protiviti®
Face the Future with Confidence

2022 Regulatory Hot Topics: Considerations for Internal Audit

Expectations are that the financial services industry will experience a more challenging regulatory environment under the Biden administration than under the former administration.[1] Those who have been tapped to lead the various regulatory agencies – and even those thought to be in contention for key agency roles – have signaled their supervisory priorities, many of which align with key Biden administration goals related to climate control; diversity, equity and inclusion (DEI); and enhancing market access and protections for underserved and vulnerable consumers.

Financial institutions and their internal auditors will want to follow closely the developments on the regulatory front as new leaders operationalize their plans, but in the interim the following are some of the hot topics that banks and non-bank providers of consumer financial products and services should consider when developing their internal audit plans for compliance in the coming year.

Compliance Management Systems (CMS)

- We've observed that the regulatory agencies have consistently and significantly raised the bar in terms of their expectations for CMS.
- Practices that used to be viewed as best in class and prevalent only among the largest institutions are increasingly expected for regional and midsize organizations as well. These include:
  - Dedicated automated compliance monitoring and risk and control self-assessment reporting functions

[1] *The Changing Regulatory Posture*, Protiviti, September 2021.

        - Predictive analytics in areas such as consumer complaints
        - Formalized issue management processes that require independent credible challenge before issues can be closed
    - Internal audit functions should consider:
        - Taking a fresh look at the design and effectiveness of the organization's CMS
        - Providing an assessment of the CMS that reflects the totality of internal audit activities related to compliance management broadly (i.e., a wrapper, or roll-up, assessment that factors in the results of the CMS audit, as well as compliance-related findings and observations from operational audits)

Products and Services

- Certain products and services continue to receive heightened attention because regulators and other interested parties are concerned that terms and conditions may not be clearly understood by consumers and/or because the target market for these products and services may include less sophisticated and more vulnerable customers.
- Internal auditors should be sensitive to the particular products and services that have drawn the scrutiny of regulators or progressive lawmakers in the past or are likely to receive attention in the current environment and ensure that they have effective compliance controls in place with respect to these products or consider reducing their exposures.
- Specific examples of these types of products and services include:
    - Fee-based services, such as overdraft fees on deposit accounts, late fees on consumer loan products or other activity-related fees
    - Add-on products (broadly speaking, but particularly related to credit monitoring, identity theft and auto loans)
    - Private student lending (particularly when offered in conjunction with for-profit universities)

        - Consumer and mortgage loan servicing and loss mitigation practices, in particular loan forbearance and other loan modification processes established as a result of pandemic relief efforts
        - Buy-now-pay-later products offered in coordination with merchants
        - Virtual currencies and similar forms of electronic payments
    - Internal audit functions should consider:
        - The marketing of these products and services
        - The disclosures provided to consumers related to these products and services
        - Their financial institution's monitoring of complaints related to these products and services and, as appropriate, the timeliness and adequacy of steps taken by the financial institution to redress identified consumer problems and harm

Financial Crimes

- Over the next few years, the industry will need to address new regulations required by the Anti-Money Laundering Act of 2020 (AMLA) and consider the impact of the myriad studies required by the law.
- Important considerations will include:
    - How financial institutions are adhering to the beneficial ownership rule requirements, even in the interim period while the industry awaits rulemaking on a national registry
    - How financial institutions are providing adequate levels of governance and oversight of financial-crimes compliance processes outsourced to third parties (e.g., transaction monitoring, sanctions screening and client onboarding)
    - How financial institutions will be required to incorporate the eight National Priorities released by the Financial Crime Enforcement Network (FinCEN) on June 30, 2021 into their AML compliance programs and how examiners will evaluate how this is done; expectations will be clearer

by the end of 2021 when FinCEN is required to publish a regulation on this topic

- How financial institutions are monitoring and adhering to the evolving sanctions landscape, particularly as it relates to China and Russia
- How financial institutions respond to current events, ranging from the release of FinCEN advisories on human trafficking and ransomware to the leak of the Pandora Papers

- The ongoing nature of the COVID-19 pandemic will likely prolong the unintended consequences of rampant fraud extending from the billions of dollars in relief funds doled out to curb the pandemic by government support programs, in addition to basic fraud schemes perpetrated by bad actors. Enforcement initiatives in pursuit of persons or companies that misappropriated federal dollars will likely continue in the post-pandemic world as investigation progress and schemes are uncovered.
- Internal auditors should consider:
  - Assessing the design and effectiveness of the holistic customer due diligence process, including the beneficial ownership rule requirements
  - Reviewing policies, procedures and processes around the adequacy of the ongoing governance and oversight of AML functions outsourced to third parties
  - Confirming actions taken to current events and developments, including any FinCEN advisories
  - Assessing compliance and fraud prevention practices as part of broad efforts to strengthen areas like third-party service arrangements and general compliance structures where gaps in oversight can easily enable fraud
  - Reviewing and testing sanctions watchlist updates for both adherence to publicly available and internally developed lists
  - Evaluating the institution's plans for implementing the regulations promulgated under the AMLA as they are finalized

