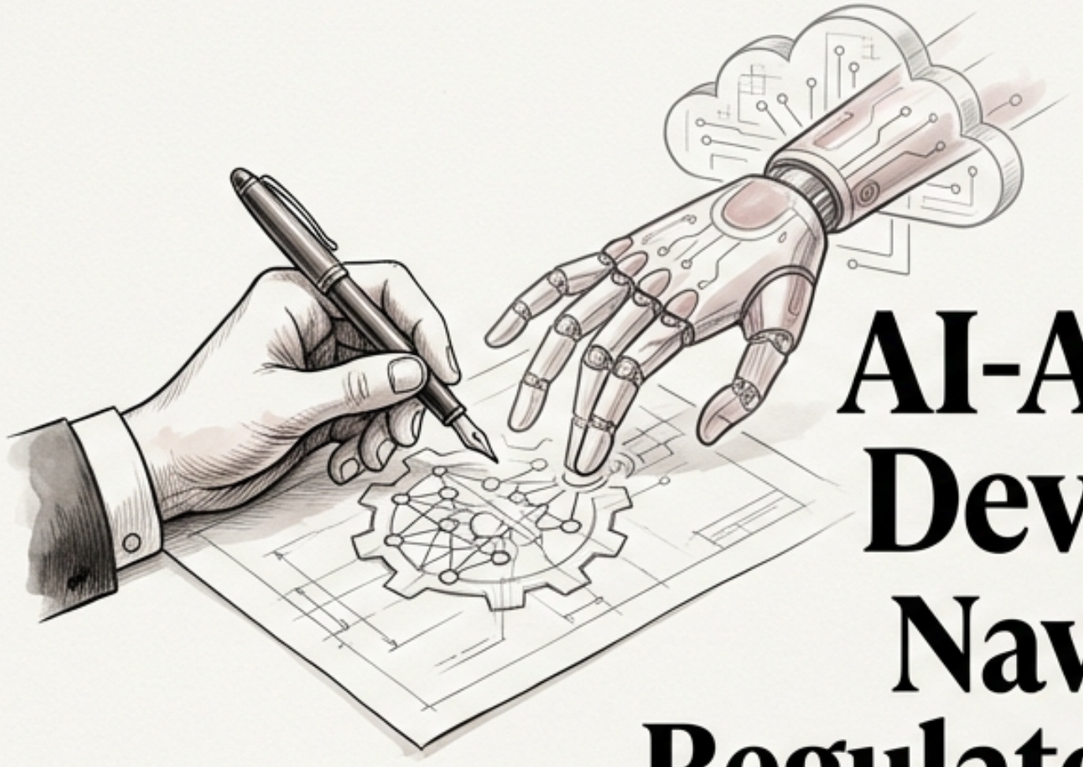
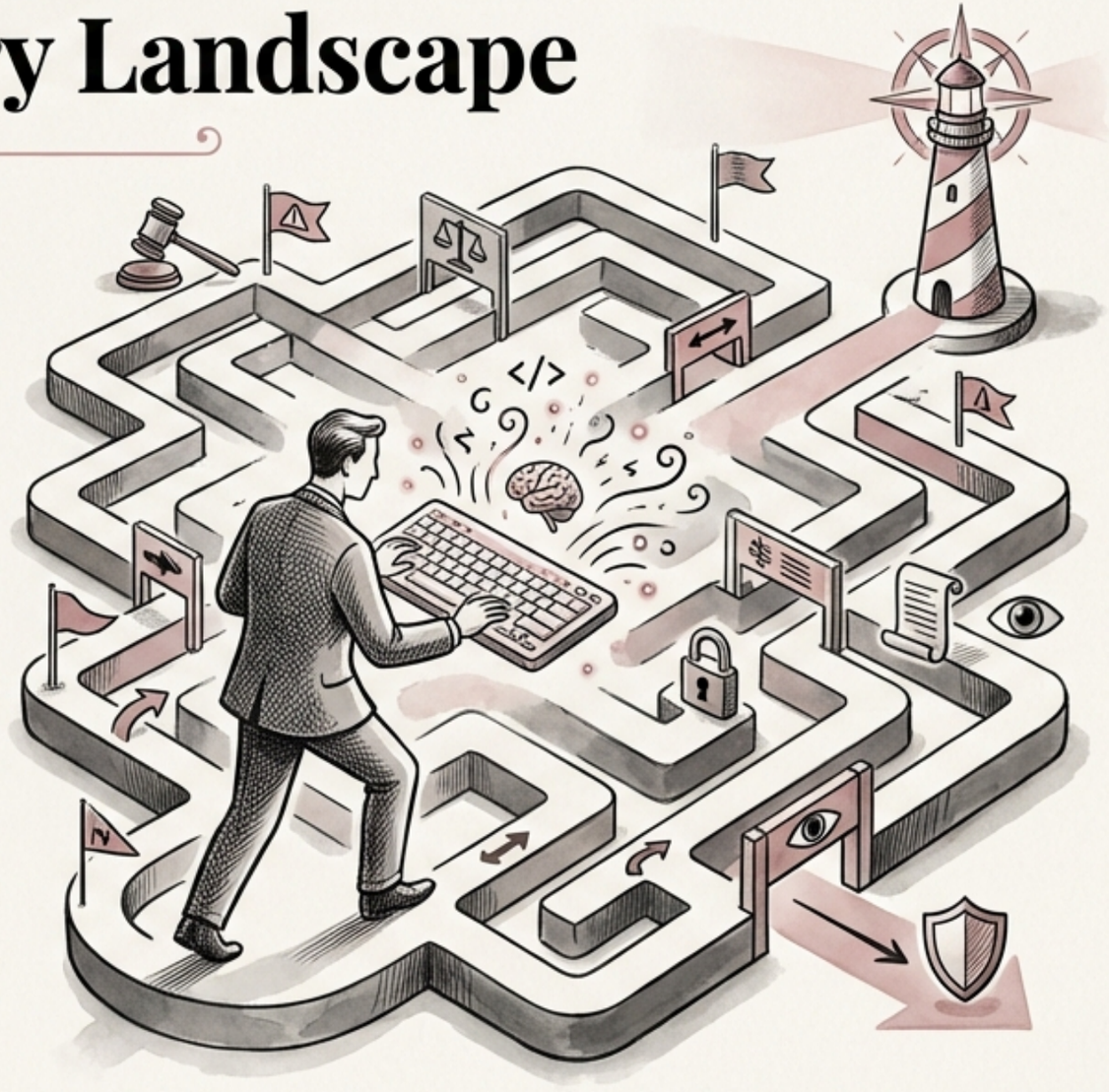


