Deloitte.

Raising the bar

Latin America and Caribbean financial sector regulatory outlook 2019

December 2018

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Contents

Global foreword

Nearly ten years after the financial crisis, the long shadow it has cast has started to fade. With the exception of one final component of Basel III, most post-crisis prudential policies have now been decided, and banks in particular are now much better capitalised and more liquid than before the crisis. Amid varied approaches and timetables to national implementation of agreed prudential reforms, attention is now more acutely focused on culture and governance, the challenges of new technology, and emerging economic, market and operational risks. Firms need to be prepared to respond to this shifting focus and the new demands that it will place on them.

Lifting of accommodative monetary policy

Globally, monetary easing and low interest rates are slowly giving way to interest rate "normalisation", although rates are expected to settle at levels significantly below historical norms. The US has led the way with a series of rate rises and the Federal Reserve has begun to shrink its balance sheet. The Bank of England has tentatively begun to raise rates, and the European Central Bank is bringing an end to the expansion of its balance sheet. In Australia, interest rates remain on hold but are expected to begin rising. Japan is the major exception to this trend, with rates expected to remain low in the near future. Given the number of headwinds to the global economy (e.g. high levels of debt, elevated levels of geopolitical risk and trade protectionism), the pace of any interest rate rises is likely to be slow.

Higher interest rates may be beneficial in net terms to certain firms: banks may enjoy higher net interest margins and insurers could benefit from rising asset yields. However, interest rate normalisation may also lead to falls in some asset values and rising credit defaults as well as revealing structural weaknesses in both the global economy and individual firms. It is unclear what the overall effect of these opposing factors will be, especially at the level of individual firms and sectors.

An uncertain economic environment

Meanwhile, a period of accomodative monetary policy has contributed to a build-up of debt, with global debt levels now at $247tn[i], significantly higher than their pre-crisis peak. In many commentators' eyes, this represents a key systemic vulnerability[ii]. Low rates also contributed to a sustained search for yield that may have led many lenders and investors to move down the credit quality curve. Further, comparatively higher capital requirements for banks have

[i] IIF, Global debt monitor, July 2018.
https://www.iif.com/publication/global-debt-monitor/global-debt-monitor-july-2018
[ii] IMF, Bringing down high debt, April 2018.
https://blogs.imf.org/2018/04/18/bringing-down-high-debt/

paved the way for a rise in non-bank lending, which means that exposure to credit markets now extends to a much wider variety of firms. Both the leveraged loan and real estate markets are likely to be vulnerable to higher interest rates, whilst consumer credit expansion and the resulting high levels of personal debt may have left many consumers vulnerable to interest rate rises, especially after such a prolonged period of low rates.

Looking at the wider global economic picture, we see a mixed outlook. Economic growth continues to be strongest in parts of Asia, although Chinese growth has slowed, while the outlook for emerging and developing economies is uneven. Recoveries in both the UK and US are now close to a decade long, while Eurozone expansion—although weaker—is also well embedded. Historically, downturns or recessions have occurred at least once each decade, suggesting that such an event may be overdue[iii].

Some commentators[iv] consider that the global economy has reached its "late cycle" phase, most evident in asset valuations that appear stretched on historic bases. In the EU, close to €731bn[v] of non-performing loans continue to act as a major risk to some banks' resilience and profitability, while globally, increasing trade protectionism and political uncertainty also weigh heavily on the minds of many in the industry. Brexit continues to be a major geopolitical and regulatory uncertainty, and both regulators and politicians will attempt to mitigate its risks and effects throughout 2019. Nevertheless, if there is a disorderly Brexit, leading potentially to new political strategies and approaches, the implications for how a number of these regulatory predictions unfold in the UK could be profound.

Against this background, we expect regulators across sectors to remain highly vigilant to the risks of economic downturn and market shocks. They will likely want to use stress testing extensively to assess firm vulnerability and resilience, recognising that during a period of unprecedentedly low interest rates some business models have grown up in relatively benign conditions and have yet to be tested in a sustained downturn.

A retreat from global coordination

The global regulatory approach is changing. The aftermath of the financial crisis saw a globally coordinated response to draw up a series of new regulations which would underpin a more robust and stable financial system. However, there is starting to be a move away from

[iii] Alex J Pollock in the Financial Times, Financial crises occur about once every decade, March 2015. https://www.ft.com/content/5148cd1e-cf01-11e4-893d-00144feab7de
[iv] Etrade, Where are we in the current business cycle? June 2018. https://us.etrade.com/knowledge/markets-news/commentary-and-insights/where-are-we-in-business-cycle
[v] EBA, Risk Dashboard Data, Q2 2018

global policy making and a reduced appetite for cross-border regulatory cooperation. As a result there are increasing signs of regulatory divergence, including geographical and activity-based ring-fencing, as different regions and countries look to tailor regulations to their own needs. Global firms are, therefore, having not only to comply with these divergent rules in the different jurisdictions in which they operate, but also to optimise their local governance structures, operating models, legal entity structure, and booking models.

A shift to supervision

We do not expect regulators to embark on a path to wholesale unravelling or reversing the post-crisis reforms implemented since 2008. But it seems that, absent a significant unexpected event, there is little prospect of major new regulation, especially in relation to bank and insurance capital. Regulators' key priorities are to consolidate and safeguard and—in some jurisdictions—refine the reforms of the past decade. What we do expect is a sharp tilt away from a period of regulatory re-design and innovation, to one of operating and embedding the reformed supervisory system.

As a result, firms in many countries are seeing rising supervisory expectations, reflecting the growth of principles-based supervisory approaches that emphasise the importance of firms' governance, culture and management approach and the outcomes, both prudential and conduct, these are delivering. Firms' conduct and the treatment of their customers are also receiving increased focus in numerous countries, driven by political and regulatory concern over the perceived poor conduct of firms across all financial sectors[vi].

Supervisors are also adopting more intrusive practices, including greater use of on-site supervisory visits. This reflects global leading practice and the increasing need for supervisors to engage directly with firms in order to understand their strategies and business models, risk profiles and appetites, risk management frameworks and approaches, and to hold boards and senior management accountable for the outcomes these deliver.

New technologies

Firms, regulators, and their customers are considering the opportunities and risks associated with new technologies. For example, due to the rapid development of artificial intelligence, machine learning, and FinTech solutions, once "new" technologies are quickly becoming mainstream. The powerful impact these technologies will have should not be

[vi] FCA, Transforming Culture in financial services Discussion Paper, March 2018, https://www.fca.org.uk/publication/discussion/dp18-02.pdf

underestimated, not only on consumers, but also on regulation and supervision, too. The pace of technological change, therefore, demands deep thinking about the appropriate regulation of processes, products, and institutions to avoid regulatory gaps and to ensure financial stability and consumer protection.

These technology developments and disruption have triggered a debate around the perimeter of financial services regulation. Many incumbent firms worry that new technology-driven entrants offer services that lie outside the boundaries of existing financial services regulation and which incumbent firms find more costly to deliver because of a "compliance leakage" from the regulated activities that they are undertaking. We do not expect regulators to "come to the rescue" of incumbents, who will have to look to their own resources to rise to the challenge of competition. However, we expect that these level playing field concerns, along with worries about the role of technology in society more generally, will drive increasing interest in how FinTech firms, and crypto assets are regulated - or rather, at present, how they are not. We expect clarification of the regulatory treatment of crypto assets, especially in the areas of investment by retail consumers, money laundering and prudential capital for banks.

Acting in the face of uncertainty

While the current regulatory environment appears more settled compared to the recent past, regulators across the world continue to set high expectations intended to maintain a strong, resilient financial sector through firms having robust financial and operational resilience, supported by strong risk management and compliance capabilities. In our view, this may provide an opportunity for leading financial firms to pivot from having to build frameworks to reflect a barrage of new regulations to optimising through taking advantage of new technologies and operating models.

The world changes and regulation changes with it

The debates around the regulatory perimeter and potential fragmentation of the financial system mean that firms' operational resilience, as well as their susceptibility to cyber and financial crime, are becoming much greater issues for regulators. As part of this, we also expect a sharpening supervisory focus on how boards and senior management teams control the risks posed to them by their exposure to outsourced providers and other third parties.

The past decade has seen profound and lasting changes in the structure of the economy, employment, and society. The providers, consumers, and regulators of financial services are all changing. Ageing populations and new millennial consumers are demanding different types of financial services and products, distributed in different ways. This changing and challenging background makes it essential to consider the future of regulation holistically, rather than in a piecemeal manner. All sectors and stakeholders have an important role here, and we hope that this year's outlook from our Regulatory Centres will both inform and stimulate this discussion.

