DevOps from Code to Compliance: The 2026 Guide to Software and AI Regulations

www.jfrog.com

Table of Contents

Executive Summary 5

Introduction 6

- Governance: Not Just Oversight 6

5 Key Trends to Watch in 2026 7

- Trend #1: The EU Leads the Way (The “Brussels Effect”) 7
- Trend #2: Continued Fragmentation in the Regulatory Environment 7
- Trend #3: The Rise of AI Regulations 8
- Trend #4: Regulations Cover the Entire SDLC 9
- Trend #5: The Need for Automated Governance 9

The Regulatory Landscape in 2026 10

- Regional 10
  - Europe: The Global Leader in Digital Law 11
  - North America: A Fragmented Environment 11
  - Asia: Balancing Privacy and Innovation 12
- Industry-Specific Mandates and Security Frameworks 13

How to Tackle the Regulatory Environment 14

- Part 1: Design Your Software Compliance Program **15**
- Part 2: Build Automation and Controls Across Your SDLC 15
  - Building Compliance into Your Pipelines with JFrog 20
- Part 3: Deliver Your Software Compliance Program 22
- Automating Governance with DevGovOps 23

Closing Thoughts 24

Legal Disclaimer **25**

Appendix: Key Software Regulations and Frameworks in 2026 **26**

- Global **26**
  - ISO/IEC 27001 26
  - MISRA C:2025 27
  - PCI-DSS 28
  - SLSA 29
- Regional 30
  - North America 30
    - CCPA 30
    - COPPA 31
    - CIRCIA 32
    - DMCA 33

Table of Contents

    - DOJ Final Rule on Bulk Data Transfers 34
    - Executive Order 14028........ 35
    - Executive Order 14144........ 36
    - MODPA........ 37
    - SOX........ 38
    - TFAIA (SB53)........ 39
- Europe 40
  - BSI TR-03183 40
  - CRA 41
  - GDPR........ 42
  - The EU Artificial Intelligence Act 43
  - NIS2 Directive 44
  - PLD........ 45
- Asia........ 46
  - APPI 46
  - Final AI Content Labeling Rules 47
  - The Information Technology Act, 2000 48
  - PIPA 49
  - Privacy Act 1988 50
  - Industry-Specific 51
  - ANSI X9.125 51
  - DFARS 52
  - DORA 53
  - FDA Cybersecurity in Medical Devices Guidance 54
  - Federal Software Security Mandate 55
  - FedRAMP 56
  - FISMA 57
  - HIPAA 58
  - Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines 59
  - SOX 60
- Frameworks........ 61
  - AI RMF 61
  - CERT-In Guidelines 62
  - Capability Maturity Model Integration (CMMI) v3.0 63
  - Guidelines and Companion Guide of Securing AI Systems........ 64
  - IT-Grundschutz Compendium........ 65

Table of Contents

- NIST AI 800-1 66
- NIST CSF 67
- NIST SSDF 68
- Plan for Global Engagement on AI Standards 69

Executive Summary

The software supply chain has never been more complex with the widespread usage of open-source, AI/ML models, and AI-powered development tools. Regulators worldwide are demanding new levels of transparency and accountability, forcing teams to rethink Governance, Risk, and Compliance (GRC).

This guide provides a practical, three-part plan to help GRC, Security, and DevOps leaders transform compliance from a reactive burden to a competitive advantage through three core objectives:

- ✓ **Navigate the regulatory environment.**
  Understand the top five trends defining the regulatory landscape in 2026, from the EU's leadership to the rise of AI-specific rules. Dive deeper into 40+ key regulations and frameworks that apply to global enterprise software companies.
- ✓ **Build a proactive compliance program.**
  Learn how to create an automated compliance framework that aligns your development lifecycle with regulatory needs.
- ✓ **Automate governance.**
  Discover how to use automation and controls (through DevGovOps principles) to centralize artifacts, scan for vulnerabilities, enforce policies, and collect immutable evidence that proves due diligence to auditors and regulators.

Organizations that embed compliance into their SDLC will build more secure software, reduce risk, and accelerate time-to-market.

Introduction

We have entered an era of hyper-speed development, where AI is intensifying the rate of software innovation. As development accelerates, so do the dangers: in 2024, there were 33,000 newly reported CVEs, an increase of 27% YoY.

Governments are responding with new legislation, but these regulations are no longer just focused on code quality or data security. Now, they're scrutinizing software for potential harmful impacts, ethical implications, and societal consequences.

Historically, regulatory hurdles caught unprepared development teams off-guard, forcing them into manual, unreliable workflows like spreadsheets and attaching screenshots. That approach is now obsolete. Every development team must align with a more proactive GRC approach.

Governance: Not Just Oversight

The modern definition of 'Governance' is more than just oversight for regulations; it is an enabler. Automated governance empowers your organization to:

- Deliver trusted applications faster to your customers
- Demonstrate safe innovation and reliability
- Develop stronger brand recognition and authority.

This guide provides insights into the software and AI/ML regulatory environment in 2026, with details on how to build a robust software compliance program that aligns your Software Development Lifecycle (SDLC) to regulatory frameworks, with automated governance.

5 Key Trends to Watch in 2026

The regulatory landscape in 2026 will be defined by more complex software and AI regulations, with a focus on accountability and the ethical use of new technology. Here are five key trends that require immediate attention:

Trend #1: The EU Leads the Way (The “Brussels Effect”)

The European Union (EU) continues to set the global precedent with groundbreaking regulations like the EU Artificial Intelligence Act, Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA). Aligning with the EU’s rigorous standards is becoming the de facto global requirement for large enterprise companies.

- **The EU Artificial Intelligence Act:** Key obligations for high-risk AI systems, including those in critical infrastructure and law enforcement, will be in effect by August 2026, mandating that AI is transparent, traceable, and non-discriminatory.
- **Cyber Resilience Act:** This landmark law mandates secure-by-design principles for all digital products sold in the EU and requires active vulnerability reporting and continuous security updates.
- **Digital Operational Resilience Act:** Fully enforceable as of January 17, 2025, DORA mandates that covered financial entities and their critical ICT third-party providers worldwide comply with active supervision requirements.

Trend #2: Continued Fragmentation in the Regulatory Environment

While the EU leads, other regions have their own unique approaches, making compliance complicated.

- The U.S. relies on a patchwork of state-level laws and executive orders, rather than a single federal law for AI or cybersecurity.
- China is governing AI through a standards-based approach, expected to take shape in 2026 with over 50 national and industrial standards.

- Many U.S. states are rolling out wide-ranging regulations that mandate supply-chain risk management and algorithmic audits for automated decision systems.
- The United Kingdom uses the voluntary Software Security Code of Practice to promote security by design in software development.
- In Australia, primary guidelines come from the Australian Cyber Security Centre (ACSC). Key resources include the Information Security Manual (ISM) and the Essential Eight mitigation strategies.

AI is not the only area that is going to be impacted. Many U.S. states are rolling out wide-ranging regulations that mandate supply-chain risk management, algorithmic audits for automated decision systems, and secure-by-design disciplines.

Trend #3: The Rise of AI Regulations

Governments are introducing new legislation to put guardrails in place for AI/ML development, focusing on new areas of risk.

The regulatory landscape is rapidly intensifying globally, demanding strict compliance in documentation and risk management.

- The EU AI Act requires providers and users of high-risk AI systems to follow strict risk assessments, transparency, and recordkeeping rules, with full implementation expected around August 2026.
- In the United States, Colorado and California are introducing their own AI regulations that focus on protecting consumers from bias, discrimination, and privacy risks, with stricter enforcement on documentation and risk management for AI-driven decision-making.

Core areas of focus include:

- **Algorithmic Discrimination:** Laws are being enacted to protect against bias and discrimination in AI systems used for consequential decisions (e.g., hiring and loan approvals).
- **Transparency and Explainability:** Developers must provide greater transparency into how their ML models work, the data they were trained on, and how they arrive at a decision.

Deepfake and Synthetic Media: New laws are emerging that regulate “deepfakes” and other forms of deceptive media generated by sophisticated AI.

Trend #4: Regulations Cover the Entire SDLC

New regulations require teams to put controls starting from the earliest stages of development.

For example, the EU's Cyber Resilience Act mandates a "secure-by-design" approach.

- **Shift-Left is Mandatory:** This means threat modeling and vulnerability management must be baked into the development process—it's now a mandate, not a suggestion.
- **Evidence is Critical:** Regulators and auditors now demand evidence for every step of the development pipeline, moving beyond mere documentation to require proof of action.
- **Compliance is Embedded:** Compliance must be designed into processes themselves, instead of being a layer applied at the end.

Trend #5: The Need for Automated Governance

The regulatory environment today is evolving rapidly, which means that manual compliance methods are now obsolete.

To keep pace, you must adopt an automated, proactive approach to GRC.

- **Automated Attestation:** SDLC tools must generate a machine-readable record of security, quality, and compliance checks with minimal manual intervention.
- **Continuous Compliance:** Regulations now mandate continuous, real-time monitoring and proactive reporting, ensuring compliance is an ongoing state of operational readiness, not a periodic audit.
- **Shift-Left Security:** Governance and security controls should be integrated directly into the software development lifecycle starting from the very first line of code.

The Regulatory Landscape in 2026

The regulatory landscape is vast and complex, representing a spectrum of obligations. This includes legally written laws (like the EU's DORA and AI Act), industry requirements (like PCI for payments), and crucial best practice frameworks (like SLSA). We've made it easier for you to navigate this landscape by evaluating the requirements of over 40 regulations and frameworks. To dive deeper into individual regulations, refer to the Appendix.

Global

Global standards are the foundation of modern cybersecurity and are often de facto standards or prerequisites for enterprise contracts.

- **Secure Development is Universal:** Global standards emphasize integrating security into the Software Development Lifecycle (SDLC). This includes secure coding, change management, security testing, and vulnerability management as mandatory practices.
- **Supply Chain Integrity is Key:** Frameworks like SLSA include controls explicitly designed to protect against supply chain attacks by verifying software provenance.

Compliance is a Non-Negotiable Cost: Failure to adhere to these standards results in severe fines, legal liability, or loss of market access.

Key Global Regulations, Standards and Frameworks

	Why It Matters	Key SDLC/Security Focus
SLSA	Provides a clear, verifiable way to demonstrate software integrity from source code to binary.	Automated Builds, Provenance Generation, Tamper Protection.
ISO/IEC 27001	The most widely adopted framework for information security worldwide.	Secure Development, Change Management, Supplier Security.
PCI-DSS	Mandatory for all organizations handling credit card data.	Secure Coding Practices, Vulnerability Management (SAST/DAST).
MISRA C:2025	Essential for safety-critical systems (e.g., automotive, aerospace) to enhance software reliability.	Static Analysis, Code Reviews, Documentation.

