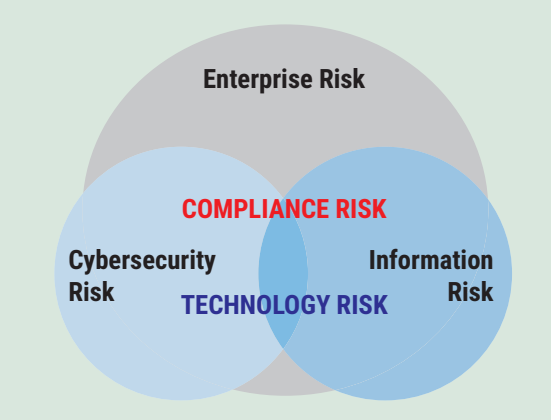
Understanding Compliance Risk in Finance and Banking

Challenges and Recommendations

Banks face multiple sources of risk. Digital transformation often increases architectural complexity and security challenges—especially considering innovations such as bring your own device (BYOD), cloud computing and cryptocurrencies. New consumer offerings and business practices, including complex financial products, acquisitions and mergers—not to mention the continuous evolution of operational management in pursuit of efficiencies—all entail their own forms of risk, even as they promise new growth and profitability. In recent years, as governments and regulators attempt to combat money laundering, terrorist financing and other illicit financial transactions, regulations have proliferated both globally and locally, in step with increasing stakeholder expectations for safe and secure operations. In this context, managing compliance risk is not just a moving target: It reflects many different targets that multiply as business and technology expand, creating new practices subject to regulation. Across the spectrum, laws, regulations, policies and standards are rapidly evolving and continue to represent the biggest overall enterprise risk. To manage compliance risk and address issues, the compliance function in banks and other financial institutions needs to build clear vision, strategies and innovative capabilities.

Compliance risk is generally considered to be an element of enterprise risk, but it is also inherited down to the roots of other risk domains.[1] Virtually all domains of enterprise risk contain significant elements of technology risk, and the intersection of technology and compliance risk, in particular, continues to be a critical focal point for regulators. Compliance risk can be incurred, for example, whenever technology compliance requirements are not met. Therefore, compliance should be construed broadly, especially as it cuts across enterprise technology, information security and cybersecurity (**figure 1**).

Figure 1—Intersection of Enterprise, Technology and Compliance Risk



The compliance landscape is changing so rapidly that banks struggle to develop and integrate their risk strategies, methodologies and frameworks across compliance, regulatory, financial and technology risk. The advancement of sophisticated technologies including cryptocurrency, big data and advanced analytics, challenges banks to proactively identify, manage and report compliance risk. Hence, relying on traditional approaches to address compliance risk is ineffective against the increasing diversity of the industry's compliance ecosystem. Compliance stakeholders are spanning senior management, media, regulators and shareholders, and defining a clear plan and strategy to regularly communicate results tailored to each stakeholder group is imperative. Therefore, banks must embrace modern and innovative strategies for risk assessment—together with an effective governance

Muhammad Waheed Qureshi, CISA, CIPP/IT, CISSP, GPEN, ITIL v3, PCIP
Is a senior IT security specialist at Nordea Bank Abp. He has approximately 10 years of experience in IT security, which includes creation and deployment of solutions and protecting networks, systems, and information assets. He is currently working as a senior IT security specialist/architect and helping with governance, risk, compliance and infrastructure security services.

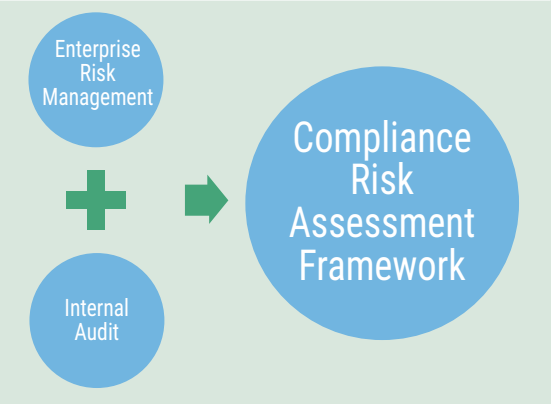
framework—to address the compliance risk across all relevant domains and align risk assessment with overall business strategy and vision (**figure 2**).

