The adoption of artificial intelligence (AI) systems and advanced analytics is accelerating across financial institutions, creating evolving regulatory and compliance challenges.

80% of risk professionals were not confident about the governance in place around AI
— KPMG’s survey of 120+ risk professionals

92% of companies question the trustworthiness of data, analytics...are worried about the impact on reputation
— KPMG’s recent Guardians of Trust report

20% of companies have a well-defined enterprise-wide strategy to automate compliance
— KPMG’s Compliance Automation Survey 2018

Through AI specifically, organizations have an opportunity to increase the potential efficiency and effectiveness of both their operations and compliance processing and analysis via continuously evolving data and model transformation. Yet, AI presents both existing and uniquely applied regulatory and compliance challenges that must be addressed in the governance and controls upfront and ongoing.

In addition, many financial institutions are dependent on third-party vendors for the rapid deployment or scalability of advanced analytics and AI-related technology applications, which is further giving rise to new issues and risks in the areas of governance and accountability.

U.S. regulators indicate they do not want to impede the development of “responsible” AI applications, especially to the extent the applications may expand access and convenience for consumers or bring greater efficiency, risk detection, and accuracy to operations. They are focusing primarily on supervision and, as such, public policies regarding AI are developing more slowly than the technologies. In some cases, regulators are working together and with the industry to help “increase the velocity of transformation” to AI and related technologies, while continuing to focus on safety and soundness and consumer protection. To evaluate the unique risks posed by advanced analytics and AI solutions, regulators are currently looking to existing laws and regulations to define the parameters, or set the “guardrails,” by which they will evaluate system outputs. In turn, this places heightened regulatory focus on those AI solutions that touch areas already subject to heightened regulatory expectations, as depicted in the following wheel.

This paper outlines the business drivers and actions organizations can take based on those areas already subject to heightened regulatory expectations.
AI is a subset of the broader category of Fintech solutions and emerging technologies. Globally, regulators and supervisors have begun taking specific actions in response to fintech-related risks, including the development of international standards and principles, the implementation of increasingly detailed and prescriptive national rules and guidance, and shifts in supervisory priorities. With regard to AI, however, they are still asking questions.

**What is AI?** Artificial Intelligence is technology that is able to perform tasks commonly associated with intelligent beings. Key elements of AI typically include sensing, learning, inference, and reasoning.

**AI is not RPA.** RPA (Robotic Process Automation) refers to advanced automation of tasks, previously carried out by humans, through hard coded/configured software. The process remains the same unless humans change the code.
Fintech developments, including AI, are continually highlighting new areas in which additional or refined regulation may be required. Additionally, the general trend towards the gathering and sharing of an ever-growing range of financial and non-financial data is establishing a wider set of active parties.

Regulators and supervisors are discussing whether there are appropriate frameworks in place for the gathering, storing, sharing, and use of data, both domestically and cross-border. Public policies, however, are lagging the development and deployment of new technologies. Established financial institutions, at least initially, face different types of regulation and supervision than many non-financial companies and start-ups entering the financial services sector. Over time, these differences may diminish. At present, regulatory activity impacting AI is being initiated in state, federal, and global jurisdictions, including beyond financial services-specific regulators, and addressing nonbank supervision, financial stability, operational resiliency and cybersecurity, and consumer protections.

Prospectively, established regulation and supervision may impact a firm’s strategy and business model, including where to locate specific activities.

**Drivers**
- Rapid advances in technology are reshaping access to and delivery of financial products and services
- Public policies are lagging the deployment of new technologies
- Federal, state, and foreign jurisdictions are acting independently; multiple regulators, including non-financial services regulators, may have jurisdiction over data, technologies, or technology providers

**Actions**
- **Apply existing “pre-regulations”:** Acknowledge existing laws and regulations as pre-regulatory applications to AI
- **Consider other regulations, policies, and principles:** Review policies and regulations in other jurisdictions for examples of possible future parameters on AI
- **Monitor regulatory change:** Identify new legislation or other requirements applicable to AI

**Regulatory coverage areas:** Public policies are lagging technology development; regulators looking to existing requirements as “guardrails;” State, federal, and global regulatory requirements differ.

