Compliance Scorecard

Executive Summary

This FTC Safeguards CaaS Facilitation Workflow is a practical playbook for Managed Service Providers (MSPs) to guide small and midsize businesses through the requirements of the FTC Safeguards Rule (16 CFR 314.4).

This workflow is not about doing the technical work (configuring MFA, running backups, etc.). Instead, it focuses on the facilitation role helping business leaders understand their obligations, make informed risk decisions, and maintain ongoing proof of compliance. Think of it as a vCISO-lite program that an MSP can deliver in just ~2 hours per month on average, while maintaining healthy margins.

By following this framework, MSPs can deliver Compliance-as-a-Service (CaaS) in a scalable, repeatable way positioning themselves as trusted compliance partners, not just IT providers.

High-Level Summary

Phase 0: Sales & Go-to-Market for FTC Safeguards CaaS

Before starting delivery, MSPs should define how the FTC Safeguards CaaS program is **positioned, packaged, and priced**.

Positioning

- **Problem:** SMBs don't know where to start, but banks, insurance, and regulators demand compliance.
- **Solution:** MSP-led **Compliance-as-a-Service (CaaS)** to **facilitate the program**, guide leadership, and prove compliance readiness.
- **Differentiator:** MSP isn't just "doing IT work" they're **leading governance** through a repeatable program, using Compliance Scorecard as the platform.

Suggested Packaging & Pricing

- **Kickstart Package (One-Time)**
    - Full FTC 314.4 gap assessment
    - Risk register setup & initial POAM buildout
    - Delivery of initial executive summary report
    - *Suggested Price:* $3000 - $5000 (depending on client size/complexity)
- **Core CaaS Facilitation (Monthly)**
    - Ongoing monthly facilitation (avg. 2 hours/month)
    - Quarterly governance reviews
    - Evidence validation
    - Annual reassessment & board report
    - *Suggested Price:* $300–$500//month*
        - Based on ~2 hrs/month @ $200/hr, with **80%+ margin** baked in

Pricing calculation for monthly service:

Staff cost: 2 hrs/month @ $58/hr = $116

Tool cost: $89/month

Total base cost: $205/month

Recommended price: $299-349/month *(provides 45-70% margin, accounts for scope creep and overhead)*

- Bundled as a **fixed monthly subscription**, not hourly

- **Plus / Governance Add-On (Optional)**
    - Deeper & more frequent meetings, with key stakeholders

    - vCISO-level strategy sessions with executives/board
    - Policy & SOP facilitation
    - *Suggested Price:* +$2,000–$3,000/month add-on*

*MSPs can flex pricing based on region, client maturity, and perceived value.

Go-to-Market Strategy

- **Trigger Events to Watch:**
    - Requests compliance proof from 4th party (their down stream clients)
    - Cyber insurance renewal
    - Regulator/FTC inquiries
- **Sales Messaging (Plain English):**
    - *"We'll help you prove you're doing the right things — not just for IT, but for regulators, banks, and insurance."*
    - *"You don't need to hire a full-time compliance officer — we guide you month-to-month, and keep you ready."*
- **Sales Tactics:**
    - Use demo assessments to spark urgency ("let's see where you stand")
    - Bundle Kickstart as the entry point → roll into monthly facilitation subscription
    - Provide tiered options (Core vs. Plus) so SMBs can scale investment

Phase 1: Assessment

- Buy in, the right people at the table

Run the gap assessment

- Score risks (likelihood × impact)

- Deliver gap report

Phase 2: Risk Register & Decisions

- Client decides how to handle risks (mitigate, accept, transfer, avoid, defer)

- Document risk register

- Assign ownership

Phase 3: Plan of Action & Milestones (POAM)

- Convert risks/gaps into projects

- Build roadmap & milestones

- Hand-off to MSP implementers (Doers)

Phase 4: Evidence & Validation

- Collect and organize proof (policies, configs, logs, attestations)

- Validate effectiveness (spot checks, interviews)

- Maintain evidence library in Scorecard

Phase 5: Governance & Reporting

- Quarterly check-ins with leadership

- Annual board-level reporting

- Update risk register and compliance score

Phase 6: Reassessment & Continuous Cycle

- Re-run assessment annually/quarterly

- Re-score risk register

- Update POAM and evidence

- Continuous improvement loop

Detailed Facilitation Workflow (Month-by-Month with Hours)

Month 1 – Kickoff & Assessment (3–4 hrs total)

- Leadership kickoff: explain FTC Safeguards & program scope
- Run FTC 314.4 assessment with stakeholders (management, IT, HR)
- Score risks with likelihood × impact
- Deliver gap report

Month 2 – Risk Register (2–3 hrs across sessions)

- Walk client through risks & treatment options
- Document decisions in Scorecard risk register
- Assign owners (client, MSP, third party)
- Leave 'homework' for client between sessions

Month 3–4 – POAM Buildout (2 hrs/month)

- Translate gaps/risks into POAM tasks
- Prioritize high-risk controls first (MFA, backups, IR plan, policies)
- Hand off to MSP implementers ('Doers') for execution
- Facilitator ensures responsibilities are clear

Month 5 – Evidence Collection (2 hrs)

- Gather policies, configs, vendor attestations, training rosters
- Validate evidence (is it operational, not just paperwork?)
- Organize in compliance library

Month 6 – Governance Review (2 hrs)

- Quarterly leadership check-in
- Review risk register, POAM progress, evidence

- Deliver executive summary report

Month 7–8 – Follow-up & Monitoring (2 hrs/month)

- Light touch: check progress on POAM, ensure risk register updated

- Validate new evidence (patches, MFA logs, training)

- Prep for next governance cycle

Month 9 – Evidence Refresh (2 hrs)

- Spot-check existing evidence

- Collect updated logs/policies as needed

- Validate incident response readiness

Month 10 – Governance Review (2 hrs)

- Second quarterly leadership meeting

- Report on compliance score, risk posture, POAM progress

Month 11 – Reassessment Prep (2 hrs)

- Review current risk register & POAM closure rate

- Identify unresolved items

- Prep for annual reassessment

Month 12 – Annual Reassessment & Reporting (3–4 hrs)

- Re-run FTC 314.4 assessment

- Re-score risks (likelihood × impact)

- Deliver annual executive/board report

- Reset POAM for next cycle