RISK MANAGEMENT PRINCIPLES

JONATHAN FOXX*

A number of years ago I coined the term "Mortgage Risk Management," in order to differentiate managing mortgage risk from the many other types of risk management. At that time, risk management was associated mostly with such areas as pharmaceutical companies, stock brokers, and information technology firms. My view was that mortgage loan originations and mortgage servicing present a unique set of risks to consumers, loan originators, mortgage servicers, and those industries and individuals that depend on the foregoing for their financial well-being. The term became popular and is in now in commonplace use.

But I also realized that managing mortgage risk would require a strong commitment on the part of companies, because regulatory oversight would fluctuate, often prey to the prevailing politics, and that meant companies had to build out an environment where managing risk could be joined to complying with the regulations themselves. I felt that a company could be successful in managing its mortgage risk if it developed a "Culture of Compliance."[i] I wrote articles on the Culture of Compliance and gave numerous talks on this subject. In due course, the term was picked up by regulators and made a feature of everyday parlance.

I think consumers, mortgage loan originators, and regulators read my articles and attend my lectures because I strive to give everyone a fair shake. I call it like I see it, without fear of whether some view or another is stepping on somebody's sacred political toes. Sometimes there really is a right and a wrong, irrespective of the controversy surrounding a regulatory mandate.

My standard is simple: doing all we can to protect the consumer is the only way to protect the viability of the mortgage loan originator and mortgage servicer in the long run.

And the only effective way to ensure that the originator or servicer is protected is to manage its risk. That is the basis for the formation of our firm so many years ago. Lenders Compliance Group®, which has grown to a national mortgage risk management firm over the years, has never lost its original mission to not only provide comprehensive risk management to mortgage industry participants but also offer ways and means to help build a Culture of Compliance for our clients.

Every loan originator and mortgage servicer should be a consumer advocate. Consumers will flock to the companies that present the very best standards of ethics and reliability. If any originating or servicing entity waits for a regulatory agency to tell it what to do on behalf of consumer financial protection, it has already lost the right to expect the consumer's loyalty.

Recently, one of those regulatory agencies, the Office of the Comptroller of the Currency's (OCC), issued a bulletin, entitled "New, Modified, or Expanded Bank Products and Services" ("Bulletin").[ii] Announced

* Jonathan Foxx PhD, MBA is the Chairman and Managing Director of Lenders Compliance Group®

in October 2017, the Bulletin offers an excellent understanding of risk management from a regulator's point of view. The Bulletin is meant to emphasize how best to manage the risk posed to financial institutions when they offer new, modified, or expanded products and services.[iii] These so-called "new activities" pose significant risks to financial institutions and, by extension, to consumers, businesses, and communities. In this White Paper, I will provide some highlights and insights involving the Bulletin, adding suggestions for ways and means to implement the regulatory guidance effectively.

If a financial institution is considering new activities, whether individual product roll-outs or establishing an entire origination or servicing platform, the need to manage and limit risk is ever present.

Certainly, regulators audit new activities consistent with regulatory guidelines. Consequently, a regulatory examination includes the effect of new activities on the financial institution's risk profile and the effectiveness of the company's risk management system, including due diligence and on-going monitoring efforts. Therefore, management might consider discussing plans with its regulator before developing and implementing new activities, most particularly if the new activities constitute substantial deviations from the company's existing business plans or the institution has recently been the subject of relevant administrative action.

NEW ACTIVITIES

In the first place, let's review a set of definitions that come under the rubric of "new activities." These are "new," "modified," and "expanding" products and services. It is important to categorically distinguish each of them, because each in its own way makes specific demands on risk and, by extension, the Culture of Compliance.

"New" is a product or service that differs from previous offerings and may result from relationships with third-parties. New products and services are not just those offered for the first time, but include those offerings that were previously discontinued yet re-offered again after a substantial period of time has passed. New products and services are usually the result of responding competitively in the marketplace, but also may actually be solutions for new financial markets, to gain a temporary advantage amongst competitors, add new convenience and capabilities for customers, or manage certain risks for customers.

"Modified" is the product or service that involves taking an existing product or service and substantially changing it in nature, terms, purpose, scale, or use. Wherever a change takes place, risk increases, sometimes exorbitantly!

