BCG
The Boston Consulting Group

Transforming Bank Compliance with Smart Technologies

Gerold Grasshoff, Bernhard Gehra, Valerie Villafranca, Norbert Gittfried, Vincent Grataloup, Katharina Hefter, Jannik Leiendecker, and Oliver Pauly

July 2017

AT A GLANCE

Banking organizations face a challenging and complex regulatory compliance environment that demands an increased focus on combating financial crime and minimizing conduct risk. Bank compliance capabilities are under the spotlight, too, following regulatory enforcement actions that have led to the imposition of billions of dollars in penalties over recent years.

Building a Compliance Target Operating Model

One crucial aspect of establishing a cutting-edge compliance framework involves building a target operating model to handle key capabilities, particularly around managing risk and implementing appropriate controls. An optimized model will include five elements: a compliance strategy, governance and organization, compliance risk management, a people strategy, and a policy framework.

Smart Technologies in Compliance Risk Management

Among the most effective ways to perform compliance risk management is to use smart technologies, many of which can mimic human capabilities in acquiring and using data to support processes such as customer onboarding. These technologies—from optical character recognition to data mining to deep learning—can serve four categories of compliance activity: collection, analysis, learning, and action.

Banking organizations operate in an increasingly complex regulatory compliance environment that demands enhanced transparency and greater focus on combating financial crime and minimizing conduct risk. In a world of multiple threats, banks must work harder to show that they have the right controls and culture in place. Bank compliance capabilities are under the spotlight, too. Regulatory enforcement actions led to approximately $321 billion in penalties worldwide during the period from 2009 through 2016, significantly affecting earnings. (See *Global Risk 2017: Staying the Course in Banking*, BCG report, March 2017.)

Many banks initially responded to the punitive regulatory environment with quick-fix remediation programs involving new controls and a flurry of hiring. Over time, however, a more considered approach to regulatory compliance has emerged, with banks defining comprehensive compliance risk taxonomies that they can use to scope and inform target operating models. These changes mark the beginning of a compliance transformation across the industry—accompanied, unfortunately, by spiraling costs and pressure on human resources.

Digitization, the final stage in the transformation process, has the potential to create a step change in compliance operations. The catalyst is the emergence of smart technologies, which offer significant performance improvements and the ability to mimic human capabilities such as learning, language use, and decision making.

Digitization, the final stage in the transformation process, has the potential to create a step change in compliance operations.

Smart technologies have multiple potential applications in the context of compliance, from support for relatively routine tasks in client onboarding to analysis of unstructured data sets—for example, in relation to money laundering. Across the board, these technologies offer a route to significant efficiency gains and can help employees work more effectively.

Developing a Compliance Target Operating Model

The starting point in building a cutting-edge compliance framework is to establish a taxonomy that describes and classifies key areas of risk. Such a taxonomy is also a prerequisite for defining the scope of a target operating model. The six most relevant types of compliance risks relate to financial crime and conduct.

Three of the six types involve forms of financial crime risk:

- **Money Laundering and Terrorism Financing.** Disguising the source of the proceeds of crime and handling funds relating to terrorist funding

- **Sanctions and Embargoes.** Dealing improperly with designated persons, entities, or countries

- **Bribery and Corruption.** Involvement of customers or employees in bribery, corruption, and (in some cases) fraud

Three other types involve forms of conduct risk:

A comprehensively defined risk taxonomy puts banks in a position to redesign the compliance target operating model.

- **Market Conduct.** Relating to global and local rules in dealings with securities (such as insider trading or market manipulation)

- **Customer Conduct.** Concerning product suitability, cross-border business, transparency obligations, and resolution of client-related conflicts of interest

- **Culture and Ethics.** Addressing the establishment of a sound corporate culture to promote ethical business behavior

In addition to handling these types of risk, the compliance function encompasses regulatory compliance, which requires a detailed understanding of global and local rules and the authority to assign responsibilities to relevant internal departments.

A comprehensively defined risk taxonomy puts banks in a position to redesign the compliance target operating model, thereby clarifying roles and responsibilities and creating a more standardized and reliable compliance infrastructure. An optimized target operating model comprises five key elements: a compliance strategy, governance and organization, compliance risk management, a people strategy, and a policy framework. (See Exhibit 1.)