Regional

Every region has their own unique, fragmented approaches, which multiplies the compliance burden for organizations.

Europe: The Global Leader in Digital Law

The EU is creating a comprehensive legal framework for cybersecurity (CRA, NIS2) and AI (AI Act), moving beyond data privacy (GDPR).

- **Mandatory "Secure-by-Design":** The Cyber Resilience Act, Product Liability Directive, and AI Act all mandate that companies embed security into the SDLC from the start.
- **Accountability on Manufacturers:** EU regulations shift the burden of proof to manufacturers to demonstrate their products are secure.
- **SBOMs are a Legal Prerequisite:** The CRA and NIS2 explicitly require companies to address supply chain risks, with SBOMs being a key tool for transparency.

Key Europe Regulations

	Focus Area	Impact on Development Lifecycle
EU AI Act	Provides a clear, verifiable way to demonstrate software integrity from source code to binary.	Automated Builds, Provenance Generation, Tamper Protection.
Cyber Resilience Act (CRA)	The most widely adopted framework for information security worldwide.	Secure Development, Change Management, Supplier Security.
DORA	Mandatory for all organizations handling credit card data.	Secure Coding Practices, Vulnerability Management (SAST/DAST).
BSI TR-03183	Essential for safety-critical systems (e.g., automotive, aerospace) to enhance software reliability.	Static Analysis, Code Reviews, Documentation.
GDPR	Data privacy for EU citizens.	Privacy-by-Design, Encryption, and Data Subject Rights (Access, Delete).

North America: A Fragmented Environment

The U.S. landscape consists of a growing patchwork of state-level laws (like CCPA and MODPA) and targeted federal mandates.

- **National Security Dictates Policy:** Regulations like the DOJ Final Rule on Bulk Data Transfers and California's TFAIA (SB53) place legal burdens on how sensitive data and powerful AI models are handled.
- **Incident Reporting is Mandatory:** The upcoming CIRCIA regulation will require critical infrastructure companies to report cyber incidents and ransomware payments to CISA within tight deadlines.

Key North America Regulations

	Focus Area	Impact on Development Lifecycle
TFAIA (SB53)	Safety and transparency for powerful AI "frontier models" (California).	Formal Risk Assessments, Secure Model Development, Incident Response Planning.
CCPA	Privacy rights for California residents.	Systems must allow consumers to easily exercise the Right to Know, Delete, and Opt-Out.
DOJ Final Rule on Bulk Data Transfers	Prevents the transfer of Americans' sensitive data to countries of concern.	Data Flow Auditing, Cross-Border Access Controls, Restricted APIs.
Executive Order 14028 and 14144	Software supply chain integrity and secure delivery.	Secure Software Development Framework (SSDF) practices become mandatory, requiring security attestations and SBOM for government-sold software.

Asia: Balancing Privacy and Innovation

Asia’s landscape is fragmented, balancing strict "hard law" (China) with voluntary "soft law" (Japan, Singapore).

- **Privacy is Foundational:** Regulations like PIPA (South Korea) and APPI (Japan) mandate "privacy-by-design" principles and security controls to protect personal information.
- **AI/ML Transparency:** China’s Final AI Content Labeling Rules mandate transparency and traceability for generative AI output.
- **Mandated Security Controls:** Frameworks like the Australian Cyber Security Centre's (ACSC) Essential Eight mitigation strategies mandate specific, foundational software security controls that organizations must implement to protect against cyber threats.

Industry-Specific Mandates and Security Frameworks

For high-risk sectors or those dealing with the U.S. government, compliance is a prerequisite for doing business.

- **Mandatory Secure SDLCs:** For U.S. government contractors, compliance with frameworks like DFARS and the Federal Software Security Mandate (aligned with NIST SSDF) is a contractual requirement.
- **Operational Integrity:** Regulations like DORA (Finance) and HIPAA (Healthcare) mandate embedding cybersecurity controls to ensure operational resilience and protect sensitive data.
- **Frameworks are Strategic Tools:** Voluntary guides like NIST CSF and NIST AI RMF provide the practical, risk-based approaches necessary to meet the requirements of legally binding regulations.

Key Industry Regulations and Frameworks

	Focus Area	Impact on Development Lifecycle
Federal Software Security Mandate	Public Sector (U.S.A)	Alignment with NIST SSDF practices, including Threat Modeling and SBOMs.
HIPAA	Healthcare (U.S.A.)	Strong Access Controls, Encryption, and detailed Audit Controls for ePHI.
DFARS	Defense (U.S.A.)	Implementation of NIST SP 800-171 controls (Access Control, Incident Response).
NIST SSDF	All (De Facto Standard)	Integrate security throughout the entire SDLC, from organization preparation to vulnerability response.
NIST AI RMF	AI/ML Development (U.S.A.)	Govern, Map, Measure, and Manage risks like algorithmic bias and security vulnerabilities.
FINOS AI Governa nce Framework	AI Financial Sector	Governs risks and mitigations for onboarding, developing, and running Generative AI solutions.

How to Tackle the Regulatory Environment

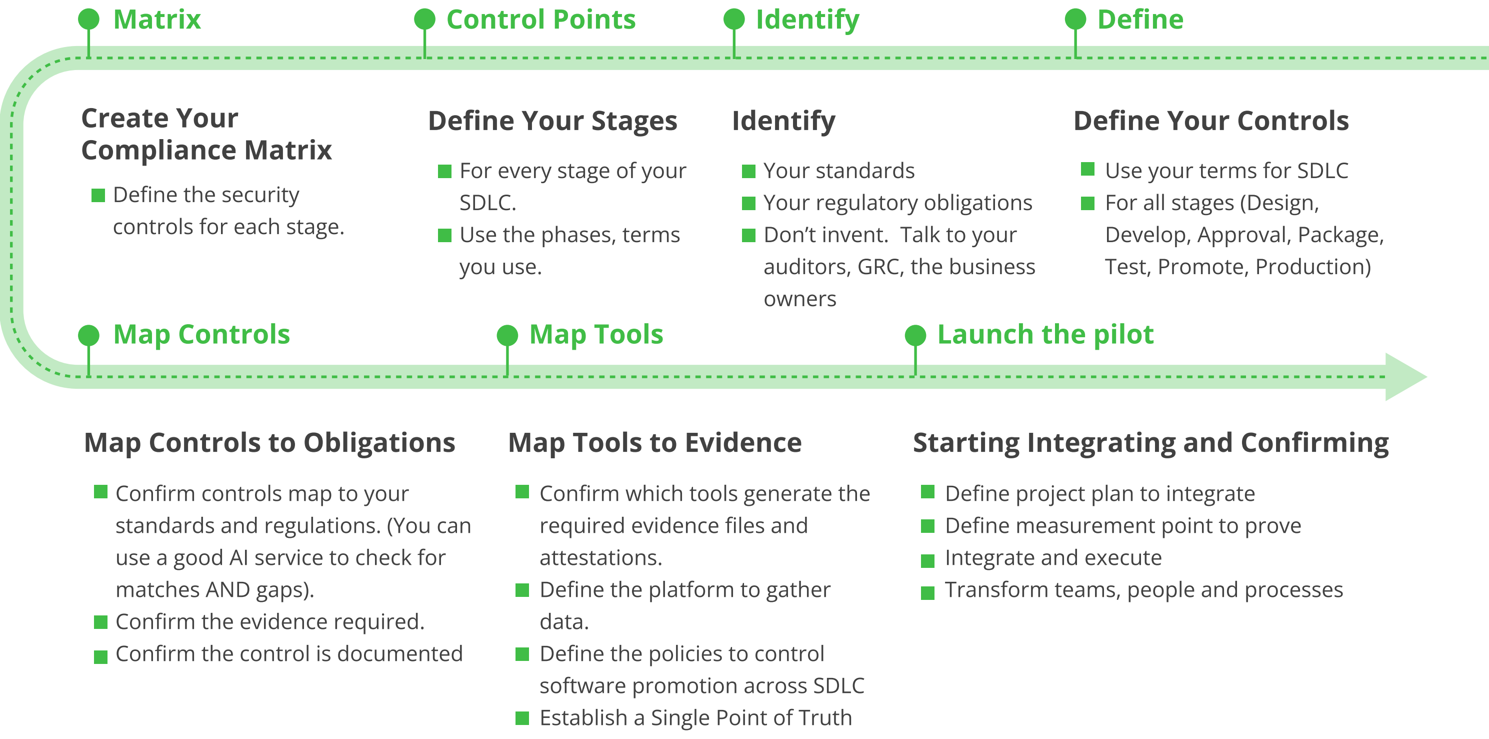
Regulators now demand greater context across the entire SDLC. Building GRC workflows into the SDLC from the very beginning is a strategic imperative, not just a checkbox.

To help organizations master this new regulatory landscape, here is a step-by-step guide to building a robust, proactive compliance program, broken down into three areas of focus:

- Part 1: Design Your Software Compliance Program
- Part 2: Build Automation and Controls Across the SDLC
- Part 3: Deliver Your Software Compliance Program

> Successful governance relies on the unified integration of people, process, and monitoring—not just technology. Without ensuring comprehension and data democratization across all teams, these programs will fail to deliver the desired results: compliance, reduced risk, and higher performance.

Part 1: Design Your Software Compliance Program



Create Your Compliance Matrix

- Define the security controls for each stage.

Define Your Stages

- For every stage of your SDLC.
- Use the phases, terms you use.

Identify

- Your standards
- Your regulatory obligations
- Don't invent. Talk to your auditors, GRC, the business owners

Define Your Controls

- Use your terms for SDLC
- For all stages (Design, Develop, Approval, Package, Test, Promote, Production)

Map Controls to Obligations

- Confirm controls map to your standards and regulations. (You can use a good AI service to check for matches AND gaps).
- Confirm the evidence required.
- Confirm the control is documented

Map Tools to Evidence

- Confirm which tools generate the required evidence files and attestations.
- Define the platform to gather data.
- Define the policies to control software promotion across SDLC
- Establish a Single Point of Truth

Starting Integrating and Confirming

- Define project plan to integrate
- Define measurement point to prove
- Integrate and execute
- Transform teams, people and processes

The first step is to design how your new governance program will integrate with your existing Software Development Lifecycle (SDLC). You need to define your obligations, map them to internal disciplines, and identify the necessary tools, people, and processes.

Step 1: Build the Foundation

01.

Define Your Application Control Stages

Identify the stages of your SDLC that will require controls (e.g., Design, Test, Certify, Promote, Production).

02.

