AARON HEBERT & ALYSSA PUGH

From Code to Contract: Securing Software Development

KEYS 2026 HORIZONS

Sign into Tandem to participate in this session.

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the presenters' opinions.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

KEYS

2

Aaron Hebert
Developer
Tandem, LLC

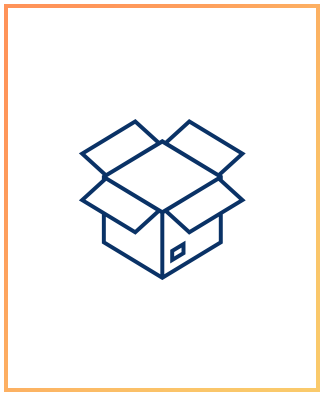
Alyssa Pugh
GRC Content Manager
Tandem, LLC

KEYS

3

WHY SECURE SOFTWARE DEVELOPMENT?

More Expensive Incidents



Less Contained Software

More Focus from Regulators

KEYS

4

THE TIME RESERVATION
I don't have time to review all software for security.

THE EXPERTISE RESERVATION
I'm not a developer. How can I know if it's secure or not?

THE RISK RESERVATION
What's the actual risk involved if I don't think about security?

THE OSTRICH RESERVATION
… software? Never heard of it. 🤔

KEYS

5

Not all software is created equal.
Your security and risk management practices shouldn't be equal either.

KEYS

6

SESSION AGENDA

1. Five Factors for Secure Software Development
2. The System Development Life Cycle (SDLC)
3. Integrated Components
4. Third-Party Risk Management
5. The Impact of Artificial Intelligence

KEYS

7

Five Factors for Secure Software Development

KEYS

8

FIVE FACTORS

1. Platform Types
2. Software Types
3. Developer Types
4. Data Types
5. Operational Criticality

KEYS

9

PLATFORM TYPES

1. Web-based applications
2. Desktop applications
3. Mobile applications
4. Client/server applications
5. Cloud infrastructure
6. Analytics solutions
7. Databases
8. Models
9. Automation and scripting
10. Application programming interfaces

⚠ Anything that manipulates or instructs a computer to do something needs to be reviewed.

KEYS

10

SOFTWARE TYPES

COTS Software

- Productivity Tools
- Collaboration Platforms
- Creative Apps
- Web Browsers

SECURITY RESPONSIBILITY
The Vendor

Enterprise Software

- Core Systems
- CRM Platforms
- ERP Solutions
- GRC Software

SECURITY RESPONSIBILITY
Shared by Both

Custom Software

- Proprietary Systems
- Custom Analytics Tools
- Workflow Automation
- API Development

SECURITY RESPONSIBILITY
The Organization

KEYS

11

DEVELOPER TYPES

In-House Developers	Third-Party Developers
Professional Developers	Vendor / Independent Developers
Citizen Developers	Open-Source Developers
Autonomous Developers	Autonomous Developers

Where your software comes from determines your visibility and control. 🤖

KEYS

12

DATA TYPES

Classification	Context Example
Public / Unclassified	Business Data
Private / Sensitive	Personnel Data
Restricted / Confidential	Customer / Member Data

➡️ The more sensitive the data, the stronger the controls you must apply.

KEYS

13

OPERATIONAL CRITICALITY

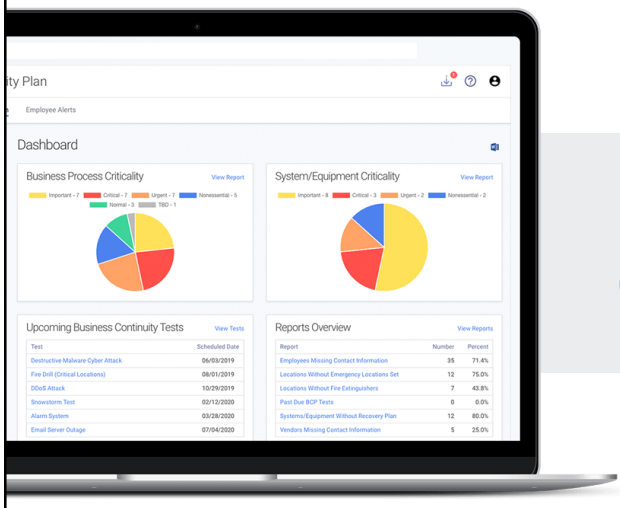
- Critical (3 Hours)
- Urgent (24 Hours)
- Important (72 Hours)
- Normal (7 Days)
- Nonessential (30 Days)

Does this software support critical business functions?

