, Legal, Compliance and internal audit.
- The Board delegates to the Fiduciary Committee. Within the risk governance structure, the second line of defense is the Operational Risk Committee.
- Committee structure and organizational structure, i.e. CRO.
- Via Risk Committees and their sub-committees.
- Covered as a category of Operational Risk.

Does the Board or a committee of the Board oversee fiduciary activities?

- Yes (13).
- No (1).
- Not Sure (0).

Has the Board delegated fiduciary oversight to a business level committee (e.g., Fiduciary Review Committee, Compliance Committee)?

- Yes (12).
- No (2).
- Not Sure (0).

Please explain here:

- Fiduciary Committee (2).
- Fiduciary Committees focusing on various specific business activities.
- A Fiduciary Risk Management Committee which represents all Fiduciary Business lines and subsequent reporting.
- Board has delegated to the Fiduciary Risk Management Committee.
- The Board has created a sub-committee, the Finance and Trust Committee of the Board, which has in turn delegated day to day operations to the Fiduciary Oversight Committee.
- While committees are not explicitly delegated by the Board, committees with mandates covering fiduciary risk do exist as part of their overall risk management responsibilities. Fiduciary oversight is shared among the Reputational Risk Oversight Committee, the Ethics and Compliance Committee, in addition to the Risk Committee of bank's Board of Directors. While it does not provide direct approval for certain types of activities, the Reputational Risk Oversight Committee is bank's senior oversight committee responsible for providing advice and counsel on the management of reputation risk. In addition, the Audit Committee of the bank Board of Directors reviews all significant compliance issues related to fiduciary risk oversight. Various new product committees also exist within the organization, whose mandates include consideration of the potential for liability exposure that may be introduced through new products and services as well as the resulting obligation to supervise and monitor those products or services within the confines of the client relationship (fiduciary or otherwise). These committees often in place at the local business level review the appropriateness of new products and services within the context of business strategy and risk mitigation, and give consideration to the overall risk appetite established by the bank. These committees meet as often as business needs and events dictate (both regularly scheduled and ad hoc as required). Compliance program activities are overseen by the Operating Committee of the Compliance function, who in turn support the Chief Compliance Officer. A second senior management committee, the Ethics and Compliance Committee (as previously mentioned), supports bank's management of regulatory, compliance and

reputation risk through approval of bank's ethics and compliance program. In addition, significant results and issues arising from the compliance program are reported directly to the Audit Committee of bank's Board of Directors as part of the quarterly compliance reporting process. Finally, local boards/various investment committees within specific businesses (Global and Domestic Trust) may also exist and delegate additional fiduciary decision-making to certain authorized individuals/committees.

- We have an overarching Trust Oversight Committee to bridge all lines of business across the company.
- • The primary governance body for fiduciary risk is the Fiduciary committee. • The fiduciary committee is a senior management committee established by a vote of the Board of Directors. • Part of the mandate of the fiduciary committee is to assist and oversee the businesses across the Corporation in the discharge of business unit fiduciary responsibilities.
- Group Regulatory Compliance & Operational Risk Committee.

What is the committee name?

- Fiduciary Risk Management Committee (3).
- Fiduciary Committee (2).
- Fiduciary Oversight Committee (FOC).
- Fiduciary Risk Committee.
- Board has delegated to the Fiduciary Risk Management Committee.
- Trust Committee.
- Audit and Fiduciary Committee.
- Group Risk Committee.
- Group Regulatory Compliance & Operational Risk Committee
- While committees are not explicitly delegated by the Board, committees with mandates covering fiduciary risk do exist as part of their overall risk management responsibilities. Fiduciary oversight is shared among the Reputational Risk Oversight Committee, the Ethics and Compliance Committee, in addition to the Risk Committee of bank's Board of Directors. While it does not provide direct approval for certain types of activities, the Reputational Risk Oversight Committee is bank's senior oversight committee responsible for providing advice and counsel on the management of reputation risk. In addition, the Audit Committee of the bank Board of Directors reviews all significant compliance issues related to fiduciary risk oversight. Various new product committees also exist within the organization, whose mandates include consideration of the potential for liability exposure that may be introduced through new products and services as well as the resulting obligation to supervise and monitor those products or services within the confines of the client relationship (fiduciary or otherwise). These committees often in place at the local business level review the appropriateness of new products and services within the context of business strategy and risk mitigation, and give consideration to the overall risk appetite established by the bank. These committees meet as often as business needs and events dictate (both regularly scheduled and ad hoc as required). Compliance

program activities are overseen by the Operating Committee of the Compliance function, who in turn support the Chief Compliance Officer. A second senior management committee, the Ethics and Compliance Committee (as previously mentioned), supports bank's management of regulatory, compliance and reputation risk through approval of bank's ethics and compliance program. In addition, significant results and issues arising from the compliance program are reported directly to the Audit Committee of bank's Board of Directors as part of the quarterly compliance reporting process. Finally, local boards/various investment committees within specific businesses (Global and Domestic Trust) may also exist and delegate additional fiduciary decision-making to certain authorized individuals/committees.

