



Digital Payment Platform Security Evaluation

Security is a standard expectation for any vendor handling sensitive financial data on your behalf. Use this checklist to evaluate your current digital billing and payment platform or arm yourself with the right questions when vetting a new solution. A trustworthy vendor will welcome every one of these.

Platform Architecture & Infrastructure

- True SaaS Model**
Is the platform delivered as true SaaS — continuous updates, no manual upgrades, always on the latest version?
- Multi-Tenant Infrastructure**
Does the architecture isolate client data in individually partitioned databases while running on a shared, monitored environment?

Authentication & Identity Management

- Native Multi-Factor Authentication (MFA)**
Is MFA built into the platform — or do you need to bolt on a third-party tool?
- Standards-Based Single Sign-On (SSO)**
Do they support SAML and OIDC? These are the enterprise standards you need for compatibility with your existing identity infrastructure.
- Deterministic Identity Matching**
Can the platform match users definitively via SSO ID to prevent duplicate accounts or identity confusion?
- Just-In-Time (JIT) Provisioning**
Is user account creation automated on first login — no manual onboarding required?
- No Additional Identity Platforms Required**
Can they deliver all of the above without adding vendor complexity to your stack?

PCI Compliance & Certifications

- PCI DSS Level 1 Service Provider**
Do they hold Level 1 certification — the highest tier? Can they provide documentation?
- Annual Security Certifications**
Do they maintain SOC 1 and SOC 2 Type 2 certifications, verified by an independent auditing firm?
- Regular Security Assessments**
Does the vendor conduct and document ongoing internal and third-party security testing per PCI-DSS requirements?

Compliance, Transparency & Trust

- Trust Center Presence**
Is there a Trust Center that's actively maintained and up to date?
- Data Center Security**
Where is data stored? How is it protected — both physically and logically?
- Data Privacy Policy**
Do they maintain audit logs and offer clear language confirming they don't sell customer data to third parties?
- Accessibility Compliance**
Are they WCAG 2.1 AA compliant? Do they meet ADA Title II requirements — including payment flows?

Quick Readiness Checklist



QUESTION	PAYMENT PLATFORM
SaaS model with no manual upgrades?	<input type="checkbox"/>
MFA built in natively?	<input type="checkbox"/>
SSO via SAML and OIDC supported?	<input type="checkbox"/>
Deterministic identity matching in place?	<input type="checkbox"/>
PCI DSS Level 1 Service Provider certification?	<input type="checkbox"/>
SOC 2 Type 2 certification current?	<input type="checkbox"/>
Trust Center available upon request?	<input type="checkbox"/>
WCAG 2.1 AA / ADA compliant?	<input type="checkbox"/>
Data privacy policy reviewed?	<input type="checkbox"/>
Monitoring & re-validation schedule set?	<input type="checkbox"/>

Want to see how InvoiceCloud approaches security?

Request a demo at invoicecloud.net.

