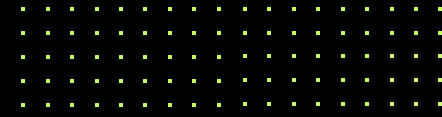
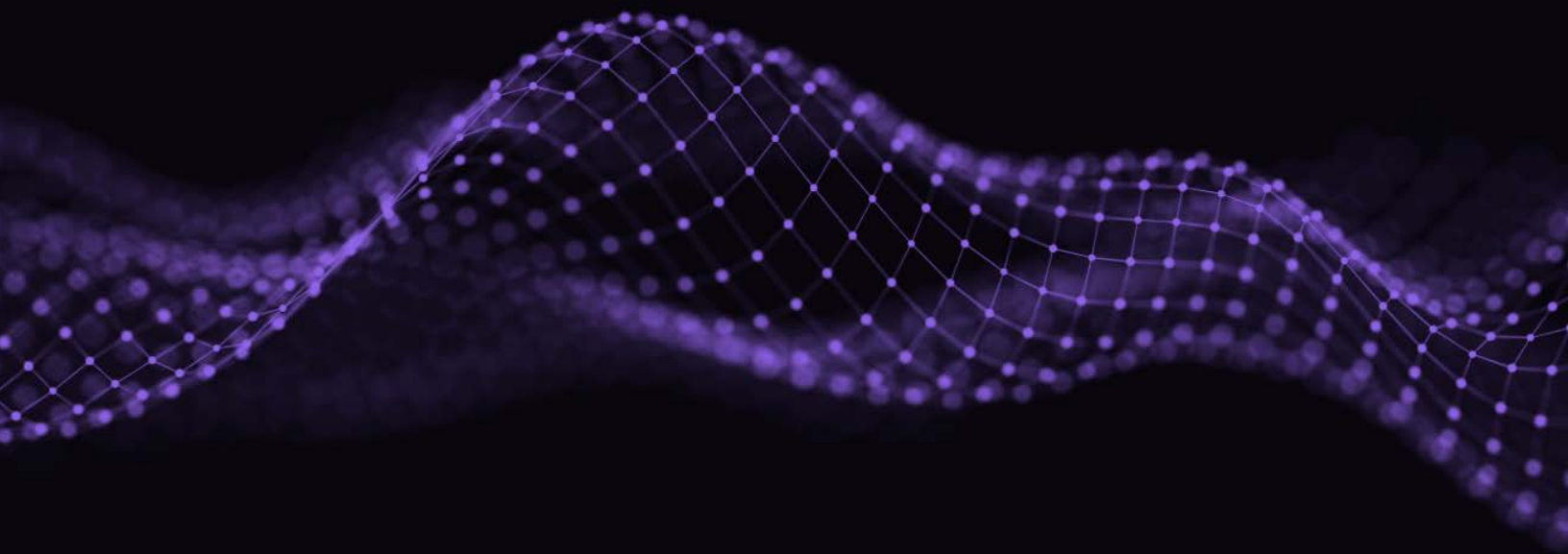


DATA



↗ **Navigating the  
Fintech Risk  
and Compliance  
Ecosystem**





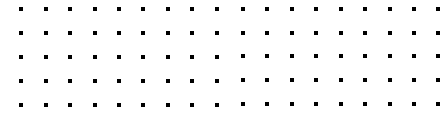
# Navigating the Fintech Risk and Compliance Ecosystem

Fintech has brought a refreshing breath of innovation to the traditionally conservative finance industry. Consumers get new, more convenient services. Financial institutions adapt more quickly to today's mobile and cloud information technologies.

But those benefits come with risks to consumers, financial institutions, and, not least, to fintech companies themselves.

Fintech risks and the compliance frameworks that address them are as varied as the fintech industry itself. What matters to a software-as-a-service (SaaS) billing provider is different from what matters to an online securities trading platform.

We will explain the sources of fintech risks and how to address them. In particular, we will highlight the key U.S. and international regulations impacting fintech companies.



# Fintech Compliance

With never-ending announcements of compromised networks, it's clear that fintech companies face risks from every direction. Compliance offers a solution to today's challenges. But what, exactly, are the risks that most affect fintech?

## What is Fintech Risk and Compliance?

From cloud-based, mobile-first payment services to innovative blockchain applications, financial technologies (fintech) play several roles in today's financial industries.



