FTC Safeguards Rule Compliance Checklist

The FTC Safeguards Rule underwent significant strengthening in 2021, with most provisions taking effect June 9, 2023, ftc Federal Trade Commission and **mandatory breach notification requirements effective May 13, 2024**. Federal Trade Commission Federal Register This comprehensive checklist covers all 16 required elements for financial institutions under FTC jurisdiction, including mortgage lenders, payday lenders, collection agencies, tax preparers, and other covered entities maintaining customer information. Federal Trade Commission +2

Critical Update: Organizations must now report breaches affecting 500+ consumers to the FTC within 30 days. Federal Trade Commission +4 The rule applies broadly to any entity "significantly engaged in financial activities," ftc with penalties up to $100,000 per violation for institutions and $10,000 for individuals. Federal Trade Commission +3

Oversight & Program Design

1. Qualified Individual Designation ✓

Regulatory Requirement: Appoint a person responsible for overseeing and enforcing the information security program ftc (16 CFR § 314.4(a)) Norton Rose Fulbright +2

Compliance Verification Steps:

□ **Written designation** document clearly identifies the Qualified Individual with specific scope of authority
□ **Job description or charter** details responsibilities including program oversight, enforcement authority, risk management, incident response, board reporting, vendor oversight, testing coordination, and change management approval
□ **Authority verification**: QI has decision-making power over security matters, budget authority or direct resource access, and access to senior management
□ **Competency documentation**: Records show appropriate experience for organization size/complexity (no specific degree required - focus on "real-world know-how") Federal Trade Commission +2
□ **Succession planning** established for QI role continuity
□ **Service provider agreements** if QI is external, including oversight provisions

Documentation Requirements:

- Written appointment with clear authority scope
- Performance evaluation criteria and ongoing training records
- Succession planning documentation

2. Written Risk Assessment ✓

Regulatory Requirement: Conduct and maintain risk assessment addressing foreseeable threats, assessing safeguards, and identifying potential harm ftc (16 CFR § 314.4(b)) Norton Rose Fulbright +2

Compliance Verification Steps:

□ **Written assessment document** includes criteria for evaluating and categorizing security risks and threats ftc

□ **Comprehensive scope**: Covers customer information inventory, information systems assessment, threat landscape analysis (internal and external), vulnerability identification, and impact analysis
□ **Risk evaluation criteria** documented for assessing confidentiality, integrity, and availability of systems and data
□ **Safeguard assessment** evaluates sufficiency of current controls against identified risks
□ **Periodic reassessment schedule** established with triggers for updates (operational changes, new threats, security incidents, vendor changes)
□ **Risk register/inventory** maintained with comprehensive list of identified risks and ratings

Documentation Requirements:

- Written risk assessment methodology and criteria
- Current and historical risk assessment documents
- Risk register with ratings and remediation priorities
- Evidence supporting risk ratings and control effectiveness

3. Written Information Security Program (WISP) ✓

Regulatory Requirement: Develop, implement, and maintain written security program tailored to the business ftc (16 CFR § 314.3 & 314.4) Federal Trade Commission Federal Trade Commission

Compliance Verification Steps:

□ **Comprehensive written program** in readily accessible format covering all nine mandatory elements
□ **Risk-based approach** tailored to organization size, complexity, activities, and information sensitivity
□ **Policy and procedure integration** provides clear implementation guidance for staff
□ **Version control system** tracks updates and changes over time with controlled distribution
□ **Formal update procedures** based on testing/monitoring results, operational changes, business arrangement modifications, and risk assessment findings
□ **Integration verification**: Program coordinates with risk assessment, QI oversight, business processes, employee training, vendor management, and incident response

Documentation Requirements:

- Written program covering all nine elements with actionable procedures
- Change management process with QI approval workflow
- Program effectiveness monitoring and continuous improvement procedures

Technical Safeguards

4. Access Controls ✓

Regulatory Requirement: Implement controls to authenticate and limit access to customer information ftc (16 CFR § 314.4(c)(1)) eCFR

Compliance Verification Steps:

□ **Authentication systems** verify identity before granting access using appropriate factors (knowledge, possession, inherence)

□ **Authorization controls** implement role-based access aligned with job functions and principle of least privilege
□ **Regular access reviews** conducted with documented approval and immediate revocation upon role changes/termination
□ **Physical controls** restrict facility access with key cards, locked doors, or equivalent barriers plus access logging
□ **Customer access controls** limit customers to their own information only
□ **Alternative control approvals** documented in writing by Qualified Individual if deviating from standard requirements

Documentation Requirements:

- Written access control policies and procedures
- Access control matrix mapping users to authorized data/systems
- Regular access review reports with approvals