Identify Your Standards and Regulatory Obligations

Consult with your GRC and legal departments to identify all relevant standards and regulations that apply to your business. You can also leverage this guide as a starting point.

03.

Define Control Points

For each SDLC stage, normalize the security and compliance requirements from legal, business, and DevOps teams into a commonly accepted set of security context definitions. These become your expected controls across the SDLC.

Step 2: Create a Compliance Matrix

The Compliance Matrix is an essential tool designed to cut through the complexity of regulatory overlap. It maps the security controls within your SDLC to the specific requirements of any relevant regulation or framework, helping prevent audit failure and saving time.

See Compliance Matrix examples below:

Discipline	Tasks	DORA	SLSA	EO-14028	NIST800 -218	NIST SP 800-160
Governance, Risk, and Secure SDLC						
Establish a Secure SDLC Policy	Define and maintain secure software policies, integrating risk management and security engineering throughout all phases	⊗	⊗	⊗	⊗	
Systems Security Engineering	Apply systems security engineering principles to ensure trustworthiness, resilience, and survivability of software and systems					⊗
Cyber Resiliency Engineering	Architect and design software to anticipate, withstand, recover from, and adapt to adverse cyber conditions				⊗	
Continuous Risk Assessment	Identify, assess, and mitigate risks at every SDLC stage, including supply chain and third-party risks	⊗		⊗	⊗	
Secure Coding, Vulnerability Management, and Testing						
Secure Coding Practices	Enforce secure coding standards and integrate them into development processes	⊗	⊗	⊗	⊗	
Automated Security Testing	Use automated tools (SAST, DAST, SCA) and manual reviews to identify and remediate vulnerabilities		⊗	⊗	⊗	
Continuous Security Verification	Integrate security checks into CI/CD pipelines for ongoing assurance		⊗	⊗	⊗	
Penetration Testing and Resilience Exercises	Regularly conduct penetration tests and resilience assessments	⊗		⊗		⊗

Example Compliance Matrix

SDLC Phase	Control Point	GDPR (Data Privacy)	AI Act (AI Governance)	CRA (Cyber Resilience)	SDLC NIS2 Directive (Risk Management)
Design	Privacy By Design	✓			
	Data Minimization	✓		✓	✓
	Secure Architecture		✓	✓	✓
	Risk Assessment	✓	✓	✓	✓
Develop	Secure Coding			✓	✓
	Vulnerability Scanning			✓	✓
	Consent Mechanism	✓			
Test	Bias/Fairness Testing		✓		
	Penetration Testing			✓	✓
	Data Subject Rights	✓			
Deploy	Change Management			✓	✓
	Incident Response Plan	✓	✓	✓	✓
Production	Data Detection	✓			
	Vulnerability Management		✓	✓	✓
	AI Content Labeling		✓		
	Logging & Auditing	✓		✓	✓

Example Compliance Matrix

Here's how to get started building your Compliance Matrix:

01. Map SDLC Stages to Security Controls

List all security control points against the corresponding stages of your SDLC.

02. Add Regulatory Standards (Horizontal Axis)

Add your relevant external regulations (e.g., GDPR, SOC 2, ISO 27001) as new columns across the top.

03. Define the Expected Activities and Results

Define the specific activities and the required results for each control point to establish a holistic view for all stakeholders.

04. Confirm Coverage and Identify Gaps (The Mapping)

This core process confirms that your security controls provide the necessary coverage for your standards and regulatory obligations. This helps you both identify common requirements you already meet and pinpoint gaps where controls are missing.

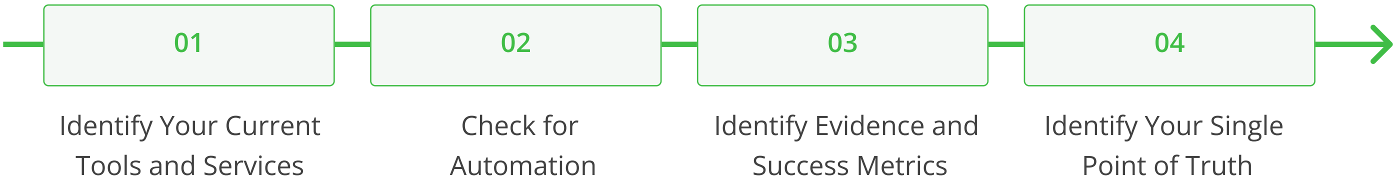
> Leverage Generative AI mindfully. Use a trusted GenAI service to quickly map controls to complex regulatory text. This saves significant time on initial cross-referencing. However, always validate every requirement against the official text. Ask the AI specific questions, such as: "Where are the gaps in my security controls that do not meet the needs of regulation X?" A blend of AI efficiency and human expertise is key.

05. Document and Link Processes (Audit Trail)

For every control point, document the detailed processes and procedures in place. The final deliverable for this step should be a URL for each control point that links to the document detailing the process, expected results, evidence files, and the supporting SBOM data.

Part 2: Build Automation and Controls Across Your SDLC

Now that your compliance program is designed, you need the right tools and controls to execute it. Focus on automating processes to accelerate your time from feature to production while reducing the burden of human error.


01
Identify Your Current Tools and Services
02
Check for Automation
03
Identify Evidence and Success Metrics
04
Identify Your Single Point of Truth

01.

Identify Your Current Tools and Services

Document all existing tools and processes (e.g., Change controls often use ServiceNow). Look for opportunities to integrate these workflow processes into your SDLC pipeline to create audit trails and exportable results.

02.

Check for Automation

Confirm which tools can fulfill your requirements while reducing the burden of compliance. Determine whether they can be triggered and if results can be exported in a machine-readable format (e.g., JSON).

03.

Identify Evidence and Success Metrics

For each control, define what "success" looks like and identify the specific evidence files and metrics needed to prove your program works. This evidence is crucial for internal and external audits.

04.

Identify Your Single Point of Truth

A critical success factor is establishing a single data store where all releases are tracked and all evidence files are uploaded. This centralized store provides verifiable proof that the required steps were followed to deliver a compliant release.

The Pillars of Automated Governance

Effective GRC requires a technological foundation built on three interconnected pillars. Your tooling must work in harmony, feeding verifiable outputs into a central system that enforces policy and generates immutable evidence for auditors.

Pillar	Description	Compliance Function
Single Source of Truth	Consolidate all artifacts and security metadata into one verifiable location. Multiple data sources create fragmentation, increase audit risk, and prevent reliable integrity checks.	Integrity
Single Chain of Traceability	Establish end-to-end visibility into all development actions. This chain of custody proves the provenance of every artifact.	Provenance
Single Points of Control	Centrally govern the application flow. This enables the organization to enforce security policies and automatically halt a release if it violates regulatory requirements. In some cases, it might not be possible to have a single point of control, but always try to limit it if possible.	Enforcement

Building Compliance into Your Pipelines with JFrog

JFrog provides the solutions at each step of your compliance journey, transforming a manual burden into a predictable, automated process.

Step 1: Centralize and Control Your Artifacts

First, establish a secure, centralized repository for all software binaries and components. This Single Source of Truth is crucial for traceability and a verifiable audit trail.

- **JFrog Artifactory** serves as this central hub. It provides an immutable record of every software artifact, ensuring you know exactly what is in your software and where it came from.
- **JFrog AI Catalog** serves as the unified AI system of record for all model types (open source, custom, and externally hosted models).
- **JFrog Curation** helps you manage how new packages enter your organization, shifting security left to keep malicious and non-compliant packages from ever entering your

Step 2: Automate Security and Compliance Scanning

Manual checks are too slow and error-prone for modern development. Automate security and compliance scans at every stage of your pipeline.

- **JFrog Xray** provides continuous Software Composition Analysis (SCA) on all components stored in Artifactory. It automatically identifies vulnerabilities, enforces compliance with license policies, and generates SBOMs.
- **JFrog Advanced Security** provides contextual analysis, Static Application Security Testing (SAST), and Secrets Detection. These capabilities drive a Secure-by-Design approach mandated by new regulations.

Step 3: Collect Tamper-Proof Evidence

To prove compliance, you need a verifiable record—a "digital paper trail"—that shows you followed all necessary checks and balances (Single Chain of Traceability).

- JFrog Evidence Collection automates evidence collection across the SDLC from vendors such as ServiceNow, GitHub, and Sonar. It captures relevant SDLC actions, from security scans to code reviews, to generate a tamper-proof record of a release.
- You can use this evidence to present verified conformance to regulations to an auditor.

Step 4: Automatically Enforce Policies and Governance

Policies are most effective when automation enforces them. A proactive GRC strategy ensures your applications always align with requirements with minimal human intervention (Single Point of Control).

- JFrog AppTrust allows you to set up evidence-based policies. For example, a policy can halt a release if it contains a critical vulnerability or if a mandatory security scan was not completed.
- JFrog Smart Retention allows you to set policies to archive, retain, or delete data to meet specific data deletion or data archival requirements.

Part 3: Deliver Your Software Compliance Program

Now that you have identified and prioritized which regulations matter to your business, and what controls and tools you need, it's time to execute. We recommend that you develop a project plan with multiple success milestones with sufficient time between them to allow all parties to measure success and adjust.

- In your plan, be sure to include not only the technical implementation steps, but also the enablement of every team involved; this includes the developer community, security teams, audit, compliance, and risk committees, and the business owners.
- Stakeholders should be able to easily see how your compliance program drives progress and delivers dual benefits: effective risk management and enabled agility.

Note how we called this a Program, not a Project. A program requires continuous upkeep, so plan to regularly review how your particular regulatory obligations have changed (multiple times per year is a good goal). While some requirements might be reduced, you will typically need to account for additional updates from existing bodies or entirely new regulatory obligations.

Automating Governance with DevGovOps

To thrive in the era of increasing regulations, you need a proactive approach that embeds governance, risk, and compliance directly into your software development lifecycle. You must move beyond manual processes and embrace automation, traceability, and a single source of truth for all your software artifacts.

The practice of DevGovOps provides the necessary capabilities to meet these new compliance demands and ensure your software is resilient, secure, and compliant from the start.

By leveraging DevGovOps solutions like JFrog AppTrust, you build GRC into your development workflows, transforming compliance from a burden to a predictable, automated process.

The Impact of AI on GRC Programs: The use of AI in GRC programs is rapidly maturing, offering solutions that significantly enhance program monitoring. These tools provide leaders, executives, and risk managers with powerful dashboards and great insight into compliance status. However, the current landscape focuses primarily on business-level concerns. Few solutions address the unique data points and enforcement gates required for software development, which remains a critical, underserved area.

Closing Thoughts

The AI revolution is changing everything we once knew about software development, including the global regulatory environment. Every business must evolve its GRC strategy as regulators increasingly demand transparency, accountability, and proof for every SDLC action.

