




# Simplifying compliance with CI/CD



Every organization in every industry has an element of risk. Whether the risk is inherent to the sector or introduced by the processes of a specific organization, it is an ever-present reality of operations. To keep things running smoothly, organizations must develop compliance policies that help minimize risk by implementing controls that serve as guardrails.

With the workplace now dominated by technology, the burden of ensuring compliance often falls to centralized platform engineering or SecOps teams. Software must comply with industry regulations, and every application requires its own controls to minimize risk. This means that designing compliant software for a specific industry requires a deep understanding of that industry's compliance regulations.


Not only must software be compliant as it performs its functions, but also often has to monitor for potential compliance issues — and it then needs the infrastructure

to identify and address these problems. Meanwhile, platform and IT security teams must observe compliance controls for their operations and implement software-based compliance controls for other departments.

With its rapid development cycles and constant impetus for evolution in software, compliance concerns can create a significant barrier for delivery teams trying to maintain a high rate of releases. Having to design with compliance in mind and continuously monitoring for compliance problems slows down development, consuming resources that might otherwise go toward value-generating tasks like designing new features or improving existing code and infrastructure.

But compliance is essential and not without benefits. In some industries, strict regulations make compliance a legal necessity. Even for enterprises without such strict regulations, effective compliance policies reduce risks that can cost time and money and damage organizations.





# The role of risk management in modern software development

Software development has become a risky business with software embedded in our daily lives and inextricably woven into our infrastructure. The most significant risks of early software were no more than crashing a single machine. But modern software can handle vast amounts of sensitive data and coordinate critical physical infrastructure – facilitating most of the world’s daily communications and transactions.

Stringent compliance policies are vital to managing this risk in modern software development. Handling the many potential vulnerabilities inherent in software development requires a diverse set of compliance policies to ensure that both code and features comply with internal and regulatory controls.

# The many risks of software development

DevOps teams have no shortage of risks to manage. Along with ensuring that application functionality is in line with industry-specific and organization-specific compliance policies, DevOps teams also observe policies that help protect the software and its users. Specific compliance policies can help minimize the risks of software development. These include the controls requiring developers to identify and eliminate vulnerabilities and strict guidelines on collecting, storing, and processing data for operations.

Because modern applications often handle sensitive data, a seemingly small failure in compliance can have serious consequences. Failure to enact and maintain proper security measures and test for vulnerabilities can expose numerous attack vectors. This failure allows malicious actors to take advantage of vulnerabilities that have the potential to expose sensitive data or execute injection attacks that causes the software to perform unpredictably.

These vulnerabilities can arise from the code in the application and from the dependencies in the project. Compliance controls should be in place to ensure dependencies have proper sources and are scanned and verified before reaching production as part of an application.

While having the right compliance policies in place can go a long way towards minimizing risk, it is also essential to recognize that compliance is not security – and security is not compliance. Compliance policies provide guardrails and controls that help ensure due diligence for cybersecurity matters.

But with the ever-evolving nature of software, compliance often lags behind cybersecurity demands. For some policies, compliance is less about preventing problems and more about documenting them. In the finance industry (where, in many respects, the idea of compliance originated), compliance is often less about avoiding risks and more about creating easily auditable paper trails. Paper trails make it easier to investigate security breaches and hold malicious actors accountable.

A more pre-emptive approach to cybersecurity is required for software to be truly secure. Compliance measures and industry regulations provide baseline measures, best practices, and policies that help handle issues after they occur. However, compliance cannot provide a flexible approach that accounts for emergent threats and the day-to-day concerns of cybersecurity operations.

# Examples of compliance requirements

## Finance

Compliance in the finance industry is concerned with protecting consumer privacy, reducing the risk of handling financial transactions, and preventing fraudulent transactions. Many government organizations and regulatory bodies dictate financial compliance. Specific compliance regulations can be broadly divided into two primary finance categories: banking and fintech

### **BANKING**

Handling large amounts of consumer and investor data and being responsible for substantial monetary transactions, the banking industry has always been at the forefront of compliance policies. Compliance regulations include day-to-day operational compliance aimed at reducing risks and combating illegal activities such as fraud and money laundering. Also, strict regulations mandate how banks collect, store, and process consumers' private information and financial data — such as transaction history, credit scores, and information about specific accounts. Other compliance rules focus on how banks communicate with and advertise to investors and customers.