5. Inventory & Classification ✓

Regulatory Requirement: Maintain complete inventory of customer data, storage locations, and access points (ftc) (16 CFR § 314.4(c)(2)) (eCFR) (VC3)

Compliance Verification Steps:

□ **Complete data inventory** covers all customer information locations (collection, storage, transmission points)
□ **System inventory** includes all information systems, connected systems, devices, platforms, and personnel with access
□ **Data flow mapping** shows how information moves through the organization
□ **Classification system** assigns sensitivity levels and handling requirements based on regulatory requirements
□ **Asset management** provides unique identification, owner assignment, and responsibility documentation for all devices/systems
□ **Regular updates** reflect system changes and integrate with change management processes

Documentation Requirements:

- Written data inventory and classification policy
- Current asset register with classification levels and ownership
- Data flow diagrams and regular inventory update procedures

6. Encryption ✓

Regulatory Requirement: Encrypt customer data both in transit and at rest, or use effective alternative controls (ftc) (16 CFR § 314.4(c)(3)) (eCFR +2)

Compliance Verification Steps:

□ **Data in transit encryption** for all customer information transmitted over external networks using current cryptographic standards (TLS 1.2 or higher)
□ **Data at rest encryption** for all stored customer information using database-level, file-level, or full-disk encryption

□ **Key management** implements secure generation, storage, distribution, regular rotation, separation from encrypted data, and recovery procedures
□ **Current cryptographic standards** verified and maintained consistent with industry best practices
□ **Alternative controls** documented with written approval from Qualified Individual showing equivalent or superior protection
□ **Regular testing** validates encryption effectiveness and proper key protection

Documentation Requirements:

- Written encryption policy and key management procedures
- Documentation of approved alternative controls with technical rationale
- Encryption implementation standards and testing results

7. Secure Development Practices ✓

Regulatory Requirement: Adopt secure practices for systems, applications, and databases handling customer information (ftc) (16 CFR § 314.4(c)(4)) (Bradley +2)

Compliance Verification Steps:

□ **Secure development lifecycle (SDLC)** implements security throughout development with threat modeling, secure coding standards, code review, and security testing
□ **Third-party application assessment** includes security questionnaires, vendor certifications, vulnerability assessments, and patch management review
□ **Database protection** covers access controls, data encryption, activity monitoring, security updates, and backup security
□ **Security testing integration** includes DAST, SAST, IAST where applicable, and penetration testing for applications handling customer information
□ **Development security controls** address input validation, output encoding, authentication/authorization mechanisms, and error handling/logging

Documentation Requirements:

- SDLC procedures with security requirements and design documentation
- Application security testing reports and third-party assessment results

8. Multi-Factor Authentication (MFA) ✓

Regulatory Requirement: Require MFA for anyone accessing customer data systems (ftc) (16 CFR § 314.4(c)(5)) (Federal Trade Commission +3)

Compliance Verification Steps:

□ **Universal MFA implementation** covers all individuals accessing information systems (employees, contractors, customers)
□ **Authentication factors** verify at least two of: knowledge (passwords), possession (tokens/devices), inherence (biometrics) (Federal Trade Commission) (ftc)
□ **System coverage** includes all information systems containing or connected to customer information
□ **Current secure technologies** prioritize phishing-resistant methods (hardware security keys, biometrics, certificates) over less secure options (SMS, push notifications)

□ **Alternative controls** documented with written approval from Qualified Individual showing equivalent or superior security
□ **Regular testing** validates MFA implementation effectiveness and bypass procedures

Documentation Requirements:

- MFA policy and implementation procedures
- Alternative control approvals with technical justification
- User training materials and deployment coverage reports

9. Monitoring & Logging ✓

Regulatory Requirement: Implement monitoring systems to detect unauthorized access and maintain activity logs (ftc) (16 CFR § 314.4(c)(8) & 314.4(d)) (Norton Rose Fulbright +2)

Compliance Verification Steps:

□ **Choose monitoring approach**: Either continuous monitoring (real-time threat detection, automated alerting, ongoing vulnerability scanning) OR periodic testing (annual penetration testing plus vulnerability assessments every six months) (Norton Rose Fulbright +5)
□ **Comprehensive logging** covers all access to customer information (successful and failed), administrative activities, authentication events, and data export/transmission activities
□ **Detection capabilities** include automated monitoring for security events, real-time alerting for critical incidents, behavioral analysis for unusual patterns, and integration with incident response
□ **Network and system coverage** monitors network traffic, system/application logs, database activity, and file access/modifications
□ **Penetration testing standards** (if chosen) include external/internal testing, application security assessment, social engineering, and wireless security testing by qualified professionals (Federal Trade Commission) (CampusGuard)