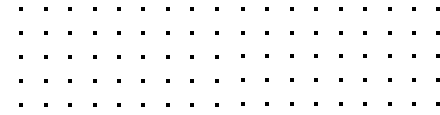
- **Innovators:** Fintech companies leverage the tech industry's innovation engine to bring new services to market faster than traditional firms.
- **Disruptors:** Rapidly-iterating technology companies disrupt established competitors by offering more convenient and efficient services or reaching untapped markets.
- **Partners:** Financial firms routinely outsource back-end functions to fintech companies that natively understand cloud, mobile, and machine learning technologies.

These companies share the standard risks that any business faces, from cash flow to credit. At the same time, fintech companies must address unique risks created by the nature of their industry. Compliance mitigates these risks.

Some companies have no choice. New regulations will demand compliance. Or the financial institutions they serve will require it to support their own compliance programs.

Other companies will choose a voluntary compliance journey. Farsighted fintech leaders understand that reassuring institutional or retail customers through compliance creates a competitive advantage.

No matter where the pressure for compliance comes from, fintech companies must address a host of risks.



# Four Major Risks in Fintech

Fintech companies face unique risks in four primary areas: regulation, cybersecurity, financial and business, and reputation.

## 1. Fintech Regulatory Risk

Unlike their traditional counterparts, fintech companies operate in a more fragmented and uncertain regulatory environment.


In some ways, federal regulators in the U.S. were slow to regulate the fintech industry. At first, this was due to the lack of institutional expertise in emerging technologies. They were also reluctant to impose regulations that could throttle a young industry.

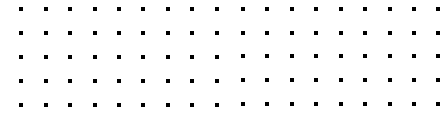
In other ways, federal regulators have aggressively pursued fintech companies. The Securities and Exchange Commission is particularly active against crypto companies that cross the line between asset classes and securities.

Some state regulators were more proactive. [New York's Department of Financial Services](#) introduced regulations covering cryptocurrencies and crypto exchanges. [California's Consumer Financial Protection Law](#) brought new financial service providers under state oversight.

Without unifying federal regulation, state-by-state variation creates more risk for companies delivering nationwide services.

The same is true globally. Different countries have different regulatory priorities. Preserving innovation may be important in the U.S., for example, but protecting consumer privacy takes precedence in the E.U.

 **Fintech companies must navigate this complex regulatory environment and anticipate change to minimize their regulatory risk exposure.**



## 2. Fintech Cybersecurity Risk

Cybersecurity is a challenge every business must meet. For the fintech industry, cyber risks are more severe. Breaches could disrupt institutional customers' operations or compromise retail customers' finances. Either case is traumatic and could end a young fintech company's existence.


The closer a company is to the country's financial infrastructure, the greater the threat from state-sponsored advanced persistent threats.

Fintech companies that store consumer financial data become targets for organized cyber criminals. Even unsophisticated hackers can launch devastating attacks thanks to malware-as-a-service providers.

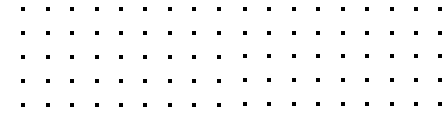
Complicating matters, fast-growing fintech startups have less time, experience, or resources to secure their infrastructure. Hardware and software vulnerabilities can appear at any time. Social engineering can breach defenses with a simple click on a link.

As software innovators, fintech companies are particularly vulnerable to third-party and supply chain risks. Cloud computing and X-as-a-service providers let startups piece together enterprise-grade operations. Fintech developers rely on repositories of third-party code to simplify and shorten project lifecycles, exposing their software to supply chain attacks.

These third-party relationships can create significant risk.

 **A fintech company's cybersecurity is entangled with its service providers' security practices. Without careful controls, code dependencies can open attack vectors into a fintech company's systems—and allow hackers into its customers' systems.**

Compliance with SOC 2 and other cyber risk management frameworks can make fintech companies—and their customers—more secure.



## 3. Fintech Financial and Business Risk

With proper funding, early-stage technology companies are agile and risk-tolerant. They quickly bring advanced technologies to market, pivot to seize new opportunities, and rapidly iterate in response to customer demand.

 **A fintech company's greatest strength is also a significant source of risk.**

### Operational Risks

The problem with moving fast and breaking things is that you break things.

That might be fine in social media, but not when you handle credit card data or process a bank's transactions. Fintech companies must balance innovation against operational risks.