AI-Augmented Development: Navigating the Regulatory Landscape

A COMPREHENSIVE GUIDE TO COMPLIANCE, ETHICS, AND INNOVATION

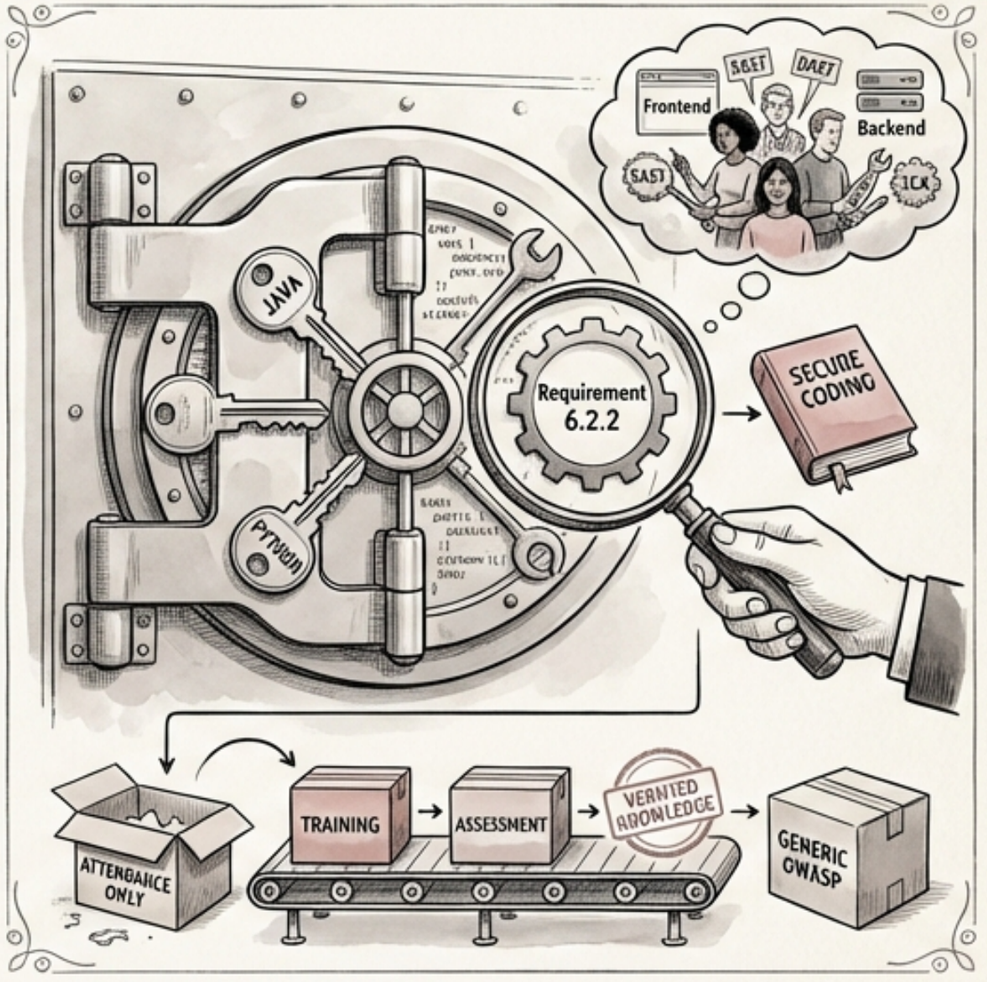
AI-Augmented Development: Navigating the Regulatory Landscape

- AI coding tools are rapidly changing software development, requiring developers to understand new compliance challenges.
- This module covers key regulatory frameworks that impact secure development, especially those related to AI.
- Understanding these regulations is crucial for avoiding legal and financial risks associated with non-compliance.
- We will focus on how these regulations directly affect development teams using AI-powered tools.
- Staying ahead of AI-specific regulations is essential for maintaining trust and ensuring responsible AI development.



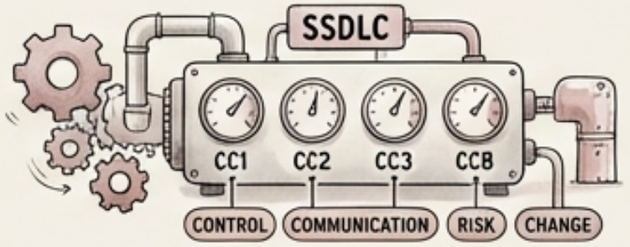
PCI-DSS 4.0: Granular Training is Key for Compliance

- PCI-DSS 4.0 Requirement 6.2.2 mandates specific developer training for secure coding practices.
- Generic OWASP Top 10 training is insufficient; training must be language-specific (e.g., Java, Python).
- Training must also be role-specific (e.g., frontend developer, backend developer) and tool-specific (SAST, DAST, SCA).
- Developers need hands-on training with the SAST/DAST/SCA tools they use daily, not just theoretical concepts.
- Annual training is required, and assessments must verify knowledge (attendance is not enough).



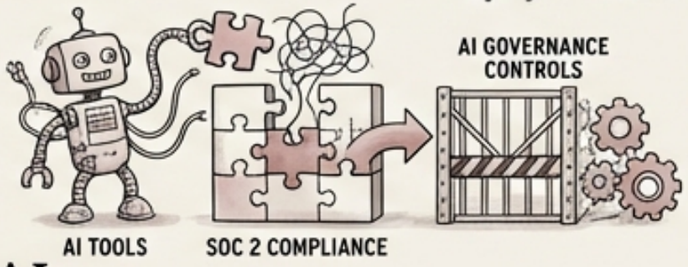
SOC 2: AI Governance in the CI/CD Pipeline

- SOC 2 Trust Services Criteria (CC1, CC2, CC3, CC8) directly impact SSDLC: Control Environment, Communication, Risk Assessment, Change Management.