Figure 2—Risk Assessment and Business Strategy Life Cycles

Emerging Risk vs. Traditional Risk Assessment in Finance and Banking

Historically, banks have taken two approaches to risk assessment—enterprise risk management (ERM) and internal audit (IA). While these approaches can help identify certain forms of compliance risk, neither is designed to detect legal or regulatory compliance risk. A bank's compliance staff traditionally worked in a largely advisory capacity and did not pay attention to actual risk identification and management and, as a result, often lacked understanding of the overall regulatory environment, business operations and underlying technologies. To understand and manage risk exposure holistically, banks need to integrate and expand existing risk assessment processes so that they fully incorporate compliance risk exposure. In addition, banks need to adapt or build risk assessment frameworks and methodologies specifically to assess compliance risk, whose assessment differs from other forms of risk (**figure 3**). A proper assessment framework will represent the entire compliance risk landscape—and identify and categorize it into the relevant, adjacent risk domains—while proper methodology will help in assessing the risk.

Figure 3—Integration of ERM and IA Into a Holistic Compliance Risk Assessment Framework



While laws and regulations are necessary, they are not sufficient to combat challenges such as money laundering and terrorist financing; banks need dedicated, skilled and experienced investigators who can monitor large numbers of transactions on a daily basis and report suspicious behavior. From 2008 to 2018, banks and other financial institutions were fined nearly US$27 billion globally for failing to comply with anti-money laundering (AML) and know-your-customer (KYC) regulations.[2] Such compliance risk is difficult to assess with traditional approaches. Banks also need to acquire or develop more sophisticated systems to monitor all transactions. Together, investigation and monitoring will help banks develop scenarios to identify illegal transactions—for example, transactions to and from countries with a high risk of money laundering, tax evasion or other financial crime. Without appropriately trained and dedicated resources, banks will fail to build the kind of compliance competencies and expert pool needed to address the risk that accompanies legal or regulatory requirements. Banks that establish dedicated compliance roles and accountabilities across legal, compliance, audit and other business functions can better establish targeted and efficient compliance governance processes in all operational geographies.

Technology Risk

Today, modern technologies take a larger role in the financial industry. Technology can affect high-impact risk factors such as data leakage, compromised accounts and system failures. Technological transformation across the whole

banking industry has led to a constantly changing business environment. Many banks are being digitally transformed with the help of sophisticated technologies, and banks are developing innovative banking products. Consequently, digital transformation is increasing compliance and cybersecurity risk. All risk domains inherit some elements of technology risk such as technology failure disrupting operations, e.g., security infrastructure or services outage. This ultimately leads to security incidents, which may result in data leakage and the resulting legal liability, reputational damage, and compliance issues. Aside from technology risk, cybersecurity risk and risk related to information and privacy are prevalent.

Cybersecurity, Information and Privacy

Today, banks are transforming into scalable, resilient, simplified, digital institutions that offer services in the cloud. As a result, cybersecurity is a top issue and poses a big challenge in terms of compliance. Senior management has become increasingly concerned about the impact that cybersecurity (and related architectural changes) can have on business outcomes. Under immense pressure to evolve technologically, banks find themselves subject to cybersecurity rules and regulations emerging from regional and global authorities, particularly in terms of data protection; in this context, digital transformation requires banks to focus not only on business opportunity, but also on data liabilities. Responding to these rules, regulations and requirements is itself arduous and potentially self-defeating from a business standpoint, since it stretches limited resources and assets—potentially even beyond expected margins of profit—and, in many cases, can require banks to discriminate among conflicting mandates and choose which to follow. These rules and regulations ensure the confidentiality, integrity and availability (CIA) of the bank's data assets and infrastructure. Therefore, compliance with cybersecurity rules and regulations must be observed and monitored regularly and uniformly, with the same vigilance applied to other domains including financial, operational and business risk.