The future of software regulations isn't about checking a box; it's about building trust. Businesses that embrace this new reality by embedding security, compliance, and governance directly into their development pipelines will not only protect themselves from fines and legal challenges, but will also build better, more resilient software.

By leveraging automation, best-of-breed tools, and modern techniques such as DevGovOps, companies can transform regulatory compliance from a burden into a competitive advantage, ensuring their software—and their business—thrives in this new era of regulations.

Legal Disclaimer:
The information is provided for general informational and educational purposes only and is not a substitute for professional advice. Accordingly, before taking any actions based upon such information, we encourage you to consult with the appropriate professionals.

Appendix: Key Software Regulations and Frameworks in 2026

Note: All regulations are subject to change. For the latest information,

Global

This category represents regulations and standards that are truly global in scope. They are created by international bodies or are universally recognized regardless of a company's location or the market it serves.

ISO/IEC 27001

Information Security Framework

Official Site
Link

Geography
Global

Type
Cybersecurity Framework

Industry
All

Year in Effect
2005

Overview: ISO/IEC 27001 is a globally recognized standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure.

Why It Matters: It's the most widely adopted framework for information security worldwide. Achieving ISO 27001 certification demonstrates a commitment to security, builds trust with customers and partners, and is often a prerequisite for doing business, particularly in enterprise and government sectors. It provides a formal, auditable way to manage risk.

Key SDLC Requirements: ISO 27001's requirements are not an SDLC themselves but directly influence a secure SDLC. They mandate that a company's ISMS includes controls for:

- **Secure Development:** Implementing secure coding standards and practices.
- **Change Management:** Controlling and documenting all changes to systems and software.
- **Testing:** Incorporating security testing into the development lifecycle, such as vulnerability scanning and penetration testing
- **Supplier Security:** Ensuring that third-party software and components meet the organization's security standards.

MISRA C:2025

Compliance Standard

Official Site
Link

Geography
Global

Type
Cybersecurity Framework

Industry
All

Year in Effect
2025

Notes
Applies to any organization using embedded C programming for safety or security critical applications, including aerospace, automotive, and defense.

Overview: MISRA C:2025 is a set of coding guidelines for the C programming language that aims to enhance the safety, security, and reliability of software. It's a de facto industry standard widely adopted in safety-critical systems.

Why It Matters: Compliance with MISRA C is essential for industries where software failure could lead to severe consequences, such as injury or death. It helps developers avoid risky programming constructs that could lead to undefined behavior, vulnerabilities, or system crashes. It is often a contractual requirement for suppliers in the automotive, aerospace, and medical device industries.

Key SDLC Requirement: MISRA C is a coding standard, but it is deeply integrated into a secure development process. The key SDLC requirements are centered on coding practices and verification:

- **Static Analysis:** Heavy use of automated static analysis tools to check for rule violations.
- **Code Reviews:** Manual code reviews are still necessary for rules that cannot be fully automated.

Documentation: Maintaining a formal compliance matrix to document which rules are followed and to justify any deviations.

PCI-DSS

Payment Card Industry Data Security Standard

Official Site
Link

Geography
Global

Type
Cybersecurity Framework

Industry
All

Year in Effect
2004

Notes
Applies to any organization handling credit card transactions

Overview: The Payment Card Industry Data Security Standard (PCI-DSS) is a global security standard for any organization that accepts, processes, stores, or transmits credit card information. It was established by the major payment card brands to reduce card fraud.

Why It Matters: Compliance is mandatory for all merchants and service providers that handle cardholder data. Failure to comply can lead to severe fines from payment brands, loss of the ability to process payments, and civil litigation from customers in the event of a breach. It is a non-negotiable cost of doing business for most e-commerce and retail companies.

Key SDLC Requirement: PCI-DSS has specific requirements for the security of applications that handle cardholder data. They are outlined in requirement 6 of the standard, and include:

- **Secure Coding:** Ensuring all applications are developed with secure coding practices and are free from common vulnerabilities.
- **Vulnerability Management:** Regularly testing applications for security vulnerabilities (e.g., using SAST and DAST).
- **Change Control:** All changes to applications that handle cardholder data must be formally documented, tested, and approved.
- **Documentation:** Maintaining a list of all application components that handle cardholder data.

SLSA

Payment Card Industry Data Security Standard

Official Site
Link

Geography
Global

Type
Cybersecurity Framework

Industry
All

Year in Effect
2021

Overview: SLSA (Supply-chain Levels for Software Artifacts) is a security framework for the software supply chain. It's a key initiative developed by Google and now stewarded by the Open Source Security Foundation (OpenSSF). Its main goal is to protect against supply chain attacks by providing a series of incremental levels for improving the integrity and security of software artifacts.

The framework's latest update, v1.2 RC1, introduces a new Source Track to complement the existing Build Track. This expansion signifies a move toward more comprehensive coverage of the entire software supply chain.

Why It Matters: SLSA provides a clear, verifiable way to demonstrate the integrity of your software from source code to binary. As supply chain attacks become more common, SLSA is a critical tool for building trust with customers and partners. It's increasingly referenced in U.S. government mandates and is becoming a de-facto standard for software procurement.

Key SDLC Requirement: SLSA is deeply integrated with the SDLC, particularly the build and distribution stages. It requires a fundamental shift in how software is created and verified. The framework's key requirements are split into two main tracks:

- **Build Track:** This track focuses on the integrity of the build process and the artifact's provenance. Key requirements include automated builds, provenance generation, and tamper protection through cryptographically signed attestations.
- **Source Track:** The newly introduced Source Track provides more rigorous requirements for managing and securing the source code itself. This helps to secure the provenance and integrity of the code throughout the entire supply chain.

Together, these tracks mandate a fundamental shift in how organizations protect software from source to binary.

Regional

These are legally binding regulations that originate from and primarily apply to a specific country, region, or state.

North America

CCPA

California Consumer Privacy Act

Official Site
Link

Geography
U.S.A (California)

Type
Data Privacy Regulation

Industry
Applicable to All

Year in Effect
2020

Other Notes
A company must comply if it is a for-profit business in California that annually exceeds $25 million in revenue, or handles the personal information of 100,000 or more consumers, or earns over half its revenue from selling consumer data.

Overview: The CCPA gives California residents specific rights over their personal information that businesses collect. It requires companies to be transparent about their data practices and provides consumers with the ability to control their data.

Why It Matters: The CCPA affects any for-profit business that handles California residents' data and meets certain revenue or data processing thresholds. Non-compliance can lead to statutory damages for consumers and significant penalties from the California Privacy Protection Agency (CPPA).

Key SDLC Requirements: You must build your software and business processes to include:

- **The Right to Know:** You must allow consumers to ask you to disclose the personal information you collect about them.
- **The Right to Delete:** Consumers can request that you delete their personal information, with some exceptions.
- **The Right to Opt-Out:** You must provide a clear mechanism for consumers to opt out of the sale or sharing of their personal information.
- **Reasonable Security:** You must implement and maintain reasonable security procedures to protect personal data from a breach.

COPPA

Children’s Online Privacy Protection Act

Official Site
Link

Geography
U.S.A

Type
Data Privacy Regulation

Industry
All

Year in Effect
2000

Overview: The Children's Online Privacy Protection Act (COPPA) is a U.S. federal law that gives parents control over what information websites and online services can collect from children under 13.

Why It Matters: COPPA affects any operator of a commercial website or online service, including mobile apps and IoT devices, that is directed to children under 13 or knowingly collects personal information from them. Non-compliance can result in civil penalties of up to $50,120 per violation.

Key SDLC Requirements: You must build your systems to:

- **Obtain Verifiable Parental Consent:** You must get a parent or guardian's verifiable consent before collecting, using, or disclosing a child's personal information.
- **Provide Clear Notice:** You must post a clear, comprehensive, and easy-to-read privacy policy that explains your data collection practices.
- **Limit Data Collection:** You must not condition a child's participation in an online activity on the child providing more information than is reasonably necessary.
- **Ensure Security:** You must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's data.

CIRCIA

Cyber Incident Reporting for Critical Infrastructure Act

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2026 (Expected)

Other Notes
Applies to any industry deemed as “critical infrastructure”.

Overview: The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is a U.S. law requiring critical infrastructure companies to report significant cyber incidents to CISA within 72 hours and ransomware payments within 24 hours.

Why It Matters: CIRCIA shifts U.S. cybersecurity from voluntary reporting to a mandatory legal obligation. It forces companies to have a robust, rapid incident response capability, holding organizations accountable for security failures.

Key SDLC Requirements: CIRCIA is focused on incident response and reporting (requiring organizations to report cyber incidents and ransomware payments). There are no specific SDLC requirements mandated by law, but a secure SDLC is a best practice that will help organizations align with the law.

DMCA

Digital Millenium Copyright Act

Official Site
Link

Geography
U.S.A

Type
Intellectual Property Protection Regulation

Industry
All

Year in Effect
1998

Overview: The DMCA is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. It also provides a "safe harbor" for online service providers who host user-generated content, protecting them from copyright infringement liability if they follow specific takedown procedures.

Why It Matters: The DMCA is a foundational law for online content platforms, social media networks, and any service that hosts user-generated content in the U.S. It matters because it protects these companies from liability, provided they have a compliant process for handling copyright infringement complaints. Without the DMCA's safe harbor provisions, many online platforms could not exist in their current form.

Key SDLC Requirements: The DMCA does not prescribe a specific SDLC, but it requires that a company's software and systems be capable of complying with its takedown and counter-notice procedures. This includes:

- **Takedown Process:** The software must have a mechanism for receiving and acting upon copyright takedown notices in a timely manner.
- **Agent Registration:** The platform's software must clearly display the contact information for a registered DMCA agent.
- **Notification Systems:** The software must be able to notify users whose content has been removed and provide them with an avenue to file a counter-notice.

DOJ Final Rule on Bulk Data Transfers

Official Site
Link

Geography
U.S.A

Type
Intellectual Property Protection Regulation

Industry
All

Year in Effect
2025

Overview: This is a U.S. federal regulation designed to prevent countries of concern from accessing and exploiting Americans' sensitive personal data and government-related data. It prohibits or restricts certain data transactions that involve the transfer of "bulk U.S. sensitive personal data."

Why It Matters: The DOJ Final Rule on Bulk Data Transfer is a critical national security regulation that places a new legal burden on companies that transfer large amounts of sensitive data. It requires a significant effort in due diligence and data security. Failure to comply can lead to severe civil and criminal penalties, and its scope affects any company that transfers data internationally, particularly in the tech, data, and telecommunications sectors.