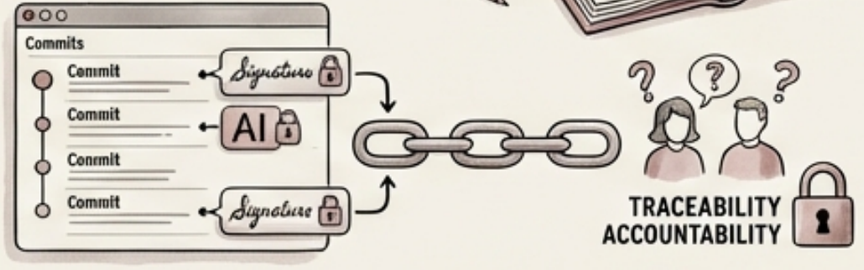
- Achieve continuous compliance through CI/CD pipeline evidence: commit signing, automated test results, deployment approvals, access reviews.

- AI tools introduce new complexities to SOC 2 compliance, requiring robust AI governance controls.

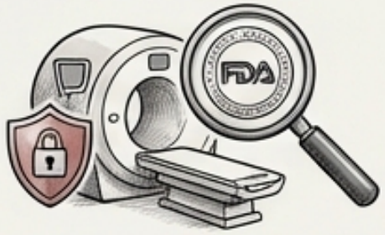


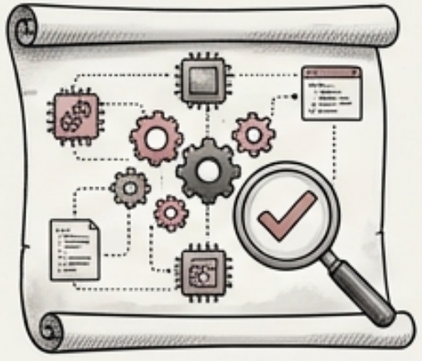
- Auditors now expect to see documented AI governance policies and procedures.

- Ensure all code commits are signed to maintain traceability and accountability when using AI tools.

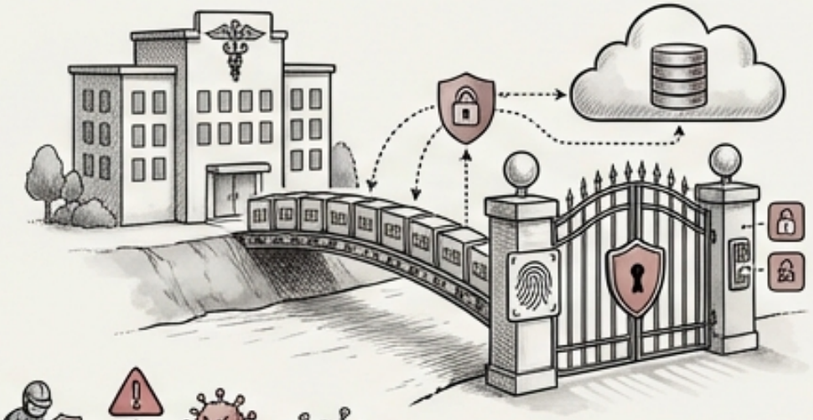


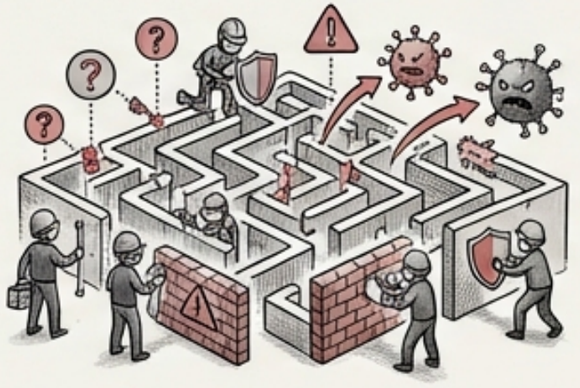
FDA Cybersecurity Guidance: Securing AI/ML Medical Devices

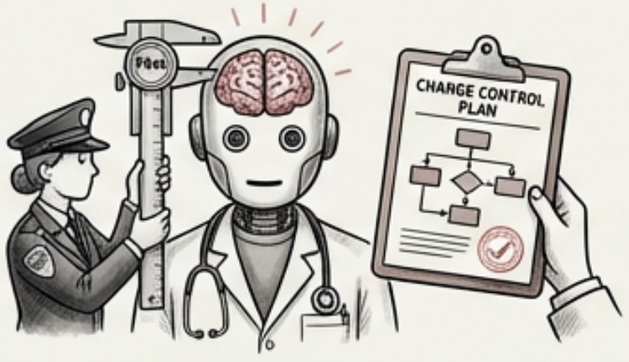




- The FDA requires premarket cybersecurity measures for medical device software.
- A Software Bill of Materials (SBOM) is mandatory for medical devices to track software components and dependencies.
- Comprehensive threat modeling is essential to identify and mitigate potential vulnerabilities.
- Post-market vulnerability management is crucial for continuous security monitoring and updates.
- AI/ML-enabled medical devices face heightened scrutiny under predetermined change control plans.