### Technology Risks

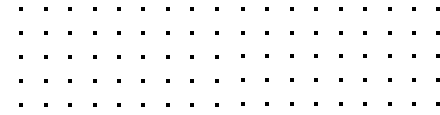
At the same time, fintech depends on technology-driven business models with inherent risks. For example, artificial intelligence and machine learning algorithms can amplify the prejudices built into training data sets.

### Consumer Risks

Fintech scales quickly by making sophisticated financial services more accessible to a broader range of consumers. However, selling to more people means selling to more financially naive people.

Consumers who do not understand a financial service and its risks can get burned even if a fintech company does nothing wrong.

If something does go wrong, impacting thousands of consumers, a fintech company could face a business-ending backlash.



## Investor Risks

Venture capital funds and other tech investors willingly place long-term bets that fund fintech innovation. That model works well as long as investor optimism remains strong.


Recession, geopolitical uncertainty, and other factors can undermine that optimism. As VC firms become pickier about their investments, fintech companies could lose the funding they need to survive.

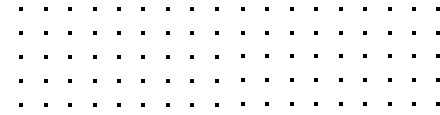
## 4. Fintech Reputational Risk

The whole point of financial regulation is to preserve confidence in the financial industry. For all the technological innovation fintech brings to market, reputation still matters.

A significant cyber incident or the collapse of a funding round will damage a fintech company's reputation. Consumers will flee to more reliable competitors. Banks will question the value of the firm's services.

Companies that manage their business well can still suffer from the mistakes of their competitors. For example, failed crypto exchanges create distrust in companies building blockchain solutions.

 **Compliance programs that keep other risks under control go a long way toward avoiding these reputational risks.**



# Addressing Major Fintech Security and Compliance Issues

Any business must manage risk. Fintech companies face unique risks by the nature of their business. These risks could disrupt their operations or impact their customers. As a result, financial institutions and regulators are paying closer attention to how fintech companies control risk.

A focused, continuous compliance program lets you manage risk in ways that reassure customers and regulators. However, achieving compliance is daunting for startups and large enterprises alike. Here are ways fintech companies can address common compliance issues.

## 1. Cyber Attacks and Vulnerabilities

Security breaches are not exclusive to the fintech industry. Hackers and advanced persistent threats can exploit any company's weaknesses. However, fintech companies often face greater risk because they work with sensitive financial data.

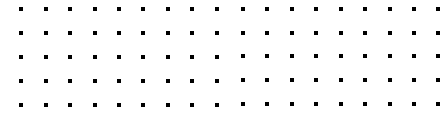
Any security breach could have devastating consequences.

In the past year, cybercriminals breached the defenses of several fintech firms, including:


- [Revolut](#): A targeted attack compromised the personal data of more than 50,000 consumers—almost half of them Europeans.
- [BankingLab](#): Supply-chain attacks compromised the banking services platform, opening pathways into other fintech companies.
- [Cash App](#): A former employee accessed as many as 8.2 million brokerage accounts.

Preventing breaches like these has always been the goal of cybersecurity. A compliance program can make cybersecurity strategies more effective.





## Addressing Cybersecurity Issues

 **Modern security frameworks such as SOC 2 and PCI DSS help fintech companies identify and close the gaps in their defenses.**

But that is not enough.

Consider the three examples above. Revolut was directly attacked. BankingLab's software dependencies compromised its customers' defenses. And Cash App forgot to deactivate a former employee's credentials.

Vulnerabilities and breaches can happen anywhere, anytime.

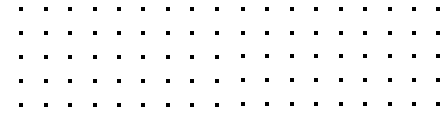
A compliance program goes beyond meeting a security framework's requirements. Continuously monitoring compliance lets you identify and close new security gaps before their impact can spread.

## 2. Crypto-Asset and Other Fintech Regulation

Fintech companies operate in a regulatory grey area. In some cases, they may not be subject to a regulation that applies to their customers. In others, regulators are slow to apply existing rules to a young, innovative industry.