David Strachan
Center for Regulatory Strategy, EMEA
Deloitte UK

Kevin Nixon
Center for Regulatory Strategy, APAC
Deloitte Australia

Chris Spoth
Center for Regulatory Strategy, Americas
Deloitte US

Jay McMahan
Center for Regulatory Strategy, Canada
Deloitte Canada

Jorge Cayazzo
Center for Regulatory Strategy, LATAM
Deloitte Chile

Introduction

The Latin American Center for Regulatory Strategy ("LCRS") commenced operations in mid-2018 as one of three branches of the regional Americas Center for Regulatory Strategy, including also the Canadian and U.S. Centers. Through regular dialogue with financial service institutions, trade associations, regulators, supervisors, and other regulatory stakeholders, the LCRS is a source of critical insight and advice, designed to help clients anticipate change and respond with confidence to the strategic and aggregate impact of national, regional, and international regulatory trends and issues.

The 2019 Latin American and Caribbean (LATAM) financial sector regulatory outlook is the inaugural publication of the LCRS, which dissects the key regional regulatory trends the financial sector will need to monitor and address in 2019. Following an economic contraction in 2016, growth in LATAM turned positive in the past two years with probable continued momentum in 2019, owing to both a favorable external environment and improving domestic conditions. This economic growth provides a solid foundation for the financial industry to focus on the various challenges it is beginning to face, which makes 2019 a critical time for financial institutions, regulators, and supervisors alike to reevaluate the adequacy of their risk management practices - nationally and regionally- in light of the challenges ahead.

Two important themes that permeate through each regulatory topic within this report are technological disruption and a need for comprehensive risk management practices and culture. Many financial institutions have tried to patchwork solution bought approaches to the new risks and threats they are facing, such as cyber threats, financial crime, data protection, among others. While this approach may work in the short term, a reevaluation of the financial institution's risk management framework and culture is necessary to develop a comprehensive and strategic approach. A critical component to this reevaluation should be the new opportunities brought by digital transformation in the industry. The newly powerful fintech sector, artificial intelligence, cognitive technology, robotic process automation, and others should be incorporated in strategic decisions to capture the benefits and transform obsolete risk management models.

With these critical cultural shifts in mind, I'm pleased to introduce the 2019 Latin America and Caribbean financial sector regulatory outlook. This overview offers information and insights on relevant regulatory and supervisory topics for 2019, examining how areas such as risk culture; market conduct; cyber risk; fintech; Basel III implementation; financial crimes; data protection; and risk-based-supervision are becoming increasingly imperative when addressing regulatory priorities and competitive demands.

Jorge Cayazzo
Executive Director
LATAM Center for Regulatory Strategy

Risk culture

In the fight against risk, rules were the easy part

Historically, risky practices and behaviors have been at the heart of most banking crises and financial scandals. This was certainly the case during the global financial crisis of 2008, and it has characterized a number of high-profile scandals since then. But a new focus by financial institutions on building a strong risk culture is driving promising change.

As consumers and the financial services community itself demand higher standards of conduct from financial institutions—and as regulators are calling for stronger supervision to promote these standards—organizations are looking inward to improve how management and employees approach and manage risk. Indeed, they are reshaping their institutions through their risk management practices, corporate governance, leadership models, and ways of relating to customers and society.

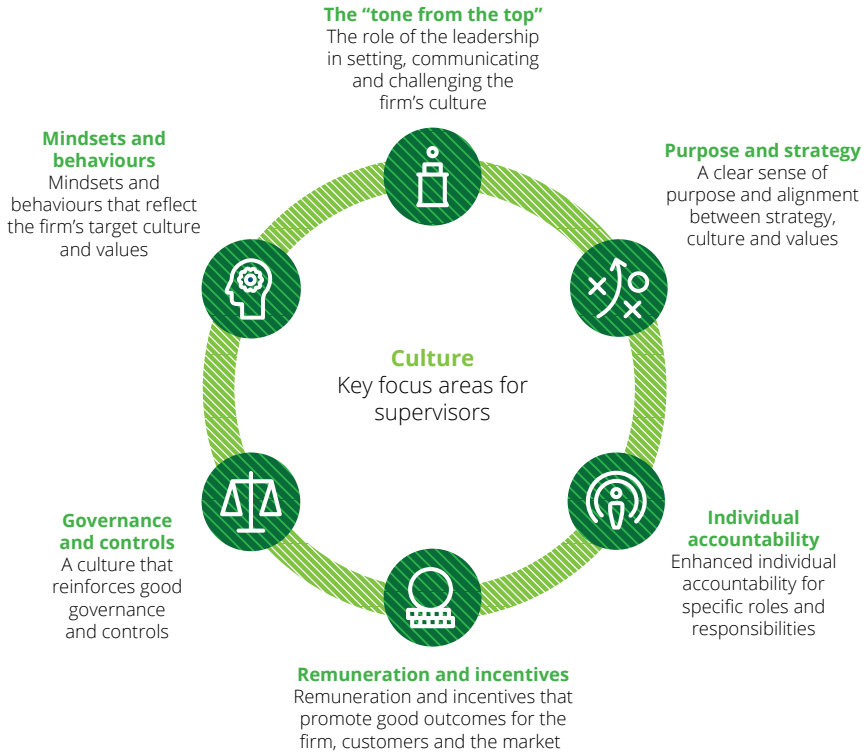
Welcome to the age of risk culture—a new focus on the values and behaviors that tie to the institution's business goals, shape risk decisions, and go beyond the simple adherence to rules and laws by embedding strong risk practices throughout the organization. Financial institutions and regulators alike now understand that well-designed controls and governance processes cannot systematically produce good outcomes without the added advantage of an effective risk culture embedded throughout an organization.

Leaving clear cut rules behind

The 2008 financial crisis focused a regulatory and supervisory spotlight on the role culture played in financial institutions' approach to managing risks. As a result, financial institutions are held to relevant regulatory standards and thresholds, and are also increasingly subject to oversight by supervisory agencies that assess the organization's risk culture and approach.

As highlighted in the G-30 Market Conduct and Culture Report[1] however, regulation has a limited role to play because culture cannot be mandated or defined simply by rules. Regulation should be used as an effective tool to outline basic principles (especially related to good risk management practices), refocus financial institutions' attention on areas of persistent conduct failure, and provide insights and lessons learned from the industry. Supervisory agencies should also play a role in monitoring and providing feedback to institutions to aid an organization's board members and senior management in addressing culture and conduct issues. Many recent regulatory initiatives have addressed general principles of behavior, which designate the leading role that the CEO and board play in promoting a tone of risk culture from the top down. These initiatives also focus on consistency and alignment across an organization's strategy, behaviors, controls, and level of employee accountability as detailed in figure A.

Figure A. Culture – Supervisory areas of focus[2]



[1] Group of Thirty (G-30), Banking Conduct and Culture, 2018.
[2] Deloitte, Culture in financial services: Scrutiny by the regulator, in principle and in practice, 2018.
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-ecrs-understanding-culture-in-financial-services-updated.pdf

Regulators and the public are holding financial institutions to a higher standard of culture.

Challenges for the LATAM region

In LATAM, a recent survey to financial institutions completed by the LCRS reveals[3] that institutions in emerging countries may have to work harder at this risk culture requirement. Most financial institutions in the region (91 percent) responded that they believe supervision over management practices is going to increase, and 86 percent said they consider improving risk management practices to be a high priority—but only 32 percent assign a high priority to risk culture.

As the awareness of and need for a stronger risk culture increase, financial institutions within the region may have to overcome lower levels of education, income distribution, health, institutionalism, lawfulness, technological development, infrastructure, and level of employment—ingredients critical for any company to move a culture forward.

Making the change real

Faced with these challenges, how can an institution in the region instill a strong risk culture that satisfies today's higher standards? The first step is to embrace the need. This is not only about satisfying others; a sound risk culture makes an institution more sustainable and promotes growth and achievement on the organization's own terms.

The most effective cultural changes will be long term initiatives and will incorporate realistic expectations from a committed senior management team. They will not be one-off exercises, but processes with regular assessments. These initiatives will instill risk culture across all three lines of defense:

Figure B. Deloitte Risk Culture Framework[4]

Risk competence
The collective risk management competence of the organisation.

Motivation
The reason why people manage risk the way that they do.

Relationships
How people in the organisation interact with others.

Organisation
How the organisational enviroment is structured and what is valued.