- CA Consumer Privacy Act, EU GDPR, NY DFS

**Regulatory perspective**

In general, the approach to regulation of AI-enabled products ... should be informed by assessment of the aspects of risk...

If a risk falls within the bounds of an existing regulatory regime...the policy discussion should start by considering whether the existing regulations already adequately address the risk, or whether they need to be adapted to the addition of AI.

— Executive Office of the President, National Science and Technology Council, Preparing for the Future of Artificial Intelligence, October 2016

As part of the American AI Initiative, federal agencies will also work to build public trust by exploring regulatory and non-regulatory approaches to govern new AI applications. To this end, the White House...will work with regulatory agencies and other stakeholders to craft guidance for AI technologies that will promote innovation while respecting privacy, civil liberties, and American values.

Regulators and supervisors are focusing on how new technologies affect the core risk governance competencies of identifying, managing, measuring, and controlling risks across the enterprise, as well as having the appropriate resources, skills, and expertise to deliver this effectively.

Firms will be expected to have strong change management capabilities; risk governance frameworks (e.g., enterprise, strategic, reputation) as well as frameworks for third party risk management (and accommodation for increased reliance, as appropriate) and IT/data governance (including technology risk and model risk validation); skilled talent to manage AI solutions; and clear accountability.

Drivers

— Regulatory focus on ethics and conduct, consumer protection, reputation risk, strategic risk
— Increasing reliance on third-parties and outside data sources

Actions

— Establish program governing bodies: Oversee review and amendment of existing policies to include AI considerations; governance should include representation from risk and compliance
— Establish controls to mitigate risks: Align AI risk programs to existing risk management programs
— Integrate with risk management programs: Integrate third-party risk management across performance-based areas, risk functions, and disciplines
— Perform independent review of AI: Perform independent review and challenge to enable Program Sponsor, Executive Management and/or other stakeholders to evaluate the AI Program delivery and success

Regulatory coverage areas: Model risk management; third-party relationships; outsourcing risks; ownership/accountability; digital labor; nonbank regulation/supervision; board oversight/risk appetite.

FRB guidance for boards and management, Model risk management; Third-party relationships; Outsourcing risks/Technology service providers

“Regulatory perspective

The vast majority of the banks we supervise will have to rely on the expertise, data, and off-the-shelf AI tools of nonbank vendors to take advantage of AI-powered processes.

The Federal Reserve’s Guidance on Model Risk Management highlights the importance to safety and soundness of embedding critical analysis throughout the development, implementation, and use of models, which include complex algorithms like AI. It also underscores “effective challenge” of models by a “second set of eyes”—unbiased, unqualified individuals separated from the model’s development, implementation and use.

— Federal Reserve Governor Lael Brainard, What Are We Learning about Artificial Intelligence in Financial Services?, November 13, 2018

AI | Compliance in control
While firms are expected to meet existing data protection requirements, they also need to take a proactive approach to the possibility that fintech developments may lead to a fundamental re-thinking of data privacy, security, and protection by financial services regulators and by data protection authorities more generally. Additionally, the millions of customers affected by high-profile data breaches now seek greater control over their personal information—its collection, use, and retention—spurring firms, independent of regulatory requirements, to reconsider policies regarding opt-in and opt-out procedures, the scope of data to be collected, how it is accessed and by whom, and how it will be used or shared.

With regard to AI, the use of large and/or expanded data sets for AI applications may be complicated by this heightened public awareness of data privacy and data security, which could restrict available data and influence machine learning. Institutions should understand the source and content of the data sets they use, and assess potential risks related to access and sharing along with limitations that could impact its use (e.g., model validation, underwriting, fair lending, sales practices).

Drivers
— Proliferation of available digital data; increased role of fintech applications and data aggregators
— Highly interconnected financial systems
— Heightened awareness/expectations around consumer data protection

Actions
— Establish governance for data and algorithms used for generating AI results and decisions: Ensure that data used for system learning is stored securely and can be retrieved in a timely manner
— Establish accountability: A Data Controller is in place for AI and can demonstrate compliance
— Conduct comprehensive data protection risk assessments: Understand AI’s necessity to obtain/ process personal information, potential risks, and processes in place. Remove higher risk data from AI use if not required

Regulatory coverage areas: Data privacy; data security, including access; international rules; cross-jurisdictional agreements.