### **FINTECH**

Banks and other financial organizations use fintech services to facilitate transactions and handle digital banking tasks. These technologies provide an intermediary between consumers and economic organizations, so they manage large volumes of confidential information, financial data, and personally identifiable information about consumers — numerous legal regulations control what types of information fintech services can collect, process, and store.

Ethical and professional standards further reinforce these legal requirements. Because fintech products are technology products, compliance for fintech is often enforced at the software level, putting the burden on developers to implement policies in code and ensure that fintech applications are designed with compliance in mind.

## Retail

The retail industry has a broad set of compliance regulations that vary widely depending on the products sold and their location. There are local government regulations and vendor and partner-specific compliance policies. Retail compliance includes controls affecting consumer privacy, data handling, inventory management, and requirements affecting when and where retailers can sell specific products. The scope and strictness of compliance regulations vary widely depending on the type of products, with some requiring extensive controls on transportation, storage, and sales. Compliance regulations also impact how retailers store and process data related to their products, employees, and customers.

## Healthcare

In a space that handles sensitive patient information and private medical records, the healthcare industry must adhere to a large set of legal and ethical compliance policies. Subject to strict government regulations specifying how patient data can be stored, accessed, and processed, any software that handles patient information must be compliant. Healthcare compliance also extends to billing, medical research, and patient care, creating a broad scope for healthcare compliance policies.

## Manufacturing

Compliance for the manufacturing industry seeks to reduce risk to consumers, employees, and any parties involved in the supply chain. Manufacturing compliance encompasses health and safety regulations for employees and equipment, operational standards of the manufacturing process (which can vary widely depending on the type of products), and customer and collaborator data privacy controls.

## Government

While the government is often the source of compliance regulations, government organizations must also adhere to their own strict compliance rules. With a highly diverse set of responsibilities and operations, what compliance looks like for government agencies can vary widely from one agency to the next. Government sectors regularly work with sensitive information that they must protect with stringent compliance policies. Many government tasks also overlap with compliance regulations of other industries, as government bodies often handle legal, financial, and even medical data.

## Legal

Law firms and other legal professionals have access to large amounts of sensitive personal information. To ensure this information is securely stored and to avoid mishandling, the legal profession must follow compliance policies covering access to sensitive information and how it can be collected, stored, and processed.

## Education

Compliance in the educational field is primarily concerned with how student information is collected, stored, and processed. Many regulations govern how educational information – such as grades and transcripts – can be accessed and by whom. Educational institutions must also observe strict rules that ensure the wide accessibility of physical and digital facilities and resources.

# Common compliance frameworks

## State and local

### CCPA

The California Consumer Privacy Act (CCPA) became law in 2018. Like GDPR, the CCPA allows consumers in California to request all the data an organization has stored about them. Any organization with over \$25 million in annual revenue that provides services to California residents must comply with CCPA and observe specific policies for collecting and storing data on California consumers.

### NEW YORK'S SHIELD ACT

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act mandates the implementation of "reasonable safeguards" to protect consumers' private information in New York state. It also requires organizations to alert consumers in the event of a security breach that may expose consumer information. The SHIELD act primarily concerns sensitive personal information, including names, addresses, credit card numbers, and the like. It also encompasses digital information, such as email addresses, usernames and passwords, and biometric data.

## International

### GDPR

The General Data Protection Regulation (GDPR) is one of the world's strictest laws on storing and transmitting data. Passed into law in the European Union (EU) in 2018, this privacy law applies to any organization that processes the personal data of citizens and residents of the EU. This makes its reach extremely broad, requiring any organization that wishes to do business within or pertaining to the EU to comply with the regulations.