Key SDLC Requirements: While the rule doesn't explicitly mandate SDLC requirements, there must be a few things in practice to comply:

- **Data Flow Auditing & Security Control:** Developers must implement robust auditing of data flows, add cross-border access controls, and keep detailed logs for software handling sensitive personal or government-related data.
- **Restricted Transactions:** Software and APIs must be engineered to block or strictly control bulk data transfers to countries of concern, requiring new technical safeguards at the application and infrastructure layers.
- **Vendor and Contractor Vetting:** Engineers need to integrate automated risk assessment tooling for third-party components and adhere to vetted supplier policies from within the codebase and DevOps workflows.
- **Compliance-Driven Architecture:** Security development processes must now include compliance checks for every upgrade or new release to meet DOJ and CISA baseline measures

Executive Order 14028

Official Site
Link

Geography
United States

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2021

Overview: Executive Order 14028, "Improving the Nation's Cybersecurity," is a U.S. executive order that directs federal agencies to modernize and implement stronger cybersecurity standards. It establishes new requirements for companies that sell software to the U.S. government, including a mandate for a **Software Bill of Materials (SBOM).**

Why It Matters: This order is a foundational document for modern U.S. cybersecurity policy. It officially establishes "security by design" as a key principle for the federal government and its supply chain. It's the primary driver behind the Federal Software Security Mandate and has set the stage for other regulations that require SBOMs and secure software development practices.

Key SDLC Requirements: The order explicitly requires a secure SDLC. Key SDLC requirements include:

- **Secure Design:** Implementing a "security by design" approach from the start of the development lifecycle.
- **Threat Modeling:** Conducting threat modeling and risk assessments during development.
- **Secure Code:** Using secure coding practices.
- **Vulnerability Management:** Having a robust process to identify, track, and remediate vulnerabilities.
- **SBOMs:** Providing a comprehensive SBOM for software sold to the government.

Executive Order 14144

Official Site
Link

Geography
United States

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2025

Overview: Executive Order 14144 was signed by President Biden on January 16, 2025, to build on EO 14028. Its goal was to strengthen the nation's cybersecurity by imposing more stringent requirements on federal software vendors and cloud providers. It mandated enhancements to the secure software attestation process, promoted the use of AI for cyber defense, and pushed for the adoption of phishing-resistant digital identities. However, a more recent Executive Order from the Trump Administration on June 6, 2025, has significantly changed its provisions. This new order did not rescind EO 14144, but it eliminated or amended key parts.

Why It Matters: EO 14144 mattered because it aimed to formalize and centralize the process of securing the federal software supply chain, a critical weakness exposed in previous attacks. It introduced key mandates, such as requiring vendors to provide machine-readable attestations and allowing CISA to centrally verify them. While the June 2025 changes scale back some of EO 14144's more prescriptive requirements, the core foundation of a secure software supply chain, established in EO 14028, remains firmly in place.

Key SDLC Requirements: Based on the new administration's Executive Order, the SDLC requirements for federal contractors are less prescriptive than the previous framework. The focus has shifted away from burdensome, centralized reporting and back to a risk-based approach. The core pillars of a secure SDLC, aligned with the NIST Secure Software Development Framework (SSDF), remain:

- **Vulnerability Management:** A formal, documented process for identifying, assessing, and remediating vulnerabilities throughout the entire software lifecycle.
- **Secure Supply Chain:** The use of a Software Bill of Materials (SBOM) remains an essential tool for providing visibility and traceability into software components. While the specific requirement for a machine-readable format was removed, the need to have a defensible list of components remains critical.
- **Attestation:** The fundamental requirement for a company to self-attest to its secure development practices remains in place, although the method of attestation is less rigid than previously mandated.

MODPA

Maryland Online Data Privacy Act

Official Site
Link

Geography
U.S.A (Maryland)

Type
Data Privacy Regulation

Industry
All

Year in Effect
2025

Notes
The Act applies to a broader range of businesses than in other states and applies if a business processes the personal data of at least 35,000 Maryland consumers, or at least 10,000 Maryland consumers if it earns over 20% of its gross revenue from selling personal data.

Overview: The Maryland Online Data Privacy Act (MODPA) is a new data privacy law that gives consumers more control over their personal data. It prohibits a company from using a "dark pattern" to obtain consent and requires companies to obtain consent before selling or sharing sensitive personal data. It also gives consumers a right to know, access, correct, and delete their data.

Why It Matters: MODPA is one of the strictest data privacy laws in the U.S. to date. It is particularly notable for its ban on "dark patterns" and its broad definition of "sensitive data." It adds another layer of complexity to the already fragmented U.S. privacy landscape, requiring businesses to adapt their data handling practices.

Key SDLC Requirements: MODPA's requirements impact the SDLC by demanding that a company’s software be designed to comply with data privacy principles. This includes:

- **Consent Mechanisms:** The software must be designed with clear and non-deceptive consent mechanisms.
- **Data Subject Rights:** Systems must be capable of fulfilling consumer requests to know, access, correct, and delete their data.
- **Data Inventory:** A company must maintain a comprehensive data inventory that identifies what data is collected and how it is used.
- **Data Minimization:** Software and systems should be designed to minimize the collection of personal data.

SOX

Sarbanes-Oxley Act

Official Site
Link

Geography
U.S.A

Type
Data Integrity Regulation

Industry
All

Year in Effect
2002

Notes
Applies to publicly traded companies

Overview: SOX (Sarbanes-Oxley Act) is a U.S. federal law enacted to protect investors by improving the accuracy of financial reporting in corporations. While a financial regulation, it mandates strict IT General Controls to ensure the integrity, security, and accuracy of financial data managed by software systems.

Why It Matters: SOX is a foundational law for all publicly traded companies in the U.S., holding CEOs and CFOs personally liable for the accuracy of their financial reports. Failure to comply can result in severe fines, de-listing from stock exchanges, and even criminal penalties, making it an essential part of corporate governance and risk management.

Key SDLC Requirements: SOX doesn't mandate a specific Software Development Life Cycle (SDLC) but requires that the process for developing and managing financial applications is controlled and auditable. Key requirements include:

- **Change Management:** A formal, documented process for managing all software changes.
- **Segregation of Duties:** Separating developer, tester, and operational roles to prevent fraud.
- **Audit Trails:** Maintaining immutable logs of all activities related to financial systems.

TFAIA (SB53)

Transparency in Frontier Artificial Intelligence Act

Official Site
Link

Geography
U.S.A (California)

Type
AI/ML Development Regulation

Industry
All

Year in Effect
2026 (Expected)

Overview: California's Senate Bill 53 (SB 53), known as the Transparency in Frontier Artificial Intelligence Act (TFAIA), is a landmark state law that imposes safety and transparency requirements on the most powerful AI systems, or "frontier models." Effective January 1, 2026, it requires developers to publish a framework for mitigating catastrophic risks and to report critical safety incidents to the state.

Why It Matters: SB 53 is significant because it is a legally binding regulation that addresses the risks of powerful AI. It mandates a "trust, but verify" model, forcing developers to disclose safety protocols and report incidents to the government. This law is pivotal for:

- Targeted Scope: It focuses on large AI models, avoiding over-regulation of smaller developers.
- Whistleblower Protection: It legally protects employees who report safety concerns, promoting internal accountability.
- Global Precedent: It's the first U.S. state law of its kind, setting a precedent that could influence future federal and international regulations.

Key SDLC Requirements: SB 53 doesn't mandate a specific SDLC, but its requirements necessitate new processes in a developer's workflow. To comply, a company's SDLC must include:

- **Formal Risk Assessments:** A dedicated step to evaluate catastrophic risks before deployment.
- **Secure Model Development:** Strong cybersecurity to protect unreleased model weights from unauthorized access.
- **Incident Response Planning:** A clear and rapid plan to detect and report "critical safety incidents" within tight deadlines.

Europe

BSI TR-03183

Official Site
Link

Geography
Germany

Type
Cybersecurity Framework

Industry
All

Year in Effect
2023

Notes
Applies to any industry that manufactures or sells with digital elements

Overview: BSI TR-03183 is a German technical guideline that serves as a practical roadmap for manufacturers to implement the cybersecurity requirements of the EU Cyber Resilience Act (CRA).

Why It Matters: Following this guideline is the most authoritative way to demonstrate due diligence and conformity with the CRA, helping manufacturers avoid severe financial penalties and loss of market access in the EU.

Key SDLC Requirements: The guideline heavily influences the SDLC by providing concrete technical requirements, including:

- **Security-by-Design:** Integrating security into every stage of a product's lifecycle.
- **Software Bill of Materials (SBOM):** Formal requirements for creating a detailed SBOM.
- **Vulnerability Management:** A system for identifying, assessing, and remediating vulnerabilities.

CRA

Cyber Resilience Act

Official Site
Link

Geography
European Union (EU)

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2024

Notes
Obligations will be phased over time. The law’s general obligations become mandatory on December 11, 2027.

Overview: The CRA is a landmark EU regulation that imposes mandatory cybersecurity requirements on all products with digital elements sold in the EU, from IoT devices to software. It aims to ensure a higher level of cybersecurity throughout a product's entire lifecycle and to hold manufacturers accountable for their security posture.

Why It Matters: The CRA is a game-changer. It's the first regulation of its kind to explicitly mandate "security by design" for a wide range of products. It shifts the burden of proof to manufacturers to demonstrate that their products are secure. Non-compliance can result in substantial fines and products being banned from the EU market.

Key SDLC Requirements: The CRA requires cybersecurity to be embedded into the SDLC. Key requirements include:

- **Risk Assessments:** Conducting a cybersecurity risk assessment for the product.
- **Vulnerability Management:** Establishing a clear process for identifying, documenting, and remediating vulnerabilities throughout the product's entire lifecycle.
- **SBOMs:** Manufacturers are explicitly required to create and maintain a Software Bill of Materials.
- **Secure Updates:** Ensuring that products can receive and install timely and secure updates to address new vulnerabilities.

GDPR

General Data Protection Regulation

Official Site
Link

Geography
European Union (EU)

Type
Data Privacy Regulation

Industry
Applicable to All

Year in Effect
2018

Overview: The GDPR protects the privacy of EU citizens, applying to any organization that handles their personal data.

Why It Matters: Non-compliance brings severe penalties of up to €20 million or 4% of global annual turnover, whoever is higher. Violations also cause major reputational damage.

Key SDLC Requirements: The core principle to the GDPR is "Privacy by Design". You must build your software to include:

- **Data Subject Rights:** Your systems must allow users to easily access, correct, or erase their data.
- **Encryption:** You must protect data at rest and in transit.
- **Vulnerability Management:** You must secure your systems to prevent breaches.
- **Data Breach Management:** You must have a plan to report breaches within 72 hours.