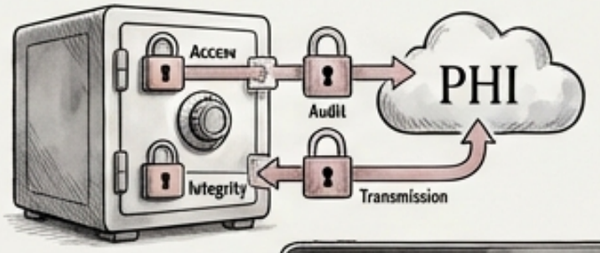


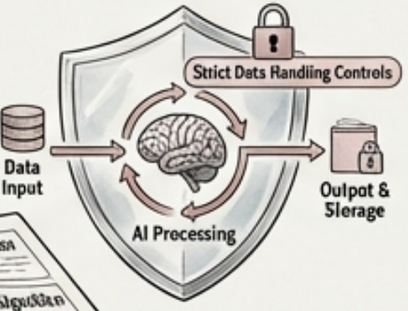


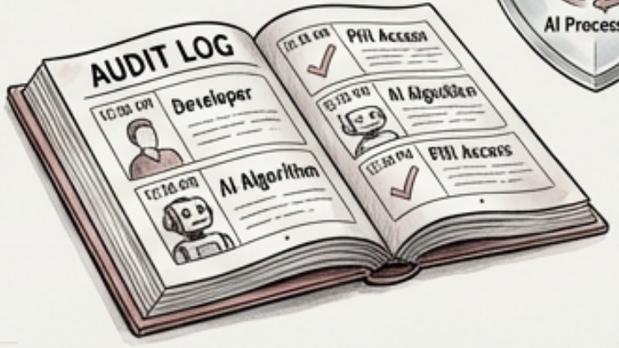


HIPAA Technical Safeguards: Protecting PHI in AI Applications

- HIPAA's Technical Safeguards include access controls, audit controls, integrity controls, and transmission security.
- Application-level requirements are often overlooked: session management, encryption at rest, audit logging of PHI access.
- AI tools processing PHI require Business Associate Agreements (BAAs) with vendors.
- Implement strict data handling controls to protect PHI throughout the AI processing lifecycle.
- Ensure robust audit logging of all PHI access, including by AI algorithms and developers.

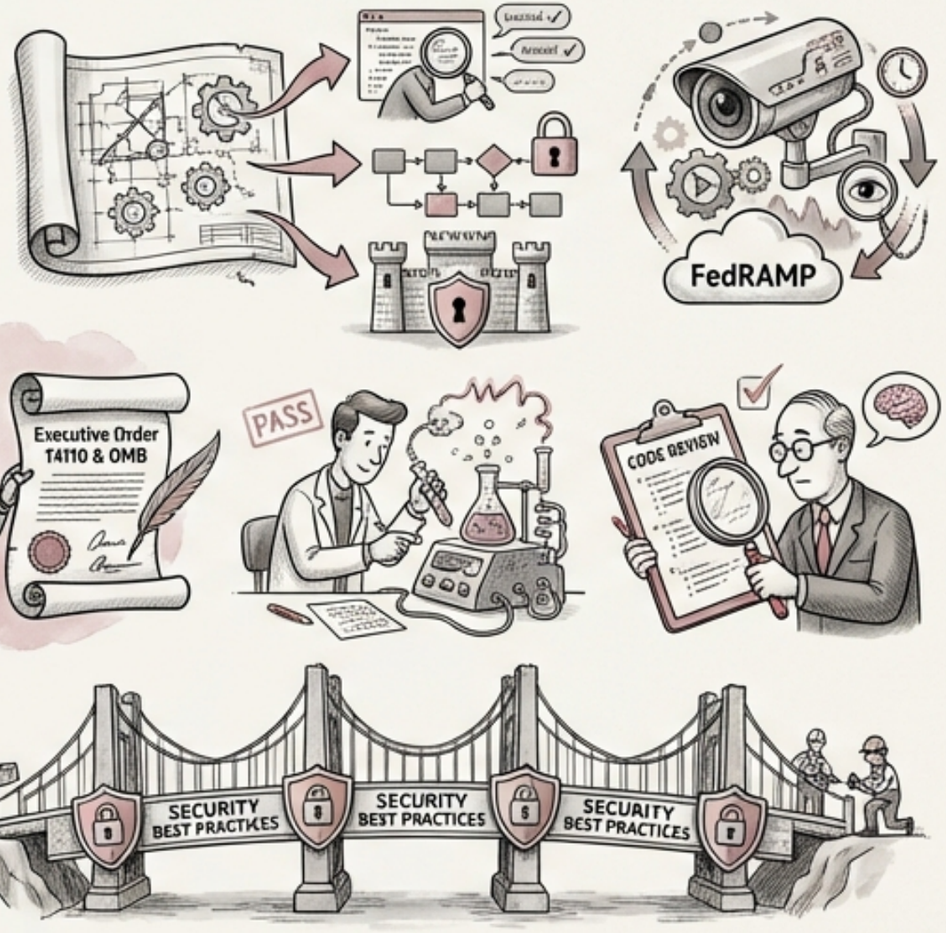




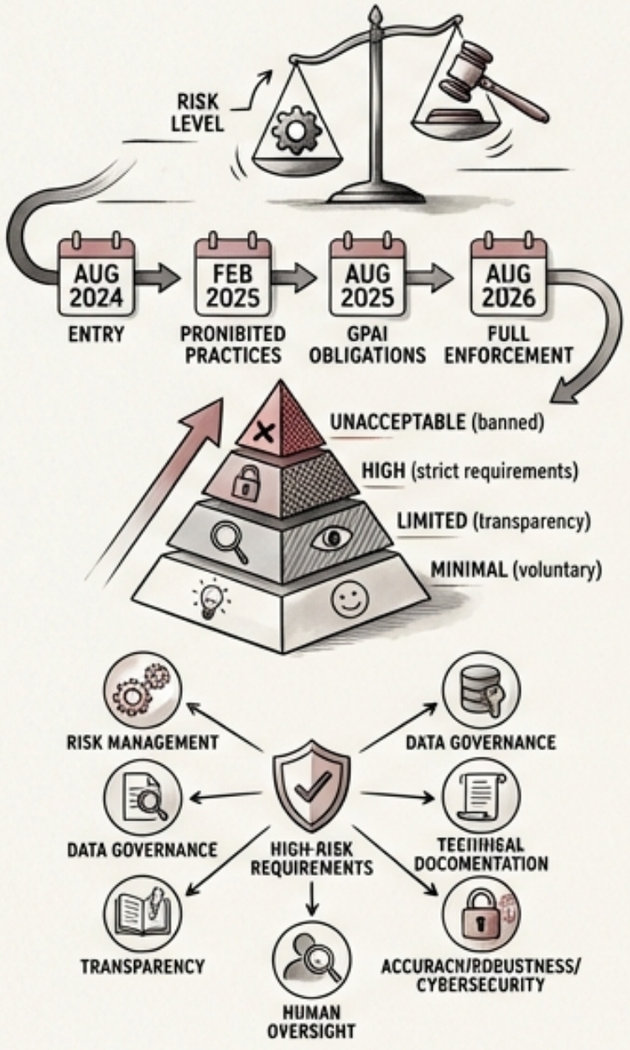


FedRAMP and NIST 800-53: Secure Development for Federal Software

- 1. NIST 800-53 outlines software assurance controls for federal systems: SA-11 (Developer Testing), SA-15 (Development Process), SA-17 (Developer Security Architecture).
- 2. Continuous monitoring is a key requirement for FedRAMP-compliant systems.
- 3. AI usage in federal software is subject to Executive Order 14110 and OMB guidance.
- 4. Ensure your development process includes rigorous developer testing (SA-11) and code reviews.
- 5. Adopt a secure development process (SA-15) that incorporates security best practices throughout the SDLC.