Debt Collection

- Supervisory and enforcement activity remains active regarding consumer debt collections, in particular third-party debt collection agencies that collect on behalf of creditors, including banks. Debt collections continue to be a significant source of consumer complaints the Consumer Financial Protection Bureau (CFPB) receives.
- The CFPB issued two final rules that will go into effect in November 2021 that impact third-party collection companies. The first rule, issued in October 2020, focuses on debt collection communications and clarifies the prohibitions of the Fair Debt Collection Practices Act (FDCPA) on harassment and abuse, false or misleading representations and unfair practices by debt collectors when collecting consumer debt. The second rule, issued in December 2020, clarifies the disclosures that debt collectors must provide to consumers at the beginning of collection communications. It also prohibits debt collectors from suing or threatening to sue consumers on time-barred debt and requires debt collectors to take specific steps to disclose the existence of a debt to consumers before reporting information about the debt to a consumer reporting agency.
- Internal auditors should consider:
  - Evaluating their institution's engagement and oversight of third-party debt collection companies, particularly in light of recent consumer complaint activity, new rulemaking from the CFPB and continued regulatory actions
  - Evaluating how their institutions are addressing debt collection practices and requirements within their internal (first-party) debt collections activities, where applicable

Third-Party Risk Management (TPRM)

- In July 2021, the banking agencies issued proposed guidance regarding the risk management of third-party relationships, which laid out a uniform set of assessment standards for TPRM programs. While the interagency guidance largely incorporates existing guidance from the various agencies, there are important additions in the guidance that financial institutions will need to consider in evaluating their TPRM programs (such as financial analysis when

conducting initial due diligence, use of consortiums for due diligence, reviewing documentation and reporting requirements against their current technology infrastructure, data models and reporting, and operational resilience). Given the interagency nature of this guidance, it is reasonable to expect renewed emphasis on third-party risk management in the near future.[2]

- In August 2021, the banking agencies issued guidance (to community banks, in particular) regarding third-party relationships and banks' assessment and usage of financial technology (fintech) companies in support of delivering products and services to consumers. Given the specialization of such firms in offering new or enhanced products and services, establishing new delivery channels and improving bank processes, partnerships with such firms are an attractive alternative to building such capabilities internally. The guidance builds on existing TPRM guidance, and its issuance signals a growing recognition of the challenges encountered by smaller banks in contracting fintech companies, as well as the potentially outsized risks these fintech companies pose to such institutions.
- Internal auditors should:
  - Routinely evaluate third-party risks to their financial institutions, both at a strategic level (i.e., a review of the TPRM program itself) as well as a tactical level (i.e., a review of high-risk third-party arrangements that impact processes subject to individual audits, such as consumer loan servicing and collections)
  - Focus on their organizations' preparedness to address the proposed TPRM guidance programmatically, as well as how their organizations manage emerging risks associated with fintech companies
  - Evaluate the manner in which their institution's TPRM and operational resilience programs intersect, including how third parties are contractually required to, and can demonstrate the ability to, deliver operations through a disruption

[2] *Proposed U.S. Interagency Guidance on Third-Party Relationships: Leveling the Playing Field for Third-Party Risk Management Requirements*, Protiviti, July 19, 2021.

Environmental, Social and Corporate Governance (ESG)

- There is rising public, political and investor pressure on firms in every sector to take ESG seriously and modify their behaviors accordingly. In particular, the financial services industry needs to adapt at both the institution level and in fund investments and loans that in turn have downstream ESG impacts.[3]
- European authorities have taken steps to require climate change-related stress testing, publication of green metrics demonstrating lending to climate-friendly companies and ESG-related investment disclosures. Further action is anticipated regarding DEI efforts in the financial sector.
- In the US, the current administration issued an executive order asking regulators to start assessing climate-related financial risks and to integrate those considerations into their policy and supervision. Banking regulators have taken steps to establish senior policy roles to monitor and study climate risk. Incoming leaders at the regulatory agencies have also signaled a focus on fairness and equity within banking, supervisory and enforcement efforts against anti-predatory and anti-discriminatory activities, addressing unbanked and under-banked populations, and renewed focus on increased diversity in bank leadership. Recently the CFPB published proposed rules regarding small-business lending that would increase the amount of data publicly available to track financial institutions' efforts. Finally, public companies already are subject to certain ESG-related reporting requirements, and more are likely to be proposed by the SEC in the near future.
- Internal auditors should:
  - Evaluate how ESG-related risks are being addressed in their corporate strategies, enterprise risk-management frameworks and risk governance programs
  - Assess how the institution is documenting its ESG-related efforts for internal and external reporting purposes

[3] *Prepare for Changes as Biden Administration Sets Sight on ESG*, Protiviti, August 2021.