KEYS

14

KEYS



Tandem Business Continuity Plan Software

15

The System Development Life Cycle

KEYS

16

GUIDANCE

FFIEC Development, Acquisition, and Maintenance Booklet

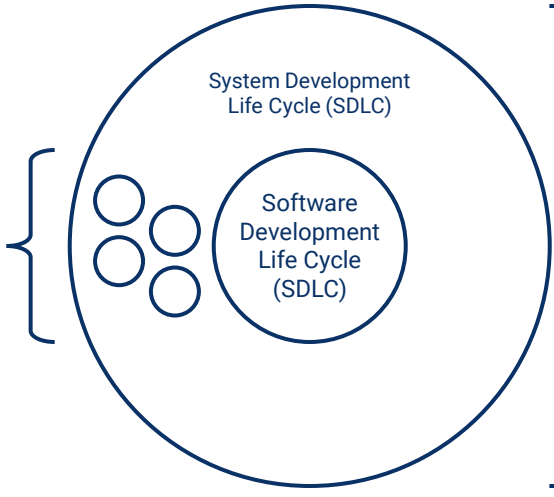
ithandbook.ffiec.gov

KEYS

17

THE "SDLC"

- Hardware Development
- Big Data Development
- Model Development
- Database Development

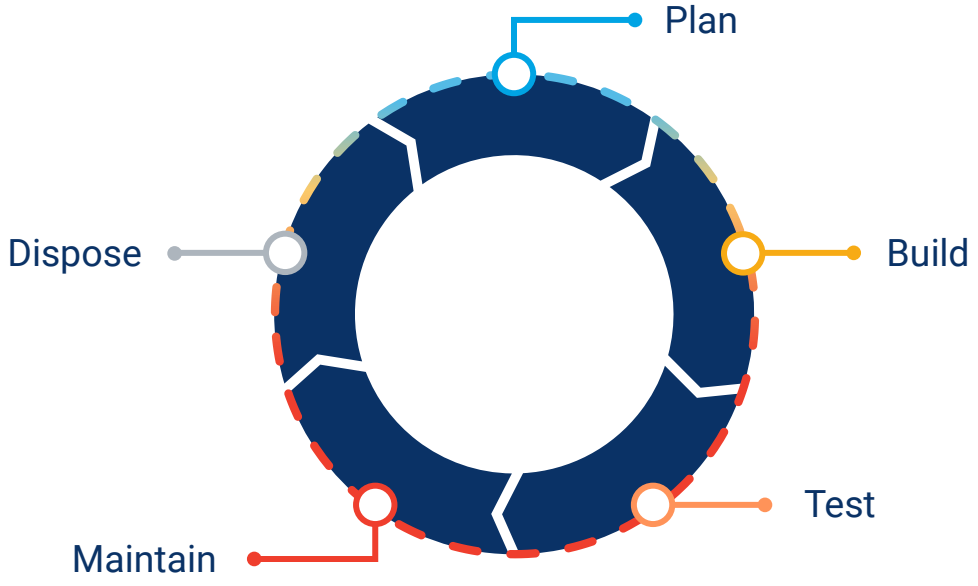


Secure Development Life Cycle (SDLC)

KEYS

18

SYSTEM DEVELOPMENT LIFECYCLE (SDLC)

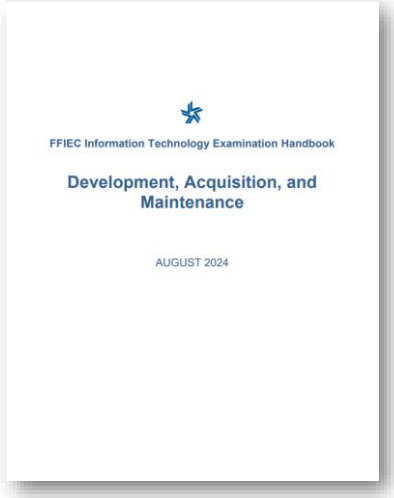


KEYS

19

THE SDLC | PLAN

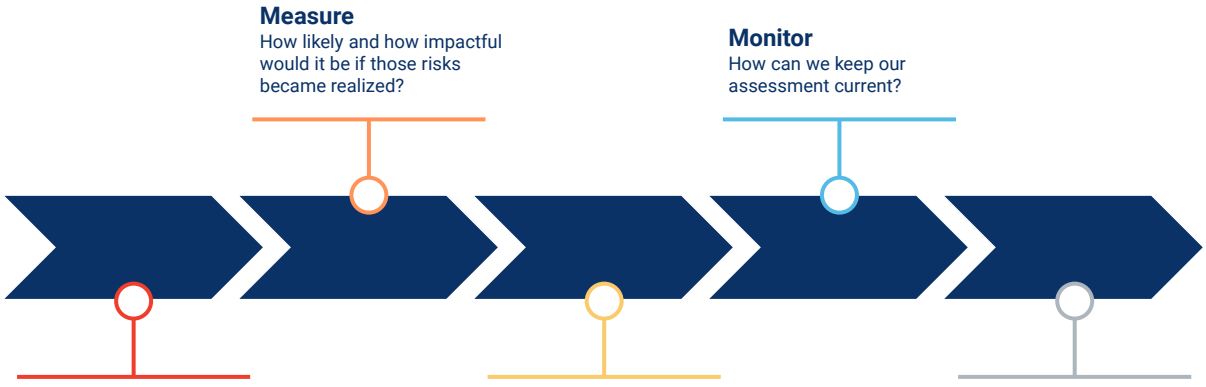
- Risk Assessments
- Policies and Procedures
- Quality Assurance Plans
- Technical Plans



KEYS

20

PROJECT RISK ASSESSMENT



KEYS

21

THE SDLC | BUILD

Industry-Standard Programming Languages

Processing Controls & Input Validation

Version Control System

Detailed Documentation

Source Code Repository Backups

"Management should establish development standards, including procedures for controlling changes during the development process that address the following: [system controls, quality management, release management, documentation, and reporting.] Development standards should articulate the entity's minimum development requirements. For example, development standards may address the selection of programming styles, languages, and tools; layout or format of scripted code; naming conventions; and program library requirements."