The EU Artificial Intelligence Act

Official Site
Link

Geography
European Union (EU)

Type
AI/ML Development Regulation

Industry
All

Year in Effect
2024

Note
Requirements are being phased in over a multi-year period between 2025-2026.

Overview: The EU Artificial Intelligence Act (or EU AI Act) is the EU's landmark regulation creating a legal framework for artificial intelligence. It classifies AI systems into different risk levels and imposes stricter requirements on those deemed "high-risk," such as AI used in medical devices, law enforcement, or critical infrastructure. It prohibits certain AI uses outright, such as social scoring.

Why It Matters: This law is the world's first comprehensive legal framework for AI. It sets a global precedent for regulating AI systems and will have a significant impact on any company that develops or sells AI products into the EU market. The requirements for high-risk AI are designed to ensure safety, fundamental rights, and accountability.

Key SDLC Requirements: The AI Act requires a secure and responsible SDLC for high-risk AI systems. This includes:

- **Risk Management:** Establishing a robust quality management system and performing a risk assessment throughout the AI lifecycle.
- **Documentation:** Maintaining detailed technical documentation, including data governance practices and a full description of the AI model.
- **Testing:** Ensuring the system is rigorously tested and validated to prevent bias and ensure accuracy.
- **Transparency:** Providing clear instructions and information to users about the AI system's capabilities and limitations.

NIS2 Directive

Official Site
Link

Geography
European Union (EU)

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2024

Note
Applies to all essential and important entities, including those in energy, transport, finance, health, and digital infrastructure.

Overview: The NIS2 Directive is an EU law that strengthens cybersecurity requirements for a wide range of "essential" and "important" entities. It expands the scope of the original NIS Directive to cover more sectors and impose more stringent security measures.

Why It Matters: NIS2 is critical for any company in a designated sector that operates in the EU. It introduces a stronger framework for risk management, incident reporting, and supply chain security. It also harmonizes cybersecurity rules across the EU, making it easier for businesses to comply but also increasing the potential for penalties.

Key SDLC Requirements: NIS2 requirements for risk management and supply chain security directly affect the SDLC. Companies must:

- **Supply Chain Security:** Address cybersecurity risks within their supply chain, including in the software they use.
- **Vulnerability Management:** Implement a formal process for handling and disclosing vulnerabilities.
- **Change Management:** Ensure that changes to systems are managed securely and are auditable.
- **Risk Assessments:** Conduct a comprehensive risk assessment of their network and information systems.

PLD

Product Liability Directive

Official Site
Link

Geography
European Union (EU)

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2024

Note
While it entered into effect in December 2024, EU Member States have until December 9, 2026 to transpose the directive into their national laws.

Overview: The Product Liability Directive (PLD) is a new EU law that holds manufacturers, importers, and distributors strictly liable for damages caused by defective products, including software and AI systems. It creates a no-fault liability regime, meaning a manufacturer is liable even if they were not negligent.

Why It Matters: The PLD marks a paradigm shift in legal liability for software by lowering the burden of proof for claimants. It extends liability to the entire digital supply chain and for post-sale defects, such as those caused by insufficient security updates.

Key SDLC Requirements: The PLD doesn't mandate a specific SDLC, but it implicitly requires a secure-by-design approach. Key requirements include:

- **Secure-by-Design:** Integrating security to prevent defects.
- **Vulnerability Management:** A formal process for identifying and fixing vulnerabilities throughout the product's lifecycle.
- **Software Updates:** A clear mechanism to provide timely security updates.
- **Documentation:** Maintaining comprehensive records of security risk assessments.

Asia

APPI

Act on the Protection of Personal Information

Official Site
Link

Geography
Japan

Type
Data Privacy Regulation

Industry
All

Year in Effect
2005

Overview: APPI is Japan's comprehensive data privacy law. It regulates how businesses and organizations collect, use, and handle personal information. The law was amended in 2022 to give individuals new rights and to increase the penalties for non-compliance. It also strengthens the law's extraterritorial reach.

Why It Matters: APPI is the primary privacy regulation for any company doing business in Japan. The 2022 amendments made the law much stricter, increasing the risk of non-compliance for foreign and domestic companies alike. It is a foundational law for any company with a presence in Japan.

Key SDLC Requirements: APPI requires organizations to take "necessary and appropriate measures" to protect personal data. This includes:

- **Data Minimization:** Designing software to only collect the necessary personal data.
- **Data Integrity:** Ensuring that data is accurate and not subject to unauthorized alteration.
- **Security Controls:** Implementing robust security controls to prevent unauthorized access to personal information.
- **Auditing:** Maintaining records of how personal data is handled and providing those records to regulators upon request.

Final AI Content Labeling Rules

Official Site
Link

Geography
China

Type
AI/ML Development Regulation

Industry
All

Year in Effect
2025

Overview: China's Final AI Content Labeling Rules are a set of legally binding regulations requiring any provider of generative AI services to label their output. The rules, which went into effect on September 1, 2025, mandate a dual-labeling system: an explicit, visible marker for users (e.g., "AI-generated") and a hidden, implicit watermark embedded in the file's metadata for traceability.

Why It Matters: China's regulations are significant because they represent the world's first nationally enforced set of rules for mandatory AI content labeling. They aim to combat misinformation, fraud, and copyright infringement by ensuring transparency. The dual-labeling system is particularly important as it allows for both human recognition and machine-readable traceability, putting pressure on major tech companies to build a robust content authentication and verification system.

Key SDLC Requirements: The regulations do not prescribe a specific SDLC, but they necessitate that developers build labeling capabilities directly into their AI systems and content pipelines. Key requirements include:

- **Model Integration:** The AI model itself must be designed to generate output with the required metadata or watermarks.
- **Content Pipelines:** Companies must adjust their content management systems to ensure that explicit and implicit labels are not stripped during editing or distribution.
- **Traceability:** The SDLC must be able to securely embed information about the service provider and content ID into the metadata, creating a clear chain of custody.

The Information Technology Act, 2000

Official Site
Link

Geography
India

Type
Cybersecurity Regulation

Industry
All

Year in Effect
2000

Overview: This is India's primary law dealing with electronic commerce and information technology. It provides a legal framework for electronic transactions and addresses issues related to cybercrime and data privacy. It also has rules for handling sensitive personal data and information (SPDI).

Why It Matters: The IT Act is the cornerstone of India's legal framework for the digital economy. It provides a legal basis for contracts made over the internet and holds service providers accountable for data breaches and security failures. It is a foundational law for any company doing business in India.

Key SDLC Requirements: The act doesn't prescribe a specific SDLC, but it requires that companies handling sensitive data maintain "reasonable security practices and procedures." This means:

- **Security Controls:** Implementing formal security controls and standards (like ISO 27001).
- **Data Protection:** Ensuring that sensitive data is protected from unauthorized access or alteration.
- **Access Controls:** Implementing strong access controls to sensitive information.
- **Incident Response:** Having a clear process to respond to and report data breaches.

PIPA

Personal Information Protection Act

Official Site
Link

Geography
South Korea

Type
Data Privacy Regulation

Industry
All

Year in Effect
2011

Overview: PIPA is South Korea's main data privacy law. It governs the collection, use, and protection of personal information by all public and private entities. It gives individuals rights similar to those in the GDPR, such as the right to access and correct their personal information.

Why It Matters: PIPA is the primary privacy regulation for companies operating in South Korea. It imposes a significant compliance burden on both local and foreign companies and carries heavy fines for non-compliance. It's a key regulation for any company targeting the South Korean market.

Key SDLC Requirements: PIPA requires a privacy-by-design approach. Key SDLC requirements include:

- **Data Minimization:** Software should be designed to only collect and store the minimum amount of personal information necessary.
- **Access Controls:** Implementing strong access controls to personal data.
- **Data Security:** Ensuring that personal data is protected from unauthorized access, loss, or alteration.
- **Destruction of Data:** Having a process to securely destroy personal data when its purpose has been fulfilled.

Privacy Act 1988

Official Site
Link

Geography
Australia

Type
Data Privacy Regulation

Industry
All

Year in Effect
1989

Overview: The Privacy Act is Australia’s main privacy law. It governs how Australian government agencies and private sector organizations handle personal information. It includes the Australian Privacy Principles (APPs), which set out the standards for handling, using, and disclosing personal information.

Why It Matters: The Privacy Act is the foundational law for data privacy in Australia. It is a core compliance requirement for any company operating in the country. Recent amendments have given the government more power to impose stricter penalties for non-compliance.

Key SDLC Requirements: The Privacy Act requires a "privacy by design" approach. Key SDLC requirements include:

- **Privacy by Design:** Integrating privacy considerations into the design and development of software systems.
- **Data Minimization:** Only collecting data that is necessary for a specific purpose.
- **Data Integrity:** Ensuring that personal information is accurate and up to date.
- **Data Security:** Implementing robust security controls to protect personal data from unauthorized access or misuse.

Industry-Specific

ANSI X9.125

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Framework

Industry
Financial Services

Year in Effect
2024

Overview: ANSI X9.125 is a new standard for Cloud Management and Security developed specifically for the financial services industry. It provides minimum requirements for a financial institution's use of cloud computing, from the initial transition to ongoing management and a secure exit.

Why It Matters: Financial services is a heavily regulated industry. This standard provides a structured roadmap for banks and other institutions to adopt cloud technology in a way that is secure, auditable, and compliant with other regulations. It helps companies establish a clear approach to identifying and mitigating key risks in the cloud, making their services more marketable as secure and compliant.

Key SDLC Requirements: The standard focuses on cloud governance rather than a specific SDLC, but it influences it by requiring a secure approach to application development and deployment in the cloud. Key areas include:

- **Secure Architecture:** Building applications with security-by-design from the ground up.
- **Authentication and Authorization:** Robust access controls for users and services in cloud environments.
- **Auditability and Logging:** The ability to log and monitor all activities for security and compliance audits.

DFARS

Defense Federal Acquisition Regulation Supplement

Official Site
[Link]

Geography
U.S.A

Type
Data Privacy Regulation

Industry
Defense

Year in Effect
1984

Notes
DFARS was amended in 2017. Applies to all Department of Defense contractors and subcontractors.

Overview: DFARS (Defense Federal Acquisition Regulation Supplement) is a set of regulations that supplements the Federal Acquisition Regulation (FAR) specifically for the U.S. Department of Defense (DoD). Its main purpose is to govern the procurement process and ensure that defense contractors and their subcontractors protect sensitive defense information, known as Controlled Unclassified Information (CUI).

Why It Matters: DFARS is critical because it is a mandatory, contractual requirement for any company that wants to do business with the DoD, whether as a prime contractor or a subcontractor. It establishes a baseline of cybersecurity practices to protect the defense industrial base from cyber threats and espionage. Failure to comply can lead to severe consequences, including loss of contracts, fines, and debarment from future DoD work.