Things have changed over the past few years. Regulators are paying closer attention to fintech in several areas:

- **Due diligence and know your customer (KYC):** Britain's Financial Conduct Authority (FCA) found that many challenger banks failed to meet due diligence standards.
- **Anti-money laundering (AML):** Acting FinCEN director Himamauli Das recently admitted that fintech payment services operate under decade-old AML regulations that do not reflect the state of today's industry.



- Asset markets: Commodity Futures Trading Commission (CFTC) Chairman Rostin Behnam discussed the risks of digital asset markets and ways the CFTC plans to regulate the digital asset industry.

As regulators focus on fintech, companies in the industry must get their compliance programs in order.

## Addressing Fintech Regulation Issues

Fintech companies must understand the regulatory landscape—the rules that apply today and how regulations will change in the future.

That way, decision-makers have a foundation for evaluating regulatory risks and developing appropriate policies and controls.

A compliance program gives you real-time visibility of these controls while making your organization more responsive to queries from regulators and auditors.

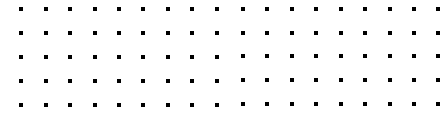
### 3. Data Privacy

Policymakers worldwide are responding to concerns about data theft and the use of personally identifiable information. While the European Union's efforts are the most prominent, privacy regulations everywhere are getting stricter.

That does not mean privacy regulations are getting more consistent.

The General Data Protection Regulation (GDPR) only applies within the European Union. The U.K. has its own version, while the United States has no national privacy law. Companies instead navigate a patchwork of state-level regulations.

 **With their cloud-first development strategies, fintech companies can serve customers anywhere. That competitive advantage gets overwhelmed by the complexity of data privacy compliance.**



## Addressing Privacy Issues

While each jurisdiction's regulatory frameworks are different, they do rhyme. A GDPR compliance control does not guarantee CCPA compliance. That doesn't mean you must duplicate compliance efforts for every framework.

Use a privacy risk assessment to:

- Identify applicable regulations for your current and future business.
- Map similar requirements and develop appropriate controls.
- Implement and monitor privacy controls.

With the right monitoring system, you can reduce redundancy and make privacy compliance more efficient.

## 4. Compliance & Non-Compliance Costs

Achieving compliance in the previous three areas has a cost. In a [recent survey](#), more than half of financial services companies expected to increase compliance spending in 2022, with nearly 20% of respondents planning a significant increase.

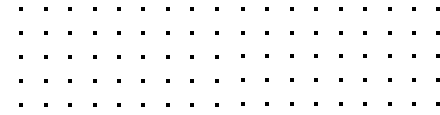
Growth-driven startups may be reluctant to divert resources to support compliance, but not doing anything carries significant costs.

Besides the risk of regulatory violations and fines, non-compliance introduces opportunity costs.

As far as the U.S. Treasury Department is concerned, banks are "[ultimately responsible](#)" for their fintech partners' activities. Fintech companies that can't pass a compliance audit should not expect much business from highly-regulated banks.

## Addressing Privacy Issues

A good compliance program starts with a risk assessment that prioritizes risks, and lets business leaders decide which to address and which to accept.



Compliance frameworks often make this prioritization easier by requiring “reasonable and appropriate” measures rather than one-size-fits-all procedures.

Small startups will not need the expensive controls of a large enterprise. On the other hand, a rapidly-growing company could find that last year’s measures have become inadequate.


## 5. Updating Your Compliance Program With New Features & Products

Rapidly-iterating technology companies can fall out of compliance without knowing it. A simple product update could open a security vulnerability or expose users’ personal information.

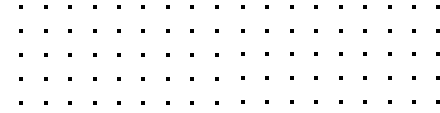
At best, checking code for compliance before it goes to production is inefficient. At worst, the review misses issues to create new compliance gaps.

### Addressing Product Development

Security, privacy, and other compliance issues must happen early in development.

 **Compliance by design embeds best practices into software development that reduce risk and make compliance more efficient.**

Shifting compliance to the left also instills a compliance culture in your development teams. Compliance becomes everyone’s responsibility.



## 6. Proactive Compliance

Reactive approaches to compliance are expensive and disruptive. Everyone in the organization scrambles to get ready for the audit. People drop everything to close newly discovered compliance gaps. Analysts spend days querying and collating data to meet auditors' requests.


Doing compliance this way disrupts operations and creates a false impression that everything is fine.