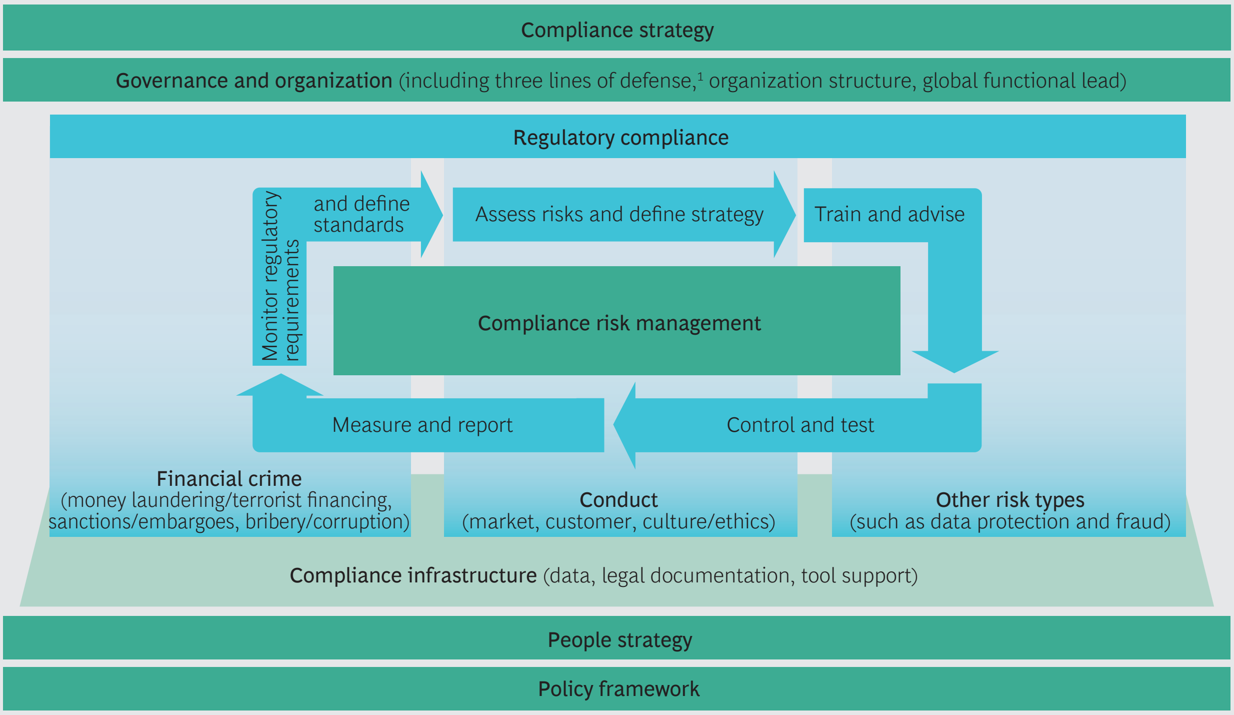
Financial institutions allocate a very large proportion (up to 90%) of their compliance resources to compliance risk management; the other four elements are much less resource intensive.

A Compliance Strategy. A groupwide compliance strategy provides a framework for the compliance function, setting out its objectives (or mission statement), rights, and responsibilities. It also encompasses a compliance risk strategy for conducting business in relation to eligible customers, certain products, and particular markets.

Governance and Organization. The target operating model mandates the first, second, and third lines of defense (the ultimate risk owner, independent reviewers of controls, and internal auditors, respectively), defines a governance structure, and provides an organizational setup for compliance operations. Compliance generally sits in the second line of defense. In support of this element, executives must specify the relationship between individual business segments and the compliance function, taking into account jurisdictional and legal variations across geographies.