[3] Deloitte LATAM Center for Regulatory, La Banca en Latinoamérica Presiones y Costos al Alza, November 2018. http://felaban.net/congreso.php?id=152

[4] Deloitte, Culture in financial services: Scrutiny by the regulator, in principle and in practice, 2018. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-ecrs-understanding-culture-in-financial-services-updated.pdf

- **First line of defense:** The board, chief executive, and management teams should create the vision and aspirational culture. They should define expected behaviors that human resources can work to reinforce as it drives employee engagement and measures performance. As this unfolds, supervisors should look for the board and senior management to challenge each other—and for senior management to challenge the rest of the business.
- **Second line of defense:** Risk, ethics and compliance, internal controls, finance, and legal teams should manage, monitor, and mitigate risk. Every function should report to the executive team on risks, set policies, and provide governance.
- **Third line of defense:** Internal audit should provide assurance, advise on culture as appropriate, and validate mitigation activities. It will take a focused assessment to fully understand an organization's current risk culture and to track the progress of cultural change.

However an organization chooses to meet this challenge, it will require establishing key elements of a formal risk culture framework, as depicted in figure B. The initial focus will likely be on building cultural awareness through communications and education. Cultural improvement will likely involve meaningful changes to established ways of operating. This is an ongoing process: once the desired risk culture is in place, the organization should keep refining it to continue to reflect the business strategy.

Conclusion

No matter the cause of previous financial disruptions, the responsibility to prevent new crises rests primarily on the shoulders of financial institutions. They are under sharp scrutiny from supervisory agencies, but even greater scrutiny from their customers and the general public. Adherence is no longer the acceptable standard for protecting the system—what people want to see is an unwavering commitment to embedding a strong organizational risk culture.

That is a difficult mandate for any institution, and furthermore, in parts of the LATAM region, macro-economic and institutional factors may make it even more difficult. Moving a culture forward isn't as easy as writing new rules, but the habits that have made financial institutions strong, including the ability to break a challenge into manageable parts, can serve them well as they approach this important task.

Market conduct

Trust matters

It's no secret that the financial services industry has had its fair share of scandals in recent years, many of which were driven by questionable behavior. Many of the misdeeds were conducted by mid-level employees, but organizational pressures and lack of oversight—ultimately, accountabilities of leadership—were often cited as the driving factor.

These cases have been highly publicized and had measurable consequences to real people, including bank account holders, homeowners, and students. Not surprisingly, the reputation of the industry has taken a hit: in a 2018 Edelman global survey[5], more than 33,000 respondents from over 28 markets ranked the financial services industry as the sector they trust the least, just as they have for the last decade. The results for the largest economies in LATAM were consistent with this trend. Trust in the financial services sector in Mexico, Brazil, and Colombia (the three countries from the region included in the survey) declined from 2017 to 2018 by 2 percent, 9 percent, and 7 percent respectively.

Financial institutions have started to take action to shore up their reputations in the marketplace, with many already working to instill a stronger market conduct across their organizations. So far, those efforts have not been enough to boost their trust factors, but as they continue to address—and mitigate—the drivers of misconduct, they should realize beneficial results.

A multi-faceted threat that runs deep

Behaving in a way that inspires consumer confidence has always been important. But three emerging phenomena are making it even more urgent today:

- The increase in consumer protection regulations and more explicit official concern for consumers' rights are generating a more complex and threatening regulatory environment.

Common behaviors that drive misconduct[6]

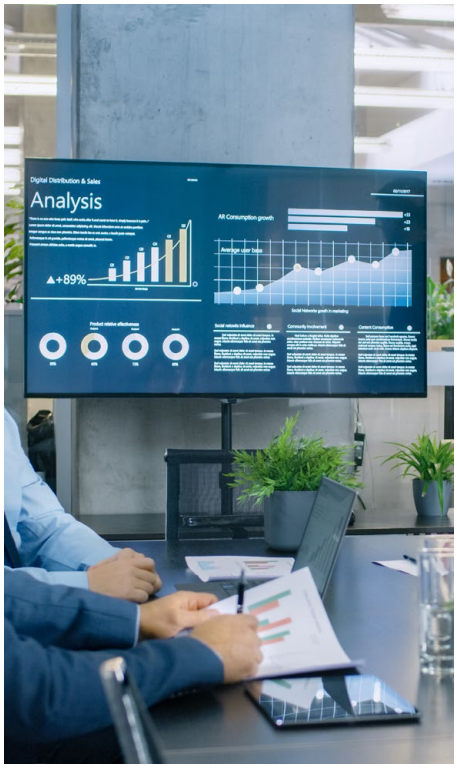
No one sets out to damage a financial institution's reputation or drive customers away, yet some common behaviors in the financial services industry can have these effects anyway. Here are eight drivers of misconduct that might be lurking in any institution today:

- **The product lifecycle is not guided by customer needs or suitability.** Product design should start with what the customer needs, not what will sell the most.
- **Human resource decisions are not based on a "balanced scorecard."** Short-term revenue cannot be the only basis for decisions that affect recruitment, promotion, or compensation.
- **Individuals and leadership are not held responsible for poor conduct.** Without visible penalties for questionable behavior, a culture of impunity can arise.
- **Conflicts of interest are not identified or managed.** People should know the correct path when they find they have competing objectives or incentives.
- **The business model is complex, disconnected, or focused on growth at all costs.** Without a clear standard for proper conduct, poor practices can incubate out of sight and spread.
- **Processes and procedures are manual and complicated.** The more labor-intensive it is to do the right thing, those who want to comply will find it harder, and those who want to misbehave will find it easier.
- **Monitoring and surveillance systems are weak.** If conduct is not detected, it can continue—or even be encouraged.
- **Disparate subcultures take hold—or the prevailing culture is problematic.** Without a consistent culture that promotes the right balance between short-term financial success and ethical business imperatives, poor conduct can take root.

[5] Edelman, 2018 Edelman Trust Barometer, 2018. https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
[6] Deloitte Centre for Regulatory Strategy, Managing Conduct Risk: Addressing Drivers, Restoring Trust, 2017. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-managing-conduct-risk.pdf

- The ever-growing adoption of technology into customer relationships can create either an advantage or a threat depending on the adequacy of the security environment.
- Increased competition can create an unlevel playing field, particularly from non-bank agents such as fintech companies that are not subject to the same regulatory and supervisory standards financial institutions have to satisfy.

If financial institutions cannot bring strong customer relationship strategies to bear against these three forces—more regulation, more technology, more competition—the associated costs will increase, and the result may compromise the foundations of the business.



Steps financial institutions can take now

There are five basic factors that can improve an institution's credibility in the eyes of consumers:

Transparency - easily understood terms and conditions
Protection - reliable fraud protection
Access - easily found product and service information
Affordability - business convenience
Support – access to real people

How can financial institutions bring those five favorable conditions into being?

- Product lifecycle: Let customer needs and suitability steer.
- Human resources: Base decisions on "balanced scorecards" that reward good conduct.
- Accountability: Hold individuals and leadership responsible for poor conduct.
- Ethics: Identify and manage conflicts of interest throughout the organization.
- Cohesion: Make the organization's business model easy to understand and follow.
- Clarity: Unify culture around a singular business purpose.
- Efficiency: Automate and streamline processes and procedures.
- Vigilance: Use advanced systems for monitoring and surveillance.
- Innovation: Manage conduct risk with new solutions.

Innovations that can help engender confidence

What kinds of tools can financial institutions use today to improve market behavior? Ones that:

- Support the ongoing assessment of customer needs and suitability
- Help build a "balanced scorecard" for HR decisions
- Streamline and strengthen accountability systems
- Identify and manage conflicts
- Help to integrate systems and teams
- Automate and streamline processes and procedures
- Modernize and automate monitoring and surveillance
- Continually test cultural values and identify red flags

Some of the tools that can accomplish these goals include robotic process automation, big data technologies and advanced analytic techniques, cognitive technologies and artificial intelligence, augmented and virtual reality, the Internet of Things, cloud applications, quantum computing, and distributed ledger technologies such as Blockchain.

Are LATAM financial institutions complacent about consumers?

A final thought: A survey of financial institutions completed by the LCRS[7] in the region reveals a paradox: two-thirds of the financial institutions (64 percent) recognize the high risk associated with consumer protection issues, yet fewer than one-quarter of them (23 percent) plan to increase the budget lines that address those needs. This signals that LATAM organizations should more closely address ways to improve their market behavior and increase consumer confidence.

Key lessons from the G-30 Market Conduct and Culture Report[8] mention that "conduct is not just about purposeful misbehavior, but also unintended consequences from decisions and/or lack of skills and knowledge." Conduct risk oversight roles and responsibilities should be clear across the various second line functions such as Human Resources, Risk, and Compliance to avoid these unintended consequences, and if that is not the reality throughout the region, budgets must be adjusted to address those needs.