Finally, "expanded" is a product or service that is not within a financial institution's own customer base, financial market, or delivery channel.

ROLL-OUTS

If a financial institution is considering implementing any of the above new activities, either by introducing a new product or service or establishing a new channel for originating a product or service, I suggest remembering that the regulator is going to do a deep dive and will take into consideration whether and to what extent risk management has been carefully, methodically, and fully engendered.

When a financial institution undertakes new activities, it should establish appropriate risk management processes, such procedures meant to effectively measure, monitor, and control the risks associated with them. Sometimes, implementation outstrips the development. This is hazardous to compliance administration. Strategic plans should always address the costs associated with new activities, but "costs" are not limited to monetary factors. I would say that costs must include the initial development and implementation overhead, increased expenses associated with control functions, management information systems ("MIS"), training, auditing, and compliance programs.

Indeed, management is responsible for the design, implementation, and ongoing monitoring of the financial institution's risk management system, but before introducing new activities, management should establish appropriate policies and procedures that outline the standards, responsibilities, processes, and internal controls for ensuring that risks are well understood and mitigated within reasonable parameters. The Board of Directors and/or management should oversee management's implementation of the risk management system, including execution of control programs and appropriate audit parameters over new activities.

To fail at a proper roll-out of a product, service, or channel is to incur quite a bit of risk. Errors are often expensive, debilitating to employees, triggering losses and unintended consequences, thereby provoking challenges to every risk category – such as strategic, reputation, credit, operational, compliance, and liquidity risks – and damaging the regulatory relationship. If a financial institution does not manage its product or service roll-out appropriately, it marks itself as unable to achieve business plan objectives, manage systems and control problems, possibly a violator of applicable laws and regulations, and a prey for litigators. Regulators will notice the effects relatively quickly and can go so far as to prevent the product, service, channel, or platform from continuing to exist in whole or in part. From a regulatory point of view, the safety and soundness issues presented in an improper roll-out are enormously complex, leading almost necessarily to administrative actions, especially of the financial institution has a history of improper roll-outs!

I'm going to outline the risk exposures presented by new activities, using the salient risk categories which a regulator would apply to such endeavors. If a financial institution lets implementation outpace the development, it is virtually axiomatic that there will be an insufficient and incomplete assessment of risk that will inexorably lead to an impaired and inadequate implementation of oversight and control.

RISK CATEGORIES

The following outline provides synopses of risk exposure by evaluating risk using the same categories that regulators use in regulatory examinations.

Strategic Risk

This is the risk posed to the current or projected financial condition and resilience arising from adverse business decisions, poor implementation of those decisions, or deficient responsiveness to changes in the financial services industry or operating environment.

Strategic risk almost always increases when new activities are not compatible with the financial institution's risk appetite or strategic plan or do not provide an adequate return on investment. When

our firm provides a Risk Appetite Statement, we take into consideration such factors as whether the company engages in new activities without performing adequate due diligence, including upfront expense analysis, and whether management does or does not have adequate resources, expertise, and experience to properly implement and oversee the new activities.

Reputation Risk

This risk category seems relatively intuitive to most executive managements, but it is far more than what it seems. Of course, it includes the hit to current or projected financial condition and resilience arising from negative public opinion, just like Strategic Risk. But it also is triggered where the new activities are offered without management's full understanding of consumers' needs or goals, let alone the appropriateness of the activities for the consumers or the effect on them.

We often see an increase to Reputation Risk when management, in an effort to achieve higher revenues, permits the offering of complex products or services that incorporate practices or operations that differ from the company's existing strategies, expertise, compliance culture, or ethical standards. If management permits or fails to notice poor service, inappropriate sales practices, or employee misconduct, it can easily run the risk of inadequately protecting consumer data or prompting violations of consumer protection, such as Bank Secrecy Act or anti-money laundering laws or regulations, which then opens additional exposure to litigation, adverse publicity, or loss of business.

Credit Risk

In this category we find a nexus between the current or projected financial condition of an institution and the resilience arising from an obligor's failure to meet the terms of any contract or failure to perform as agreed.