How many members are on the committee?

- 4.
- 5.
- 7 (2).
- 10 (2).
- 15 (2).
- 17.
- 20 (2).
- 24.

Is the committee a subcommittee to the Board of Directors?

- Yes (5).
- No (7).
- Not Sure (1).

Who chairs the committee (functionally)?

- Chief Operational and Fiduciary Risk Officer.
- Head of the Business.
- Head of Operational Risk with Fiduciary Risk Officer as the Secretary.
- Global Head of Fiduciary Risk Management and Compliance.
- Fiduciary Risk Officer.
- Chief Fiduciary Risk Officer.
- Two business line managers.
- Corporate Risk.
- Chief Fiduciary Officer.
- Independent director.
- Non-Executive Director.
- Chief Governance Risk Officer.
- N/A

Is the committee comprised of employees from both the business and control areas of the organization?

- Yes (9).
- No (3).
- Not Sure (1).

If yes, what is the split between the business and control functions?

- 60/40 (3).
- 50/50.
- 4 LOB and 3 Control Functions.
- One business and one compliance manager for each business division.
- 8 from the control functions, 7 from the business areas.
- Business - 85% Control - 15% (legal, risk).
- 75% Business, 25% Control.
- N/A (2)

Does the committee have approval authority for certain types of activities (e.g., new discretionary services, policies) or products (e.g., CTFs, Group Trust products)?

- Yes (9).
- No (4).

How often does the committee meet?

- Monthly (3).
- Monthly and as needed.
- Quarterly (3).
- Bi-monthly (six times per annum) (4).
- Seven times a year.
- N/A.

What is the process for agenda items and issues to flow to the committee?

- Fiduciary officer works with businesses and sub-committees of FRMC.
- Compliance Officer who serves as the gatekeeper for collecting materials and creating agenda.
- Fiduciary Risk Officer as governance and advisory role pulls on subcommittee risk materials, emerging issues, notable items, industry hot-points, breaches, losses, action planning, audit matters, formal and informal risk meetings throughout quarter, etc.
- Coordinated committee/subcommittee structure - escalation based on judgment and thresholds depending on the topic.
- Several channels to escalate topics.

- Submit to committee secretary.
- Legal and compliance prepare the draft agenda for review by the line of business managers.
- The agenda is generally determined by the committee Chair with input from the committee Secretary and committee members. Business unit fiduciary committees provide periodic reporting into the fiduciary committee.
- Many subcommittees meet regularly and report actions to the Fiduciary Committee.
- Results from review process input from group Audit and control functions and agenda set by secretary and chairperson.
- Fiduciary risk presentations made periodically.
- Predominantly items raised or reported via control functions. Committee makes requests for information.
- N/A.

What are some examples of topics that might be brought before the committee?

- Business changes, account guideline exceptions.
- Material edits to policies & procedures, audit findings, regulatory findings, material business matters.
- Industry events, emerging events within businesses, new products, outstanding issues, statistical information impacting Fiduciary Business lines, performance materials, breaches etc.
- Current audit issues, regulatory changes, products, policy, etc.
- New products or business ventures.
- Valuation issues, collective fund major changes, audits, exams, etc.
- Offshoring of fiduciary activities.
- A few examples include: quarterly updates by the chairman of the asset management fiduciary committee on committee decision-making and activities; quarterly reports from the trust committee of the personal trust business; updates on emerging regulatory developments that could have an impact on our businesses; briefings by senior management of fiduciary businesses on commercial activity and business unit control programs; escalated matters requiring committee direction and support.
- All Personal Trust and Institutional Trust Administration and Investment Minutes, all fiduciary policies, fees, new products, litigation reports, etc.
- Reports of fiduciary sub-committees, audit results, insurance coverage.
- General papers presented.
- Regulatory breaches, Operational Risk loss events.
- N/A.

Does the committee provide periodic reporting to the Board of Directors?

- Yes (11).
- No (1).
- Not Sure (1).

If yes, provide how often and in what form (oral/written report)?

- Monthly CEO updates, 6 monthly Internal Audit Report.
- Quarterly via written materials and orally.
- Quarterly reporting, oral and dashboard report.
- Quarterly minutes and an annual state of the union update.
- Semi-annually in the form of a risk report and risk analysis.
- There is an annual report provided to a committee of the Board of Directors.
- Annually, a written and oral report is presented to the Board of Directors.
- Every board meeting in writing and oral.
- Report with oral presentation.
- Written.
- Oral.
- N/A.

Does the committee oversee compliance activities or are compliance program activities reviewed under a separate governance committee?

