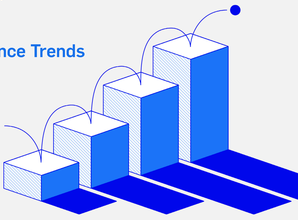
securitymetrics

2025

PCI Compliance Trends



How Does Your Organization Rank?

2024 SecurityMetrics Customer Trends

73.4%
of SecurityMetrics customers that started their SAQ have achieved a passing status

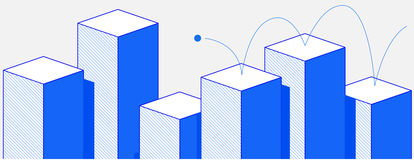
1.03 times
Average number of support incidents before customers became compliant

7.8 days
Average time from finished first scan to first passing scan

19.5 days
Average time to reach PCI DSS compliance

75.8%
percent of SecurityMetrics customers that passed their first scan

1.3 scans
Average number of times scanned until merchants pass their PCI scan



Top 10 Failing SAQ Sections

We reviewed our merchant database in search of the top 10 areas where organizations struggle to become compliant. Starting with the least adopted requirement, these are the results:

1. **Security Policy** (Requirement 12.1.1)
   Establish, publish, maintain, and disseminate a security policy.
2. **Monitor Providers** (Requirement 12.8.4)
   Monitor third-party service providers' (TPSP) PCI DSS compliance status at least once every 12 months.
3. **Service Provider** (Requirement 12.8.5)
   Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
4. **Written Agreement** (Requirement 12.8.2)
   Written agreements with all TPSPs are maintained with which account data is shared or that could affect the security of the CDE.
5. **Due Diligence** (Requirement 12.8.3)
   An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.
6. **Provider List** (Requirement 12.8.1)
   A list of all TPSPs with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.
7. **Incident Response** (Requirement 12.10.1)
   An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident.
8. **Response Testing** (Requirement 12.10.2)
   The security incident response plan is reviewed, updated, and tested at least annually.
9. **Incident Personnel** (Requirement 12.10.3)
   Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.
10. **Evolving Response** (Requirement 12.10.6)
    The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.

Top 5 Failed Vulnerabilities

1

TLS Version 1.0 Protocol Detection
Exists if the remote service accepts connections using TLS 1.0 encryption

2

SSL Self-Signed Certificate
Occurs when organizations use an identity certificate that they create, sign, and certify rather than a trusted certificate authority (CA)

3

TLS Version 1.1 Protocol Detection
Exists if the remote service accepts connections using TLS 1.1 encryption

4

SSL 64-Bit Block Size Cipher Suites Supported (Sweet32)
Exists if a remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites

5

TLS Version 1.1 Protocol Deprecated
Exists if the remote service accepts connections using TLS 1.1 encryption, which should be deprecated

Learn more about PCI compliance

Download our Guide to PCI Compliance.

Download