KEYS

22

THE SDLC | TEST

1 Code Assessments

2 Quality Assurance Assessments

3 Security & Compliance Assessments

"Testing is essential to the development process to promote confidentiality, integrity, availability, and resilience. Whether developed internally or by a third party, appropriate personnel should test systems and components to identify and correct defects before deployment, including security-related defects. […] The types of testing performed should be appropriate for the development activity's inherent risk. Effective management has a methodical process to define and conduct testing necessary to demonstrate the effectiveness of a developed system or component. Typically, testing is performed in stages, and knowledgeable testing specialists and relevant stakeholders should be involved in testing."

KEYS

23

THE SDLC | MAINTAIN

Improve Performance

Enhance Security

Correct Problems

"The maintenance and operations SDLC activities are necessary whether systems and components have been developed internally or by a third party. They include the routine servicing and periodic modification of everything needed for a system or component to run correctly including the network, hardware, system software, databases, and the related documentation. An entity's maintenance policies and procedures should include maintenance roles and responsibilities (which may include third-party roles and responsibilities), maintenance access policy (internal and remote), and maintenance monitoring and auditing mechanisms."

KEYS

24

THE SDLC | DISPOSE

1

End-of-Life / End-of-Support

(Examples: Windows 10 EOS, Post-Quantum Cryptography, FFIEC CAT Sunset)

2

Termination & Disposal

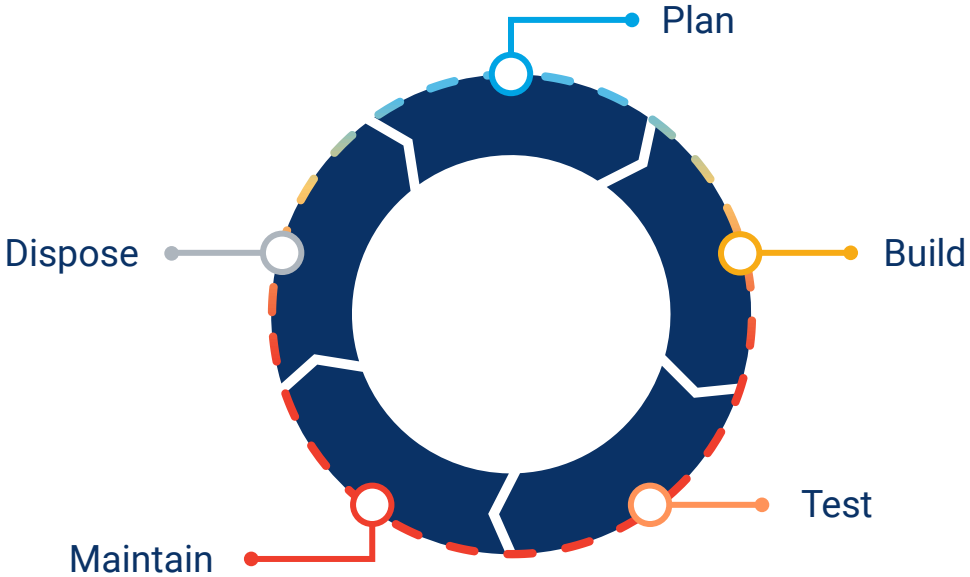
(Example: Morgan Stanley Hard Drives Disposal)

"When a system or component becomes obsolete, is no longer supported, no longer meets the users' or entity's needs, or becomes too costly to maintain, management may decide to terminate its use and dispose of the system or component. Effective management has appropriate termination and off-boarding procedures. The procedures should identify who has the responsibility to decide whether to terminate a vendor relationship, as well as an approval and acknowledgment process in which contracted parties agree to the relationship termination."

KEYS

25

SYSTEM DEVELOPMENT LIFECYCLE (SDLC)



KEYS

26

If developers work for your organization, they need to have and follow a written system development life cycle (SDLC).

KEYS

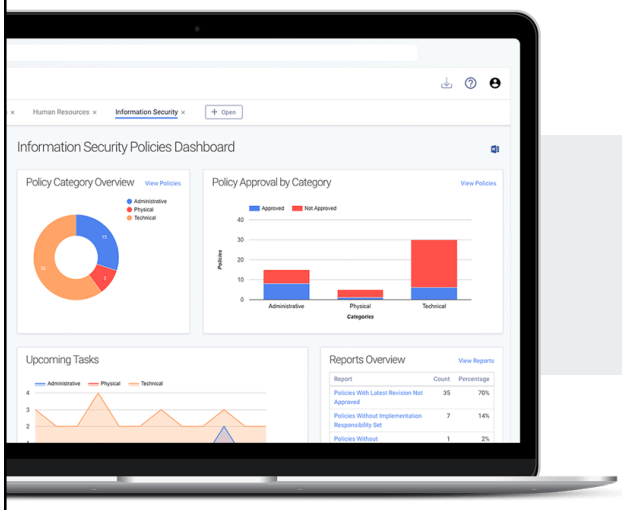
27

DISCUSSION TOPIC

Do you have a formal SDLC?
What areas would you say are strongest or that need to be improved?