CA Consumer Privacy Act, GLBA, FCRA, FTC Act, US/EU Privacy Shield, EU GDPR

Regulatory perspective

By 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009.

While consumers have to some extent become conditioned to opt for convenience over security, they nevertheless continue to look to their primary financial institutions for protection of their personal and financial data.

— U.S. Treasury Report, A Financial System That Creates Economic Opportunities, Nonbank Financials, Fintech, and Innovation, July 2018
New technology can introduce risk, but it can also help institutions and regulators to identify and mitigate risk sooner. AI and automation present opportunities to incorporate digital transformation into compliance challenges including “real-time” compliance risk management and reporting in areas such as conduct/culture, data privacy, financial crimes, consumer lending, and trading and investment as well as data retention.

AI tools can facilitate faster, more comprehensive, and more accurate monitoring and testing, freeing staff from repetitive and “low-value” tasks and allowing them to focus on high value activities that require expert judgment and domain knowledge. The opacity of some AI tools, however, may make it challenging to explain AI outcomes to regulators and consumers, increasing compliance risks. Regulators are increasingly setting rules or guidelines that focus on ensuring that boards and senior management have sufficient awareness and understanding of the fintech applications being used by their firms, in order to assure these risks are highlighted and managed effectively.

Drivers
— Expectations for “real-time” compliance and risk management
— Increased market competition and pressure to cut operating costs
— Converging risk management and controls across operating and business units

Actions
— Embed risk and compliance in strategic objectives:
  Include adequate risk management and compliance with legal, regulatory as a strategic priority
— Integrate compliance throughout AI development:
  Understand regulatory and compliance requirements for the future state processes prior and throughout development
— Continuously monitor changes to requirements:
  Identify and continuously monitor changes to applicable regulations at the AI Program and solution level

Regulatory coverage areas: Board oversight/risk appetite; trade surveillance; misconduct; BSA/AML reporting; consumer/investor laws; change management; risk assessments/prioritization.

FRB guidance for boards and management, FinCEN CDD Rule, BSA/AML, Consumer Laws,

The ability to digitize rule-sets and consume, process, and analyze data in real-time could very well be the capability that allows us to explore application of so-called ‘agile regulation.’

As machines assume more economic tasks and functions, we would expect that these machines can be programmed with rules that ensure compliance with laws and regulations.

— CFTC Chair Christopher Giancarlo,
  Quantitative Regulation: Effective Market Regulation in a Digital Era, November 7, 2018
Financial institutions are using AI for a range of applications, including to assess credit quality, back-test models, analyze markets and optimize trades. The application of AI in credit scoring models in particular has captured the attention of the industry and regulators, as much for the benefits it could potentially provide creditors by allowing them to more accurately model and price risk (and expand credit access to consumers) as for the potential risks from “unexplainable” credit decisions, learned bias, or other fair lending and consumer compliance risks.

Most regulated financial institutions are accessing AI-powered resources through nonbank vendors, increasing the risk of third-party dependencies, market concentration (as certain vendors begin to dominate through scale economies), and an over-reliance on similar/same data sources.

Drivers
— Expanded credit access for consumers
— Availability/application of expanded and less-structured data sets
— Identified supervisory priority

Actions
— Understand AI credit decisions: Review AI that supports credit decisions in accordance with strict standards and guidelines to can demonstrate unbiased decision making
— Monitor AI outcomes and trend analysis: Increase scrutiny over AI that looks at trends
— Comply with evolving regulatory requirements: Ensure AI that is used to support credit management demonstrates compliance with changes to accounting standards and regulatory requirements

Regulatory coverage areas: Interconnectedness, overreliance on third-party technologies, auditability of AI learning methods, independence of credit-scoring models.

Interagency leveraged lending guidance, FASB CECL, Fannie Mae/Freddie Mac criteria, FSB Benchmark Reform

Regulatory perspective

AI allows massive amounts of data to be analyzed very quickly. As a result, it could yield credit scoring policies that can handle a broader range of credit inputs, lowering the cost of assessing credit risks for certain individuals, and increasing the number of individuals for whom firms can measure credit risk...