EU AI Act: A Game Changer for AI Development



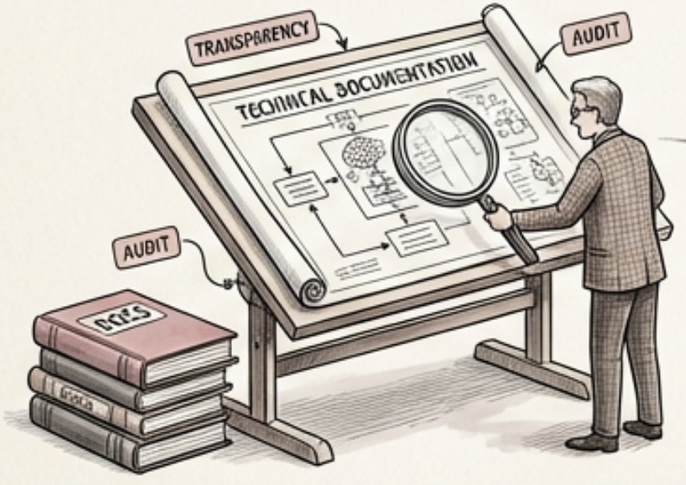
- The EU AI Act aims to regulate AI systems based on their risk level.
- Key timelines: August 2024 entry, February 2025 prohibited practices, August 2025 GPAI obligations, August 2026 full enforcement.
- AI systems are classified into four risk categories: Unacceptable (banned), High (strict requirements), Limited (transparency), Minimal (voluntary).
- High-risk AI systems require risk management, data governance, technical documentation, transparency, human oversight, and accuracy/robustness/cybersecurity.
- Development teams using AI coding tools must assess whether AI-assisted output falls under regulated categories.

EU AI Act: Requirements for High-Risk AI Systems

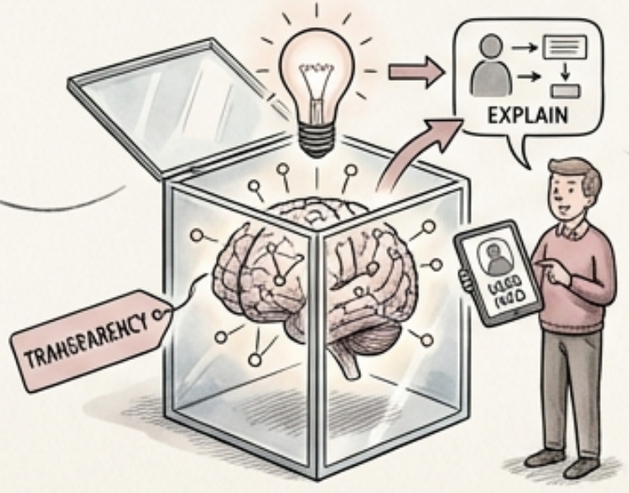
- High-risk AI systems must undergo rigorous risk management processes.

- Strong data governance is required, including data quality, integrity, and privacy.

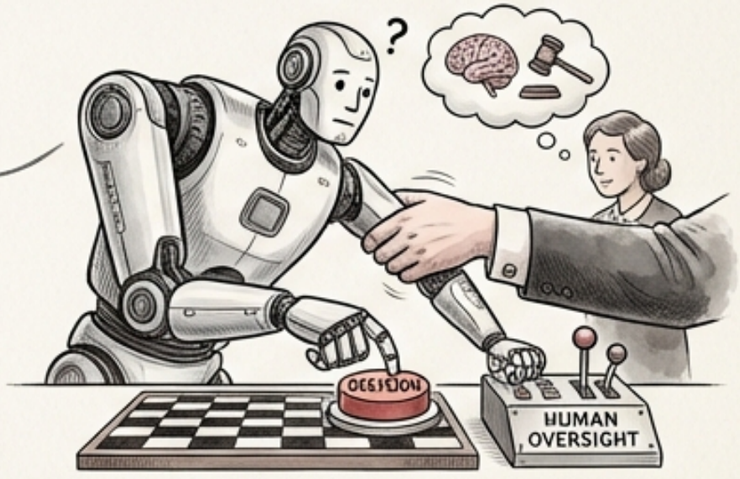
- Comprehensive technical documentation is essential for transparency and auditability.



- Transparency requirements include and providing information to users.

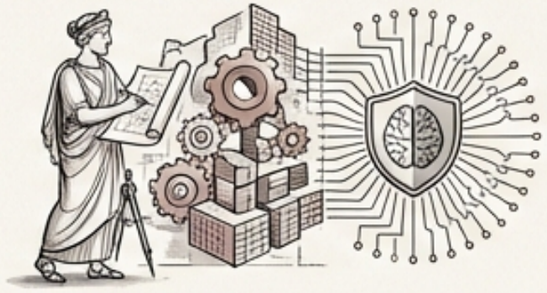


- Human oversight is necessary AI from making harmful decisions.



NIST AI Risk Management Framework: Govern, Map, Measure, Manage

- The NIST AI Risk Management Framework provides a structured approach to managing AI risks.



- The framework consists of four functions: Govern, Map, Measure, Manage.

- **Map:** Identify and document AI risks throughout the development lifecycle.

- **Govern:** Establish policies and processes for AI risk management.