Conclusion

The low trust statistics for financial institutions can serve as a wake-up call for the sector. A decade ago, the alarms rang because of deficiencies in reserve policy, regulatory compliance, and other familiar factors that related to the global recession such as employment, housing supply, and consumer spending. Today, the statistics show institutions that, despite their hard work to shore up compliance, a gap still exists in the positive perception of their ability to deliver a strong customer experience.

No matter how much a financial institution spends on marketing and branding, its real reputation will come from behavior. To curb inappropriate behaviors, institutions should know and look for the drivers that often lie at their own roots. At the same time, they should make a cultural effort to promote positive behaviors that center on access, transparency, support, and other pillars that can help make consumers feel like valued partners in a two-way relationship.

To rebuild consumer trust, financial institutions must embed ethical market conduct as a core institutional value.

[7] Deloitte LATAM Center for Regulatory, La Banca en Latinoamérica Presiones y Costos al Alza, November 2018. http://felaban.net/congreso.php?id=152

[8] Group of Thirty, Banking Conduct and Culture: A Permanent Mindset Change, 2018. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/december/Oliver_Wyman_G30_Report_on_Banking_Conduct_and_Culture.pdf

Cyber risk

Cyber risks have matured—controls must mature as well

Cyber threats and crimes against financial institutions are not only increasing, but are more sophisticated than ever. Well-organized and well-funded cybercriminals easily reach across borders, so geography is no safeguard. Yet despite a consensus that cyber risk is a significant threat for financial institutions, many entities lag behind in implementing a comprehensive response to this risk.

The damage from cyber-attacks can extend far beyond direct financial losses, which are undoubtedly damaging to the books, but are usually absorbable. It is much harder to overcome the reputational risk that results from interrupting service or losing control of confidential data. The reputational effects can distress not only a single financial institution, but the entire financial industry. As a result, cyber risk is increasingly a top priority for regulators, supervisory agencies, and financial institutions themselves.

Jurisdictions in LATAM have long instituted traditional IT security requirements, but regulators are beginning to introduce stronger cyber regulations, including cloud processing, information security, and cybersecurity. These new regulations place special responsibility on the board of directors and CEO for these areas and require enhanced information reporting systems.

Building better safeguards must be an industry wide response

There is a strong sense that cybersecurity regulation must be strengthened throughout the region to combat the increasingly sophisticated risk of cyber-attacks, and it is evident that regulators and supervisors have taken note. For example, recent initiatives in Brazil, Chile, Mexico, and Colombia are enhancing their cyber risk frameworks through developments such as cyber incident disclosures, minimum risk management practices, supervisory reporting systems, data processing and storage services, and business continuity and response action plans.

Part of a systemic response must be to strengthen supervisory capacities able to perform on-site assessments of risk management and corporate governance practices that deal with cyber risk. This includes improving the industry's ability to identify and remediate potential cyber-attacks in a timely manner. Given the nature of cyber risk, supervisory agencies should consider the establishment of secure information sharing arrangements that would allow financial institutions to collaborate across shared network to allow members of the industry to be aware of developments and help coordinate response to attacks to minimize expansion.

Financial institutions acknowledge the problem, and are working to develop comprehensive solutions that are proportional to the risk observed. Many of their core efforts to date have focused on buying packaged technological solutions, which in the short term may be sufficient to address cybersecurity. However, a detailed revision of the entire corporate governance and risk management framework is also critical, which should include the

The risk is not theoretical[9]:

In the last year, **9 out of 10** banking institutions suffered cyber incidents.

Digital security response and recovery efforts cost LATAM banking institutions **US$809 million** in 2017.

73 percent of banking institutions consider the risk of cyber breaches to be high, and **82 percent** assign cybersecurity technologies a high priority.

37 percent of LATAM banking institutions were victimized (successful attacks) and the main motivation for these attacks during 2017 were economic reasons (**79 percent** of the victim banks).

[9] Organization of American States, State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, 2018. http://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

A comprehensive risk management program would help financial institutions mitigate increasingly complex cyber risks and associated reputational risks.

incorporation of technological solutions. Given the nature of cyber risk, articulating those practices throughout the three levels of defense is also vital. Relevant questions to consider include[10]:

- Should a centralized, decentralized, or hybrid approach be taken for cybersecurity functions?
- Which factors determine the role of Chief Information Security Officers (CISOs) in terms of reporting relationships and influence within their companies?
- What role does the innovation agenda play in deciding how much of the cyber risk budget could be used for transformative vs. operational investments?
- Is there an "efficiency ratio" that can be applied to cyber risk management functions?

What is at stake and how to proceed

The reality is that cyber risks inevitably result in a degree of materialization in practice, which translates into a dangerous reputational risk for financial institutions. Due to the strong correlation between these two risks, financial institutions should consider developing and implementing an institutional wide cyber risk culture before they can develop mitigations and responses to address the full size and nature of the problem.

Each financial institution can benefit by seeing beyond its local jurisdiction to regional and global industry risks and regulatory requirements, and working from there to tailor measures to its own specific risks. Reliance on established standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework can help, as can collaboration and information-sharing mechanisms among financial institutions, even ones in competition. Awareness, preparation, and policies that promote "cyber-hygiene" are all part of an effective regime of protection.

For all these individual initiatives to work, however, it is imperative to incorporate them as part of an overarching risk culture and strategy across the institution. This will lead to a comprehensive risk management framework instead of the isolated cyber risk responses that have been the predominant approach to date. Senior management buy-in and involvement will promote a culture in which everyone embraces cybersecurity as a shared responsibility.

Digital advancements and analytics should be considered to assist in the development of a proactive cyber risk strategy. Big data and predictive analytic techniques can assist to help detect suspicious patterns, anomalies, and trigger alerts.

For regulators, it is important to keep frameworks and standards up to date as cyber risks evolve, and to foster collaboration among financial institutions to meet those challenges in a consistent, timely and unified manner.

Conclusion

Cyber risk is a disruptive force that is increasingly present in the business activities and processes of financial institutions, which can elevate other institutional risks. It thus requires an equivalent mitigating response that consists of a strategic and comprehensive risk management framework that articulates an effective institutional risk culture that permeates the entire organization.

[10] Deloitte Insights, The state of cybersecurity financial institutions, 2018. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/state-cybersecurity-financial-institutions.pdf

Fintech

Keeping up with fintech

Like most other industries, financial services is embracing the use of innovative technologies, many of which are offered by new types of companies providing electronic payments, collective financing, virtual assets, blockchain, financial advice, and other services. The benefits are easy to see: greater financial inclusion, incentives to competition, better rates and yields, services tailored to customers, and lower operational costs.

Less visible, but equally important, is the risk inherent in financial technology or "fintech"—after all, every transaction or exchange of data introduces cybersecurity and data protection risks. Institutions must fold these considerations into their enterprise-wide risk management approaches if the business structures that use the technologies are to grow and prosper.

Additionally, since much of this technology growth has taken place in a deregulated environment, or in countries whose regulatory structures are still developing, the fintech companies' irruption often creates tension within the traditional financial system and threatens to complicate efforts to maintain a level regulatory playing field.

To safeguard financial stability and transparency, authorities have started to articulate a regulatory framework for the fintech sector. These efforts are serving as a driver and accelerator for the sector's consolidation, and may result in a more prominent role for fintech in the overall financial services industry. The way in which traditional organizations will adjust to this emerging scenario is still to be determined.

What is fintech and how is it evolving?

Various bodies such as the Financial Stability Board (FSB) have defined fintech as technology-driven innovation in financial services that can result in new business models, processes, or products, with a material effect on the provision of financial services. The financial services industry is no stranger to this: ATMs, electronic payments, mobile banking, credit cards, and other technology-based tools have been commonplace for decades. So why is there renewed urgency now?

The key difference today is the pace of change in the development of new technologies and the bold impact the technologies can have on financial operations. While regulatory and public policy changes scramble to keep up with innovation and adoption, other aspects of the financial sphere have become inextricably linked with technology, including customer experience, operating efficiency, management of operating and intermediation costs, and high levels of financial inclusion.