Key SDLC Requirements: DFARS mandates that companies implement the 110 security controls outlined in NIST Special Publication 800-171. This indirectly requires a secure SDLC that includes practices such as:

- **Access Controls:** Limiting access to CUI and development systems to authorized personnel.
- **Configuration Management:** Establishing secure baselines for software and systems.
- **Incident Response:** Having a formal plan for detecting, responding to, and reporting cyber incidents to the DoD within 72 hours.
- **System Monitoring:** Continuous monitoring of systems and networks for threats and vulnerabilities.
- **Supply Chain Management:** Ensuring that subcontractors also comply with the security requirements.

DORA

Digital Operational Resilience Act

Official Site
[Link]

Geography
European Union (EU)

Type
Cybersecurity Regulation

Industry
Financial Services

Year in Effect
2023

Overview: The Digital Operational Resilience Act (DORA) is an EU regulation that enhances the digital operational resilience of financial institutions. It ensures that financial entities can withstand, respond to, and recover from all types of technology-related disruptions and threats.

Why It Matters: DORA is a critical regulation for the financial sector and its technology partners because it creates a single set of rules for financial entities across the EU. This harmonized approach strengthens the sector's collective resilience against cyber threats. DORA also places a significant burden on third-party ICT service providers, making compliance a prerequisite for any technology company that wants to do business with EU financial institutions.

Key SDLC Requirements: DORA's requirements for operational resilience have a direct impact on the SDLC. The five core pillars of DORA translate into the following key SDLC practices:

- **Governance and Risk Management:** Integrate risk management into the SDLC to systematically identify and mitigate vulnerabilities.
- **Resilience Testing:** Embed security testing, including penetration testing and vulnerability assessments, into the development process.
- **Incident Reporting:** Ensure the SDLC includes robust logging and monitoring solutions to detect anomalies and comply with timely incident reporting obligations.
- **Third-Party Risk Management:** Enforce strict security certifications and compliance checks for all third-party entities, including outsourced development teams and software providers.
- **Information & Intelligence Sharing:** Foster a DevSecOps environment where teams can collaborate and share threat intelligence to build collective resilience.

FDA Cybersecurity in Medical Devices Guidance

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Regulation

Industry
Healthcare

Year in Effect
2022

Notes
Applies to medical device manufacturers.

Overview: The FDA Cybersecurity in Medical Devices Guidance is a set of regulations from the U.S. Food and Drug Administration (FDA) that mandates cybersecurity as a core component of medical device safety. It requires manufacturers to implement robust security controls throughout the entire product lifecycle, from design to post-market monitoring.

Why It Matters: This regulation is a pivotal shift because it makes cybersecurity a non-negotiable part of FDA approval, treating cyber risks as a direct threat to patient safety. The guidance is significant for three reasons:

- **Mandatory Compliance:** It's a required part of a premarket submission for a "cyber device."
- **Lifecycle Security:** It forces a "secure-by-design" approach with a plan for ongoing vulnerability management.
- **Supply Chain Transparency:** The guidance explicitly requires a Software Bill of Materials (SBOM), which is crucial for managing third-party risks.

Key SDLC Requirements: The guidance doesn't mandate a specific SDLC, but it requires a Secure Product Development Framework (SPDF). This means a manufacturer's SDLC must include:

- **Threat Modeling:** Identifying and mitigating security threats early.
- **Vulnerability Management:** A formal process for identifying, assessing, and remediating vulnerabilities.
- **Secure Updates:** A formal plan to provide timely and secure software updates.

Federal Software Security Mandate

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Framework

Industry
Public Sector

Year in Effect
2021

Notes
Applies to any company serving the federal government, including software, tech cloud, and defense contractors

Overview: The Federal Software Security Mandate is a U.S. government directive from Executive Order 14028. It requires any company selling software to a federal agency to attest that its product was developed using secure practices, primarily those in the NIST Secure Software Development Framework (SSDF).

Why It Matters: This mandate is a pivotal shift, moving the burden of proof for software security from the government to the developer. It holds suppliers accountable for protecting the software supply chain and promotes a standardized approach to secure development across the industry.

Key SDLC Requirements: The mandate requires a company's SDLC to align with the NIST SSDF. This implicitly mandates:

- **Threat Modeling:** Identifying threats early.
- **Vulnerability Management:** A formal process for finding and fixing vulnerabilities.
- **Software Supply Chain Transparency:** Encouraging the use of a Software Bill of Materials (SBOM).

FedRAMP

Federal Risk and Authorization Management Program

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Regulation

Industry
Public Sector

Year in Effect
2022

Notes
Applies to vendors providing cloud products and services

Overview: FedRAMP (Federal Risk and Authorization Management Program) is a U.S. government program that provides a standardized security review for cloud products and services. It helps federal agencies securely adopt cloud technologies by centralizing the security assessment process.

Why It Matters: FedRAMP is a mandatory requirement for any company that wants to sell a cloud service to the U.S. government. It saves companies from having to undergo separate security reviews for each agency, and it assures the government that the cloud service has been rigorously vetted.

Key SDLC Requirements: FedRAMP requires cloud service providers to implement security controls from the NIST Special Publication 800-53. This implicitly mandates a secure SDLC with practices such as:

- **Continuous Monitoring:** Ongoing security assessments and vulnerability scans.
- **Change Management:** A formal process for controlling and documenting all changes.
- **Secure Coding:** Using secure coding practices to minimize vulnerabilities.

FINOS AIGF

FINOS AI Governance Framework

Official Site
Link

Geography
Global

Type
AI Framework

Industry
Financial Services

Year in Effect
2024

Overview: The FINOS AI Governance Framework (AIGF) is an open-source framework developed by major financial institutions to address the unique and rapidly evolving risks posed by Generative AI (GenAI). It is a shared, vendor-neutral catalogue of 23+ specific risks (e.g., hallucinations, data leakage, availability) and corresponding mitigations that organizations can adopt to use GenAI safely, ethically, and in a compliant manner.

Why It Matters: GenAI adoption in finance is critical but presents new risks that traditional governance frameworks don't cover. The AIGF matters because it allows competing financial institutions to collaborate on a pre-competitive challenge, creating a unified, defensible standard for responsible AI. This collaboration speeds up safe adoption, reduces the cost of building internal governance from scratch, and facilitates better engagement with regulators.

Key SDLC Requirements: The framework imposes requirements throughout the AI Software Development Lifecycle to build trust, transparency, and accountability into GenAI systems. These requirements include:

- **Risk-Based Design:** Using the framework's Heuristic Assessment Process to proactively identify, classify, and mitigate risks specific to each AI use case before deployment.
- **Continuous Security:** Implementing automated controls to guard against new AI-specific threats like Prompt Injection and Chain-of-Thought Leakage.
- **Auditability & Explainability:** Ensuring all AI-driven decisions are reproducible and auditable, which is crucial for regulatory bodies in the financial sector.

FISMA

Federal Information Security Modernization Act

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Regulation

Industry
Public Sector

Year in Effect
2022

Notes
Applies to vendors providing cloud products and services

Overview: FISMA (Federal Information Security Modernization Act) is a U.S. federal law that mandates all federal agencies and their contractors create and implement a formal information security program to protect government data.

Why It Matters: FISMA is a cornerstone of U.S. cybersecurity, holding agencies and their vendors accountable for data security. It enforces a risk-based approach and sets a mandatory standard for security through NIST guidance.

Key SDLC Requirements: FISMA doesn't mandate a specific SDLC. Instead, it requires agencies to follow the NIST Risk Management Framework (RMF), which implicitly mandates a secure SDLC with practices such as:

- **Security Controls:** Implementing controls from NIST SP 800-53.
- **System Security Plan (SSP):** Documenting all security controls.
- **Continuous Monitoring:** Ongoing security assessments.

HIPAA

Health Insurance Portability and Accountability Act

Official Site
Link

Geography
U.S.A

Type
Data Privacy Regulation

Industry
Healthcare

Year in Effect
1996

Overview: HIPAA establishes national standards for the security of electronic Protected Health Information (ePHI). It governs how healthcare providers, health plans, and their business associates handle patient data.

Why It Matters: Non-compliance can result in severe civil and criminal penalties, including fines of up to $50,000 per violation, with an annual cap of $1.5 million. It can also lead to operational disruption and a complete loss of patient trust.

Key SDLC Requirements: The core principle of HIPAA is to protect the confidentiality, integrity, and availability of all electronic PHI. You must build your software to include:

- **Access Controls:** You must limit access to ePHI to only authorized users.
- **Encryption:** You must implement strong encryption to protect ePHI both at rest and in transit.
- **Audit Controls:** You must maintain a detailed record of all access to, and activity on, systems containing ePHI.
- **Integrity Controls:** You must ensure that ePHI remains unaltered and is not improperly destroyed.

Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines

Official Site
Link

Geography
Singapore

Type
Cybersecurity Regulation

Industry
Financial Services

Year in Effect
2013

Overview: These are a set of guidelines from the Monetary Authority of Singapore (MAS), the nation's central bank. They provide a comprehensive framework for financial institutions to manage and mitigate technology risks, including cybersecurity. They cover everything from IT governance and software development to incident response and third-party risk management.

Why It Matters: While a guideline, they are mandatory for financial institutions in Singapore and serve as the de-facto regulatory standard for the country's financial sector. Failure to comply can result in regulatory action. They are a critical component of Singapore's strategy to maintain a secure financial hub.

Key SDLC Requirements: The MAS guidelines are highly specific about a secure SDLC. Key requirements include:

- **Secure by Design:** Integrating security into the entire SDLC.
- **Secure Coding:** Using secure coding practices to prevent vulnerabilities.
- **Testing:** Conducting rigorous security testing, including penetration testing and vulnerability scanning.
- **Change Management:** Implementing a strict change management process for all IT systems.
- **Supplier Management:** Performing due diligence on third-party software providers to ensure their security practices meet the guidelines.

Frameworks

AI RMF

Artificial Intelligence Risk Management Framework

Official Site
Link

Geography
U.S.A

Type
AI/ML Development Framework

Industry
All

Year in Effect
2023

Overview: The AI Risk Management Framework (AI RMF), created by the National Institute of Standards and Technology (NIST), is a voluntary guide designed to help organizations manage the unique risks associated with the use of artificial intelligence. It provides a flexible and structured approach to responsibly develop, deploy, and use AI systems. The framework is built around four core functions: Govern, Map, Measure, and Manage.