Credit Risk will certainly increase in the presence of ineffective due diligence and lax oversight of third-parties that market or originate loans on behalf of the financial institution. Often, this failure leads to low-quality loan product originations. Identifying the factors contributing to this risk category include how third-party service providers solicit and refer customers, conduct underwriting analysis, or implement loan product programs on the institution's behalf. Credit Risk, as a risk category subject to regulatory review, is a key risk found in activities in which success depends on counterparty, issuer, or borrower performance.[iv]

Operational Risk

This risk category is particularly pernicious and devastating, as it points to the difficulty in mitigating risk associated with inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.[v]

In our reviews, we have found operational risk increases when new activities do not align with the company's operational capacity, internal controls, or strategic objectives or affect the ability to maintain confidentiality, integrity, or availability of customer data. This is no small matter! A review should begin with the purpose of identifying a management failure somewhere along the line, caused usually by insufficient expertise to manage new activities. But that's the easy part!

Sometimes, new activities are not effectively implemented through well-controlled "Change Management" processes, nor even implemented by new information technologies or processes; indeed,

such defects lead to adverse results in the offering of new activities. Unfortunately, my firm has been presented with new activities being rolled out where there is no appreciable Change Management process even in place! We then scramble to ensure that the Operational Risk is correctly adjusted, so as to reduce the effects of its elevated impact. It is worth emphasizing, however, that a company's internal controls and audit plan may not be commensurate with the risks associated with the new activities.

Compliance Risk

This is where the Culture of Compliance finds its roots! Obviously, Compliance Risk involves violations of laws or regulations or non-conformance with prescribed practices, internal policies and procedures, or ethical standards. But just following the law does not fully mitigate risk! A company can promulgate all the rules it would like to see enforced, but if there is a fragile Culture of Compliance, those rules are no more than puffery and pontification.

Managing Compliance Risk is the cement that holds the company together. This risk increases when new activities are developed and implemented without adequately considering compliance with laws, regulations, ethical standards, or the company's policies and procedures.

The need to identify and mitigate Compliance Risk should happen in the roll-out process, thereby ensuring the chances that proper controls will be in place prior to the products and services being offered to consumers. In our practice, we have seen how new activities, where not properly managed, go from 'flourishing flowers' to 'choking weeds,' gradually cutting off the life of many other products and services. This is because, as new activities are developed and implemented, the potential for violations or non-compliance will increase, especially if the company's risk management system does not include appropriate audit and control features that evaluate and monitor for Compliance Risk.

The inevitable fallout from this dereliction of duty can lead to instances where the privacy of customer records is not protected or there are conflicts of interest between the financial institution and affiliated third-parties. As to any weak link in affected third-party relationships, one of several remedies would be to ensure procedures are engaged to ascertain that the company's third-party service providers and third-party originators have implemented appropriate compliance management, third-party relationship management, and information security programs.

Liquidity Risk

The risk here may be stated in no uncertain terms: it refers to the inability to meet obligations when they come due. Liquidity Risk will increase when implementing new activities, because these include a slew of financial mechanisms, such as investment alternatives for retail depositors or even sophisticated off-balance-sheet products with complicated cash-flow implications.

More often, though, Liquidity Risk is exacerbated because an offered product or service affects current or future funding costs, introduces or increases the volatility of asset/liability mismatches that are inappropriately hedged or managed, increases the rate of credit-sensitive liabilities, or affects a company's ability to meet collateral obligations.

RISK MANAGEMENT PRINCIPLES

The concept of Risk Management Principles has been a feature of regulatory compliance for a very long

time.[vi] At their most rudimentary level, these principles call for management to design an effective risk management system that identifies, measures, monitors, reports, and controls risks when developing and implementing new activities. Every financial institution, bank or nonbank, should apply these principles to the overall compliance administration structure.

There are four Risk Management Principles.

These are:

1. Adequate due diligence and approvals before introducing a new activity;
2. Policies and procedures to properly identify, measure, monitor, report, and control risks;
3. Effective change management for new activities or affected processes and technologies; and
4. Ongoing performance monitoring and review systems.

I am going to provide a generic understanding of these principles, but keep in mind that while all financial institutions should include these components in their risk management systems for new activities, the sophistication of risk management systems must reflect the company's size, complexity, and risk profile. An analysis of a risk management system should be deployed by using competent compliance professionals thoroughly familiar with risk management requirements.