Documentation Requirements:

- Written monitoring and logging procedures with retention policies
- Penetration testing reports with remediation plans (if applicable)
- Security event response procedures and effectiveness assessments

Testing & Maintenance

10. Regular Testing of Safeguards ✓

Regulatory Requirement: Conduct continuous monitoring OR annual penetration testing plus vulnerability assessments every six months (ftc) (16 CFR § 314.4(d)) (Norton Rose Fulbright +3)

Compliance Verification Steps:

□ **Testing option selected**: Document choice between continuous monitoring or periodic testing approach
□ **Continuous monitoring** (if chosen): Real-time security monitoring, automated threat detection, ongoing vulnerability scanning, continuous security event analysis
□ **Periodic testing** (if chosen): Annual penetration testing by qualified professionals, vulnerability assessments every six months, testing covers all in-scope systems (Federal Trade Commission) (CampusGuard)

□ **Material change testing**: Additional testing triggered when operational or business changes occur that may impact security

□ **Qualified assessors**: Testing performed by qualified internal staff or external professionals (human testers required, not just automated tools) CampusGuard

□ **Remediation tracking**: Document findings, track remediation actions, verify completion of security improvements

Documentation Requirements:

- Written testing procedures and schedules
- Test results with findings and remediation actions
- Evidence of continuous monitoring capabilities (if applicable)

11. Change Management ✓

Regulatory Requirement: Implement procedures to manage system changes that could impact security ftc Federal Trade Commission (16 CFR § 314.4(c)(5)) Federal Trade Commission

Compliance Verification Steps:

□ **Written change management procedures** evaluate security impact of system/network changes before implementation

□ **Security impact assessment** process covers all changes with pre-change approval involving security review

□ **Pre-implementation controls**: Security assessment, approval documentation, risk evaluation for all material changes

□ **Post-implementation validation**: Change implementation logging, monitoring results, updated security configurations

□ **Integration with other processes**: Coordinate with vulnerability testing schedule, update security documentation, align with risk assessment updates

□ **Qualified Individual oversight**: QI approves change management procedures and significant security-impacting changes

Documentation Requirements:

- Change requests with security impact assessments
- Approval documentation showing security review
- Updated security configurations and controls documentation

12. Data Disposal ✓

Regulatory Requirement: Securely dispose of customer information no later than two years after last use ftc (16 CFR § 314.4(c)(6)) Norton Rose Fulbright +3

Compliance Verification Steps:

□ **Two-year disposal rule**: Securely dispose of customer information within two years of most recent use to serve the customer Federal Trade Commission

□ **Legal retention exceptions**: Document legitimate business needs or legal requirements to retain data beyond two years

□ **Secure disposal methods**: Physical documents burned, pulverized, or shredded; electronic data destroyed/erased to prevent reconstruction; secure disposal of storage media Federal Trade Commission
□ **Periodic policy review**: Regular review of retention policies to minimize unnecessary retention (at least annually)
□ **Disposal execution**: Use approved disposal vendors with certificates of destruction, immediate disposal when retention period expires
□ **Exception documentation**: Maintain legal hold and exception documentation for retained data

Documentation Requirements:

- Written data retention and disposal policies with schedules
- Certificates of destruction from disposal vendors
- Legal hold and exception documentation with regular review records

Human Element

13. Training ✓

Regulatory Requirement: Provide security awareness training to employees and update regularly ftc (16 CFR § 314.4(e)) Norton Rose Fulbright +4

Compliance Verification Steps:

□ **General staff training**: Security awareness training for all employees with access to customer information
□ **Specialized training**: Enhanced training for employees with information security program responsibilities
□ **Training content coverage**: Data security awareness, threat recognition, customer information handling, incident reporting, role-specific responsibilities, phishing/social engineering awareness
□ **Regular updates**: Training on emerging threats and countermeasures, refresher training (typically annual minimum), additional training for significant changes
□ **Competency verification**: Assessment results, training completion records, effectiveness evaluation for key personnel
□ **Comprehensive coverage**: All employees, enhanced coverage for security personnel, service providers with access, management/supervisory personnel

Documentation Requirements:

- Training completion records by employee
- Training content and curriculum documentation
- Assessment results and competency verification records

14. Service Provider Oversight ✓

Regulatory Requirement: Ensure third-party vendors maintain appropriate safeguards through due diligence and contract requirements ftc (16 CFR § 314.4(f)) Norton Rose Fulbright +4

Compliance Verification Steps:

□ **Due diligence process**: Evaluate security capabilities, review policies/procedures, assess financial stability, verify insurance coverage, review independent assessments/certifications