All these factors will combine to determine the way in which financial systems are ultimately reconfigured. In the LATAM region, there will be jurisdictional variations in areas such as the legal permissibility of technology adoption by regulated entities and the legal ability of new entities to offer financial services. Right now, regional definitions of key principles are taking shape, including the laws and secondary regulations to regulate the actions of

Many fintech companies fall outside the regulatory umbrella that governs traditional financial institutions, but they are evolving fast and integrating into financial activities even faster. Regulators are working to catch up, but financial institutions should take their own steps to understand fintech and develop a clear strategy.

fintech entities. For example, in March 2018, Mexico finalized its law to regulate financial technology institutions, and subsequently published its first set of regulations covering their collective financing and electronic payments.

Amid the rapid growth of the fintech ecosystem lies an important distinction: fintech entities do not automatically fall under the traditional regulations that apply to financial institutions, but nonetheless, the safety and transparency of their services is vital to the health of the financial system. As long as technology paces ahead of regulation, this will be an area that will demand strategic focus for financial institutions and their leaders.

State of the region

The cross-border operation of entities throughout LATAM is increasingly common, which also includes companies from the United States, Europe, and Asia. Entrants seek to establish themselves in markets with high levels of consolidation and regulatory stability.

Within LATAM jurisdictions, the fintech ecosystem is growing, chiefly through entities that handle payments and remittances, loans, and business finance management. According to the Inter-American Development Bank (IDB) and Finnovista[11], between 2017 and 2018, the number of fintech ventures grew 66 percent, as 1,166 entities registered in 18 countries in the region. Brazil and Mexico are home to the most fintech entities in the region, followed by Colombia, Argentina, and Chile.

Traditional financial institutions are beginning to appreciate this sector's growth because of the benefits it provides, such as increased operational efficiencies that allow resources to focus on improving client needs. Providing faster, less costly services at any time has become a common goal for intermediaries and financial institutions alike.

Following the aforementioned publication of Mexico's financial technology regulations in March 2018, additional regional efforts have evolved to mirror those rules so entities can operate more easily across jurisdictions. For example, Chile, Colombia, Peru, and Mexico have met several times with the IDB to establish shared guiding principles. Other countries in the region such as Argentina, Brazil, Peru, and Paraguay have also worked with the IDB in different ways; in their cases, to create regulations for the collective funding (crowdfunding) of debt and capital, and to establish regulatory "sandboxes" that provide a controlled environment where innovation can flourish.

It appears, however, that regional financial institutions do not share a clear strategy on fintech companies. Some are taking a wait-and-see approach as the market matures. Some have struck strategic alliances with the new companies, while others are carrying out their own fintech initiatives in parallel, sometimes through acquisitions.

The evolution of fintech regulation in the region can positively or negatively affect the prospects for growth. Similar operating and associated regulatory conditions within individual LATAM countries provide consistency and attractiveness for new market entrants by reducing the cost and effort to adapt to each jurisdiction.

Fintech evolution will not wait

Technology will continue to grow in importance within the financial services industry, with increasingly transformational effects. New applications for disruptive technologies like blockchain, machine learning, artificial intelligence, and others are continually discovered. The connected fintech economy has been a key element in the evolution of collaborative practices like crowdfunding, and automation of client-related processes has made it easier to extend services to companies and people previously outside the scope of the financial system.

It is important to note that regulators are also riding the same wave of greater technological ability. The use of technology in the supervisory process is helping to lower the cost and effort of supervision through automated processes, improvements in customer identification, and faster delivery of high-volume information.

[11] Banco Interamericano de Desarrollo, FINTECH América Latina 2018: Crecimiento y consolidación, 2018.

The path forward

Because fintech regulation is developing rapidly, institutions should remain attentive to changes in each jurisdiction and in the overall region. They should be conscious and deliberate in determining how technology advances and regulatory changes help shape their banking strategies: whether to grow by acquisition, to partner, or to wait and see. Regardless of the short-term strategy, financial institutions should accept technological disruption in the financial services industry and leverage and adapt technologies to their businesses in a similar way.

Conclusion

While every industry is experiencing a wave of new digital technology, the financial services industry has an impressive historical track record of successfully integrating new tools. This new wave should not be any different. Financial institutions should embrace fintech, its creators, and its methods as central elements in a long-term strategy. Indeed, this may be the only way to compete in the new financial era.

Technologies and recent developments driving disruptive innovation[12]

- **Robotic process automation** (RPA) is allowing software of robots to perform routine business processes, such as moving files between folders, filling in forms, and validating data.
- New **big data technologies** and techniques are accommodating the varied and colossally-sized data sets that organizations hold so they can be efficiently aggregated, stored, and managed.
- **Cognitive technologies and artificial intelligence** (AI) are making it possible for machines to perform more and more tasks that previously required human intelligence, such as decision making, visual perception, speech recognition, analysis of unstructured data, and natural language processing (NLP), as well as learning on the basis of pure exposure to large sets (rather than through instruction).
- **Advanced analytics techniques**, such as behavioral and video analytics, that enlist sophisticated algorithms and cognitive technology allow meaningful insights to be gleaned from huge pools of data in a fraction of the time it would take a human to perform the task.
- **Augmented reality** (AR) and **virtual reality** (VR) are intersecting with Internet of Things (IoT) technology to bring virtual and real worlds together, integrating and extending the digital and physical landscapes to create a mixed reality with applications such as 3D training models and remote operation of machinery.
- **Application programming interfaces** (APIs) are facilitating the integration of systems, technologies, and functionalities.
- **Biometric technology** is providing new ways to verify identity, such as through fingerprint sensors, iris scanning, or typing tempo.
- **Cloud applications** are facilitating the hosting of data, systems, and services on the Internet, providing significant savings and greater flexibility, scalability, and configurability.
- **Quantum computing** is promising to deliver millions of times the processing capacity of a traditional computer.
- **Distributed ledger technology** (DLT), which provides a distributed, shared, and encrypted database that maintains nearly tamper-proof data, has the potential to significantly improve data security and integrity, enhance transparency and auditability, reduce the chance of single point of failure, and remove the need for third-party intermediation.

[12] Deloitte Centre for Regulatory Strategy, Managing Conduct Risk: Addressing Drivers, Restoring Trust, 2017. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsimanaging-conduct-risk.pdf

Basel III implementation

Basel moves forward, and LATAM must catch up

In December 2017, the Basel Committee on Banking Supervision (BCBS) released the second tranche resulting from the revision of the Basel II Capital Accord. The first tranche of Basel III was capital consuming, but the effect of the second tranche is expected to fall more in the areas of operational costs and the revision of business lines.

The first tranche, which revised the numerator of the capital ratio, was released two years after the 2008 financial crisis. Today, it is either in place or being implemented in many jurisdictions across the LATAM region. According to a survey conducted by the Association of Supervisors of Banks of the Americas (ASBA)[13], 16 of the 24 regional participants consider that their regulation is mainly based on Basel I and Basel II, six of them consider that their regulatory framework is aligned with the Basel III standards, and two consider that their regulation is a combination of Basel I, II, and III standards.

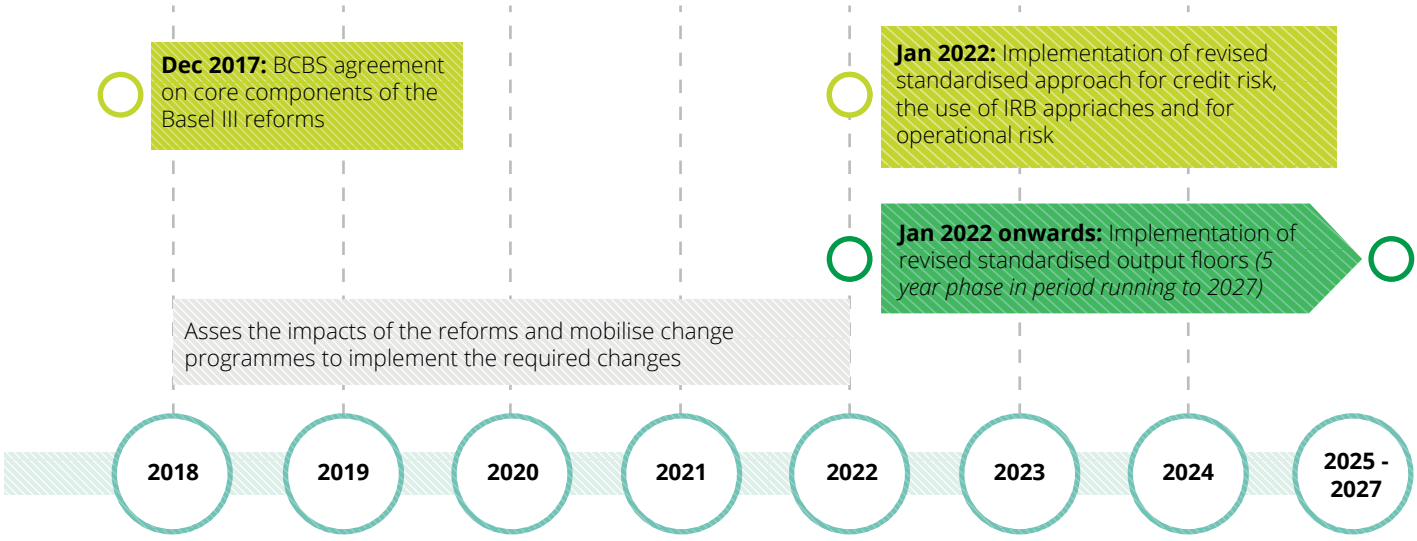
In the most recent tranche, the BCBS finally reached an agreement toward the end of 2017 over the more intricate part of the revision: calculating the denominator of the capital ratio of total risk-weighted-assets (RWA). Figure C below depicts the Basel III implementation timeline. The five-year implementation window for this second tranche extends until 2022, with an additional five-year period to phase in the output floor rule, which consists of a ceiling on the use of internal models set at 72.5 percent of the standardized model. Although the implementation period may appear reasonable, in practice, it involves various complex issues for the region—including the design of secondary regulations, the preparation of both financial institution and supervisor, and the implementation of the second tranche of the Basel Accord amendment itself.