I have written elsewhere on managing risk according to aspects of the Risk Management Principles;[vii] essentially, risk management systems should be sufficiently robust to keep pace with additional complexities of planned activities, and would include internal stakeholders from business units and individuals with expertise in applicable functional areas, such as legal, information technology, information security, audit, risk management, and compliance.

Risk Management Principle # 1: Due Diligence and Approvals

Management and the Board of Directors should understand the rationale for engaging in new activities and how proposed new activities meet the company's strategic objectives. Care should be taken to ensure that the due diligence review is broad enough to encompass the full exposure to the risks and benefits before any implementation commences.

A typical due diligence review should include, but not necessarily be limited to, the following undertakings. This is a "check the box" approach that is basic to such reviews.

- Identify the customer demand for the proposed new activities.
- Assess whether the risks associated with the proposed new activities are consistent with the company's strategic plan, risk profile, and risk appetite.
- Assess how the new activity affects the company's current and projected capital position; in other words, to identify risks, concerns, and necessary controls, by consulting with relevant functional areas, such as:
    - Credit,
    - Asset management,
    - Payments,
    - Compliance,
    - Accounting,

- Audit,
- Independent risk management,
- Legal,
- Operations,
- Information technology,
- Information security,
- Marketing, and
- Treasury or Asset-Liability committee.

- Determine the requirements of applicable laws and regulations and consider the principles set forth in agency guidance.
- Identify potential conflicts of interest, actual or perceived, using such information to assess any potential negative effect on the company's reputation.
- Appropriately protect any intellectual property rights.
- Determine the expertise needed to effectively manage the new activities (i.e., the need to hire or otherwise acquire additional expertise).
- Determine the operational infrastructure requirements to support the new activities (such as controls and technology architecture).
- Conduct appropriate research and analysis on relevant third-party service providers.

But the due diligence and approval process does not ever stop, even if all the boxes are checked! The financial institution should develop a business and financial plan that includes expected costs. In addition, the review would consider sales revenue targets, an assessment of the company's competitive position if it engages in the new activities, objectives and strategies for how the new activities will be brought to market, consideration of fair access to financial services and fair treatment of customers in all aspects related to the new activities, and performance or risk metrics that signal the need to pursue an exit strategy.

And, indeed, an exit strategy should be considered! Viable alternatives ought to be positioned or contemplated in the event an exit from the new activities is needed, especially if such new activities demonstrate a weakness from a performance monitoring review.

Although the Board of Directors may delegate daily managerial duties to others, it is still ultimately responsible for providing the appropriate oversight to ensure that the company operates in a safe and sound manner and in compliance with applicable laws and regulations. There is no escaping the mandates of governance.

Thus, in fulfilling its responsibilities, the Board of Directors should hold management accountable for appropriate policies and due diligence processes for new activities. This requires a set of procedures that make it incumbent on management to inform the Board of Directors of all material new activities, including due diligence findings. Plans that clearly articulate and appropriately manage risks and returns, such as through a Risk Appetite Statement, should be presented to the Board of Directors on a periodic basis.

Risk Management Principle # 2: Policies, Procedures, and Controls

Management should establish and implement policies and procedures that provide guidance on risk

management of new activities. Policies and procedures should outline not only the processes, roles and responsibilities throughout departments and functions but also any standards required to ensure implementation of and adherence to an adequate risk management system.

If a financial institution cannot check each and every one of the following boxes, it is in clear and present danger to its own viability. Read through these factors to understand the demands of implementing Risk Management Principle # 2.

- ☐ Expand or amend, as appropriate, existing policies and procedures to adequately address the new activities. This means:
  - Identifying policies and procedures relating to key business lines,
  - Establishing management's responsibility for monitoring the process, and
  - Providing for exception reporting.
- ☐ Develop and deploy MIS as necessary to monitor adherence to established objectives and properly evaluate the new activities:
  - If warranted, effectuate a timely response.
- ☐ Incorporate the new activities into the institution's independent risk management; in other words:
  - Ensure that the compliance management system and audit processes conform to policies, procedures and customer safeguards.
- ☐ Periodically review the adequacy of third-party risk management policies and procedures.