Compliance Risk Management. Compliance risk management is a core capability that forms the basis of the target operating model and provides an operating framework for managing the key compliance-related risks—financial crime and conduct. This capability includes five key areas of focus, each with a primary task:

Exhibit 1 | Structure of a Compliance Target Operating Model



Compliance strategy
Governance and organization (including three lines of defense,[1] organization structure, global functional lead)
Regulatory compliance
Monitor regulatory requirements
and define standards
Assess risks and define strategy
Train and advise
Compliance risk management
Measure and report
Control and test
Financial crime (money laundering/terrorist financing, sanctions/embargoes, bribery/corruption)
Conduct (market, customer, culture/ethics)
Other risk types (such as data protection and fraud)
Compliance infrastructure (data, legal documentation, tool support)
People strategy
Policy framework

Source: BCG analysis.
Note: This compliance target operating model is valid globally, in regions as varied as Europe, the Americas, Asia, and the Middle East and Africa.
[1] The three lines of defense are the ultimate risk owner, independent reviewers of controls, and internal auditors.

- **Monitoring Regulatory Requirements and Defining Standards.** Understand global and local requirements, and codify internal risk policies and procedures.

- **Assessing Risks and Defining Strategy.** Conduct an assessment of inherent risks and mitigating measures to identify residual risks, as a starting point for defining a compliance risk strategy.

- **Training and Advising.** Establish a program of internal training and guidance on compliance obligations, backed by ad hoc support, particularly for the first line of defense.

- **Controlling and Testing.** Implement controls in the first and second lines of defense to mitigate inherent risks, and test the controls' effectiveness.

- **Measuring and Reporting.** Assess areas of risk exposure, and report findings to internal and external stakeholders. This activity should include regular production of written evidence related to compliance response metrics.

Effective compliance risk management should also provide an infrastructure to organize and analyze data, support legal documentation, and ensure that the right tools for implementation are in place.

A People Strategy. Securing the right talent in sufficient numbers is crucial, as is suitable training across lines of defense.

A Policy Framework. Executives need a comprehensive compliance policy framework, including a blueprint for creating, maintaining, and retiring policies and procedures.

Smart Technologies in Compliance Risk Management

Banks have implemented digital solutions across numerous lines of business in recent years. For compliance purposes, the most effective tools are smart technologies that collect and assess large volumes of data and perform related tasks. (See Exhibit 2.) Applications such as optical character recognition, data mining, and deep learning fall into one of four basic activities: collection, analysis, learning, and action.

For compliance purposes, the most effective tools are smart technologies that collect and assess large volumes of data and perform related tasks.

Collection. This activity focuses on gathering and converting analog data to digital format for analysis and processing. This area has three relevant smart technologies:

- **Optical Character Recognition.** Extraction and conversion of text from scanned documents and images (including handwriting) into editable, searchable data
- **Voice and Speech Recognition.** Analysis of speech to identify and translate spoken language into digital text—for example, during trade surveillance
- **Image and Facial Recognition.** Digital matching techniques for classification or identification purposes—for example, in the account-opening process