Challenges along the way

Secondary regulations to govern the calculation of RWA are yet pending, and when issuing those, supervisors will have to decide whether to fully adopt the standardized Basel-proposed models for credit, operational, and market risk, or create standardized models that adapt to the reality of the domestic market while preserving the capital adequacy principle behind the Basel Accord.

The locally-based option makes sense on one level given that standardized Basel models have been calibrated to conditions in developed economies, which does not represent the reality of most countries in LATAM. In particular, the complexity of the activities and the composition of the loan portfolio are different in LATAM. However, supervisory agencies in LATAM may face criticism if they diverge too much from the Basel Accord. They should strive to strike

Figure C. BCBS Basell III Implementation Timeline[14]



[13] Association of Supervisors of Banks of the Americas, Supervisory And Regulatory Standards Implementation Report 2018, 2018. http://www.asbasupervision.com/es/bibl/i-publicaciones-asba/i-2-otrosreportes/ 1766-supervisory-and-regulatory-standards-implementation-report/file

[14] Deloitte, The Calm before the Reform: Basel III, 2018. www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fs-basel-iii.pdf.

the right balance in adhering to the accord while addressing local realities.

There seems to be international agreement over the need to apply proportionality to smaller and less complex financial systems as a way to avoid unintended consequences when implementing Basel III. These unintended consequences include the possibility of penalizing or favoring certain groups of financial institutions or specific segments of the loan portfolio through standardized capital charges that do not represent their inherent risks. Similarly, there may exist subsequent incentive for financial institutions to develop internal models that represent the true risk of their activities. In either case, supervisors will feel pressure to look for a balanced solution, as well as the necessity to develop a new level of preparedness to calibrate standard models, approve and supervise internal models, and ultimately help financial institutions adjust to this new regulatory environment.

The new regulations will require an entire revision and recalibration of internal models, in addition to the requirement to run the regulatory standardized model in parallel in order to compare results and apply the output floor rule. In order to carry out this new two-model regulatory approach to the satisfaction of regulatory and internal information requirements, financial institutions will need to implement new and more detailed information systems. In addition, the use of internal models will make the ongoing supervisory oversight and internal model authorization process much more complex and demanding than it is today.

Meeting the challenges

One of the main impacts of the new requirements rests in the need to streamline current management practices and operational infrastructure, particularly for risk modeling and information systems. Leadership support and consensus on strategic approaches would be key to the success of these changes. The next challenge will be the implementation of these strategies: assigning ownership, execution, controls, testing, and reporting. Financial institutions will have to reconcile governance and budget decisions, develop business requirements, and stand up new infrastructure elements to support new sourcing and reporting requirements.

Financial institutions that develop a sound strategy for the implementation of these new regulations will be well positioned for compliance purposes, for supervisory approval of their internal models, and to avoid supervisory pressures, which could include additional capital charges under Pillar 2 of the Basel Accord. These advantages will also promote efficiencies that have the potential to bolster competitiveness.

Smart steps ahead

As these new regulations come into force and drive changes across the operating model, financial institutions have a robust to-do list:

- Build capacity by training and hiring specialized risk professionals.
- Design strategic plans for capital planning and implementation.
- Calibrate internal models, including new credit and risk calculators that reflect the new methods and risk weights.

Global requirements will necessitate local translation to apply and function as intended.

- Redesign validation processes.
- Enhance information systems by adopting new data requirements such as LTV ratios, SME boundary definitions, retail credit definitions, and reference data.
- Determine the new inputs and architectures that will be required, as the increased complexity and frequency of calculations will call for performance improvements.

For supervisors, the change will also require building new capacities that are able to interpret, revise, and oversee the adequacy of internal models submitted for approval. Standardized regulatory models will have to be (re)calibrated, including possible adjustments to the standardized Basel models that may become necessary because of domestic realities. Finally, prior to releasing final regulation, supervisors should conduct an impact study to understand the full implications and avoid unintended consequences.

Conclusion

This newly realized last tranche of the Basel Accord represents a necessary step for the global community toward a one-size-fits-all approach; however, LATAM is a region where one size does not fit all. Within this region, there is a rationale to tailor Basel standards to reflect the size, complexity, and risk profile of both individual financial institutions and regional banking systems.

In practice, applying proportionality is not an easy task: it requires strong evidence to demonstrate that the divergence will positively mitigate competitive distortions without undermining key prudential safeguards.

Financial crimes

A unified front on financial crime

The financial system has always been a natural target for criminals. As horse-drawn wagons gave way to armored cars and later digital transfers, the ways institutions move value from one place to another have been a focal point of criminal threats. Today the risks are greater—not only of financial loss and penalties, but also of losses to integrity, reputation, and trust. Even without a breach, the costs associated with vigilance and compliance are rising fast.

As institutions upgrade their safeguards and operating models to keep a step ahead of the risk, the high stakes and fast pace of change make financial crime a "stay-awake" issue for senior management and board directors.

The state of threats and safeguards

Financial crime comprises an array of threats including bribery, corruption, antitrust, insider trading, market abuse, money laundering, and cybercrime. These threats—and the resulting consequences—have been especially high in the LATAM region. For instance, the World Economic Forum attributes part of the decline of competitiveness in LATAM over the last decade to corruption scandals throughout the region.[15]

Anti-money laundering (AML) authorities in LATAM are overburdened with suspicious transactions reporting that often includes little informative content and many false positives. Additionally, supervisory capacities have not progressed at the same speed or complexity as financial crime, adding to the threat. Thus, regulations to combat these risks are multiplying, which requires a new level of investment and coordination.

Without an integrated financial crime strategy, a single breach within one of the many potential risk areas could destroy value that took years to build.

Financial institutions in LATAM face a need to invest in a more comprehensive financial crime strategy—with deep knowledge of customers, markets, and threats. This approach may be less costly in the long run, and more consistent with the desires of regulatory authorities, who are expecting financial institutions to take holistic, enterprise-wide approaches.

The growing need for an interconnected strategy

An effective strategy against financial crime relies on several interconnected elements that tie together processes around customer types, third parties, products and services, and channels.

- **Strategy and risk appetite:** A clear strategic approach to financial crime with appropriate policies and standards to support the strategy.
- **Governance and oversight:** A consistent governance framework with clear senior management accountability and an effective control and assurance framework across all lines of defense.
- **Analytics, RPA, market intelligence, and reporting:** Advanced analytics to focus resources and efforts, paired with comprehensive and accessible market intelligence for effective risk management and decision-making.
- **Organization and culture:** A clearly defined organizational design with roles and responsibilities defined across all lines of defense, and experienced and knowledgeable capabilities, especially in financial crime, throughout the organization.
- **Process, policy, and procedures:** Efficient client onboarding and refresh processes with sufficient levels of consistency, control, and automation across the business.
- **Technology and systems:** Innovative financial crime tools and technologies to improve operational efficiencies and productivity and detect potential criminal threats.
- **Data:** Financial crime data clearly defined, consistently captured, and used across the business.