Risk Management Principle # 3: Change Management

Occasionally, when we discuss Change Management with a client, we discover that there is hardly any such mechanism in place. To my way of thinking, this is unfathomable, as the lack of Change Management procedures virtually exposes the financial institution to nearly limitless risk across all risk categories. Change Management is not some mysterious process devoid of logistical application. When properly deployed, it provides the foundation of effective corporate governance.

Effective Change Management processes enable a company to manage and control the implementation of new or modified operational processes. It makes it possible for new technologies to be added to the institution's existing technology architecture. Change Management processes always should include reviews by appropriate risk management, line managers, and senior managers in applicable business units (viz., including lending, finance, treasury, deposits, sales, underwriting, secondary, servicing, payments, compliance, audit, legal, technology, and information security). No new or modified operational process should be implemented until the foregoing departments have been consulted.

Change Management is effectively implemented when:

- ☐ Proper testing takes place on new or modified operational systems, processes, and technology.
- ☐ Risk parameters and exception reporting is approved by appropriate management.
- ☐ Mechanisms are adopted for ensuring that delivery to customers occurs as intended.
- ☐ An exit strategy is ratified by the Board of Directors that identifies and limits the adverse effect to the company and its customers in the event of a failed or flawed implementation.
- ☐ Employee training is provided for the new or modified operational process associated with the

new activities.

Risk Management Principle # 4: Performance and Monitoring

Where there is no monitoring and testing, there can be no performance metric. If the only performance criterion is the pecuniary bottom line, the financial institution has denoted its willingness to accept excessive risk. However, if management has appropriate performance and monitoring systems, including MIS, to assess whether the activities meet operational and strategic expectations and legal requirements, the company is usually able to gauge its risk appetite.

Monitoring systems must always determine the limits on the size of risk exposure that the Board of Directors and management are willing to accept with the addition of new activities.

Consider these check boxes, beginning with the risk appetite itself, such as:

- Ratifying the limits on the size of risk exposure to the new activities (viz., "Risk Appetite").
- Identifying specific objectives and performance criteria to evaluate whether the new activities are successful:
    - Being sure to include processes to periodically compare actual results with projections, such as:
        - quantitative and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- Testing processes to periodically monitor the effectiveness of operational controls and safeguards.
- Testing processes to periodically ensure compliance with applicable laws, regulatory requirements, and the institution's policies and procedures (i.e., potential risks for unfair or deceptive acts or practices).
- Specifying the "triggers" to changes in the business plan for the new activities, based on performance results.
- Ratifying a cohesive exit strategy for activities that fail to achieve projections.

THIRD-PARTY RELATIONSHIP RISK MANAGEMENT

I should like to provide a few observations about third-party risk management, which I define as any business arrangement between the financial institution and another entity, by contract or otherwise.[viii] We have extensive experience in vetting third-parties through our Vendors Compliance Group,[ix] which provides not only compilation of documents but, unlike many auditors retained for such purposes, also conducts an actual due diligence review of each vendor subject to audit.

A financial institution's management of third-party relationships should include comprehensive oversight of third-party relationships, particularly those involving critical activities. Critical activities are significant company functions, significant shared services, or other activities that could cause an institution to face significant risk.

Risk is increased if the third-party service provider or the company's relationship with the third-party service provider fails to meet expectations, causes significant customer impact, requires significant

investment in resources to implement the relationship and manage risk, or could have major impact on the financial institution's operations – especially if the company must find an alternate third-party or if the outsourced activity must be brought in-house. We have found that the nexus between third-parties and new activities is a critical juncture, but will vary in risk exposure as they may pertain to payments, clearing, settlements, custody, information technology, and other operational areas.[x]

Effective risk management processes should be commensurate with the level of risk, risk tolerance and complexity of a company's third-party relationships. A third-party service provider's inferior performance or service may result in loss of business, increased legal costs, and heightened risks, including credit, operational, compliance, strategic, and reputational risks. Such risks may be exacerbated by so-called "turnkey" or "plug and play" arrangements for products or services or the use of "white label" product branding. If there is a difference between "turnkey" and "white label," it seems that often a "turnkey" product or service is provided to a financial institution fully complete and ready for immediate use with no modifications, whereas "white label" products or services may be modified or customized and offered under the institution's own brand name. Whatever the case, there is inherently elevated risk in "turnkey" and "white label" activities, given that they are essentially designed for minimal involvement by the financial institution in administering the new activities.