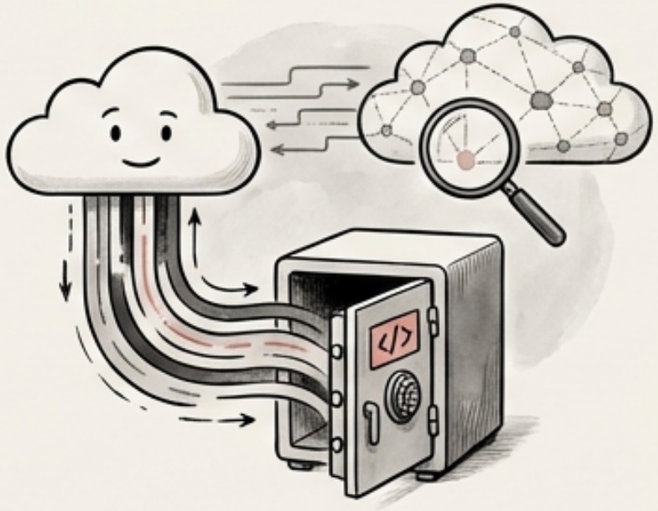
- **Map:** Identify and document AI risks throughout the development lifecycle.

- **Measure:** Assess the likelihood and impact of AI risks.

Risk Assessment for AI Coding Assistants: Data, Output, Dependency

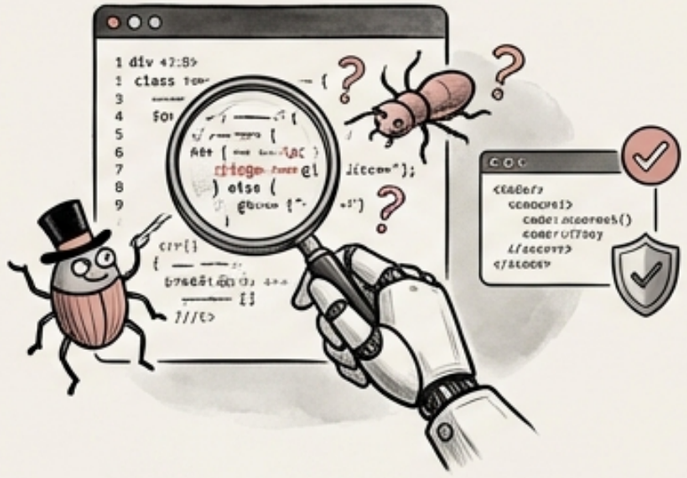
Risk assessment for AI coding assistants should focus on **data exposure**, **output quality**, and **dependency** on AI availability.

DATA EXPOSURE



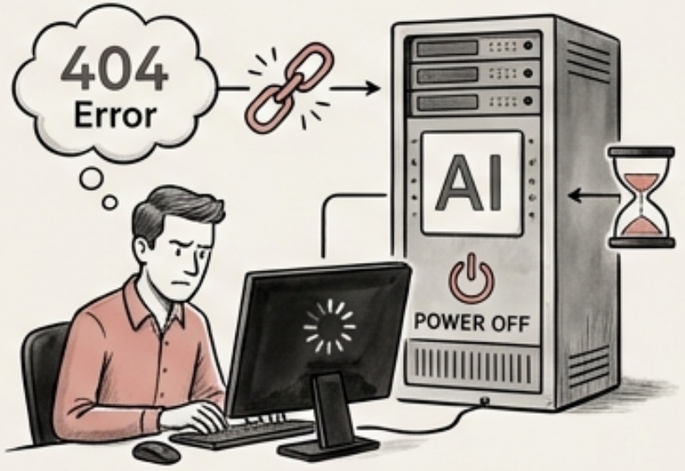
- **Data Exposure:** Evaluate the risk of sensitive data being leaked to the AI provider or other users.
- Implement data masking and anonymization techniques to protect sensitive data used by AI coding assistants.

OUTPUT QUALITY



- **Output Quality:** Assess the accuracy, completeness, and security of AI-generated code.

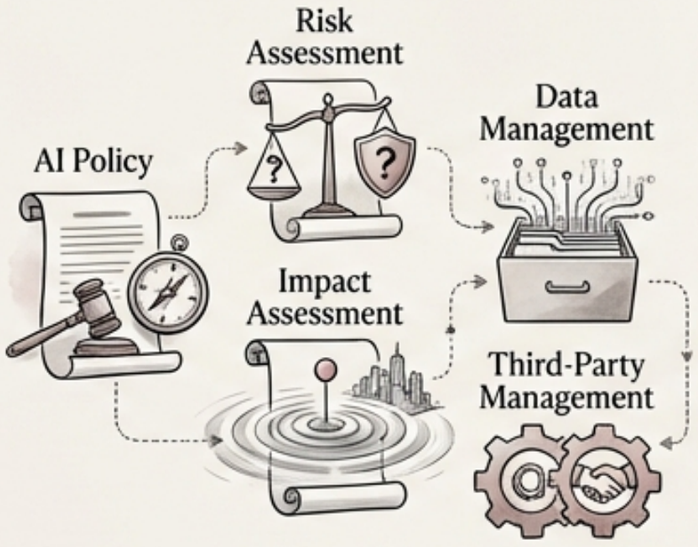
DEPENDENCY ON AI AVAILABILITY

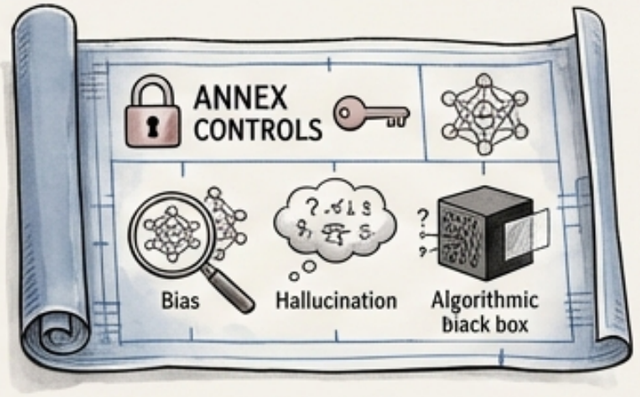


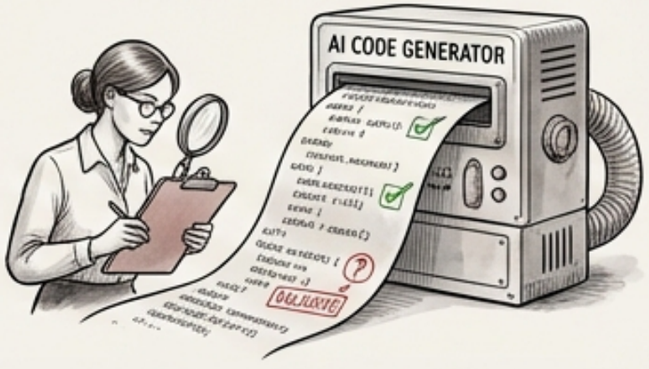
- **Dependency on AI Availability:** Consider the impact of AI tool outages or performance degradations on development productivity.