That's a mistake. A successful audit only tells you that you complied. You may not be compliant anymore.

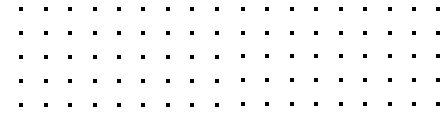
### Addressing Compliance Proactively

An audit only gives you a baseline. The only way to know that you are still compliant is by continuously monitoring your compliance status.

You can't hire enough people to do that manually.

 **Systems that automate compliance monitoring let you prioritize your compliance efforts. Automations can resolve minor issues while flagging those that require human decision-making.**

Proactive compliance identifies and addresses gaps faster while making audit requests easier to meet.



## Trust Through Compliance

Addressing these issues by assigning a tiger team to address security gaps or writing a data protection policy is not enough. Fintech's success—and some high-profile failures—have put the industry under a spotlight.

Consumers need to know their personal finances are safe.

Banks need to know their fintech partners won't compromise their own security.

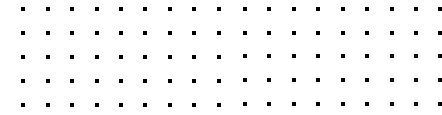
Inspiring trust through compliance is just good business. However, fintech companies are facing increased scrutiny from another direction: regulators. Here again, compliance will make a difference.

## Fintech Regulations Around the World

In two recent examples, unaddressed fintech risks caused cryptocurrency exchange FTX's collapse and the \$140 million civil penalty imposed on USAA Federal Savings Bank. As a result, regulators are paying closer attention to risk in the fintech industry:

- Acting Comptroller of the Currency Michael J. Hsu recently explained how his office will [scrutinize bank-fintech relationships](#).
- The U.S. Department of the Treasury recommends [more robust regulation and oversight](#) of fintech services.
- New third-party risk management rules in the E.U. Digital Operational Resilience Act (DORA) will require fintech companies to [strengthen their cybersecurity practices](#).

The fintech industry's ability to do business anywhere exposes them to regulations everywhere. This section will review just some of the regulations fintech companies may face doing business in the major economies.



## Fintech Regulation in the United States

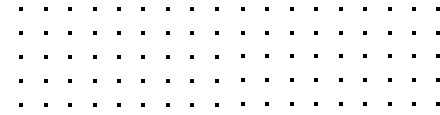
Strong financial and technology industries make the United States a global fintech innovation center. America’s unique regulatory structure, however, makes fintech compliance challenging.

### U.S. Federal Regulations

Congress has passed few fintech-specific laws. In its place, regulators have extended existing rules to the new industry.

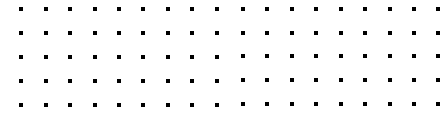
Federal regulations that may apply to fintech include:

<p><b>Bank Secrecy Act</b></p>	<p>Anti-money laundering (AML) law requires the tracking of certain transactions. Institutions must report large transactions and suspicious activity to FinCEN.</p>
<p><b>Anti-Money Laundering Act (AMLA)</b></p>	<p>Refocuses AML rules from reactive reporting to proactive risk management. AMLA also emphasizes the use of financial technology in AML compliance and enforcement.</p>
<p><b>Bank Service Company Act</b></p>	<p>Refocuses AML rules from reactive reporting to proactive risk management. AMLA also emphasizes the use of financial technology in AML compliance and enforcement.</p>
<p><b>Consumer Financial Protection Act</b></p>	<p>Authorizes the CFPB to oversee the transparency, fairness, and competitiveness of consumer financial products.</p>
<p><b>Dodd-Frank Wall Street Reform and Consumer Protection Act</b></p>	<p>Strengthens oversight of the US financial industry as well as its transparency and accountability. Reforms passed in 2018 reduced the burden on smaller institutions.</p>