KEYS

28



KEYS

Tandem Policies Software

29

Integrated Components

KEYS

30

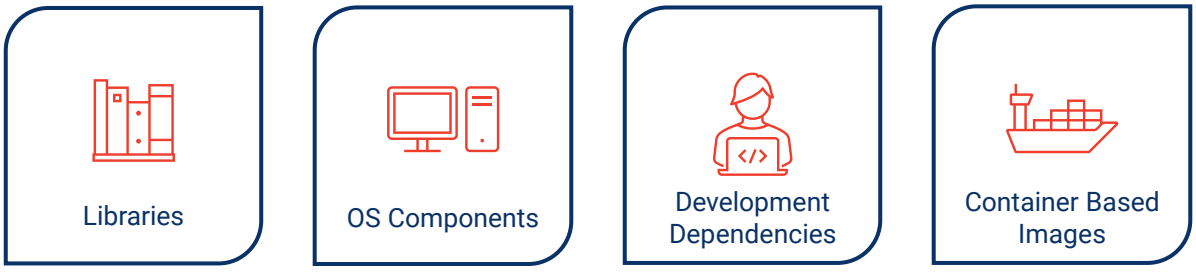
INTEGRATED COMPONENTS

- Open-Source Components
- Application Programming Interfaces
- Development Tools