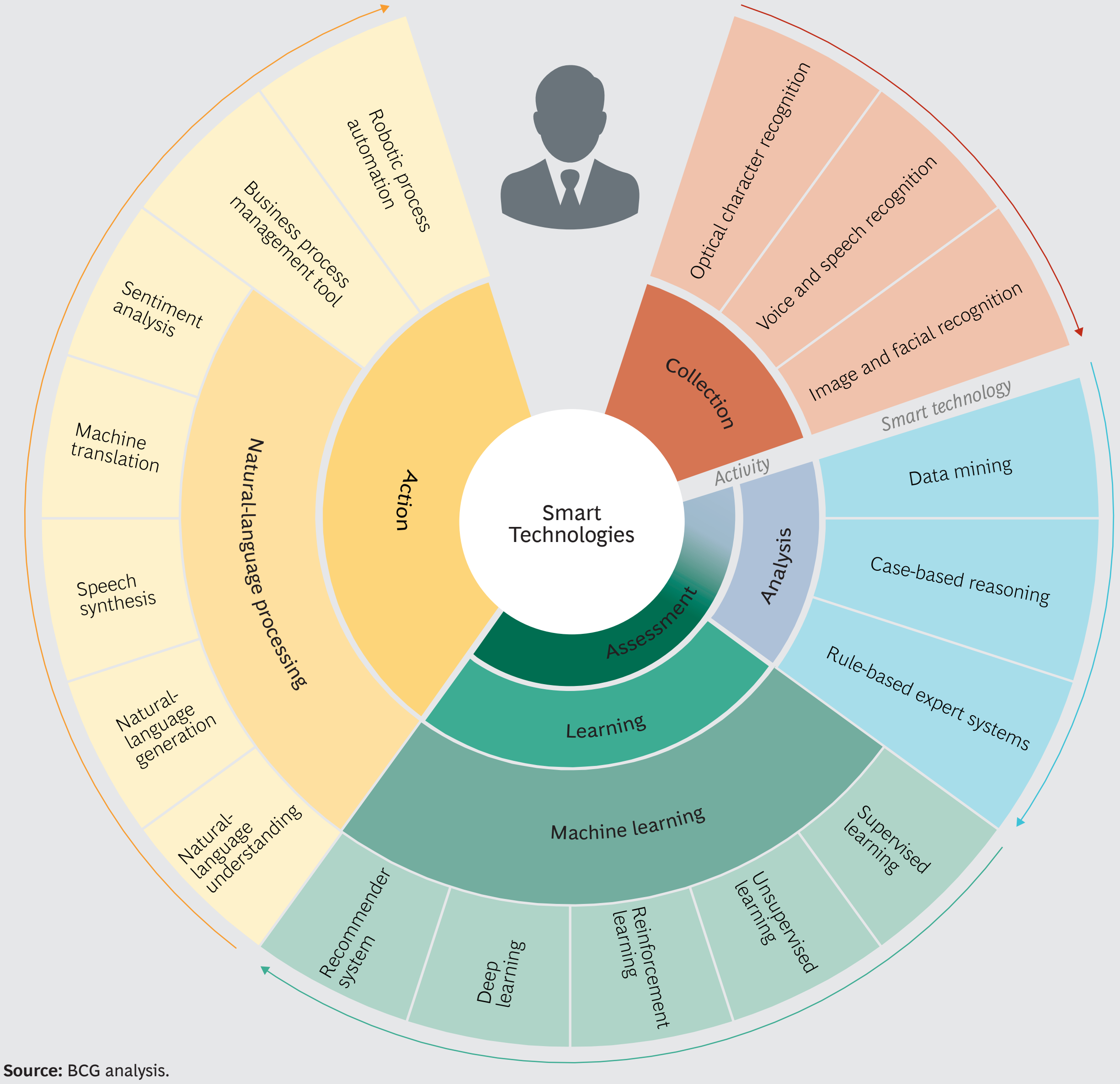
Analysis. This activity involves analyzing data for pattern recognition. Essential smart technologies in this area include the following:

- **Data Mining.** Use of statistical methods to identify patterns in large data sets, for purposes such as transaction monitoring
- **Case-Based Reasoning.** Decision making on the basis of a similarity metric that analyzes a database of existing cases—for example, previous occurrences of money laundering
- **Rule-Based Expert Systems.** Decision making that mimics the knowledge and reasoning of a human expert—for example, in know-your-customer risk ratings

Learning. Machine learning from data involves training machines to improve their performance. Five smart technologies focus on specific forms of such learning:

- **Supervised Learning.** Use of a data set of problem instances with known answers to train a machine so that its performance constantly improves—for example, in managing information across files
- **Unsupervised Learning.** Use of techniques including clustering, dimensionality reduction, and anomaly detection to find structures in data—for example, to improve detection models related to money laundering

EXHIBIT 2 | Smart Technologies Segmented by Activity



Source: BCG analysis.