Why It Matters: The AI RMF is crucial because it provides a common language and set of best practices for navigating the complex risks of AI, such as algorithmic bias, security vulnerabilities, and data privacy issues. While voluntary, it is becoming a de facto standard for AI governance. Adopting the AI RMF helps companies build stakeholder trust, prepare for future regulations (like the EU AI Act), and demonstrate a commitment to developing trustworthy and ethical AI.

Key SDLC Requirements: The AI RMF is not an SDLC framework itself, but it provides guidance for integrating risk management into the entire AI system lifecycle. It implicitly requires several key practices within the SDLC:

- **Govern:** Establish a culture and formal policies for managing AI risks across the organization.
- **Map:** During development, identify and document the context, potential harms, and risks of the AI system.
- **Measure:** Use metrics and testing to continuously assess and monitor risks (e.g., for bias, security, and performance).
- **Manage:** Prioritize and implement strategies to mitigate identified risks, and prepare for incident response.

CERT-In Guidelines

Official Site
Link

Geography
India

Type
Cybersecurity Framework

Industry
All

Year in Effect
2022

Overview: The Indian Computer Emergency Response Team (CERT-In) is the national agency for coordinating responses to cyber incidents in India. Its guidelines are a set of directives for companies to report and respond to cyber incidents in a timely manner.

Why It Matters: These guidelines are mandatory for all companies operating in India, and they impose strict requirements on what data to collect and how to report incidents. They are a critical part of India's national cybersecurity strategy and aim to provide CERT-In with a complete picture of the cyber threat landscape.

Key SDLC Requirements: The guidelines are focused on incident response, not SDLC. However, to comply with the guidelines, a company's software and systems must be built to support a robust incident response process. This includes:

- **Logging:** Ensuring all systems and applications generate detailed logs that can be used for forensic analysis.
- **Asset Inventory:** Maintaining a complete and up-to-date inventory of all hardware and software assets.
- **Threat Detection:** Implementing systems that can detect and report on cyber incidents in real time.

Capability Maturity Model Integration (CMMI) v3.0

Official Site
Link

Geography
Global

Type
Information Security Framework

Industry
All

Year in Effect
2023

Overview: CMMI (Capability Maturity Model Integration) v3.0 is a globally recognized process improvement framework and maturity model. It provides structured best practices to help organizations build better products and services by increasing process predictability. It is not a regulation but a voluntary model that rates an organization's capability across Maturity Levels (1-5), with Level 3 (Defined) being a common target.

Why It Matters: CMMI is a critical factor in global business because achieving a high Maturity Level (e.g., Level 3) demonstrates organizational stability, capability, and low risk to customers. While it carries no direct penalty, companies often lose large contracts in sectors like defense, finance, and technology if they cannot prove their processes meet a certain CMMI level, making it a competitive prerequisite.

Key SDLC Requirements: CMMI v3.0 significantly influences the entire SDLC by requiring organizations to standardize, document, and measure their development activities. Key requirements include:

- **Configuration Management:** Establishing strict control, versioning, and integrity checks for all work products, including source code and build artifacts.
- **Requirements Management:** Implementing defined, repeatable processes for developing, tracing, and managing project requirements from inception to delivery.
- **Measurement and Analysis:** Building a formal capability to collect data, analyze process performance, and use data-driven insights to manage projects and guide continuous improvement.

Guidelines and Companion Guide of Securing AI Systems

Official Site
Link

Geography
Singapore

Type
AI/ML Development Framework

Industry
All

Year in Effect
2024

Overview: The Guidelines and Companion Guide of Securing AI Systems is a voluntary, community-driven resource to help organizations secure AI systems. Created by the Cyber Security Agency of Singapore (CSA) in collaboration with international partners, it provides a practical roadmap for managing both traditional and novel AI-specific risks, like adversarial machine learning.

Why It Matters: This guide is crucial because it offers a holistic, lifecycle-based approach to securing AI, recognizing that simply hardening the model is insufficient. Its multi-national collaboration makes it a valuable resource for global companies by incorporating best practices from multiple nations and industry experts.

Key SDLC Requirements: The guidelines are structured around four key areas of the AI system development life cycle: secure design, secure development, secure deployment, and secure operation and maintenance. They implicitly require organizations to integrate the following into their SDLC:

- **Risk Assessment and Threat Modeling:** Identifying AI-specific vulnerabilities before development.
- **Supply Chain Security:** Protecting against risks from third-party models and tools.
- **Continuous Monitoring:** Implementing ongoing security monitoring and logging.
- **Incident Management:** Establishing a plan for responding to security incidents and providing secure updates.

IT-Grundschutz Compendium

Official Site
Link

Geography
Germany

Type
Cybersecurity Framework

Industry
All

Year in Effect
1994
(Updated 2022)

Overview: The IT-Grundschutz Compendium, published by Germany's Federal Office for Information Security (BSI), is a widely recognized framework that provides practical guidance for establishing and maintaining a robust Information Security Management System (ISMS). While mandatory for German public sector and government agencies, private-sector companies, particularly in critical infrastructure, widely adopt it. IT-Grundschutz aligns with international standards like ISO/IEC 27001.

Why It Matters: IT-Grundschutz is a highly respected framework across the EU and serves as a roadmap for aligning with strict cybersecurity best practices. By following its guidelines, organizations can systematically identify, mitigate, and manage information security risks. For companies doing business in Germany or the EU, or those seeking to align with high security standards, adopting IT-Grundschutz principles is a strategic advantage that demonstrates a commitment to robust security.

Key SDLC Requirements: The IT-Grundschutz framework heavily influences the SDLC by providing detailed, practical controls. Based on the document you provided, these key requirements include:

- **Secure Component Use:** Organizations must procure external libraries and components from trusted sources, verify their integrity, and check them for vulnerabilities before use.
- **Automated Process Security:** CI/CD and automation processes must operate with the principle of least privilege, with strict access controls and detailed audit logs to ensure accountability.
- **Software Inventory**: Companies must maintain a complete, up-to-date inventory of all software and licenses, including security-relevant settings.
- **Secure Procurement:** The procurement process must include requirements for using trusted software sources, verifying integrity, and ensuring vendor accountability for vulnerability remediation.
- **Secure Image Management:** The framework mandates using secure, verifiable, and non-deprecated container images from trusted sources, with a defined test and release process before they are deployed to production.
- **Trusted Storage:** Organizations must implement trusted storage for business-critical applications, including documented code and security-relevant information, to protect against vendor outages.

NIST AI 800-1

Official Site
Link

Geography
U.S.A

Type
AI/ML Development Framework

Industry
All

Year in Effect
2024

Overview: NIST AI 800-1, a voluntary guide from the U.S. AI Safety Institute, helps developers of powerful dual-use foundation models manage the risk of their AI being deliberately misused to cause harm.

Why It Matters: This guide is important because it is one of the first official government-backed resources to address the unique, severe risks of advanced AI models. It provides a de facto standard for the industry, helping companies proactively manage national security and public safety threats before a model is deployed.

Key SDLC Requirements: The guide requires developers to integrate misuse risk management throughout their SDLC, which implicitly includes:

- **Red Teaming:** Rigorously testing a model to anticipate how it could be misused.
- **Secure Development:** Protecting the AI system's assets (like unreleased model weights) from theft or tampering.
- **Continuous Monitoring:** Monitoring for misuse after deployment and updating the model to mitigate new risks.

NIST CSF

NIST Cybersecurity Framework

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Framework

Industry
All

Year in Effect
2014

Overview: The NIST Cybersecurity Framework (CSF) is a voluntary, risk-based framework that helps organizations manage their cybersecurity risks. It provides a flexible structure with five core functions: Identify, Protect, Detect, Respond, and Recover, which help organizations prioritize investments and communicate risk.

Why It Matters: The CSF is a cornerstone of modern cybersecurity because it provides a common language that bridges the gap between technical teams and business leaders. While voluntary, it is a de facto standard used by many companies to improve their security posture, demonstrate due diligence, and prepare for other regulations.

Key SDLC Requirements: The CSF does not mandate a specific SDLC. However, it provides a high-level structure that helps organizations integrate security into their development lifecycle, which implicitly requires the following:

- **Identify:** Categorizing and understanding risks to software assets early in development.
- **Protect:** Implementing safeguards like secure configurations and access controls throughout the development process.
- **Detect:** Integrating continuous monitoring and logging to identify security events.
- **Respond & Recover:** Having a formal incident response and recovery plan in place as a part of the product's overall lifecycle management.

NIST SSDF

NIST Secure Software Development Framework

Official Site
Link

Geography
U.S.A

Type
Cybersecurity Framework

Industry
All

Year in Effect
2020

Notes
Requirement for U.S. federal contractors starting in mid-2024

Overview: The NIST Secure Software Development Framework (SSDF) is a set of best practices for integrating security throughout the entire Software Development Life Cycle (SDLC). It is a flexible, outcomes-based framework designed to help any organization build more secure software by "shifting left" and addressing security issues in the earliest stages of development.

Why It Matters: The SSDF provides a common language and a structured approach for secure software development. While voluntary, it has become a de facto standard—most notably for U.S. federal contractors, as it is referenced in Executive Order 14028. By following the SSDF, organizations can reduce vulnerabilities, minimize the impact of security breaches, and demonstrate due diligence to customers and regulators.

Key SDLC Requirements: The SSDF is not a specific SDLC model (like Agile) but provides practices to be integrated into any existing workflow. These practices fall into four main groups:

- **Prepare the Organization:** Establish a culture of secure development and define roles.
- **Protect the Software:** Safeguard all software components from tampering.
- **Produce Well-Secured Software:** Minimize vulnerabilities by conducting threat modeling and robust security testing.
- **Respond to Vulnerabilities:** Have a formal process to identify and address vulnerabilities in released software.

Plan for Global Engagement on AI Standards

Official Site
Link

Geography
U.S.A

Type
AI/ML Development Framework

Industry
All

Year in Effect
2024

Overview: The Plan for Global Engagement on AI Standards (NIST AI 100-5) is a U.S. government strategy to guide federal agencies in influencing international AI standards. It aims to promote a U.S.-led, market-driven approach that ensures global standards are consistent with U.S. values and technical expertise.

Why It Matters: This plan is crucial because it helps the U.S. take a leadership role in shaping global AI regulation and preventing a fragmented market. By influencing international standards, it aims to reduce trade barriers and ensure U.S. economic and national security interests are protected.

Key SDLC Requirements: It is guided by the NIST AI Risk Management Framework, which implicitly encourages a secure SDLC that includes:

- **Risk Management:** Integrating risk assessment throughout the AI lifecycle.
- **Transparency and Explainability:** Ensuring AI systems are understandable.
- **Security and Privacy:** Building security into systems from the start.
- **Validation:** Rigorously testing AI systems for performance and reliability.