

Overcoming the Compliance Challenges of AppSec

Why you need automated compliance reporting and real-time visibility with Legit Security's ASPM platform



require proof of cybersecurity as part of their RFPs, showing that security posture reporting is for more than just regulatory compliance.

Nearly half of all companies now

just a headache for CISOs

Compliance challenges are more than



Security incidents are

three times more expensive for noncompliant companies

Half of all companies spend as much as 10%

of revenue on compliance costs



CISOs from all industries report spending up to

40% of their time on compliance reporting

Companies say their

analysts spend at least half of their time on lowlevel admin tasks

Compliance is difficult and growing



Over 4/5 of organizations lack automated

processes for reporting and IT risk data collection

Nearly 2/3 of orgs report difficulty automating due to apps changing with

every release

in complexity Below are several examples of common AppSec requirements

Software Delivery **Application Security**

systems and applications

PCI DSS - Requirement 6: Develop and maintain secure

- NIST SP 800-53: SA-11 -Developer Security Testing and Evaluation
- protection by design and by default, and Security of processing

GDPR - Articles 25 and 32: Data

- **GLBA** Not explicitly stated SOX - Section 404: Assessment of Internal Control
- HIPAA §164.306(a): Security standards: General rules
- Vulnerability

PCI DSS - Requirement 6: Develop and maintain secure

systems and applications

NIST - SP 800-53: RA-5: Vulnerability Scanning

Management

processing GLBA - 501(b): Assess and identify vulnerabilities in

GDPR - Article 32: Security of

SOX - Section 404: Assessment of Internal Control

HIPAA - §164.308(a)(1): Risk analysis and management

information systems

Practices PCI DSS - Requirement 6: Develop and maintain secure

systems and applications

Secure Development

- Evaluation
- HIPAA §164.306(a): Security standards: General rules
- cardholder data NIST - SP 800-53: AC-6: Audit Trail

network resources and

and monitor all access to

for unauthorized access

of Internal Control

SOX - Section 404: Assessment

controls

HIPAA - §164.312(b): Audit

- **NIST** SP 800-53: SA-11: Developer Security Testing and
 - GDPR Articles 25 and 32: Data protection by design and by

default, and Security of

processing

Audit Trails

PCI DSS - Requirement 10: Track

GLBA - Not explicitly stated SOX - Section 404: Assessment

of Internal Control

processing activities GLBA - 501(b): Monitor systems

GDPR - Article 30: Records of

processing

GDPR - Article 32: Security of

NIST - SP 800-53: CM-7: Configuration Change Control

PCI DSS - Not explicitly stated

- GLBA Not explicitly stated
- SOX Section 404: Assessment of Internal Control **HIPAA** - Not explicitly stated

Risk Management

PCI DSS - Requirement 12: Establish, maintain, and follow an

NIST - SP 800-53: RM-3: Risk

incident response plan

- Assessment GDPR - Articles 24 and 32: Responsibility of the controller,
- management program SOX - Section 404: Assessment

of Internal Control

GLBA - 501(b): Implement a risk

and Security of processing

- HIPAA §164.308(a)(1): Risk analysis and management
- **Regular Security** Testing

PCI DSS - Not explicitly stated

GDPR - Article 32: Security of

GLBA - Not explicitly stated

NIST - SP 800-53: CM-7: **Configuration Change Control**

SOX - Section 404: Assessment of Internal Control **HIPAA** - Not explicitly stated

processing

PCI DSS - Requirement 7: Restrict access to cardholder

data by business need to know

Access Controls

NIST - SP 800-53: AC-2: Account Management

personal data

Reports

controls

GLBA - 501(b): Limit access to customer information

> SOX - Section 302: Corporate Responsibility for Financial

HIPAA - §164.312(a)(1): Access

GDPR - Article 5: Principles

relating to the processing of



faster remediation

Continuous Scanning Real-time issue alerting and prioritization for

discovery, centralized data,

application security processes

Simplification Visibility Easy implementation, auto Deep visibility and context

and automated processes runtime deployment



AppSec security guidance and development

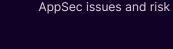
deviation monitoring

Security Guardrails

from code creation to

Legit Security delivers tangible

benefits for compliance-related



Demonstrability Easy to use reporting and dashboards for

real time reporting

Single Pane of Glass

A one-stop shop for

managing all your



Management from Code to Cloud

Book a Demo



www.legitsecurity.com www.linkedin.com/company/legitsecurity

Connect With Us



www.youtube.com/@legitsecurity

- 100+ Compliance Statistics You Should Know in 2023 How Al Will Transform Compliance for Banks and
- © Copyright 2023 Legit Security