- **Reinforcement Learning.** Method of learning by doing as opposed to learning by observing, without knowing the results of individual steps or considering the long-term effects of decisions

- **Deep Learning.** Use of deep neural networks to analyze data without requiring manual feature engineering or problem segmentation

- **Recommender System.** Ranking of items by predictions about user preference based on previous users' preferences (content) and similar users' preferences (collaborative)—for example, to clear Level 1 alerts in transaction monitoring

Action. Mechanical actions may occur as a result of explicit instructions, or they may involve learned responses. Seven types of smart technology apply here:

- **Natural-Language Understanding.** Translation of natural language into machine-readable models through the use of syntactic and semantic analysis
- **Natural-Language Generation.** Translation from machine language into natural language—for example, for automated advisory services
- **Speech Synthesis.** Conversion of written text into speech
- **Machine Translation.** Automatic translation of one natural language into another, for multiple services across geographies
- **Sentiment Analysis.** Extraction of information (such as the author's attitude, evaluation, emotional state, and personality) from text
- **Business Process Management Tool.** Support for the design and implementation of multiple process solutions on a single platform—for example, to facilitate alert and case management or customer onboarding
- **Robotic Process Automation.** Automation of previously manual tasks through the use of static rules to make decisions—for example, to screen for negative press reports during customer onboarding

Mechanical actions may occur as a result of explicit instructions, or they may involve learned responses.

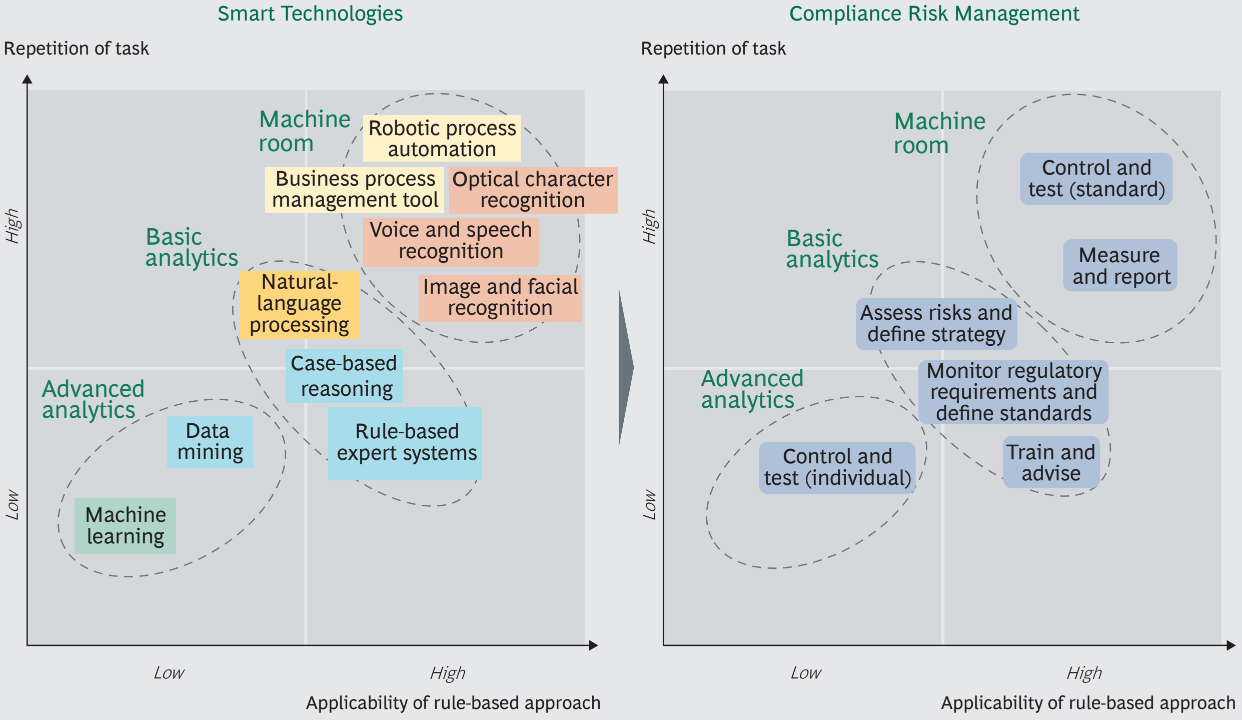
An Assessment Framework for Smart Technologies

Just as technologies can be segmented into specific capabilities, so can the tasks that they perform. Some of these tasks may be fairly routine, while others require intelligent capabilities to work with unstructured data sets. (See Exhibit 3.)

