ONSEC

WHAT REGULATORS SEE WHEN THEY AUDIT YOUR FINTECH

The Examination Perspective

The Regulatory Reality

Your fintech operates in one of the most regulated industries on earth.

Whether you're a neobank, payment processor, lender, or wealth platform, regulators have authority over your security.

ONSEC

What Examiners Request:

Regulator	Focus Area
OCC	National banks, federal savings
FDIC	State banks, deposit insurance
Federal Reserve	Bank holding companies
CFPB	Consumer financial products
State regulators	Money transmission, lending
SEC	Securities, investment advisers
FINRA	Broker-dealers
FinCEN	AML/BSA compliance
Examination Trigger	Likelihood
Routine examination cycle	High (scheduled)
Consumer complaints	Medium-High
Suspicious activity	High
News of incident	Very High
Sponsor bank examination	High

- Governance Documentation
- Board minutes discussing security
- Security policies and procedures
- Risk assessment documentation
- Organizational charts
- Technical Evidence
- Penetration test reports
- Vulnerability scan results
- Incident response records
- Change management logs
- Compliance Artifacts
- SOC 2 reports
- PCI compliance documentation
- Third-party assessments
- Audit findings and remediation
- Operational Records
- Security training records
- Access control documentation

- Encryption implementation
- Backup and recovery tests

Beyond Checkboxes:

Domain	Key Requirements	
Governance	Board oversight, risk management	
Access Controls	Authentication, authorization	
Data Security	Encryption, classification	
Incident Response	Detection, response, recovery	
Business Continuity	Disaster recovery, resilience	
Vendor Management	Third-party oversight	
Audit	Independent assessment	
Common Finding	Frequency	
Inadequate vendor oversight	Very Common	
Weak access controls	Very Common	
Missing/outdated policies	Common	
Insufficient board reporting	Common	
Poor incident response	Common	
Inadequate encryption	Moderate	
Missing penetration tests	Moderate	
Rating	Meaning	Response Required
Observation	Minor issue	Addressed in normal course
MRA	Significant concern	Formal response and timeline
MRIA	Immediate risk	Urgent action required

- Board Engagement
- Do directors understand security risks?
- Is there meaningful oversight?
- Are resources adequate?
- Culture
- Is security embedded or bolted on?
- Do employees understand their role?
- Is there a speak-up culture?
- Follow-Through
- Are audit findings remediated?
- Do pentests lead to fixes?
- Is there continuous improvement?
- Reality vs. Documentation
- Do practices match policies?
- Are controls actually operating?
- Can staff explain their roles?

If You Use a Sponsor Bank:

Their regulators examine them. Their examination includes you.

What This Means:

- Your security affects their rating
- They have contractual rights to audit you
- They can terminate for security failures
- Regulatory pressure flows through

Pre-Examination:

Activity	Frequency
Policy review and update	Annual
Penetration testing	Annual minimum
Risk assessment	Annual
Board security briefing	Quarterly
Incident response test	Annual
Vendor assessment	Annual
Access review	Quarterly

- Document request list
- Scope communication
- Scheduling

On-Site/Remote:

- Document review
- Staff interviews
- System demonstrations
- Testing and sampling

Post-Examination:

- Preliminary findings discussion
- Draft report
- Response period
- Final report and ratings

Questions Examiners Will Ask

→ How does the board oversee information security?

→ Describe your incident response process

→ How do you assess and manage vendor risk?

→ What were your last pentest findings and remediation status?

→ How do you ensure employees follow security policies?

→ Describe your access management process

ONSEC's Regulatory Readiness Services

We help fintechs prepare for regulatory scrutiny:

Examination Readiness Assessment

- Gap analysis against FFIEC guidelines
- Documentation review
- Interview preparation

Remediation Support

- Address findings before examination
- Build required documentation
- Implement missing controls

Ongoing Compliance

- Regular security assessments
- Policy maintenance
- Board reporting support

Regulators aren't looking for perfection. They're looking for competence, honesty, and continuous improvement.

Fintechs that take security seriously, document their efforts, and remediate findings fare well. Those that cut corners, hide problems, or treat compliance as checkbox eventually face enforcement.

Know what they're looking for. Be ready.

Key Takeaway:

The examination is coming. The only question is whether you'll be ready.

Prepare like your charter depends on it—because it might.

Sources:

- FFIEC IT Examination Handbook
- OCC Examination Procedures
- FDIC Risk Management Examination Manual
- State Regulatory Examination Guidelines
- ONSEC.io - Razor-Sharp Security for Fintech

About ONSEC

ONSEC is a boutique penetration testing and security assessment team specializing in fintech platforms. We help financial technology companies identify vulnerabilities in payment systems, banking APIs, and customer-facing applications before attackers do—whether the risk is fraud, data exposure, or regulatory non-compliance. Our team has worked with neobanks, payment processors, and lending platforms across multiple jurisdictions. If you'd like to discuss how we can help strengthen your platform, reach out.

Our Services:

- ✓ Penetration Testing — Full-scope security assessments of your platform, APIs, and mobile apps
- ✓ PCI DSS Assessment — Compliance-focused reviews for payment card security
- ✓ Fraud & AML Assessment — Evaluate your defenses against payment fraud and money laundering
- ✓ Incident Response — 24/7 support when security incidents occur
- ✓ Security Architecture Review — Design secure financial systems from the ground up
- ✓ API Security Testing — Deep-dive into Open Banking and payment API vulnerabilities

https://onsec.io • request@onsec.io

ONSEC.io — Razor-Sharp Security for Fintech

Trusted by leading organizations worldwide.