KEYS

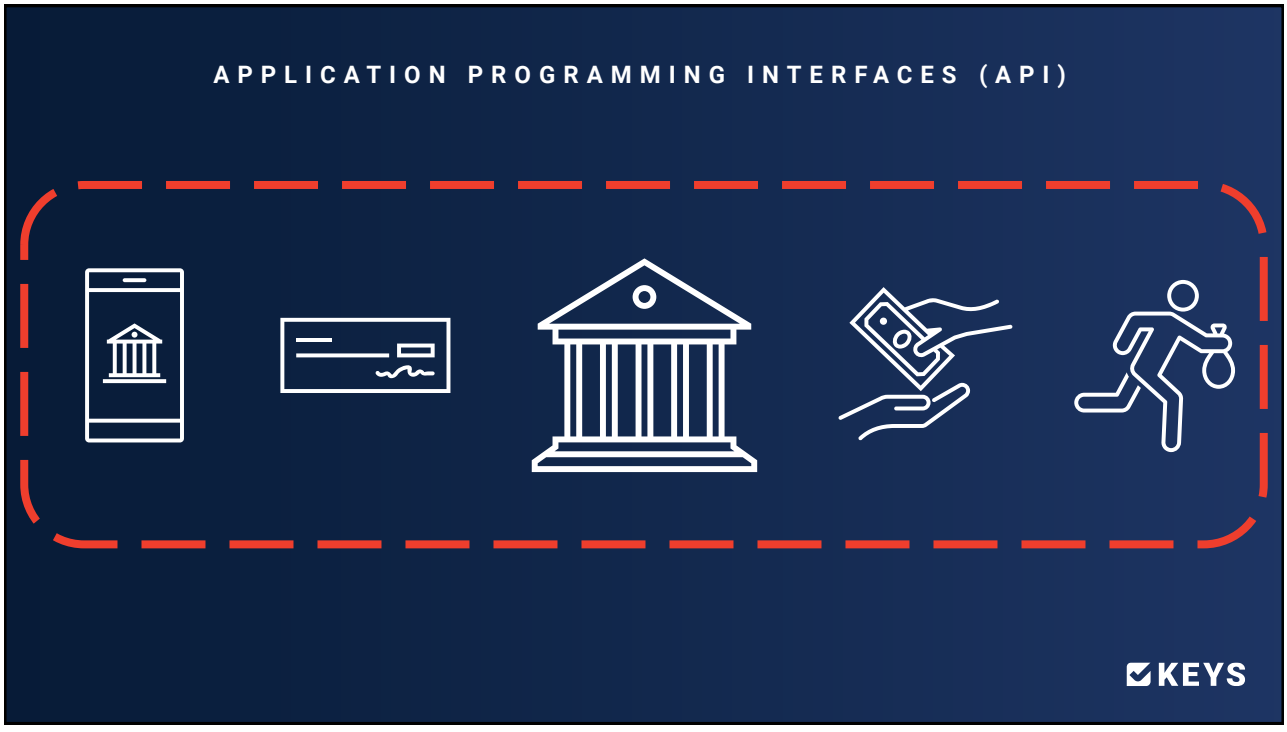
31

OPEN-SOURCE COMPONENTS

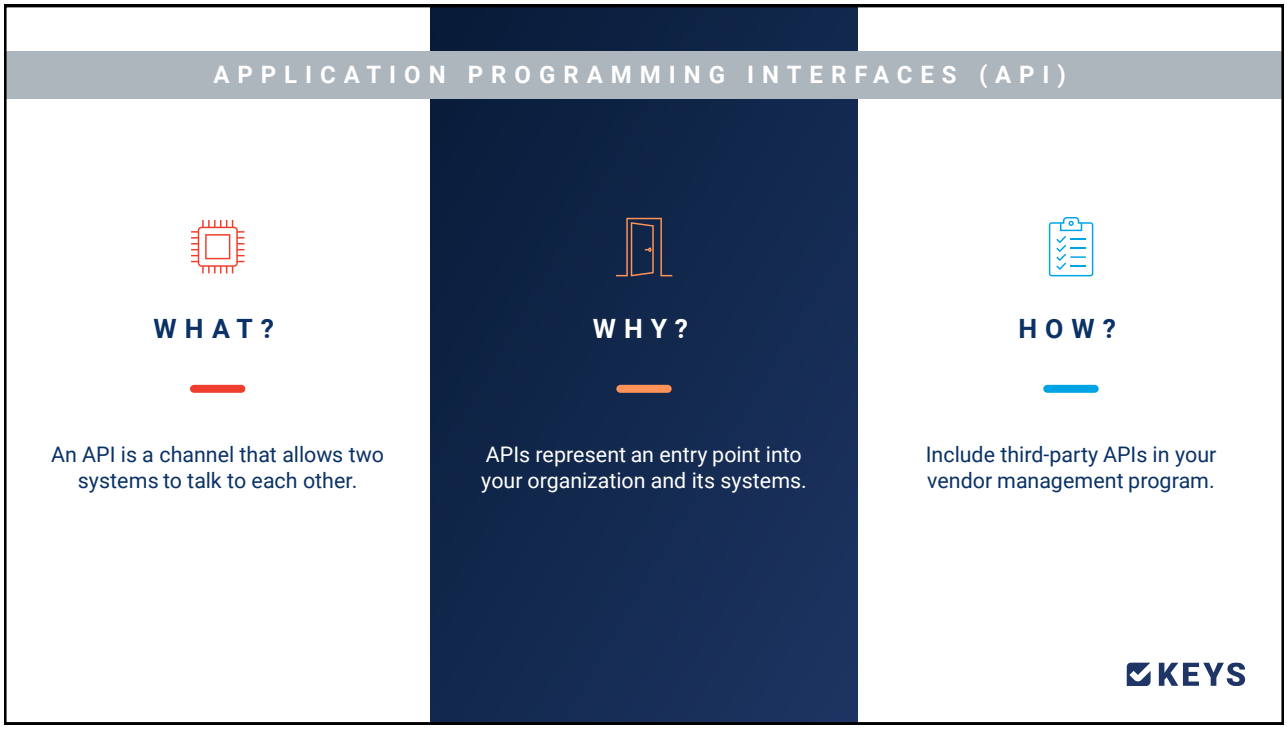


KEYS

32


APPLICATION PROGRAMMING INTERFACES (API)
KEYS

33


APPLICATION PROGRAMMING INTERFACES (API)
WHAT?
An API is a channel that allows two systems to talk to each other.
WHY?
APIs represent an entry point into your organization and its systems.
HOW?
Include third-party APIs in your vendor management program.
KEYS

34

First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records

May 24, 2019

The Web site for Fortune 500 real estate title insurance giant **First American Financial Corp.** [NYSE:FAF] leaked hundreds of millions of documents related to mortgage deals going back to 2003, until notified this week by KrebsOnSecurity. The digitized records — including bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers license images — were available without authentication to anyone with a Web browser.

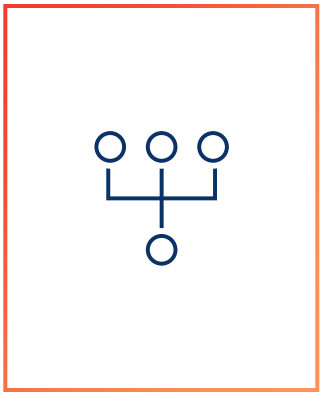
First American Financial Corp. Image: Linkedin.

https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

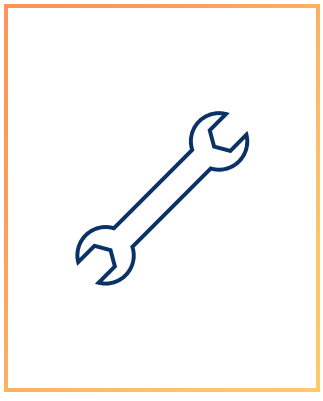
KEYS

35

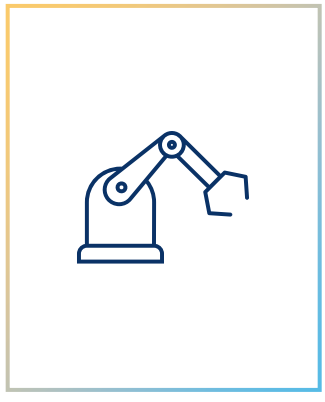
DEVELOPMENT TOOLS



Code Repositories



CI/CD Pipelines



AI Coding Assistants

KEYS

36

KEY TAKEAWAY

If components are accessing your data, then you need to treat them with the same level of review as you'd apply to a developer.