The tasks and technologies fall into three basic groups:

- **Machine Room.** This group comprises tasks and technologies that facilitate simpler and standardized activities, leading to significant efficiency gains. Applications include robotic process automation, business process management tools, and the voice, speech, and other recognition systems that are part of the data collection process. Machine room content tends to account for the largest portion of a smart technology rollout, particularly in the early stages.
- **Basic Analytics.** Tools for basic analytics support relatively straightforward activities based on defined rule sets, such as alert generation arising from transaction monitoring or from rule-based customer risk ratings. Applications include case-based reasoning and expert systems. Basic analytics tends to be a medium-term priority on a rollout timeline.
- **Advanced Analytics.** This group of tasks and technologies serves to analyze large and unstructured data sets, leading to new insights (such as pattern recognition in transaction payments). Relevant applications include learning

Exhibit 3 | Assessment Framework for Smart Technologies and Compliance Risk Management



Smart Technologies
Repetition of task
High
Low
Machine room
Robotic process automation
Business process management tool
Optical character recognition
Voice and speech recognition
Image and facial recognition
Basic analytics
Natural-language processing
Case-based reasoning
Rule-based expert systems
Advanced analytics
Data mining
Machine learning
Low
High
Applicability of rule-based approach
Compliance Risk Management
Repetition of task
High
Low
Machine room
Control and test (standard)
Measure and report
Basic analytics
Assess risks and define strategy
Monitor regulatory requirements and define standards
Train and advise
Advanced analytics
Control and test (individual)
Low
High
Applicability of rule-based approach

Source: BCG analysis.

algorithms and natural-language processing. The implementation of advanced analytics normally follows the rollout of machine room and basic analytics.

In the context of core compliance risk management activities, the various actions are subject to different requirements. For example, basic analytics such as data mining, case-based reasoning, and expert systems may offer the best support for monitoring global and local regulations, assessing risks, and implementing training. Some control and reporting activities, meanwhile, are so highly standardized that banking organizations can use machine room technologies such as robotic process automation, business process management tools, and voice and speech recognition to perform them. Others still—for example, analysis of specific trading patterns—are more complex and may require advanced analytics solutions such as natural-language processing and machine learning. (See the sidebar, “A European Bank Graduates to Compliance Smart Technologies.”)

Deep Dive: Smart Technologies in Customer Onboarding

As part of their obligation to guard against financial crime, financial institutions need to know their customers. This requires robust management of the customer life cycle, which consists of three key stages: onboarding, review, and offboarding. Essential elements of the onboarding stage are client identification and verification, which also help banks meet reporting requirements and build a better understanding of customer needs.

Drawing on our work with financial institutions seeking to develop harmonized standards for compliance risk management, we have built a tool that defines the key tasks and data fields (including documentation) required to comply with global and local regulatory requirements for onboarding. The tool provides the basis for defining a global onboarding process.

The eight-step onboarding process encompasses four major stages: identification, customer due diligence, enhanced due diligence, and confirmation. Customer identification (steps 1 and 2) entails the collection of public and private information that the institution uses to conduct customer due diligence—customer verification, conduct screening, and the generation of a customer risk rating (steps 3 through 6). The outcome of that assessment may prompt the institution to undertake enhanced due diligence (step 7) before confirming the onboarding (step 8).

Until recently, banking organizations performed many onboarding steps manually, simply because collecting information from—and checking—diverse sources re-

A EUROPEAN BANK GRADUATES TO COMPLIANCE SMART TECHNOLOGIES

Rising regulatory requirements obliged a European bank to increase its compliance head count, so it sought to boost efficiency and effectiveness through automation. The bank gathered information from across the business—for example, collecting data related to end-to-end process flows, number of full-time equivalent (FTE) staff members involved in each process, volume of alerts, percentage of false positives, and alert processing times.

Working with that information, the bank identified smart-technology initiatives applicable to different processes and evaluated their benefits on the basis of several metrics: decline in number of false positive alerts, speed of alert investigation, lead times to report suspicious activities to regulators, and resulting impact on FTE buildup. To prioritize initiatives, the bank mapped benefits against the effort necessary for implementation, leading to a project roadmap that prioritized quick wins and saved relatively complex challenges for a later date.