<p><b>Electronic Fund Transfer Act</b></p>	<p>Defines consumer rights and company responsibilities for electronic financial transactions such as debit cards, online payments, and remittances.</p>
<p><b>Electronic Signatures in Global and National Commerce Act (E-Sign)</b></p>	<p>The E-Sign act authorizes the use of electronic records and signatures while specifying consumer disclosure, informed consent, and record retention requirements.</p>
<p><b>Equal Credit Opportunity Act (ECOA)</b></p>	<p>Bans discrimination by creditors or card issuers. Consumers denied credit must receive an adverse action notice explaining the reasons for the denial.</p>
<p><b>Federal Deposit Insurance Act</b></p>	<p>Gives the FDIC authority to supervise its member banks for operational soundness and compliance with consumer protection laws, including how member banks apply financial technologies.</p>
<p><b>Gramm-Leach-Bliley Act (GLBA)</b></p>	<p>The GLBA eliminates barriers between different financial services and requires financial institutions to protect customer information—including how they disclose information to their third-party service providers.</p>
<p><b>Jumpstart Our Business Startups Act (JOBS Act)</b></p>	<p>The JOBS Act eases regulatory burdens on small businesses and lets certain companies delay compliance with regulations such as Sarbanes-Oxley. The law also authorized equity crowdfunding by smaller firms.</p>
<p><b>Health Insurance Portability and Accountability Act (HIPAA)</b></p>	<p>Businesses that serve the healthcare and insurance industries may be subject to HIPAA's rules protecting patient information, including their financial data.</p>





<p><b>Securities Act of 1933</b></p>	<p>Authorizes the Securities and Exchange Commission to regulate who may invest in, sell, or manage securities. These regulations can apply to tokens, initial coin offerings, and other blockchain applications.</p>
<p><b>Truth in Savings and Truth in Lending Acts</b></p>	<p>Regulate how financial institutions disclose information to consumers about deposit accounts, credit cards, loans, and other services.</p>

These laws provide the framework for financial regulation but leave specific rule-making to the executive branch. For example, the GLBA authorized the Federal Trade Commission to decide how financial institutions should protect customer information. The resulting Safeguards Rule requires an information security program that:

- Ensures the security and confidentiality of customer information.
- Protect against security threats.
- Prevents unauthorized access to customer information.

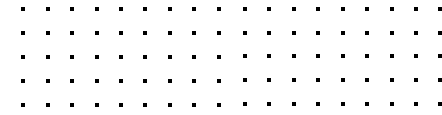
Court decisions also limit or clarify federal rules. For example, the Supreme Court ruling in Securities and Exchange Commission v. W. J. Howey Co established the “Howey Test” determining what financial products are securities.

## U.S. State Regulations

Federal law may not apply to business transactions confined within a state’s boundaries. Doing business in that state requires compliance with that state’s regulations.

For example, most companies engaged in lending or money transmitting must comply with the regulations in each state where they offer their services.

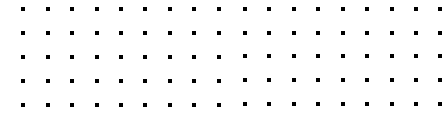
State-level variation also occurs when some states take more proactive approaches to fintech. New York’s BitLicense strictly regulates virtual currency companies. Wyoming, Virginia, and other states offer more attractive regulations.



## Fintech Regulation in the European Union

Financial technology companies once navigated similarly fractured European regulations. However, recent E.U.-level legislation has begun to harmonize compliance demands in Europe.

<p><b>Anti Money Laundering Directives (AMLD)</b></p>	<p>The 5th and 6th AMLDs expand the E.U.'s anti-money laundering laws to virtual currency and other fintech sectors while tightening due diligence and disclosure requirements.</p>
<p><b>Digital Operational Resilience Act (DORA)</b></p>	<p>Financial institutions and their third-party providers, including cloud platforms and data analytics firms, must adopt an IT risk management framework that includes resilience testing, incident reporting, and third-party risk assessments.</p>
<p><b>General Data Protection Regulation (GDPR)</b></p>	<p>GDPR defines the individual privacy rights of E.U. citizens, how companies must protect those rights, and the penalties for violations.</p>
<p><b>Markets in Crypto Assets (MiCA)</b></p>	<p>Sets E.U.-wide regulations for asset-referenced tokens, electronic money tokens, and other crypto assets not already addressed in E.U. legislation.</p>
<p><b>Payment Services Directives (PSD)</b></p>	<p>PSD harmonizes payment service provider regulations. Its 2015 revision introduced the use of strong authentication to protect customer transactions and extended regulation to emerging fintech services.</p>
<p><b>Regulation on European Crowdfunding Service Providers (ECSPR)</b></p>	<p>ECSPR brings crowdsourced lending and investment under a single umbrella. The law defines disclosure rules, how crowdfunding platforms manage risk, and how nations oversee these platforms.</p>



## E.U. Member States

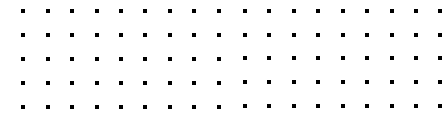
Before the E.U.’s updated regulations, individual member states took the initiative to become centers for fintech innovation. For example, cryptocurrency companies flocked to Malta for its blockchain-friendly regulations.