GDPR imposes stringent rules on data collection, processing, and storage. It minimizes the amount of data collected and ensures that it is used only for legitimate purposes. It requires data to be stored securely and confidentially and includes strict accountability rules for any organization that collects or stores personal data. Under the GDPR, EU residents may request copies of all information an organization has collected about them.

### ISO

The International Standards Organization creates and maintains a vast body of international standards and best practices used as the basis for numerous compliance frameworks. The ISO/IEC 27000 family provides a set of standards for information security, offering detailed IT security policies for keeping data secure.

## National

### NIST

The National Institute of Standards and Technology (NIST) is a non-regulatory body operating within the US Department of Commerce. NIST works to establish best practice standards for a variety of industries. The most well-known is the cybersecurity framework, which prescribes a series of best practices and standards that minimize cybersecurity risks. The standards and best practices recommended by NIST are the foundational elements of many other compliance frameworks in the US, including HIPAA and SOX compliance.

### PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) is a set of regulations specifically designed to protect consumers' payment information, such as credit and debit card numbers and associated personal information used for transactions. PCI DSS requires organizations to protect relevant network systems and maintain secure payment applications. It imposes restrictions on the types of payment and transaction data that can be retained and includes rules on how long an organization can retain such data.

### FEDRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a set of cyber-security policies that apply to all government agencies in the US, mandating how federal agencies can use cloud services. FedRAMP compliance is required for the government agencies themselves and any cloud services that interact with national data.

### HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides a set of standards for handling patients' sensitive health information, such as medical records and personally identifiable information related to patients' conditions and treatment. Broadly, HIPAA is five rules:

- Privacy rule
- Transactions and code sets rule
- Security rule
- Unique identifiers rule
- Enforcement rule

Any organizations handling US medical data and patient information must by law be HIPAA compliant.

### FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal law mandating how organizations can interact with information about students and educational records. Compliance with FERPA is necessary for any organization that handles student information, governing what student information can be disclosed and under what circumstances it can be stored or shared. This includes information such as test scores, grades, student health information, and student financial information.

### SARBANES-OXLEY (SOX)

The Sarbanes-Oxley Act became US law in 2002. Created in response to high-profile incidents of accounting fraud in the early 2000s, SOX compliance requires adherence to a strict set of data security policies that help combat fraud. By mandating specific financial disclosures, the act improves reliability in financial reporting. SOX is broadly applied to all public companies in the US and does not apply to private companies.



# Automate compliance with CI/CD and DevSecOps

CI/CD supports the rapid pace of change necessary for modern software development. With new additions to software often introduced multiple times a day, an effective CI/CD pipeline allows developers to maximize the velocity of development cycles and deliver essential changes such as bug fixes and new features to production environments with minimal delay.

However, this rapid pace of change can also create compliance concerns. With every addition to code comes further questions about maintaining compliance. Manually handling compliance can significantly reduce DevOps's flexibility, hampering the team's ability to deploy new code.

A CI/CD pipeline automates the process of building, testing, and deploying code. Organizations can implement compliance measures throughout the pipeline, especially during the automated testing phase, where controls can test incoming code for compliance standards to ensure the implementation is in line with compliance requirements.

As the number and types of risks, **the evolution of DevOps into DevSecOps** has integrated security as a core tenet of developing and operating applications. While security and compliance are not the same, there is enough overlap between compliance controls and some aspects of cybersecurity that DevSecOps teams can simultaneously tackle certain compliance and security concerns.

Enforcing compliance as a part of CI/CD can help teams shift left from DevOps to a DevSecOps model, where key processes such as **vulnerability scanning** are automated to observe compliance policies and improve the security of code that makes its way to production. The **Continuous Application Security (CAS)** model addresses ongoing concerns about securing new implementations by continuously scanning, assessing, and auditing application security, allowing Agile and DevOps teams to rapidly iterate their code base without conducting time-consuming manual security reviews. Observing security measures as part of CI/CD is essential for organizations looking to adopt a CAS model.