ISO/IEC 42001: Establishing an AI Management System

- ISO/IEC 42001 is the first certifiable AI management system standard.
- Requirements include: AI policy, risk assessment, impact assessment, data management, third-party management.
- Annex controls specific to AI systems address unique challenges.
- Development teams must document AI tool usage, including purpose, inputs, and outputs.
- Quality assurance processes are needed to validate the outputs of AI-assisted code generation.



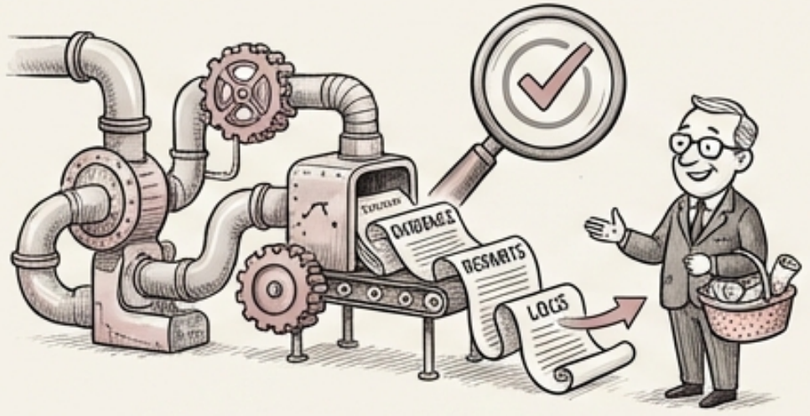




Implications for Development Teams: AI Tool Documentation and QA

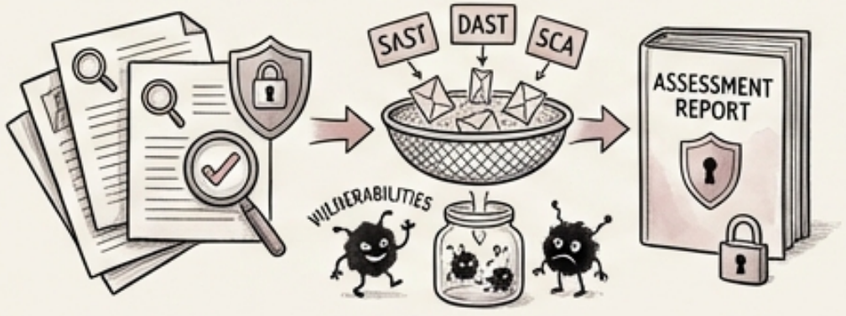
- **Document all AI tools** used in the development process, including their purpose and functionality.
- Maintain **detailed records** of AI tool **inputs and outputs** for traceability and auditability.
- Implement **rigorous quality assurance (QA) processes** to validate AI-generated code.
- Establish **code review procedures** to ensure the accuracy, security, and reliability of AI outputs.
- **Track** the **performance** of AI tools and identify areas for improvement.

COMPLIANCE EVIDENCE AUTOMATION: CI/CD AS EVIDENCE GENERATOR

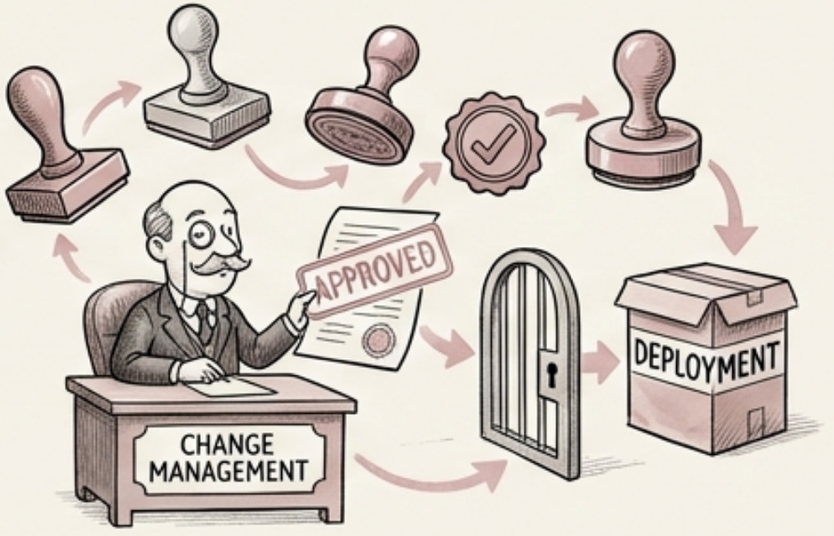


- **CI/CD pipelines** can serve as **compliance evidence generators,** reducing the audit burden.

- **Automated test results** provide evidence of **code quality** and **security.**



- **SAST/DAST/SCA scan** reports document **vulnerability assessments.**

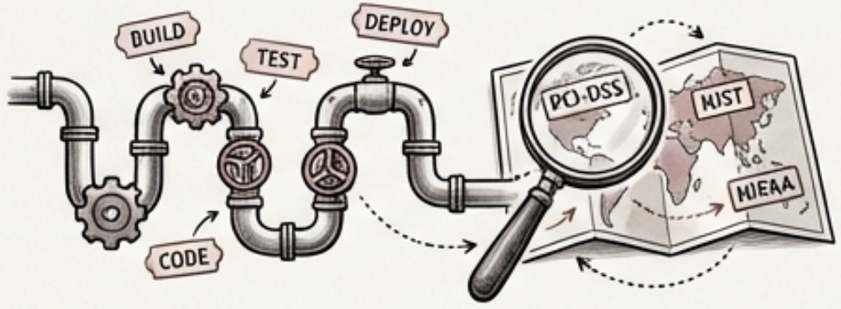


- **Deployment approvals** demonstrate adherence to **change management procedures.**

- **Access logs** track user access and **activity** for auditability.