E.U. legislation eliminates some of these advantages by making fintech regulation more uniform. At the same time, regional variations persist. The Bank of Lithuania’s regulatory sandbox has made the country a European hub for fintech investment.

## Fintech Regulation in the United Kingdom

After its departure from the E.U., the U.K.’s financial regulations remained aligned with Europe. That is changing as outlined in the U.K. government’s Future Regulatory Framework (FRF) Review. U.K. financial regulations that may apply to fintech include:

<p><b>Financial Services and Markets Act (FSMA)</b></p>	<p>FSMA reforms the Bank of England and authorizes the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) to regulate the U.K. financial industry.</p>
<p><b>Proceeds of Crime Act (POCA)</b></p>	<p>POCA updates AML legislation in the U.K., requiring financial institutions to monitor transactions and report suspicious activities.</p>
<p><b>Sanctions and Anti-Money Laundering Act</b></p>	<p>Immediately after Brexit. SAMLA kept the U.K. aligned with international AML standards and filled regulatory gaps once covered by E.U. law.</p>
<p><b>Money Laundering, Terrorist Financing and Transfer of Funds Act (MLA 2017)</b></p>	<p>MLA 2017 requires firms to conduct a money laundering and terrorist financing risk assessment, develop controls to mitigate those risks, and conduct due diligence on customers. Firms must also be aware of practices at any third parties they contract with.</p>



## Fintech Regulation in Other Countries

Chinese fintech companies have come under ever-harsher regulation, culminating in the suspension of Ant Group's initial public offering. The 14th Five-Year Plan makes fintech a strategic goal for China's financial system—provided it supports the “real economy” under strengthened supervision.

Hong Kong maintains a separate financial regulatory regime from mainland China. By interpreting existing rules, Hong Kong's regulators have created a favorable environment for crypto, virtual banking, and other fintech services. While making it easier to set up shop in Hong Kong, these efforts do not exempt fintech companies from AML or privacy regulations.

The Monetary Authority of Singapore (MAS) applies the same regulatory standards to fintech companies as it does to the country's traditional financial industry. Recent legislation, the Payment Systems Act (PSA), brought seven types of payment services—any of which may apply to fintech—under a single regulatory regime.

## Complying From Country to Country

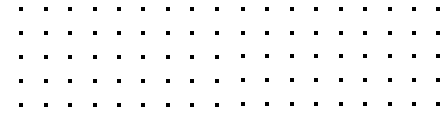
From country to country, fintech-related regulations are different—but they do rhyme. Every country shares common goals, from preventing money laundering to protecting consumers. Even though compliance at home does not guarantee it in other countries, a fintech business can deploy domestic compliance systems in ways that meet requirements in other nations.


## 2 Steps to Compliance

Once you've understood all the risks, issues, and regulations that could impact your fintech business, it's time to develop your compliance program. The first step towards compliance is a formal review of risk across your organization. Once that's in place, you can apply a security framework to mitigate and control those risks.

## Creating a Risk Assessment

A risk assessment evaluates every aspect of your business to understand your risk exposure.



 Each assessment includes an estimate of how the risk could impact your business, as well as the probability of the risk occurring. The magnitude of the impact and the risk's probability lets you set priorities and make better decisions.

There are several approaches to building this matrix of risks, impacts, and probabilities. In most cases, companies use a combination of the following:

## Quantitative vs. Qualitative

Ideally, every risk will have a **quantifiable impact** and probability. Measuring the dollar value of risk lets you conduct cost/benefit analyses that decision-makers will understand. However, getting to that dollar value can be complex. For some risks, it may be impossible.

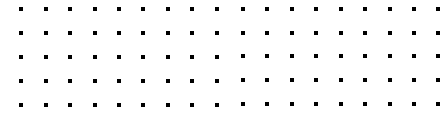
**Qualitative methods** categorize risk. Using labels such as Red, Yellow, and Green lets decision-makers know which risks to address first. Alternatively, risk managers can rank risks on a finer numerical scale, allowing semi-quantitative analysis.