Technologies such as **CircleCI's orbs** allow development teams to seamlessly integrate critical security and compliance measures into a CI/CD pipeline. Orbs can take the form of reusable commands and executors and be integrated into the CI/CD flow with minimal development time, allowing DevOps teams to stay focused on innovation and problem-solving while **offloading repetitive security and compliance tasks to automated systems**.

## Continuous compliance techniques

As CI/CD has become an industry standard for software development, continuous compliance has gained popularity. Though it may sound challenging to implement and maintain, there are a few fundamental techniques and technologies that make continuous compliance an achievable goal for any CI/CD pipeline:

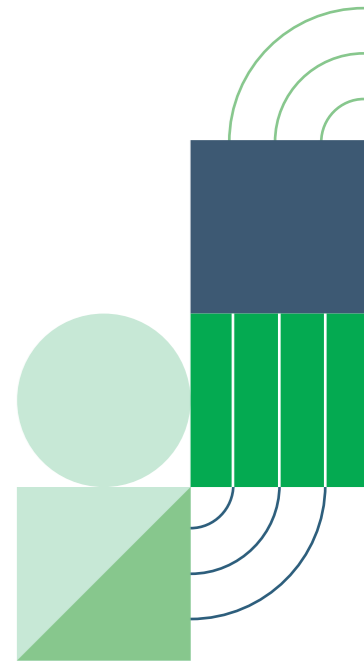
- **Automate security scans from development to production:** **Security scanning and automated testing** for new code ensure that all code is compliant before it reaches a production environment.
- **Enforce compliance requirements through programmatic configuration policies:** With the use of **org-wide configuration controls**, central admin teams can automatically ensure every pipeline follows the policies and practices that their industry requires.
- **Limit the use of static credentials:** Teams can reduce their risk exposure by using **short-lived authentication tokens** instead of static credentials to authenticate with infrastructure providers and other third-party services.
- **Implement manual checks in deployment pipelines:** Occasionally, automation falls short and needs manual intervention. By **deploying with approval-based workflows**, issues that require manual intervention are automatically flagged and addressed to the appropriate authority for review.
- **Make approved pipeline components reusable with container images and orbs:** Why reinvent the wheel? Reusable components such as orbs and container images mean that compliance controls and tests can be packaged for later use and reused when appropriate.
- **Store test results and audit logs:** **Test results** and **audit logs** provide valuable data for tracking compliance issues. Should a problem with continuous compliance arise, test results and audit logs can be consulted to find the root cause and inform a remediation strategy.
- **Incorporate monitoring and observability tools for risk detection and report generation:** It is difficult to detect potential risks without adequate insight into a system and its behavior. **Observability** tools can continuously monitor for issues and automatically generate reports with relevant metrics and actionable data to address the issues.

## Benefits of continuous compliance

With continuous compliance integrated into a smoothly-flowing CI/CD pipeline, DevSecOps teams can expect much faster risk detection and remediations when an issue is spotted. Automation assists in detecting problems but can also help with basic remediation tasks.

Continuous compliance generates a substantial amount of helpful information by collecting detailed reports from observability tools and maintaining a large volume of audit logs and other data. This data can be applied to address existing compliance concerns or create new compliance policies and controls. It can also help teams pass audits more quickly and maximize actionable insights from an audit.

Ultimately, continuous compliance gives developers, operations teams, and managers extra peace of mind and security. It lets them rest easy knowing they have done their due diligence with effective compliance policies, reinforced with software controls and richly detailed information in the form of observability metrics and audit logs.



# Ease compliance headaches with CircleCI

In many ways, continuous compliance is a logical progression of the automation introduced by CI/CD. By enabling teams to ease the burden of manually ensuring compliance and providing a superpower in the form of automated compliance controls and continuous monitoring of compliance issues, continuous compliance is an essential approach for any organization. An investment in continuous compliance pays dividends for years to come — particularly for organizations operating in industries with strict compliance regulations.

Interested in learning more about adding continuous compliance to your CI/CD pipeline?

Contact [CircleCI](#) today to learn more.