> "CYBERSECURITY RISK AND COMPLIANCE RISK ARE CLOSELY RELATED, AND IT CAN BE VERY DIFFICULT TO DRAW A BORDER BETWEEN THEM."

Cybersecurity risk and compliance risk are closely related, and it can be very difficult to draw a border between them. For example, the US Patriot Act requires all US financial institutions to appoint a minimum of two Bank Secrecy Act (BSA) contacts, who are responsible for reporting suspicious transactions that may identify money laundering. On 30 January 2019, BSA officers at some credit unions began to receive spoof emails that appeared to be sent from BSA officers at other credit unions.[3] A PDF file with links to malicious sites was attached to the emails. This attack reflects a targeted spear-phishing campaign—a serious cybersecurity threat. If the attack had been successful—if BSA officers had opened the PDF file, followed its malicious links and thereby allowed an attacker to breach any credit union system(s)—it could have realized both compliance and cybersecurity risk, as the breach may have compromised data privacy alongside infrastructure.

The organizational home of cybersecurity programs can sometimes complicate the management of compliance risk for cybersecurity, which, in many

> WHEN DIGITAL STRATEGY FAILS TO CONSIDER COMPLIANCE RISK IN EMERGING TECHNOLOGIES, BANKS CAN MISS OPPORTUNITIES TO DEVELOP SUSTAINABLE, RISK-BASED DIGITAL ARCHITECTURE.

banks, is still managed by the IT organization(s). IT sometimes fails to grasp the business importance of protecting information assets and, as a result, banks may lose the appropriate focus required to reduce threats and mitigate risk. When IT drives cybersecurity initiatives but lacks an understanding of the business implications of security strategy and/or relevant compliance requirements, the result can be cybersecurity outcomes that do not adequately support the overall banking business. The following questions routinely arise in cybersecurity implementations and serve to illustrate this point:

- How will encryption and decryption of online transactions be performed inside or outside a particular jurisdiction?
- Where and how will alerts and logs be generated and stored?
- While decrypting traffic externally, who will have access to the decrypted data?
- How will accountability be traced and substantiated in the event of a breach or data leakage, and how will fines be applied, if imposed by regulatory authorities?

These questions not only reflect the intersection of compliance and cybersecurity, they also underscore the perennial possibility that cybersecurity risk can turn into compliance risk, and they can only be answered by a clearly defined compliance risk strategy, especially as it informs cybersecurity execution.

Achieving compliance, it should be noted, does not necessarily guarantee a secure infrastructure; banks today are fined for security breaches even when they are considered compliant with a specific set of regulations. Banks tend to rely on *ad hoc* approaches for demonstrating cybersecurity compliance and—when the compliance function leads the charge—are often primarily motivated by a desire to avoid sanctions, fines and other consequences. Ideally, the cybersecurity function at a bank will retain the primary responsibility for identifying and documenting compliance obligations. To optimize security and manage cybersecurity compliance risk, cybersecurity initiatives should not be driven by the compliance function: Considerations around optimal cybersecurity exceed any particular set of compliance requirements. Legal and compliance functions can contribute to the discovery of such obligations, but never drive the activities.

Digital Transformation

Across the banking industry, digital transformation not only constantly reshapes the business environment, but also offers exponentially greater business opportunities based on new capabilities and services. Top management often treats digital transformation as a business proposition—whether to establish footprints in new geographies, streamline operations or increase retention. Key functions in banks that directly affect business profit and loss are heavily involved in digital transformation, and they expect to see a return on investments. Meanwhile, the compliance function is left out—or may even be considered an obstacle to achieving enterprise goals.