When contracting with third-party service providers, company management should understand the risks associated with the new activities and conduct adequate due diligence of service providers. Due diligence includes assessing a service provider's management, reputation, product or service performance, and may also include its financial condition.[xi]

The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. Regulators are not satisfied with compilation of documents. They expect to see actual due diligence reviews conducted by the institution as part of the on-boarding and maintenance of third-party relationships.

Importantly, management should determine whether service providers and the company's new activities align with the financial institution's strategic plans and risk appetite. To accomplish this endeavor, the company must implement an on-going and effective third-party risk management program for service providers. Regulators refer to this process as the "third-party relationship's life cycle," so as to emphasize the risk management monitoring process that should continue throughout the course of the relationship. The "life cycle" should set forth an outline for managing a contingency plan in the event the financial institution terminates the relationship, a contract expires,[xii] the service provider cannot perform as expected, or the provider changes its business strategy.

FINANCIAL TECHNOLOGY

As I close, I want to emphasize that financial institutions these days are directly impacted by financial technology, so called "Fintech." Entities providing Fintech leverage emerging technologies to provide delivery channels and accessibility to financial products and services. Fintech continues to grow significantly in importance as it relates to effectuating the risk involving new activities.

Any financial institution that uses Fintech should only do so through the prudent risk management of such relationships. Often, the management of Fintech is left to the "Techies" on staff, which is

understandable, but not acceptable as a way to meet Risk Management Principles.

If the institution decides to offer Fintech solutions for the purpose of offering new activities, it is incumbent on the Board of Directors and management to understand the technologies that these companies offer, the risk and controls associated with those technologies, and the effect that a new delivery channel will have on existing operational controls.

---

[i] See, for instance, Foxx, Jonathan, *Creating a Culture of Compliance*, National Mortgage Professional Magazine, February 2014

[ii] OCC Bulletin 2017-43, *New, Modified, or Expanded Bank Products and Services, Risk Management Principles*, October 20, 2017

[iii] Bulletin 2017-43 rescinds and replaces OCC Bulletin 2004-20, *Risk Management of New, Expanded, or Modified Bank Products and Services: Risk Management Process*, issued on May 10, 2004, and Office of Thrift Supervision Examination Handbook section 760, *New Activities and Services*.

[iv] See, Foxx, Jonathan, Controlling Credit Risk, National Mortgage Professional Magazine, January 2012

[v] See, Foxx, Jonathan, The Rules of Operational Risk, National Mortgage Professional Magazine, July 2012

[vi] There are a number of policy directives set forth by the OCC over the years. The most recent include OCC - Bulletin 2013-29 - Third-Party Relationships. I have provided a Synopsis of the Supplement to that bulletin (the OCC's Synopsis was in OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"), available at our website for www.VendorsComplianceGroup.com. I would recommend also the booklet "Corporate and Risk Governance" of the *Comptroller's Handbook* and *The Director's Book: Role of Directors for National Banks and Federal Savings Associations* provide guidance on strategic planning and risk management for new activities.

[vii] For instance, see Foxx, Jonathan, *Policy, Procedures, and Examinations - Part II: Mortgage Bankers*, National Mortgage Professional Magazine, July 2013; and *Policy, Procedures, and Examinations - Part I: Mortgage Brokers*, National Mortgage Professional Magazine, March 2013

[viii] As detailed in OCC Bulletin 2013-29, third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements when a financial institution has an ongoing relationship or may have responsibility for the associated records. Also refer to OCC Bulletin 2017-21.

[ix] See www.VendorsComplianceGroup.com

[x] See OCC Bulletin 2013-29 for more information on critical activities.

[xi] See OCC Bulletin 2013-29 for a full list of due diligence responsibilities.

[xii] All third-party relationships should be governed by written contracts, and management should not overly rely on a service provider's assertions.