Anti-Retaliation Program Assessment

Checklist Resource

For Compliance Officers Seeking to Strengthen Retaliation Prevention & Response

Use this checklist to ensure your cybersecurity risk assessment captures current threats, regulatory requirements, and organizational changes—even if you're not a technical expert.

Policy Foundations & Training

Written Policies

- [ ] Non-retaliation policy exists in plain language and defines retaliation broadly
- [ ] Policy covers all protected activities and is easily accessible in workforce languages
- [ ] Consequences for retaliation are clearly stated and consistently enforced

Training & Communication

- [ ] Annual anti-retaliation training provided to all employees
- [ ] Specialized training for managers/supervisors on recognizing and preventing retaliation
- [ ] Regular communications reinforce protections and share success stories

Intake & Investigation Protocols

Initial Response

- [ ] Retaliation risk assessment conducted for every report
- [ ] Reporter informed of protections and preferred contact method documented
- [ ] High-risk cases flagged immediately (powerful individuals, severe allegations)
- [ ] Temporary separation protocols and interim measures available when needed

During Investigation

- [ ] Investigators trained to recognize retaliation red flags
- [ ] Reporter's baseline work conditions documented (role, projects, performance, schedule)
- [ ] Subject warned explicitly that retaliation will result in discipline
- [ ] Regular check-ins scheduled using reporter's preferred contact method

Post-Investigation Monitoring

Structured Follow-Up

- [ ] Written monitoring plan created for substantiated and high-risk cases
- [ ] Follow-up schedule established (30, 60, 90 days, then 6 months, 1 year)
- [ ] Monitoring responsibilities assigned with automated reminder system

What to Monitor

- [ ] Performance reviews, compensation, work assignments, and schedule changes vs. baseline
- [ ] Informal treatment changes (meeting exclusion, social isolation, project removal)
- [ ] Check-ins probe for changes in treatment, responsibilities, and comfort level

Response to Suspected Retaliation

Immediate Actions

- [ ] Retaliation allegation treated as new case and investigated promptly
- [ ] Interim protective measures implemented; legal counsel consulted
- [ ] Documentation reviewed to establish timeline and causation

Investigation & Remediation

- [ ] Legitimate business reasons scrutinized; similarly-situated employees compared
- [ ] Remedial measures restore reporter's position if retaliation substantiated
- [ ] Enhanced monitoring implemented; discipline demonstrates consequences

Program Effectiveness & Accountability

Cultural Measures

- [ ] Leadership regularly communicates commitment; metrics tracked organization-wide
- [ ] Managers evaluated on creating speak-up environments and face consequences for chilling effects
- [ ] Report volume increases viewed as sign of trust, not program failure

Documentation & Metrics

- [ ] All risk assessments, monitoring plans, and check-ins documented
- [ ] Key metrics tracked: retaliation allegations, monitoring plan completion rate, substantiation rate
- [ ] Board/leadership receives regular program effectiveness reports

Continuous Improvement

- [ ] Annual program review conducted with benchmarking
- [ ] Case management system flags high-risk cases and generates automated reminders
- [ ] Recent case law and regulatory requirements reviewed annually