The first stage of implementation focused on process management solutions for anti-money-laundering/sanctions alerts and case investigations across business units, aiming to boost operational efficiency and cut risk. Next, the bank initiated a more ambitious program to introduce smart technologies, such as machine learning, in order to improve alert detection algorithms and facilitate early investigation procedures, thereby reducing processing times.

In terms of investment, the bank anticipated that year two of the effort would see the highest level of expenditure, with the budget tapering to zero over the following four years. It projected that compliance function costs would stand at 130% of base costs after two years, after which they would gradually decline.

quired significant human intervention. Further, most banks did not have integrated workflow tools to help manage and monitor tasks. In the future, however, the commercial availability and increasingly common internal development of smart technologies will lead to greater automation. Three technologies will prove particularly useful in this regard (see Exhibit 4):

- **Optical Character Recognition.** OCR enables the transformation of analog data into digital formats, for later automated processing in the onboarding process.

- **Machine Learning.** This technology permits the enhancement of scoring algorithms, for improved accuracy of currently rule-based customer risk ratings.

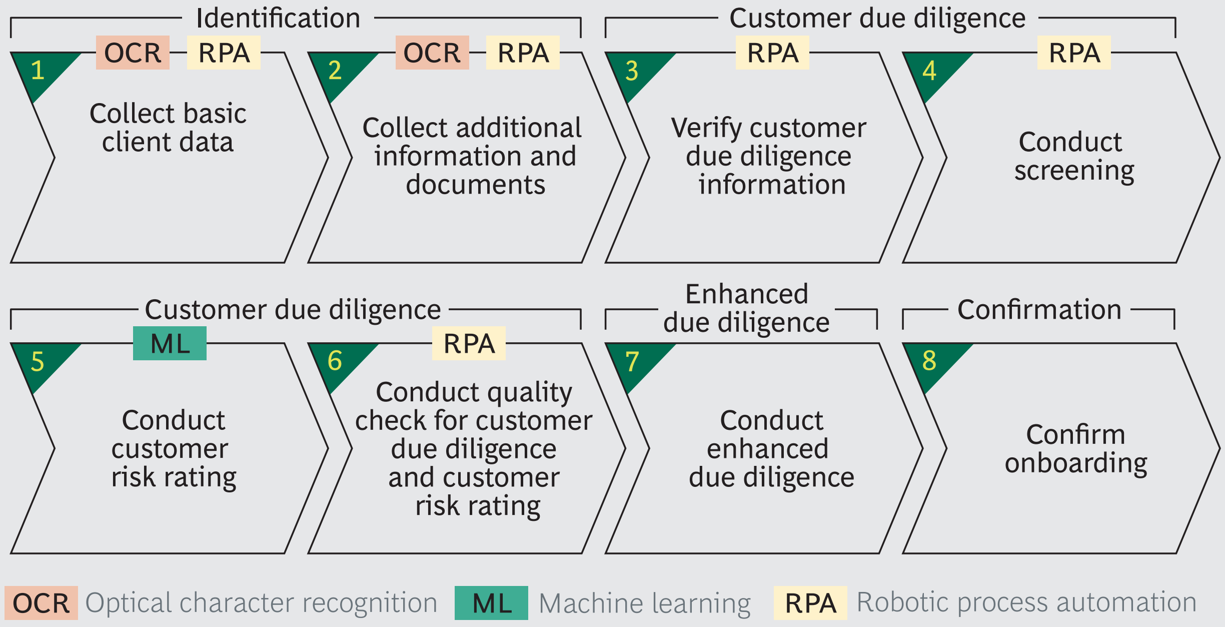
- **Robotic Process Automation.** This smart technology permits automated collection and checking of data in the identification phase (including data from external data providers), verification of information and follow-up screening in the due diligence phase, and quality checks for due diligence and risk ratings.

The automation and standardization of compliance risk management processes for onboarding are likely to become more and more deeply embedded in bank systems as institutions apply technology across the customer life cycle.

What Should Banks Do Next?

