Overcoming the Compliance Challenges of AppSec

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

44% Nearly half of all companies now require proof of cybersecurity as part of their RFPs, showing that security posture reporting is for more than just regulatory compliance.

Compliance challenges are more than just a headache for CISOs

Expensive

3x

Security incidents are three times more expensive for non-compliant companies

6-10%

Half of all companies spend as much as 10% of revenue on compliance costs

Time Consuming

40%

CISOs from all industries report spending up to 40% of their time on compliance reporting

50%

Companies say their analysts spend at least half of their time on low-level admin tasks

Inefficient

82%

Over 4/5 of organizations lack automated processes for reporting and IT risk data collection

61%

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

Compliance is difficult and growing in complexity

Below are several examples of common AppSec requirements

Application Security

- **PCI DSS** - Requirement 6: Develop and maintain secure systems and applications
- **NIST** - SP 800-53: SA-11 - Developer Security Testing and Evaluation
- **GDPR** - Articles 25 and 32: Data protection by design and by default, and Security of processing
- **GLBA** - Not explicitly stated
- **SOX** - Section 404: Assessment of Internal Control
- **HIPAA** - §164.306(a): Security standards: General rules

Vulnerability Management

- **PCI DSS** - Requirement 6: Develop and maintain secure systems and applications
- **NIST** - SP 800-53: RA-5: Vulnerability Scanning
- **GDPR** - Article 32: Security of processing
- **GLBA** - 501(b): Assess and identify vulnerabilities in information systems
- **SOX** - Section 404: Assessment of Internal Control
- **HIPAA** - §164.308(a)(1): Risk analysis and management

Secure Development Practices

- **PCI DSS** - Requirement 6: Develop and maintain secure systems and applications
- **NIST** - SP 800-53: SA-11: Developer Security Testing and Evaluation
- **GDPR** - Articles 25 and 32: Data protection by design and by default, and Security of processing
- **GLBA** - Not explicitly stated
- **SOX** - Section 404: Assessment of Internal Control
- **HIPAA** - §164.306(a): Security standards: General rules

Audit Trails

- **PCI DSS** - Requirement 10: Track and monitor all access to network resources and cardholder data
- **NIST** - SP 800-53: AC-6: Audit Trail
- **GDPR** - Article 30: Records of processing activities
- **GLBA** - 501(b): Monitor systems for unauthorized access
- **SOX** - Section 404: Assessment of Internal Control
- **HIPAA** - §164.312(b): Audit controls

Software Delivery

- **PCI DSS** - Not explicitly stated
- **NIST** - SP 800-53: CM-7: Configuration Change Control
- **GDPR** - Article 32: Security of processing
- **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 incident response plan
- **NIST** - SP 800-53: RM-3: Risk Assessment
- **GDPR** - Articles 24 and 32: Responsibility of the controller, and Security of processing
- **GLBA** - 501(b): Implement a risk management program
- **SOX** - Section 404: Assessment of Internal Control
- **HIPAA** - §164.308(a)(1): Risk analysis and management

Regular Security Testing

- **PCI DSS** - Not explicitly stated
- **NIST** - SP 800-53: CM-7: Configuration Change Control
- **GDPR** - Article 32: Security of processing
- **GLBA** - Not explicitly stated
- **SOX** - Section 404: Assessment of Internal Control
- **HIPAA** - Not explicitly stated

Access Controls

- **PCI DSS** - Requirement 7: Restrict access to cardholder data by business need to know
- **NIST** - SP 800-53: AC-2: Account Management
- **GDPR** - Article 5: Principles relating to the processing of personal data
- **GLBA** - 501(b): Limit access to customer information
- **SOX** - Section 302: Corporate Responsibility for Financial Reports
- **HIPAA** - §164.312(a)(1): Access controls

Legit Security delivers tangible benefits for compliance-related application security processes

Simplification

Easy implementation, auto discovery, centralized data, and automated processes

Visibility

Deep visibility and context from code creation to runtime deployment

Single Pane of Glass

A one-stop shop for managing all your AppSec issues and risk

Continuous Scanning

Real-time issue alerting and prioritization for faster remediation

Security Guardrails

AppSec security guidance and development deviation monitoring

Demonstrability

Easy to use reporting and dashboards for real time reporting

LEGIT SECURITY

Application Security Posture Management from Code to Cloud

Book a Demo

Connect With Us

www.legitsecurity.com

www.linkedin.com/company/legitsecurity

www.youtube.com/@legitsecurity

SOURCES:

- The True Cost of Compliance with Data Protection Regulations
- 100+ Compliance Statistics You Should Know in 2023
- How Regulatory Compliance Helps Your Bottom Line
- 70 Compliance Statistics to Know in 2022
- 10 Cybersecurity Compliance Statistics That Show Why You Must Up Your Cybersecurity Game
- How AI Will Transform Compliance for Banks and Financial Institutions
- Cyber Risk Institute 2018