Digitally transformed business models in the financial industry have intensified competition, especially among banks, to become multichannel operators and accommodate ever-evolving customer behaviors. Banks embrace modern application architectures for services and find innovative ways of offering products to customers. Consequently, banks increasingly risk liability whenever customer data are not sufficiently safeguarded. The misuse of Facebook data by Cambridge Analytica and the Equifax data breach, for example, illustrate the business risk of losing or misusing data. While many banks are digitally transformed, traditional methods remain in place for internal and external audit, risk assessment, and compliance assurance. The disparity is especially

concerning given that the development of innovative banking products can multiply compliance risk factors. When digital strategy fails to consider compliance risk in emerging technologies, banks can miss opportunities to develop sustainable, risk-based digital architecture. By involving the compliance function in their digital journey, banks can better manage new risk factors and minimize their impact on existing infrastructure and business. The challenge is to manage compliance risk in more innovative ways so that compliance functions remain sustainable and relevant to the banking environment and risk ecosystem. Sustainable compliance risk management requires innovative thinking, resources whose skills are continually refreshed and updated, and investment in the right technologies. Banks have an opportunity to transform compliance activity from a cost center to a function that delivers value and instills compliance culture throughout the organization—if they equip it with the right skills and experience, for example, in emerging regulatory domains such as artificial intelligence (AI) systems and big data analytics, which are often overlooked today.

While building new capabilities around AI, advanced analytics and managed services, now more than ever, banks can establish partnerships to share infrastructure, skills and capabilities; the compliance role could be evolved to engage, support and balance business expectations, and take a more active part in supporting business processes and strategy. Compliance activities are still time-consuming and highly manual in most banks and tend to lag behind the rate of change in the risk ecosystem; consequently, they might benefit from business insights into new tools and technology.

Political Risk: Domestic and International

Compared with technical innovation, political uncertainty can pose a different kind of challenge—often less predictable and more disruptive—as banks try to manage compliance risk. In many countries, changes in domestic governments and executive administration lead to changes in regulatory priorities, variation in levels of enforcement and other challenges. International borders have always been a point of friction for banks: Shifting or ambiguous international regulations can increase geopolitical risk factors, which, in turn, can exacerbate compliance risk.

To address compliance risk, banks operating in international geographies must incorporate geopolitical risk in their overall risk management practices. Domestic compliance officers should remain alert and embrace international changes quickly. Even if regulations become more relaxed with new political winds (whether domestically or internationally), compliance officers are responsible for assessing the vacuum left in the wake of prior regulations and/or interpreting the relevance of new regulations.

Many banks have not yet developed clear processes for conducting business with politically exposed individuals, e.g., politicians, policy makers, public office personnel, and have yet to develop robust, efficient KYC procedures. As a result, banks fail to verify the identity of clients and/or fail to anticipate the risk of illegal transactions such as money laundering, terrorist funding or financial fraud in newly established business relationships. In this domain, the compliance function could take a more influential role in the front office—for example, by counseling officers with regard to the risk in doing business with politically exposed persons.

> “BANKS THAT OPERATE ACROSS INTERNATIONAL GEOGRAPHIES ARE OFTEN CHALLENGED WITH INAPPROPRIATE RISK BIAS IN ADDRESSING FINANCIAL RISK.”

The European Union (EU) continues to tighten money-laundering regulations and recommend new control measures; therefore, banks must comply not only with regional regulations, but also laws of extraterritorial origin and effect. Banks struggle to enable their IT infrastructure to accommodate stricter laws and regulations that combat money laundering, financial fraud and terrorist funding. Banks need to be adaptable, and compliance

officers must be sufficiently skilled to find opportunities for mitigating risk proactively and remain compliant. Successful banks will define and implement repeatable, manageable processes that accommodate both international and country-specific requirements.