## Assets vs. Vulnerabilities vs. Threats

Risk assessments commonly start by evaluating the assets a company's IT team manages. **Asset-based risk assessments** build upon existing IT security processes, making them relatively straightforward.

However, many risks do not come from IT infrastructure. They may emerge from internal processes, such as how a hospital distributes patient information. Human nature also creates risks from social engineering attacks. A **vulnerability-based risk assessment** collects these non-technical risks.

With their internal focus, asset and vulnerability-based assessments may only capture some risks the organization faces. **Threat-based methodologies** start with the external sources of risk to the company's security and continuity. In this approach, you evaluate how your systems and processes respond to the threats your company is most likely to face.




## Third-Party Risks

Finally, you must evaluate how your third-party relationships expose your company to risk. For example, the code repositories your developers use could become a vector for a supply chain attack. Even service providers like your HVAC repair company could become a bridge into your network.

Audit each third-party relationship to understand the impact and probability of every risk it creates. You can provide many of these companies with a self-reported security questionnaire.

Others will require more due diligence to understand their security practices.

 **Do not treat third-party risk lightly. In an ever more connected business world, other companies' practices could severely impact your security. That's why modern security frameworks require formal third-party risk management processes.**

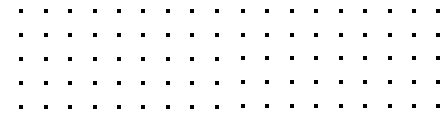
## Top Fintech-Related Security Frameworks

Rather than developing your own risk management system from scratch, you can apply frameworks developed by industries and governments to streamline risk management. Compliance with a standard framework also makes it easier for your customers to evaluate your security practices.

Here are four security frameworks that often apply to fintech companies:

### NIST CSF

Growing threats of cyberattacks on America's critical infrastructure spurred the creation of the National Institute of Standards and Technologies Cybersecurity Framework (NIST CSF).



**This voluntary collection of guidelines, best practices, and standards give organizations a flexible approach to mitigating cyber risk.**

Fintech companies may be considered part of the nation's critical infrastructure based on the nature of their business or of the financial institutions they serve. Compliance with NIST CSF will reassure customers and regulators that your company can protect sensitive financial information.

## ISO/IEC 27000

Companies operating internationally may choose compliance with security frameworks developed by the International Organization for Standardization (ISO).

**The family of standards under ISO/IEC 27000 help organizations secure their information management systems and protect data privacy.**

For example, ISO/IEC 27001 describes "the requirements for establishing, implementing, maintaining and continually improving an information security management system." The latest version of ISO/IEC 27001 specifies 93 controls to address physical, technological, organizational, and human risks.

## PCI DSS

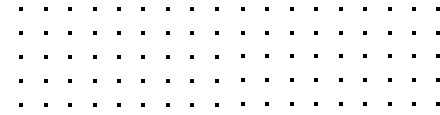
**Fintech companies that handle credit card data must comply with the Payment Card Industry Data Security Standard (PCI DSS).** Visa, American Express, and other credit card brands unified their security policies to better protect card issuers from fraud and cybercrime.

Any organization that stores, processes, or transmits credit card data must comply with a dozen PCI DSS requirements. These range from technical tasks like protecting networks behind a firewall to policies like granting access to cardholder data on a need-to-know basis.

## SOC 2

Fintech companies that provide cloud-based services should consider compliance with the American Institute of CPAs (AICPA) Service and Operations Controls (SOC) framework.

**Those directly handling financial data will need SOC 1 compliance, while SOC 2 compliance will apply to those that provide other services to financial institutions.**



# Charting a Course to Fintech Compliance

The financial industry's potential to impact individual consumers, the national economy, and the international monetary system created a conservative culture. Fintech companies are bringing the innovation and agility of the tech world into that stable environment.

As the two cultures collide, trust becomes even more critical. Fintech firms need the freedom to innovate, but they cannot put their customers at risk. Compliance provides the roadmap fintech companies need to navigate their complex security and regulatory ecosystem.

Choosing the frameworks that apply to your business lets you bring your risks under control. Almost as importantly, security framework compliance provides auditable evidence that regulators and your customers can trust.

If you're ready to pursue compliance for 14+ frameworks including SOC 2, PCI DSS, NIST CSF, and GDPR, [book a demo](#) with Drata. Automated evidence collection, continuous control monitoring, a robust risk management solution, and more will help you scale securely and efficiently.