KEYS

37

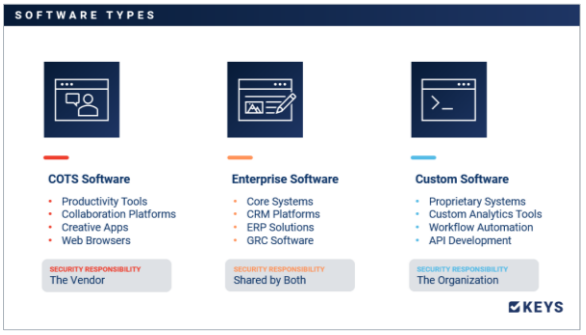
Third-Party Risk Management

KEYS

38

KEYS

Buy
(Acquire)



Build
(Develop)

39

KEYS

Buy
(Acquire)

🤔 Do I trust this software or not?

CONTRACTS	DUE DILIGENCE
• Terms of Service	• SOC Reports
• Terms of Use	• Privacy Policies
• User Agreements (EULA)	• Certifications
	• Market Adoption

40

TECHNOLOGY

Nebraska bank to settle MoveIt data breach for $2.4M

By Carter Pape

Published March 17, 2026, 5:14 p.m. EDT | Updated March 17, 2026, 5:14 p.m. EDT 5 Min Read

Aftermath of a breach

204,291
PEOPLE AFFECTED
Union Bank & Trust data breach

$2.4 million
SETTLEMENT AMOUNT
Preliminary class action agreement

Source: Court Filings

Visualization created with AI assistance based on original reporting

https://www.americanbanker.com/news/nebraska-bank-to-settle-moveit-data-breach-for-2-4m

KEYS

41

💛 **The Golden {Vendor} Rule**
Treat your vendors the way you would treat your own organization.

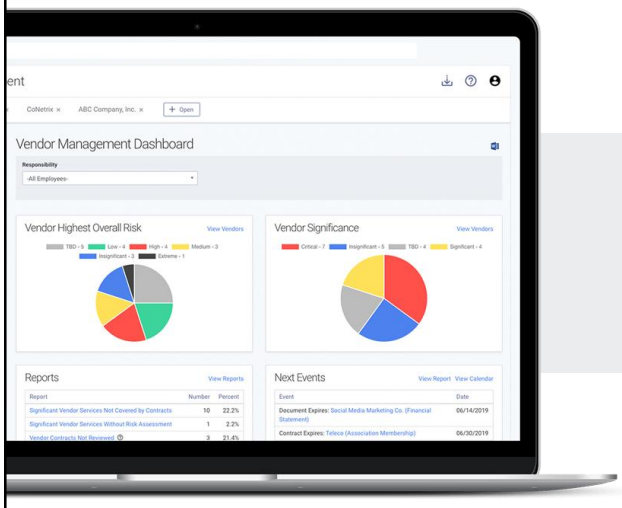
CONTRACTS	DUE DILIGENCE
• Intellectual Property	• SOC Report
• Service Level Agreement	• Privacy Policies
• Termination Contingency	• SDLC Documentation
• Escrow Agreement	• Vendor Management

KEYS

Build
(Develop)

42

KEYS



Tandem Vendor Management Software

43

The Impact of Artificial Intelligence

KEYS

44

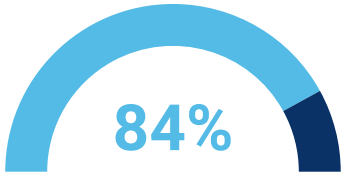
"We are only limited by our imaginations. And our tokens."

Aaron Hebert

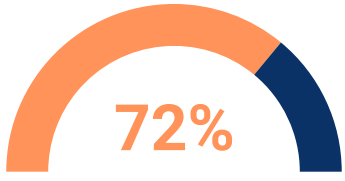
KEYS

45

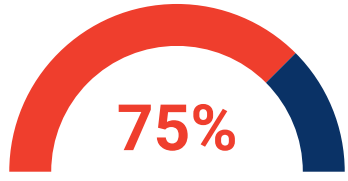
DEVELOPER SURVEY RESULTS



Developers who report using or planning to use AI in development



Developers who report not using AI to "vibe" code



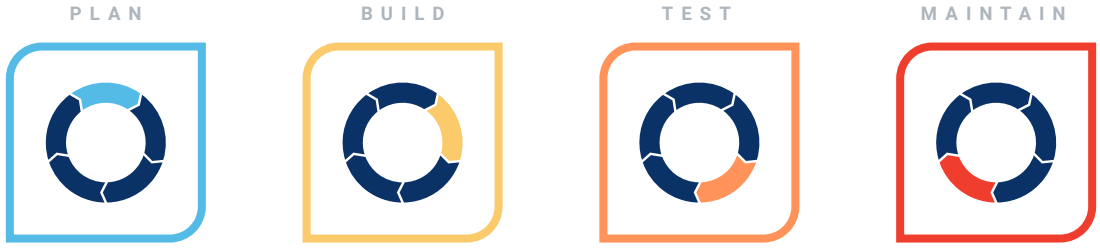
Developers who say "When I don't trust AI's answers" is the top reason for involving human developers

SOURCE: Stack Overflow 2025 Developer Survey

KEYS

46

HOW AI IS IMPACTING SOFTWARE DEVELOPMENT



KEYS

47

FEATURE DESIGN

DEVELOPING SPECIFICATIONS

Translate business requirements into a draft specification, user stories or a data model.