Steps to cement the approach

Institutions that aim to transform their previously ad hoc financial crime safeguards into data-driven, coordinated, enterprise-wide regimes can break the challenge down into a progression of discrete components:

Take a holistic approach. Learn to see financial crime as a lifecycle that comprises four stages — compliance, prevention and detection, investigation and remediation,

[15] World Economic Forum, The Global Competitiveness Report 2017–2018, 2017. http://www3.weforum.org/docs/GCR2017-2018/05FullReport/TheGlobalCompetitivenessReport2017%E2%80%932018.pdf

and monitoring and testing — then address each item. Know that no single organization has mastered it all yet, and even the most advanced are early in the journey.

Be prepared for significant cultural change. Do not underestimate what it will take on the cultural and operational fronts to revamp your approach to financial crime. Asking previously separate teams to see and act as one takes time. Set the tone at the top of the organization and work diligently to earn stakeholder buy-in. Communicate clearly and build the principles into training and workforce transitions.

Improve the quality of your data. The larger the organization, the harder it is to standardize access to high-quality data, especially in instances where multiple technology systems operate separately. Jurisdictions with restrictive data transfer laws can complicate this mandate as well. New cognitive technologies that can learn as they go and apply analytics to unstructured sources can help.

Secure the right talent — centrally and locally. An effective defense requires effective defenders. As cyber threats encroach on more industries, there is a race to attract and retain the people who have the top skills, and LATAM is among the geographies where that race is most acute. Experienced and knowledgeable financial crime resources is one of the most critical factors to operate, maintain, and sustain an effective program.

Prepare for the future. Financial crime threats evolve quickly, and a framework to address them should be built to expect the unexpected and allow for rapid change. Not only do criminals gain sophistication, but the expansion of financial products and services supplies them with an ever-broadening choice of targets.

Conclusion

Regulatory jurisdictions expect financial institutions to be aggressive partners in keeping operations legal. Financial crime keeps getting more sophisticated, but the principles of protection have largely remained the same. Keeping up with the threat to safeguard value and reputation requires heightened awareness and new tools that operate across the entire organization. There is a cost associated with meeting this challenge, but it is far smaller than the cost of failing it.

Data protection

New rules, new responsibilities, heightened risks

As data use grows exponentially and data breaches increase, the global regulatory landscape continues to adapt. This is no less true in LATAM, where some jurisdictions are evolving to modify their laws to the standards set forth in the European Union's General Data Protection Regulation (GDPR), and other countries are working to regulate data privacy for the first time. Many countries are setting up enforcement bodies with fining powers, but local organizations and multinational companies with operations in these regions should pay close attention to the way requirements and enforcement actions are taking shape in order to establish a comprehensive privacy legal framework.

Where we stand today

Various LATAM jurisdictions now have comprehensive privacy laws, including Antigua and Barbuda, Argentina, Aruba, Bahamas, Bermuda, Brazil, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, St. Maarten, Trinidad and Tobago, and Uruguay.

In other countries, these protections are still under development. Saint Lucia adopted legislation in 2011 that has yet to take effect; the Cayman Islands, Ecuador, El Salvador, Jamaica, and Panama are among the territories with draft bills that have been or may soon be introduced to their legislatures; and Chile, Costa Rica, and Peru recently enacted amendments to their existing laws.

Some of these comprehensive laws can be used as a good standard for the developing legislation. For example, the European Commission has already certified that the data protection laws of Argentina and Uruguay provide adequate protection, and Brazil has recently passed the Brazilian General Data Protection Law, which will become effective in February 2020 (see "Brazil forges its own path" sidebar ahead for further details).

Where things are heading

The reality is that countries within LATAM have to comply with the GDPR, and increased data protection risks in the industry require these countries to amend or pass new legislation to mitigate them. New or amended data privacy legislation should embody core data protection principles and requirements in some form, such as notice, choice, security, access and correction, data integrity, and data retention. Legislation should also define requirements for cross-border transfers, registration, data security, data breach notification, and the appointment of a data protection officer (DPO). The progress to pass such comprehensive legislation currently varies in degree across the region.

How changing regulations affect business

These laws are meant to protect, but violations can result in significant criminal and civil and/or administrative penalties. So far, enforcement by the region's authorities has been relatively low, in part because it has taken time to establish the local data protection authorities (DPAs). The DPAs in Colombia, Mexico, and Peru have shown active enforcement, and fines from those authorities have been quite high. For example, the Peruvian DPA levied a large fine to a foreign organization for non-compliance with the right to be forgotten. This was an important development for the region given that the Peruvian authority ruled that the foreign company was required to comply with Peruvian laws because it processed personal information of Peruvians that was accessible from Peru.

Do protections stop at the border?

The Peruvian case holds important implications for foreign organizations that conduct business in LATAM, independent of where their data processing operations are located. Most of the countries in this region restrict cross-border transfers of personal information to countries that do not provide adequate protection, similar to most privacy regulations. Within the region however, there is a heavy reliance on consent or contractual necessity to legitimize transfers to inadequately protected countries. This distinction remains largely theoretical as of now because most of the DPAs in the region have yet to issue lists of which countries they consider to provide adequate protection. Until that changes, companies are left to treat all countries as inadequate in their protections, and they must use consent, contracts, or other mechanisms to satisfy the rules and justify the exchange of information.

LATAM countries are enhancing their regulatory approach to data protection rules, which involves high costs for financial institutions. The cost of falling behind, however, may be far greater in both legal fines and reputational repercussions.

As it stands, this can result in a fairly inefficient data privacy environment for financial institutions. Until local and regional legislations (and DPAs) mature, however, institutions should consider setting up comprehensive privacy frameworks to avoid costly fines and reputational damages.

How to move forward

Organizations that process high volumes of personal information as part of their business operations in the region should research and understand all applicable data protection requirements, not only locally but country by country. For institutions that outsource more and more of their business operations, third-party and data protection risk management become even more correlated and important. Of course, there is a cost involved with this precautionary compliance, but financial institutions should think of this as an investment in competitive readiness.

Within each organization, creating a privacy legal framework for all applicable laws in every country of operation can help harmonize the approach to each applicable regulation and identify outliers. An inventory of data flows can be a complementary structure that helps financial institutions understand the requirements in each jurisdiction. As with any regulatory change, an assessment of current practices and legal obligations is likely a wise starting point. It can serve as the basis for a compliance roadmap that breaks the challenge into discrete steps, such as:

- A diligence process to identify what personal data processing activities the financial institution is engaged in (including via vendors) that are covered by relevant data protection laws.
- A gap analysis to identify which data processing activities do not satisfy the data protection requirements.
- A remediation process to close any identified gaps.
- A revision (or creation), implementation, and testing of any internal policies and procedures needed to comply with the data protection, including responding to data subject requests for access, correction, and deletion.
- Revision or creation of appropriate vendor agreements.

Brazil forges its own path

A comprehensive new data privacy law is taking shape in Brazil. The Data Privacy Protection Law (LGPD), set to take effect in February 2020, follows global trends and brings administrative sanctions that will change the way companies operate in the country.

Like the GDPR, the Brazilian LGPD establishes strict rules on processing personal data, online and offline, in both the private and public sectors. The new legislation imposes a higher standard of protection and significant fines—from 2 percent of an enterprise's gross sales to a maximum of R$50 million Brazilian reals (approximately US$12 million) for each transgression.

The main principles of LGPD are user consent and transparency. With limited exceptions for personal, journalistic, state, and other special uses, the law applies to any activity that transfers personal data of Brazilian individuals.

Like other laws in the region, Brazil's laws claim authority over activities that take place outside the country's borders, though the practical scope of enforcement remains to be seen. The law also sets an important distinction between companies with "appropriate" levels of data protection and ones without.

Conclusion

The maturity of local data protection requirements is an uneven landscape across the region as all countries race to develop the plans and tools to comply with strong multi-jurisdictional data protection requirements. Although the cost of compliance may be high, financial institutions should develop comprehensive data privacy frameworks to minimize data risk, not only to satisfy the regulations, but also to avoid costly fines and reputational damage.

Risk-based supervision

The time has come for Risk-based supervision (RBS)

In hindsight, a major contributing cause of the 2008 financial crisis was a supervisory regime that was not able to effectively identify and correct the systemic risks that arose from reckless banking practices. Reaching that conclusion has been easier than addressing it, though, in part because the response to the crisis focused first on the regulatory arena and the entire revision of the Basel Capital Accord, which took almost 10 years to finalize.

One element of that response that is finally coming into focus is Risk-based supervision (RBS). This is a risk-oriented approach to improving the effectiveness of supervision: a forward-looking approach to detect emerging risks before they materialize. Across the banking community, including among supervisors, regulators, international institutions, and the financial institutions themselves, there is a consensus that this development is overdue.

That does not make RBS easy, though, because it requires changes not only to rules and methodologies but also to organizational cultures. Implementation results so far have been modest in general. The challenge is to move people and institutions from a culture of rules to a culture of principles.