When using machine learning to assign credit scores make credit decisions, it is generally more difficult to provide consumers, auditors, and supervisors with an explanation of a credit score and resulting credit decision if challenged.

Additionally, some argue that the use of new alternative data sources, such as online behavior or non-traditional financial information, could introduce bias into the credit decision.

— Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services, November 2017
Just as cybersecurity analytics help to predict cyberattacks before they occur, the patterns detected through AI techniques such as machine learning and deep learning can be used to highlight vulnerabilities that may be otherwise difficult to find.

However, the use of AI can also introduce new cyber risks through an overreliance on third-party technologies, the increasing interconnectedness of markets and systems, and cyber threats/cyber crimes powered by AI that manipulate market functions. Regulators are focusing on governance, risk analysis and assessment, controls (access management, information security, monitoring and testing, and information sharing), and incident response.

Drivers
— Proliferation of digitized data, increasingly sophisticated technologies
— Highly interconnected financial systems
— Consumer demand for access through multiple innovative technology sources
— Increased reliance on third-party providers and data

Actions
— **Consider cybersecurity throughout AI development:** Include cybersecurity considerations in development process, including secure protection of AI and protection from malfunctioning AI
— **Develop AI consistent with policy and risk appetite:** Manage cybersecurity risks and activities, including use of third parties and data exchanges
— **Establish an end-to-end AI technology policy, standards, roles and responsibilities:** Govern key technology components through AI technology policies and standards

**Regulatory coverage areas:** Resiliency (adaptable tools); third-party data security and privacy


Regulatory perspective

The wide availability of AI’s building blocks means that phishers and fraudsters have access to best-in-class technologies to build AI tools that are powerful and adaptable. Supervised institutions will likely need tools that are just as powerful and adaptable as the threats that they are designed to face.

— Federal Reserve Governor Lael Brainard, What Are We Learning about Artificial Intelligence in Financial Services?, November 13, 2018
Institutions are expected to effectively monitor and mitigate misconduct by employees, third parties, and partners/affiliates. Embedding an organization's ethics and values into AI systems could prove challenging but regulators will evaluate AI outcomes with the same lens they use for more traditional operations, looking for bias, fairness, accuracy, and fraud in the context of consumer data privacy, product suitability, and sales/trading practices. AI systems are dependent on the data they are trained to analyze as well as the tools and algorithms that power the system.

**Drivers**
- Supervisory expectation that firms must manage the misconduct risk of employees, third parties, partners/affiliates
- Focus on consumer protection
- Increased awareness of nonfinancial risks (reputation, strategic, fraud) that can result from misconduct

**Actions**
- **Implement AI ethics and code of conduct:** Ensure that ethical principles and a code of conduct are in place and applicable for AI and define escalation and whistleblowing procedures. Guidance should be in line with enterprise and enterprise-wide ethics and codes
- **Develop training for AI ethics and conduct:** Roll out ethics and conduct trainings to not only end-users, but also AI system designers, developers, risk managers, and other stakeholders involved in AI programs

**Regulatory coverage areas:** Code of Conduct; conflicts of interest; suitability/fiduciary duty; market misconduct; trade surveillance and monitoring

FRB guidance for boards and management, SEC Regulation BI, SEC Business Conduct Rule

---

**Regulatory perspective**

The likelihood of possible fraud or misconduct identified based on a machine learning predication cannot—and should not—be the sole basis of an enforcement action.

…while the major advances in machine learning have and will continue to improve our ability to monitor markets for possible misconduct, it is premature to think of AI as our next market regulator.

The science is not yet there. The most advanced machine learning technologies used today can mimic human behavior in unprecedented ways, but higher-level reasoning by machines remains an elusive hope.

— Scott Bauguess, The Role of Big Data, Machine Learning, and AI in Assessing Risks: A Regulatory Perspective, June 17, 2017
A primary objective of consumer financial protection is to make financial services and markets fairer for all consumers. AI can contribute to this goal in a number of ways, such as by expanding access to financial products and services to consumers that are “credit invisible” or have limited credit histories through credit scoring models using alternative data and machine-learning algorithms. Similarly, the pattern detection in AI models can highlight anomalies in consumer complaints and estimate the potential for emerging risk.