MAPPING PIPELINE ARTIFACTS TO REGULATORY REQUIREMENTS

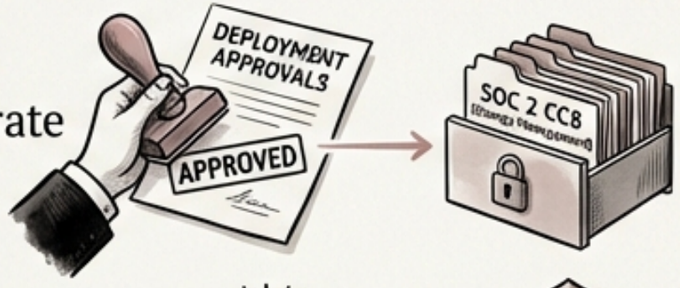
COMPLIANCE INTEGRATION & EVIDENCE



- Create a mapping table linking specific CI/CD pipeline artifacts to the relevant regulatory requirements.

- For example, SAST scan reports can demonstrate compliance with PCI-DSS 6.2.2.

- Automated test results can provide evidence of compliance with NIST 800-53 SA-11.

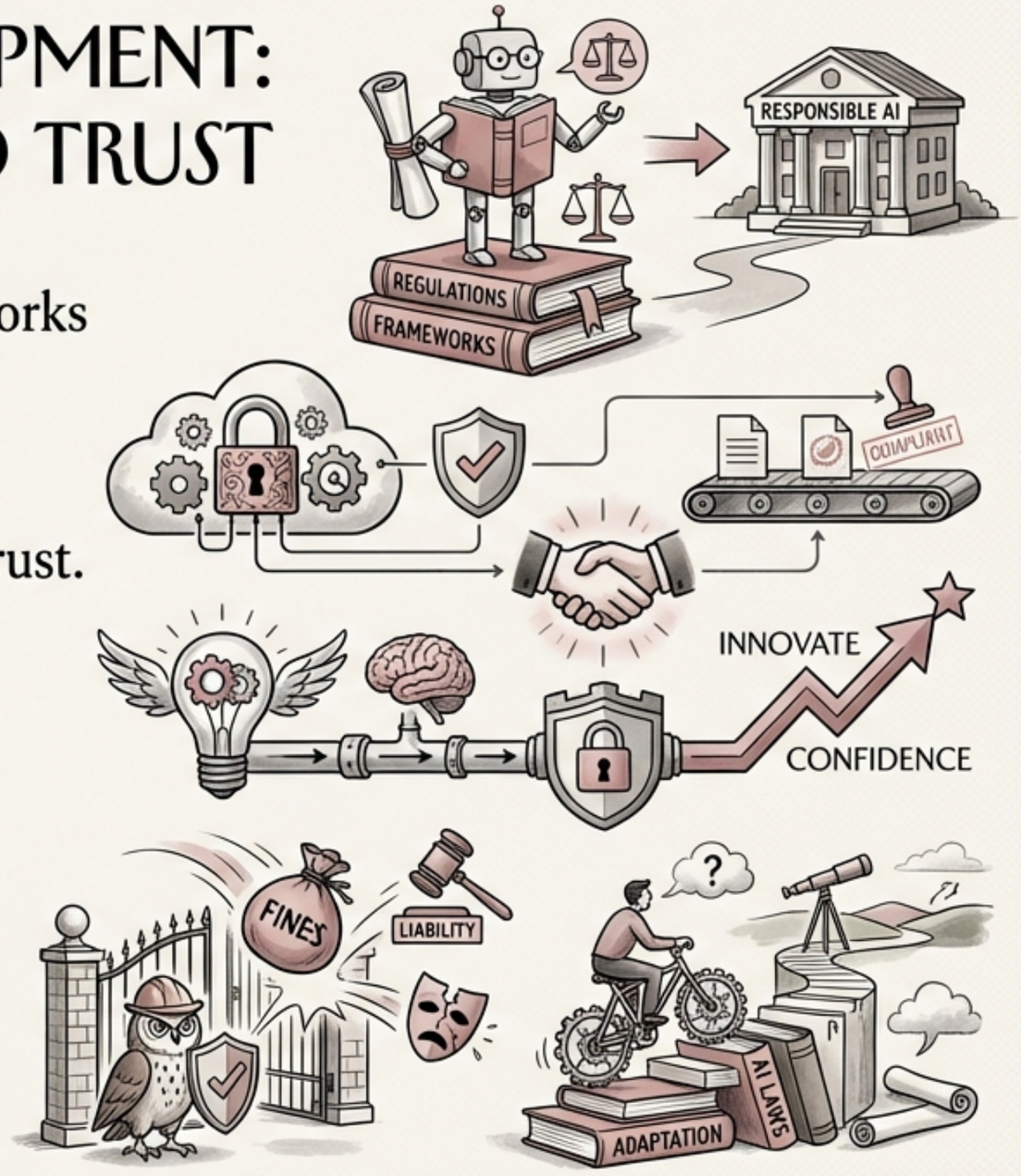


- Deployment approvals can demonstrate adherence to SOC 2 CC8 (Change Management).

- Access logs can provide evidence of compliance with HIPAA access controls.

EMBRACE SECURE AI DEVELOPMENT: A PATH TO INNOVATION AND TRUST

- Understanding and adhering to regulatory frameworks is crucial for responsible AI development.
- Implementing robust security measures and compliance automation reduces risks and fosters trust.
- By embracing secure AI development practices, organizations can innovate with confidence.
- Proactive compliance efforts can prevent costly fines, legal liabilities, and reputational damage.
- Continuous learning and adaptation are essential for staying ahead of evolving AI regulations.



Thank You

- 1. Questions?