Heavier regulation and punitive fines have obliged banks to revisit target operating models and leverage smart technologies to improve the efficiency and effectiveness of the compliance function. What banks do next will depend on where they are in

Exhibit 4 | Smart Technologies Suitable for Different Steps of the Onboarding Process


Identification
Customer due diligence
1
OCR
RPA
Collect basic client data
2
OCR
RPA
Collect additional information and documents
3
RPA
Verify customer due diligence information
4
RPA
Conduct screening
Customer due diligence
Enhanced due diligence
Confirmation
5
ML
Conduct customer risk rating
6
RPA
Conduct quality check for customer due diligence and customer risk rating
7
Conduct enhanced due diligence
8
Confirm onboarding
OCR Optical character recognition
ML Machine learning
RPA Robotic process automation

Source: BCG analysis.

the compliance transformation process. Executives interested in optimizing a bank's target operating model should focus on three essential steps:

- **Conduct a compliance health check.** This step consists of assessing the status of the current compliance target operating model, including conducting interviews with senior management and comparing the existing situation with industry best practice. One useful tool at this stage is a questionnaire covering dimensions such as compliance strategy, governance and organization, and compliance risk management, with each topic area weighted by its importance.

- **Define the target operating model.** An appropriate definition should include the design of a detailed target operating model for compliance (including groupwide risk taxonomy) and for alignment with stakeholders. Also essential are clarification of roles and responsibilities, and efforts to align a global framework with local and business requirements. Development of a comprehensive database of global regulatory requirements may be a key lever.

- **Create a roadmap for implementation.** The final step in target operating model optimization is to draw a roadmap for implementing the model, including setting up the project structure. Preparing to roll out new systems while continuing the daily conduct of the compliance function poses a significant challenge. From an early stage, project teams must work across lines of defense and cooperate with business lines.

The increased availability of smart technologies permits compliance risk management that employs machine room, basic analytics, and advanced analytics activities.

For banks that have successfully established a target operating model, the increased availability of smart technologies permits compliance risk management that employs machine room, basic analytics, and advanced analytics activities. A strategic approach would involve the following preliminary actions:

- **Assess digitization opportunities and technologies.** A critical review of the compliance process landscape should include an appraisal of the frequency and structure of tasks and available smart technologies, leading to categorization and prioritization of needs. At this stage, decision makers must have a detailed technical understanding of the processes and underlying requirements.

- **Conduct pilot for proof of concept.** Executives must select specific technologies for piloting to provide proof of concept and ensure sufficient stakeholder buy-in.

- **Create a roadmap for large-scale rollout.** A roadmap is crucial for any large-scale rollout of smart technologies (including setting up an adequate governance structure). Vendor selection is a key challenge. Lengthy testing programs may be appropriate, as they may reveal mismatches, shortcomings, or conflicts—for example, between IT requirements and data security needs.

There is no simple or standardized way to develop state-of-the-art compliance frameworks, but as banks move away from a remedial approach, through the development of target operating models, to new smart-technology platforms, they are likely to generate benefits for the business and stakeholders and to build a capability equipped for the demands of modern global banking.

About the Authors

Gerold Grasshoff is a senior partner and managing director in the Frankfurt office of The Boston Consulting Group. He is BCG's global head of risk management and regulation/compliance. You may contact him by email at grasshoff.gerold@bcg.com.

Bernhard Gehra is a partner and managing director in the firm's Munich office. He supports European banks in large-scale compliance transformation projects and is the primary contact person for this publication. You may contact him by email at gehra.bernhard@bcg.com.

Valerie Villafranca is a director in BCG's Paris office. You may contact her by email at villafranca.valerie@bcg.com.

Norbert Gittfried is an associate director in the firm's Frankfurt office. You may contact him by email at gittfried.norbert@bcg.com.

Vincent Grataloup is a principal in BCG's Paris office. You may contact him by email at grataloup.vincent@bcg.com.

Katharina Hefter is a principal in the firm's Berlin office. You may contact her by email at hefter.katharina@bcg.com.

Jannik Leiendecker is a principal in BCG's Munich office. You may contact him by email at leiendecker.jannik@bcg.com.

Oliver Pauly is a principal in the firm's Zurich office. You may contact him by email at pauly.oliver@bcg.com.

For Further Contact

If you would like to discuss this report, please contact one of the authors.