DESIGNING MODERN RISK MANAGEMENT PRACTICES FOR A DIGITAL-FIRST VALUE PROPOSITION

The global pandemic and related disruption further accelerated the financial services sector's migration into the digital age. The benefits of offering digital services are many – cost savings, enhanced customer experience, expanded customer base, revenue opportunities and resiliency. However, as banks migrate towards digital-first value propositions and increase their dependency on modern compliance methods, the risk function must also evolve.

We believe banks must develop specific practices for embedding effective risk management into their digital activities.

DIGITAL RISK OPERATING MODEL

Banks looking to manage risks related to digitization should consider forming a Digital Risk Operating Model (DROM) to centralize the bank's ability to define, measure and manage digital risk in a more uniform manner. The DROM, with input from other critical functions such as legal and compliance, would be responsible for:

- Identifying the regulatory requirements applicable to digital services
- Evaluating the impact of applicable regulations to the bank's business units
- And, centralizing the bank's change management response to such requirements

The DROM should identify the roles and responsibilities for digital risk across the enterprise and should identify the processes required to meet ongoing compliance obligations and increased customer expectations. These could include:

- New product approval procedures for digital services, including those provided to the bank by third parties
- Digital risk assessments, including customer data protection assessments
- Developing digital risk metrics and management reporting
- And, regulatory intake and interpretation

PRODUCT, PROCESS & PEOPLE ANALYSIS

Through the DROM, banks should evaluate existing corporate policies, procedures and processes to understand whether any gaps in regulatory coverage exist and to subsequently develop a risk-based remediation plan. The gap analysis should include a full inventory of regulatory requirements affecting a bank's digital footprint mapped to specific controls and control owners to encourage traceability.

Understanding the full regulatory environment applicable to digitization may prove more complicated than some banks anticipated. More recently, certain states have introduced comprehensive legislation designed to protect consumer data, including increased disclosure and internal risk management requirements for banks.

For example, to comply with requirements of the California Privacy Rights Act (the "CPRA") and the Virginia Consumer Data Protection Act (the "VCDPA"), banks will have to introduce new processes to identify and protect certain categories of customer data online; ensure that certain customer disclosures are made; and conduct ongoing data protection assessments. In addition, as more US states introduce their own privacy laws which may be inconsistent with each other, banks must have a process to quickly assess and respond to these requirements (such as building better data protection programs) where required. Banks with a global presence will need to further consider the impacts of requirements from the EU and APAC, such as the EU's General Data Protection Regulation (the "GDPR").

As gaps are identified and assigned to a remediation plan, banks should consider the manner in which they adopt a digital risk management function - either through large enterprise transformation or pilot programs designed to target critical areas of risk (e.g., data privacy).

DYNAMIC RISK ASSESSMENT SCANS

Banks should consider developing a digital risk assessment process that evaluates the impact of new or changed products and services offered to customers, as well as, internal compliance controls which rely on some element of digital technology. The methodology should identify risks specific to a bank's digital activities and prescribe a uniform manner to measure those risks in light of the existing control environment. As mentioned above, banks should ensure they have a process to monitor and ingest applicable regulations as they are released (e.g., state data privacy laws).

OTHER AREAS FOR CONSIDERATION

Other areas for banks to consider include:

- Reliance on third parties for new technologies
- The potential biases that ungoverned AI could introduce into redit decisioning
- The prevalence of bots without proper governance over their intended use
- The need to have risk management imbedded early in the product and service development lifecycle

A bank's digital strategy should balance risk management with the ability to foster an innovative culture. Digital governance processes must be agile enough to respond to a rapidly-evolving regulatory and technology environment without sacrificing compliance obligations or deprioritizing the customer. As the customer experience remains a driving motivation behind creating and transitioning to digital banking products and services, a comprehensive digital risk management framework can strengthen a bank's relationship with its customers by increasing confidence that each customer's personal and private data is protected from misuse.

AUTHORS

Bryce VanDiver, Partner
Spencer Schulten, Executive Director

WWW.CAPCO.COM

CAPCO

© 2021 The Capital Markets Company. All rights reserved.

JN_2949