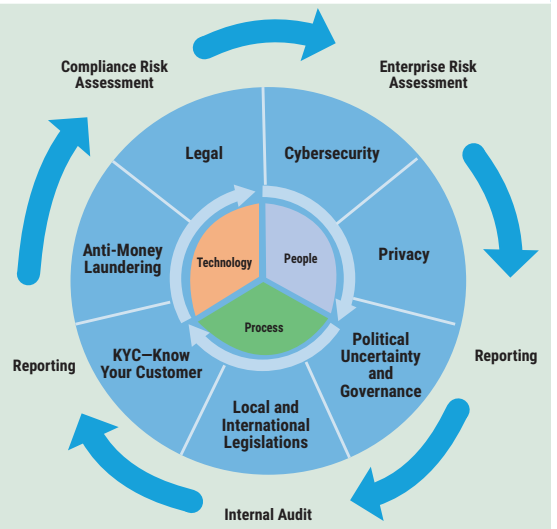
Banks that operate across international geographies are often challenged with inappropriate risk bias in addressing financial risk. Many banks prioritize risk factors related to the integrity of financial information over operational risk. Management views addressing financial risk as its top priority. Consequently, financial risk is assigned a higher proportion of risk-mitigation budget relative to nonfinancial risk.

Conflicts among regional and international regulations and/or authorities can create a challenging risk and compliance landscape for larger banks, which may even be compelled to favor one regulation over another. For example, in Europe, banks may have to choose between complying with the EU General Data Protection Regulation (GDPR) and Payments Services Directive 2 (PSD2), also known as Directive (EU) 2015/2366.[4] Banks may wonder which regulation stipulates fewer penalties? According to researchers, "In effect, a bank not 100 percent certain about the provenance of a TPP (third-party provider) requesting customer data will need to decide between declining the request (and being noncompliant with PSD2) or accepting it and, if there is a data breach, becoming liable for a sanction of up to 4 percent of global turnover under GDPR. As things stand, the outcome would presumably be to risk noncompliance with PSD2 and reject the request."[5] As transparency and privacy receive increasing emphasis from regulatory authorities worldwide, banks will operate in a risk ecosystem of increasing complexity and potential conflict.

Conclusion

Neither cybersecurity nor compliance functions are typically well positioned organizationally to influence thinking and direction at a strategic level. Consequently, banks often lack a holistic view of risk resulting from imperatives around cybersecurity, privacy and transparency. Yet, legal and regulatory landscapes across the globe are becoming more complex—and not necessarily more mutually consistent. As compliance risk emerges from new technology, products and services, the compliance risk ecosystem is also transforming rapidly. The challenge for banks to remain compliant has perhaps never been more complex and critical. Integrating regulatory changes with impacted internal policies will help to identify impacted business domains. In addition, automating workflows and tasks to trigger relevant resources, i.e., people, process and technology, in impacted business domains that are integrated with internal policies will help to achieve adequate compliance levels. Banks need to maintain internal policies and relevant technology by integrating with various regulations with which compliance is needed. To remain compliant, banks need to design automatic and continuous risk assessment workflows that draw the synergies among the compliance polices, business domains and their processes, resources (people, technology), and regulatory requirements. (**figure 4**).

Figure 4—Convergence of Multiple Risk Factors in the Compliance Risk Ecosystem



Endnotes

1 The Basel Committee of Banking Supervision defines compliance risk as "the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities." See Basel Committee on Banking Supervision, *Compliance and the Compliance Function in Banks*, Bank for International Settlements, April 2005, *https://www.bis.org/publ/bcbs113.pdf*.

2 Fenergo, "Global AML/KYC/Sanctions Fines: 2008-2018," *https://go.fenergo.com/global-regulatory-fines-2018.html*

3 Krebs, B.; "Phishers Target Anti-Money Laundering Officers at U.S. Credit Unions," Krebsonsecurity.com, 8 February 2019, *https://krebsonsecurity.com/2019/02/phishers-target-anti-money-laundering-officers-at-u-s-credit-unions/*

4 Trulioo, *Innovations in Identity*, "PSD2 vs GDPR: How to Navigate Through Conflicting Regulations," 17 August 2017, *https://www.trulioo.com/blog/psd2-vs-gdpr*

5 *Ibid*.