Expanded data sets and the opacity of machine learning, however, may also introduce unintended and/or unexplainable consumer and retail investor protection outcomes related to data privacy, fair lending, credit reporting, sales practices, and trading activities, thus placing organizations at heightened reputation and strategic risk. It is increasingly important that consumers understand and affirmatively consent to the use of their transactional and personally identifying data. Regulators are increasingly looking to transparency and disclosure to raise consumer awareness.

### Drivers
- Consumer demand for integrated, personalized products and services
- Consumer demand for control of personal data
- Demographic shifts toward digital products

### Actions
- **Monitor outcomes of AI solutions:** Use data analytics, audit trails, and management review to examine AI solution outcomes and determine if the AI meets performance and business requirements
- **Demonstrate fair, unbiased treatment:** Demonstrate adequate review, examination, and investigation of AI decisions and outcomes for inherent biases
- **Consider consumer-impacting AI as potentially higher risk:** Consider AI that impacts consumers—directly or indirectly—as potentially higher risk that should be subject to increased scrutiny and more frequent review

### Regulatory coverage areas:
- UDAP/UDAAP; disparate impact; ECOA/fair lending; data privacy
- GLBA, FCRA, CA Consumer Privacy Act, Consumer laws, Americans with Disabilities Act, SEC Regulation BI (Best Interest) and Regulation SP, FTC Act

It should not be assumed that AI approaches are free of bias simply because they are automated and rely less on direct human intervention. Algorithms and models reflect the goals and perspectives of those who develop them as well as the data that trains them and, as a result, AI tools can reflect or “learn” the biases of the society in which they were created.

— Federal Reserve Governor Lael Brainard, What Are We Learning about Artificial Intelligence in Financial Services?, November 13, 2018
Digital transformation is driving innovation across financial crimes compliance efforts, including facilitating data analytics/predictive analytics that are aggregated across various types of financial crimes and process automation in areas such as customer due diligence and transaction monitoring and reporting. Much of anti-money laundering analysis occurs after the fact and, although an abundance of information is collected, only a small fraction of alerts prove to be productive. This dilutes resources and potentially redirects attentions away from useful information. AI can be used along with predictive analytics to understand for each customer what is normal and expected activity in contrast to what is unique or unusual activity, permitting organizations to gain a better understanding of where to focus their attentions.

The new technologies can also help organizations better understand which information to collect to be most helpful to law enforcement and to more reliably predict customer behaviors.

**Drivers**
- Proliferation of digital data and technology providers; innovative competition
- Regulatory scrutiny; increased reliance on third parties
- Cost pressures; converging risk management and controls across operating/business units

**Actions**
- Test AI against existing FinCrime tools: Test AI for performance against existing models; frequently test and verify random subsets of money laundering and fraud analyses to ensure that AI-driven systems are not unfairly penalizing certain group
- Provide evidence that AI is working as intended: Maintain ability to provide evidence that AI is working as intended and identify gaps and additional risks created by AI and governance structures

**Regulatory coverage areas:** BSA/AML compliance (risk identification, SARs, customer due diligence, onboarding); resource sharing, collaborative arrangements

BSA/AML, FinCEN CDD Rule, Interagency guidance on innovation, NYDFS Transaction Monitoring Rule, FINRA Rule 3310

---

**Regulatory perspective**

New technology, such as artificial intelligence and machine learning, can provide better strategies for banks of all sizes to better manage money-laundering and terrorist-financing risks, while reducing the cost of compliance.

— FDIC Chairman Jelena McWilliams

Some banks are becoming increasingly sophisticated in their approaches to identifying suspicious activity, commensurate with their risk profiles, for example, by building or enhancing innovative internal financial intelligence units devoted to identifying complex and strategic illicit finance vulnerabilities and threats. Some banks are also experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs... The Agencies welcome these types of innovative approaches...

— Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, December 3, 2018
Large firms are expected to continue to invest in the ability to measure capital, liquidity, credit exposures, and counterparty relationships in a more integrated fashion, allowing for more frequent and efficient reporting processes. They are using AI solutions to increase the efficiency, accuracy, and speed of capital optimization as well as to conduct back-testing and model validation, notably related to stress testing and operational risk.

AI Solutions may serve to increase capital and liquidity risks associated with an institution’s risk profile and business model through increased dependence on third parties (who provide/perform AI technologies); interconnectedness to other institutions (through technologies and data sets), markets (through technologies and data sets), and systems; credit concentrations (resulting from machine-learning/data bias); and unintended model decision-making/outcomes (due to opacity of machine-learning, diminishing human expertise).

AI can make sense of large, unstructured datasets, though over time, organizations may be challenged to ensure/explain that the data being used to train the AI system and its decision-making continues to be sufficient and of high quality.

### Drivers
- Data management requirements, including materiality, taxonomy, and lineage
- Models management for capital and liquidity requirements, including stress testing

### Actions
- **Document the AI decision making process:** Maintain ability to provide audit trail of AI decision-making to show that conclusions comply with liquidity and capital regulations
- **Test results of capital and liquidity tools:** Review and compare AI processing results and analysis across multiple models
- **Review quality of data:** Ensure that data used for analysis is compliant with data quality requirements

### Regulatory coverage areas:
- Capital optimization, capital structure, liquidity vulnerabilities; systemic risk (interconnectedness, substitutability/dependencies, business model complexity)

---

**Regulatory perspective**

As these types of models are deployed in increasingly high-value decision-making use-cases, such as determining who gets access to credit or how to manage an investment portfolio, questions regarding how to maintain accountability become fundamental...

The opacity of the models may raise challenges for supervisors and users of these models to monitor risks and understand how they may interact with one another, particularly in times of broad market stress.

— U.S. Treasury Report, A Financial System That Creates Economic Opportunities, Nonbank Financials, Fintech, and Innovation, July 2018
The pace of change, particularly in AI, will accelerate. Expectations are high for the potential value of these new technologies—but there are some people who also express skepticism and even fear about our ability as humans to manage the risks and assert control over the technology in the long term. They ask: Can “control velocity” (the speed with which a control or suite of controls operates) keep pace with “risk velocity” (the speed with which the risk materializes)? Can humans keep pace with the machine learning, duplicating or validating its outcomes, in order to effectively supervise and manage the AI system? In the worst case scenario, the loss of human involvement and expertise would mean that no one will know how processes work and no one will have the expertise to evaluate or repair the outcomes.

The new risks of AI require new approaches to control.

KPMG’s Artificial Intelligence in Control, or AI in Control, is a risk and control framework developed to help entities proactively consider the risks associated with implementing increasingly advanced AI systems. The framework is tailored to AI solutions, including machine learning, and covers risk management and controls across four areas: enterprise management, project management, solution/data management, and technology management.

It is designed to help entities build AI solutions that:
- Have integrity (trustworthy data, analytics, and outcomes)
- Are explainable (describes how decisions are made, new learnings and related changes)
- Are free from bias (data and analyses are inclusive, meet regulatory requirements)
- Have agility and robustness (interoperable between various runtimes, providers, or frameworks; consumable through apps or processes; models are secured from harm or adverse attacks).
The top 4 reasons cited for pursuing automation are:

1. Better risk management
2. Enhance quality
3. Better support for new products or services, with greater agility
4. Remove friction from compliance processes/address current pain points

Source: Innovating compliance through automation (cross industry)

High expectations but little readiness
KPMG research concludes that companies recognize the potential value of intelligent automation (IA) but are moving slowly toward using AI technologies and are still in the early stages of deploying software robots.

The results nevertheless reveal broad plans to adopt IA. Nearly two-thirds of respondents indicate plans to fully implement RPA within three years. Another 18 percent plan selective use. As for cognitive automation, nearly half noted intentions to use these approaches at scale within 3 years, while 29 percent indicated selective reliance on cognitive automation capabilities. Some 10 percent said they would launch pilots and proof of concepts projects.

Cognitive use today and in three years

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.