Oversight is your control

BREAKING TASKS APART

Deconstruct large features into distinct development tasks via an implementation plan, before a developer writes any code.

Set your expectations

ASSIGNING TECHNICAL DEBT

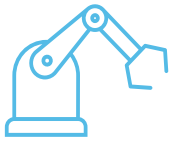
Documenting and addressing maintenance tasks, so that changes may be easily addressed.

AI-generated = Tech Debt

KEYS

48

CODE AUTHORING



AI Coding Agents

Authoring ➡️ Directing

Repeatable Workflows

🚀 Boost Productivity

Documentation

🤔 What does the code do?

KEYS

49

CODE REVIEW

Reviewing Incoming Changes

Finding Vulnerabilities

Following Best Practices

🏅 Code review is a **quality** gate.

KEYS

50

BUG DETECTION

- How quickly will we find it?
- How thoroughly do we understand it?
- How confidently can we fix it?

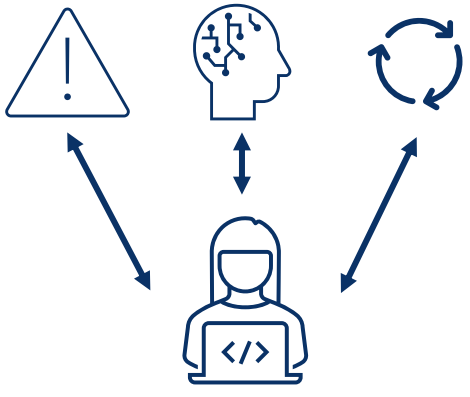
KEYS

51

BUG DETECTION

"How did we get here?"

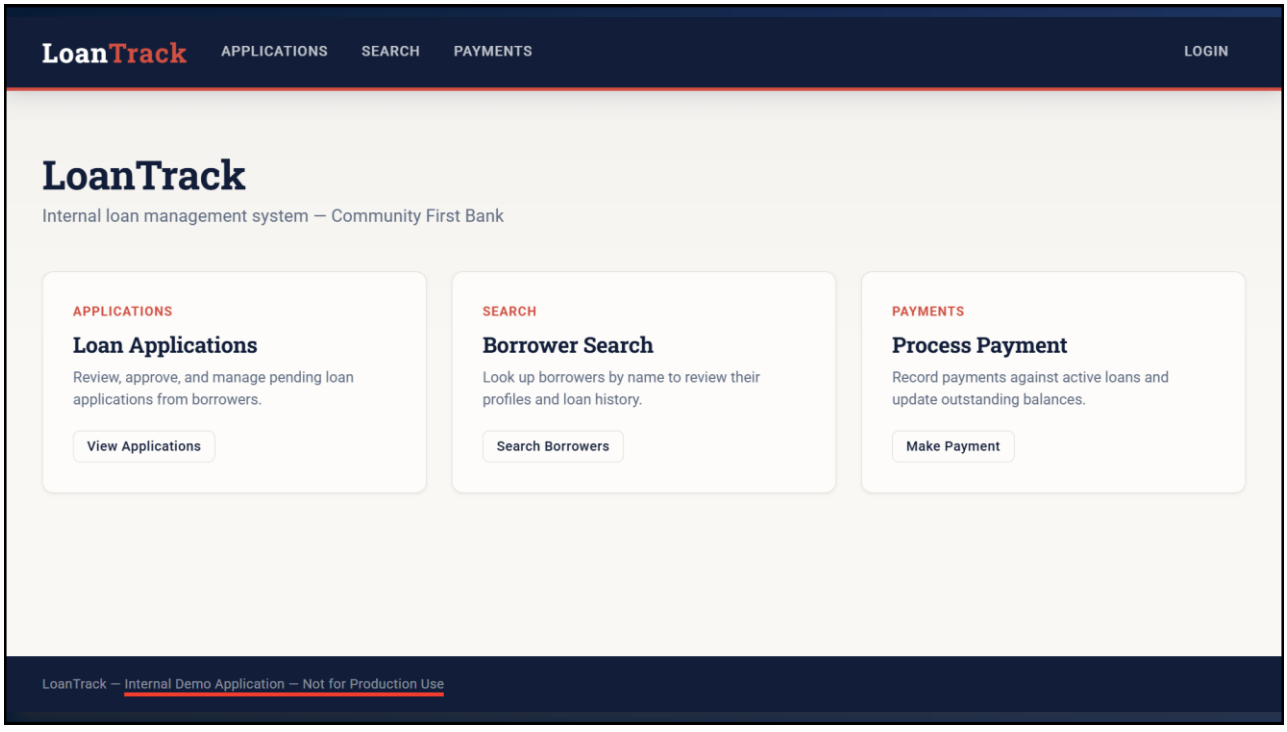
"Find the bug."