□ **Required contract provisions**: Obligation to maintain appropriate safeguards, access restrictions, security incident notification (within 72 hours), audit rights, data breach notification obligations eCFR Inputoutput

□ **Ongoing monitoring schedule**: High-risk providers reassessed annually minimum, lower-risk providers every two years or upon material changes Inputoutput

□ **Service provider inventory**: Complete inventory with risk classifications, contact information, contract status

□ **Continuous monitoring**: Regular review of security reports, monitoring of provider security posture, incident response coordination

□ **Documentation maintenance**: Due diligence records, assessment reports, contract compliance verification, monitoring results

Documentation Requirements:

- Service provider inventory and risk classifications
- Due diligence documentation and security assessments
- Contracts with required security provisions and monitoring reports

Governance & Reporting

15. Incident Response Plan ✓

Regulatory Requirement: Develop and maintain written plan to respond to and recover from security events ftc (16 CFR § 314.4(h)) Federal Trade Commission +2

Compliance Verification Steps:

□ **Comprehensive written plan** includes detection/response procedures, assessment processes, containment steps, investigation protocols, notification procedures, recovery steps, post-mortem analysis

□ **Required plan components**: Clear incident definitions, roles/responsibilities, communication protocols, contact information, evidence preservation, regulatory notification requirements, business continuity procedures

□ **Testing requirements**: Regular procedure testing, tabletop exercises, simulations, post-incident reviews, plan updates based on lessons learned

□ **Notification procedures**: FTC notification within 30 days for breaches affecting 500+ consumers, Federal Trade Commission +3 immediate internal notification to QI/management, customer notification per state laws, law enforcement coordination as appropriate Federal Trade Commission Federal Trade Commission

□ **Plan maintenance**: Regular updates, team assignments, contact information currency, training on procedures, revision history with approvals

Documentation Requirements:

- Written incident response plan with team assignments
- Testing and exercise documentation
- Actual incident documentation and lessons learned with plan revisions

16. Board/Management Reporting ✓

Regulatory Requirement: Qualified Individual reports in writing, at least annually, on program status, risks, incidents, and recommendations Federal Trade Commission ftc (16 CFR § 314.4(i)) Federal Trade Commission +2

Compliance Verification Steps:

□ **Reporting frequency**: Written reports at least annually to Board of Directors, governing body, or senior officer responsible for information security Federal Trade Commission
□ **Required content coverage**: Overall compliance assessment, risk assessment findings, risk management decisions, service provider arrangements, testing results, security events/violations, management responses, program change recommendations eCFR +3
□ **Additional reporting elements**: Program effectiveness evaluation, resource requirements, regulatory compliance status, emerging threats, training effectiveness, service provider oversight results
□ **Documentation standards**: Board meeting minutes showing presentation, written reports with executive summaries, supporting documentation for material matters, action items and follow-up tracking
□ **Board engagement**: Board feedback and direction documentation, resource allocation decisions, oversight of program improvements

Documentation Requirements:

- Board meeting minutes showing report presentation
- Written reports with executive summaries and supporting documentation
- Action items tracking and Board feedback documentation

Implementation and Compliance Verification

Critical Success Factors

- **Executive commitment**: Board and senior management engagement with adequate resource allocation
- **Qualified Individual effectiveness**: Appropriate authority, competency, and organizational support
- **Risk-based approach**: Tailored implementation matching organization size, complexity, and risk profile
- **Documentation discipline**: Comprehensive policies, procedures, and compliance evidence
- **Continuous improvement**: Regular testing, monitoring, and program updates

Compliance Verification Methods

- **Internal assessments**: Regular gap analysis, internal audits, self-assessment checklists
- **External validation**: Third-party security assessments, independent penetration testing, compliance audits by qualified firms
- **Ongoing monitoring**: Continuous compliance tracking, regular policy reviews, effectiveness measurement
- **Documentation review**: Policy currency, implementation evidence, training completion, testing results

Regulatory Enforcement Context

The FTC has brought 89 data security cases through 2023, [Federal Trade Commission] with penalties ranging from program oversight requirements to major monetary settlements. Recent enforcement priorities include AI misuse, junk fees, and data protection failures. **Organizations must now report qualifying breaches to the FTC within 30 days**, [Hinshaw & Culbertson LLP +3] with reports potentially made public, creating new transparency obligations that align with broader federal cybersecurity initiatives. [Federal Trade Commission] [Federal Trade Commission]

This comprehensive checklist provides actionable verification steps for all 16 required elements, enabling organizations to conduct thorough self-assessments and maintain ongoing compliance with the strengthened FTC Safeguards Rule.