- Separate (2).
- A separate governance committee. First line of defense, the Management Committee, reports issues to the Fiduciary Committee. These issues are also shared with the Operational Risk Committee. A representative from the bank law group is a member of both Committees.
- The FOC oversees compliance activities.
- Committee includes compliance matters.
- It does oversee fiduciary compliance related matters.
- Fiduciary Compliance has a seat at the table - Fiduciary Risk sets the table - best way to explain it.
- Yes - we provide reports to the Trust Committee.
- Compliance program activities are generally overseen by a senior subject matter committee.
- Yes.
- No, but they get reports on progress.
- N/A.

Does compliance monitor the regulatory landscape for potential changes to regulations covering fiduciaries?

- Yes (13).
- No (0).

Are there business-unit specific fiduciary committees?

- Yes (12).
- No (1).
- Not Sure (1).

How do these committees function?

- Weekly to monitor new business, personal trust committee and institutional trust committee.
- Monthly and quarterly (Fiduciary Risk-driven) - subcommittees to the Fiduciary Risk Management Committee.
- Report up through corporate FRC.
- Formal charter that ties back to Fiduciary Risk Management Committee.
- Yes, business unit-specific fiduciary committees exist in certain businesses (Global Trust for instance). These committees are made up of senior trust professionals within the business whose authority is delegated to them by the Boards of Directors of the local operating companies. These Boards define who is authorized to act on their companies' behalf and also define the parameters under which they can do so. For example, the Global Trust Advisory Board (GTAB) sits over all of the Global Trust Platform entities. GTAB is responsible for policy development and oversight for the Global Trust platform, as well as for the escalation of cases that meet defined criteria.
- Independently with a reporting line to the fiduciary committee.
- Subcommittees for Personal Trust, Institutional Trust and Investments align with business units.
- Part of the Risk Governance in the business.

Do business unit fiduciary committees provide periodic reporting to a corporate fiduciary committee?

- Yes (9).
- No (3).
- Not Sure (1).

Is there a separate committee that oversees conflict issues?

- Yes (5).
- No (8).

If yes, what types of issues are within the committee's scope (e.g., affiliated trading, protection of material non-public information, business entertainment and workplace gifts, etc.)?

- Ethics & Compliance.
- No, there are 3 committees that oversee conflict issues at our bank. These include the Risk Committee of the Board, the Group Risk Committee, and the Ethics and Compliance Committee. The Risk Committee of the bank Board of Directors has responsibility for ensuring management has policies and procedures in place to identify and manage potential conflicts. Responsibility for the establishment of such policies on an enterprise wide basis (i.e. bank's Code of Conduct, and Conflicts of Interest Policy) is with the Compliance function. The Ethics and Compliance Committee is the management-level approval body for such policies. The Ethics and Compliance Committee will recommend approval to the Group Risk Committee who will in turn, once in agreement, recommend approval to the Risk Committee of the bank's Board of Directors.
- Conflict issues are managed at the business unit level by business unit compliance and/or fiduciary committees.
- Code of Ethics Officer is a member of the second line of defense risk management team.
- Anything that could put the franchise at risk.
- Regulated issues and bribery issues are covered in separate committees.

Can you describe how the committee is currently constituted (i.e., number of members, areas represented, etc.)?

- The Risk Committee is composed of at least 5 directors of the Board. The chair is appointed by the directors once a year. The Group Risk Committee is comprised of the Group Executive or senior management team of our bank and is chaired by the President and CEO. The Ethics and Compliance Committee is chaired by the CRO, with senior representatives from all functions and businesses as members.
- Membership on these committees is composed of senior business-unit and control personnel.
- Senior members of control functions.
- Various.

If no, how are conflict issues managed within your firm?

- The Fiduciary Oversight Committee.
- Through the current governance structure.
- Although we have multiple committees with a role in overseeing conflicts issues, the management of such issues is primarily via enterprise and business-specific policies. Conflicts are addressed generally in bank’s Code of Conduct. As well, bank has an enterprise-wide Conflicts of Interest Policy that provides minimum requirements to identify conflicts of interest in order to eliminate or satisfactorily manage them. Supporting this policy are separate Control Standards for Outside Activities, External Directorships and Gifts and Entertainment. We also have an enterprise-wide Personal Trading Policy which is aimed at preventing all employees of the bank globally from breaching the prohibitions against improper trading, including insider trading, either intentionally or inadvertently. Conflicts of interest must be disclosed and approved in writing where it is known to exist and can be appropriately managed. Each business and functional unit must keep a central record of all such disclosures and approvals within the unit and report them and all corrective action through the Human Resources Code Centralized Reporting Process. Additionally within the businesses there are a variety of committees that review potential issues with client relationships (i.e. Equity Commitments Committee).
- e.g., Gift registers, Insider trading controls.

If there is any additional feedback you would like to provide in regard to fiduciary risk, please provide below:

- Fiduciary Risk is not currently managed as a discrete risk category within the Group, but is incorporated within regulatory compliance and operational risk policies and procedures.