The struggle toward RBS

The distinguishing feature of RBS is that it empowers the supervisor to assess the quality of financial institutions' risk management practices, which can be only done through a qualitative analysis performed through intrusive on-site supervision, in contrast to the historical prescriptive or checklist approach.

What is Risk-based supervision?

There are various definitions of RBS, which also vary in scope. However, the most common and important feature of a risk-based supervisory approach is that it should include the supervisory assessment of the adequacy and suitability of risk management practices, including corporate governance issues, board involvement, the sufficiency of policies and procedures, the role of independent risk control instances, and the quality of risk information systems.

By any definition, this is a far deeper supervisory approach than checking adherence to rules. Still, the practice of rule-based supervision remains valuable, and RBS should be an addition, not a replacement.

Perhaps the most useful way to define an effective RBS regime is to describe what it should be able to do. This includes two important mandates:

- *An RBS regime can assess financial institutions' compliance with the prudential regulatory framework.* This requires the implementation of a comprehensive, rule-based supervisory approach aimed at identifying and recognizing risks already incurred resulting from a financial institution's business activities (financial risks) and the way they are carried out (operational risks). This is a backward-looking approach, reactive to events that have already happened.
- *An RBS regime can assess financial institutions' adherence to prudent risk management practices.* This is achieved with the implementation of a comprehensive, principles-based supervisory approach that identifies potential risks that have not yet materialized—and which may not arise if financial institutions head them off with corrective measures. This is a forward-looking approach intended to prevent emerging risks before they occur.

RBS is a cultural change from rule-based to principle-based supervision.

No matter how well-accepted RBS is, though, its main impact will be on the way supervisors and financial institutions interact. It will be natural to expect some friction. As risk increases and regulations evolve to match, supervisory expectations will grow as well.

Most countries are still applying rules-based supervisory approaches, with the hope of implementing RBS in the future. Those that have tried to adopt a more risk-oriented approach in line with RBS have usually failed and ended up reverting to the old checklist approach.

Part of the complexity lies within cultural tendencies throughout the LATAM region, which makes it difficult to overcome many of the specific challenges of RBS:

- It requires supervisors to have a comprehensive understanding of a financial institution's businesses and activities—what does the institution do, and how?
- It requires supervisors to identify the main risk exposures that arise as a natural consequence of the financial institution's activities, operations, and methods.
- It requires supervisors to assess the adequacy of risk management practices and determine whether a financial institution has a sufficiently prudent risk management environment in place to mitigate the risk it is exposed to.

Meeting these challenges requires supervisors to cultivate judgment where once they merely received and verified reports in keeping with the traditional, checklist-heavy supervisory manual that is not sufficient today. A principles-based approach requires experienced and judicious supervisors who can discriminate among different realities and apply proportional minimum management standards to gauge a financial institution's compliance with leading practices.

How to move forward

Making the operational and attitudinal switch from old methods to RBS will require both supervisors and financial institutions to take a number of concrete steps.

Supervisors should prepare and improve their approaches to RBS so they can "hit the ground running" and know what the new approach will demand of them. They should not abandon the rule-based approach for compliance however — principles-based supervision should complement the traditional approach, not replace it. Supervisors should also build the capacities they will need to create the new RBS culture and approach so they will be able to implement it adequately during assessments of financial institutions.

Within financial institutions, officers should be prepared to deal with increased supervisory expectations and help supervisors to understand their institution from the inside on an ongoing basis. As with any regime of supervision and enforcement, they should also develop strategies to deal with the challenges and risks this change will bring to their daily operations.

Conclusion

RBS is a challenge for both supervisors and supervisees because it takes them to a new arena of expectations over risk management practices: a principle-based environment that requires new and more sophisticated ways of interaction. The leaders of financial institutions in LATAM should expect to see changes in both internal and external relationships, and should plan ahead to more effectively handle these changes.

The Chilean case – main lessons learned[16]

More than two decades of experience applying an RBS approach has enabled the Superintendency of Banks of Chile (SBIF) to identify five key elements that have contributed to its success:

- ***Information system:*** The assessment of risk exposure and risk management not only relies on the on-site evaluation of financial institutions, but also significantly on the off-site work needed to monitor their performance in a timely manner. For that reason, the SBIF has a broad and solid set of standardized information, which enables the SBIF to know in general and in detail financial operations on the level of clients, products, regions, etc. This information system has enabled the SBIF not only to have an updated vision of the risk profile of each institution, but also to produce internal modeling of risk quantification and standards that facilitate the identification of risk sources and guide supervisory actions.
- ***Intrusive supervision:*** The SBIF performs extensive on-site reviews of all financial institutions with the purpose of classifying their management at least once a year. Moreover, the SBIF maintains ongoing contact with their main counterparts at the financial institutions as part of its monitoring process, in order to have an updated view of their management in terms of business, organization, products, and risk development. This practice has made the supervision process more effective, since the permanent proximity to supervised institutions has been a key factor in promoting discipline and self-regulation.
- ***Set of principles:*** In the RBS model employed by the SBIF, the assessment of the adequacy of risk management is based on the verification of the level of compliance with a set of principles that were established based on best practices in risk management. Specifically, this set of principles clearly specifies the SBIF's expectations regarding the conditions that financial institutions should meet in managing the risks they are exposed to. This practice has enabled the SBIF to define and make transparent the scope of the its assessment regarding the management of financial institutions, and it has facilitated the application of a systematic and homogeneous supervision process to all supervised institutions.
- ***Governing bodies:*** The SBIF's supervision model employs knowledge, experience, and expert judgment as pivotal elements in most of its supervision process. For this reason, it has been deemed necessary to form internal committees, so that everything that requires expert judgment is jointly analyzed and duly substantiated. This practice has facilitated the application of homogeneous assessment criteria to the different supervised institutions and, at the same time, has promoted the formation of supervisory judgment based on objective and institutionally agreed elements.
- ***Constant review of the model:*** The dynamic nature and complexity of financial activities, the experience accrued in the supervision process, and the constant evolution of the tools of knowledge determine that the RBS model must be constantly reviewed and updated to maintain its efficiency. In fact, the current RBS model employed by the SBIF is the result of successive modifications made over the course of many years. To facilitate this process, an area has been recently created within the SBIF which, among other things, constantly reviews the model. This involves verifying its correct application and identifying the changes needed to keep it up-to-date and thus ensure its effectiveness.

[16] Superintendencia de Bancos e Instituciones Financieras Chile, Chilean Model of Risk-Based Supervision, 2018.

Contacts

Leadership

Jorge Cayazzo
Executive Director, LATAM Center for Regulatory Strategy
Partner | Deloitte Chile
jcayazzog@deloitte.com

John Lowell
Manager, LATAM for Regulatory Strategy
Manager | Deloitte US
jlowell@deloitte.com

Authors

Andres Gil
Partner | Deloitte Argentina
angil@deloitte.com

Beth Dewitt
Partner | Deloitte Canada
bdewitt@deloitte.ca

Carlos Orta
Partner | Deloitte Mexico
corta@deloittemx.com

Carlos Perez
Partner | Deloitte Mexico
caperez@deloittemx.com

Gustavo Lucena
Partner | Deloitte Brazil
gustavolucena@deloitte.com

Jorge Cayazzo
Partner | Deloitte Chile
jcayazzog@deloitte.com

John Lowell
Manager | Deloitte US
jlowell@deloitte.com

Maria Mercedes Domenech
Partner | Deloitte Argentina
mdomenech@deloitte.com

Ronaldo Perez Fragoso
Partner | Deloitte Brazil
rfragoso@deloitte.com

The LCRS wishes to thank the following Deloitte professionals for their insights, contributions, and support for this report:
Mauricio Roa, Partner | Deloitte Risk Advisory, Deloitte Colombia
Allan Le Senechal Leitao, Director | Deloitte Risk Advisory, Deloitte Brazil
Veronica Rivanera, Senior Manager | Deloitte Risk Advisory, Deloitte Argentina
Giovana Gonzalez, Manager | Deloitte Risk Advisory, Deloitte Mexico
Elia Del Monte, Manager | Deloitte Marketing, Deloitte Mexico
Karina Perez, Designer | Deloitte Marketing, Deloitte Mexico

CENTER *for*
REGULATORY STRATEGY
AMERICAS

About the LCRS

The Deloitte Latin American Center for Regulatory Strategy (LCRS) provides valuable insight to help organizations in financial services keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the LCRS exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research ,forums, webcasts, and events.

Deloitte.