Fair and Equitable Banking

- Fair and equitable access to banking products and services is an example of the social aspect of an ESG risk management program. The concept of fair lending, however, is not new – requirements prohibiting discrimination in all aspects of credit and housing are rooted in long-standing banking regulatory laws and regulations (in particular, the Equal Credit Opportunity Act, or ECOA, and the Fair Housing Act, or FHA). Financial institutions have long been required to provide reporting on their lending and community investments publicly (under the Home Mortgage Disclosure Act, or HMDA, and the Community Reinvestment Act, or CRA).
- The focus of the new administration in reducing inequality and enhancing fairness in the banking industry is playing out in the leadership changes it is making at the federal banking regulators. Stated priorities from OCC leadership include vigorously enforcing fair lending laws and strengthening the CRA. The new CFPB leader's goals include making fair-lending enforcement a top priority, elevating and expanding existing investigations and exams, and adding new ones to address racial inequality.
- The CFPB has already been granted extensive authority to address unfair, deceptive or abusive acts or practices (UDAAP), which many expect will allow it to address conduct by financial institutions related to vulnerable consumers, beyond just fair lending.
- Already we have seen increased regulatory activity regarding redlining, mortgage and small-business lending reporting, the beginning of collaboration among the federal banking agencies on revising CRA requirements, and an increased scrutiny of products, services and practices that may pose risks to fair and equitable access for certain populations.
- Given the increased regulatory focus, internal auditors should:
    - Continue to evaluate the manner in which their institutions address programmatically and technically these long-standing anti-discrimination, mortgage reporting and community reinvestment requirements, including through fair lending-related reviews.

- Remain aware of and address emerging fair lending – and, more broadly, fair banking – risks to their institutions from new products, services and partnerships to underwriting techniques or servicing practices, and in turn should challenge how their institutions identify, assess and monitor these risks.

Conduct Risk

- While much of the public attention has focused largely on sales practices-related risk, conduct risk is a broader topic that can be defined as the risk of financial loss to a firm or of customer harm resulting from any willful act or omission by an employee, contractor or third party.
- The intersectionality between conduct risk and ESG programs will likely continue to put pressure on conduct risk programs now that ESG programs are facing increased scrutiny from regulators, the media and the public.
- To provide comprehensive coverage of conduct risk, internal audit should focus on the key elements of an effective conduct risk management program[4] including the following:
  - The tone being set by executive leadership should establish clear values for the fair treatment of all stakeholders
  - Management of the product lifecycle during product development should explicitly consider customer outcomes and market impacts
  - Employees should be equipped with the training and tools needed to identify and report potential conduct risk issues
  - Compensation, incentives and talent management programs should be aligned with company values and the tone being set by executive leadership.
  - Monitoring and reporting should focus on more than reward metrics such as customer complaints and look to identify proactive metrics with appropriate escalation protocols

[4] *Five Reasons for Conduct Risk Failures — With One Shared Cause*, Protiviti, 2019.

Contacts

Carol Beaumier
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Shelley Metz-Galloway
Managing Director
+1.571.382.7279
shelley.metz-galloway@protiviti.com

Steven Stachowicz
Managing Director
+1.312.931.8701
steven.stachowicz@protiviti.com

About our financial services industry practice

Disruptive technologies, evolving customer loyalty and pressure to enhance economic returns define just some of the challenges financial services organizations need to overcome by innovating and managing risks in order to succeed over the next decade. The dynamic regulatory landscape and increased emphasis on cost reduction only adds to the complexity of financial services organizations achieving profitable growth.

Protiviti's global financial services team brings a blend of proven experience and fresh thinking through a unique 50/50 mix of "home grown" talent combined with former industry professionals, including risk and technology executives, commercial and consumer lenders, compliance professionals, and financial regulators.

As a major global consultancy, we have served more than 75% of the world's largest banks, many large and midsized brokerage and asset management firms, and a significant majority of life as well as property and casualty insurers, solving our clients' issues across all three lines of defense of the business to meet the challenges of the future, today.

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO 06/21
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®