Model Context Protocols

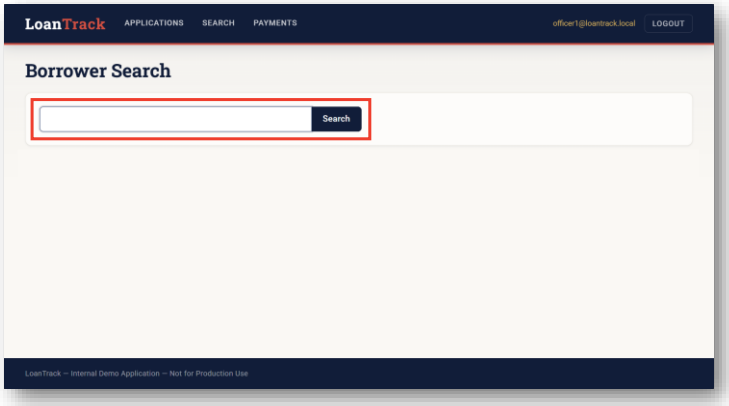
KEYS

52



53

AI RISK | SQL INJECTION




```
SELECT *
FROM Borrowers
WHERE FullName LIKE '%" + name + "%'
```

An attacker enters a crafted search term and retrieves every customer record in the database, bypassing all authorization.

The borrower search function does not use parameterized queries. User-supplied input is concatenated directly into the database query string, creating an SQL injection vulnerability that could allow unauthorized access to all customer records.

KEYS

54

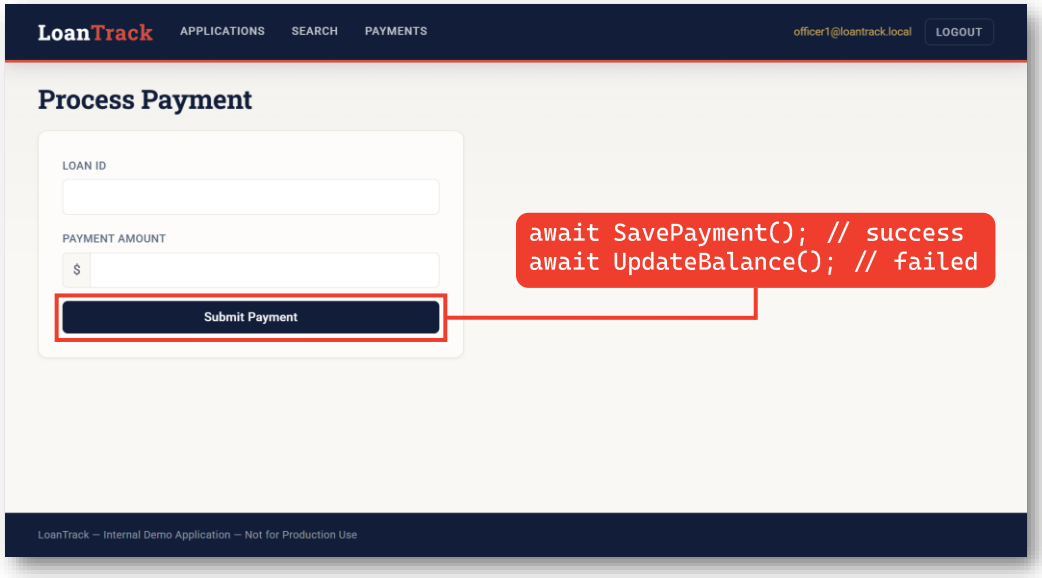
AI RISK | HARDCODED CREDENTIALS

```
"Server=prod-db.bank.internal; User Id=sa; Password=BankAdmin2026!"
```

KEYS

55

AI RISK | NON-ATOMIC PROCESSING



KEYS

56

DEVELOPER PROMPT	EXPLOIT
"Write a query to look up a borrower by name."	An attacker enters a modified search term and retrieves every customer record in the database, bypassing all authentication.
"Write a method to connect to the bank's database."	Every developer, contractor, or auditor with access to the source code repository can read the production database password.
"Write a method to process a loan payment and update the balance."	A payment is recorded as received, but the loan balance is never reduced. The customer is charged; the bank's records don't reflect it.

KEYS

57

ARTIFICIAL INTELLIGENCE | RISKS

KEYS

Data Exposure & Confidentiality

Attribution Gaps

Skill Erosion

Regulatory Blind Spots

58

ARTIFICIAL INTELLIGENCE | CONTROLS

SAY NO TO PROD

Development tools stay in development.

SAY NO TO PII

✅ Production Code
❌ Production Data

FILL THE GAP

What does secure development look like in our environment?

KEYS

59

"Although AI agents are advancing rapidly, human expertise remains essential in software development. Programming is not software engineering. Even the most reliable systems cannot fully replace the judgment, creativity, and adaptability required to handle uncertainty, make complex decisions, and maintain security."

RUSSINOVICH AND HANSELMAN

https://dl.acm.org/doi/10.1145/3779312

KEYS

60

SESSION RECAP

1. Five Factors for Secure Software Development
2. The System Development Lifecycle (SDLC)
3. Integrated Components
4. Third-Party Risk Management
5. The Impact of Artificial Intelligence

KEYS

61

KEYS

62

Fill out the survey to get your sticker!

KEYS

63

Thank You!

CONNECT WITH OUR SPEAKERS AT TANDEM.APP/AGENDA

KEYS

64