

Actinon Compliance Readiness Checklist

Info@Actinon.net | 262-393-5552

Be Audit-Ready. Stay Secure. Simplify Compliance.

Use this checklist to prepare your organization for cybersecurity compliance.

1. Determine Applicable Standards

- Identify industry-specific regulations (HIPAA, CMMC, NIST, etc.)
- Determine client, partner, or contractual compliance obligations

2. Identify Data Types and Sources

- Catalog current data held (PII, PHI, financial, etc.)
- Forecast future data types expected to be collected
- Classify data sensitivity and retention requirements

3. Review Systems Architecture and Data Flow

- Map data flow across systems and third parties
- Document network architecture and access points
- Identify cloud services and storage locations

4. Risk Assessment

- Identify critical assets and data
- Conduct threat and vulnerability assessments
- Evaluate current security controls

5. Documentation

- Develop and maintain security policies and procedures
- Document roles, responsibilities, and access controls
- Maintain records of compliance activities

6. Training & Awareness

- Conduct regular employee security training
- Ensure awareness of phishing and social engineering threats
- Track training completion and effectiveness

7. Monitoring & Response

- Implement continuous monitoring tools
- Establish incident response procedures
- Log and review security events regularly

8. Periodic Reviews

- Review and update asset inventory
- Audit user accounts and access rights
- Verify patch management and system updates
- Track and document configuration changes

9. Document Evidence of Compliance

- Maintain audit logs and reports
- Store signed policies and training records
- Retain proof of risk assessments and remediation

10. Audit Preparation

- Perform internal audits and gap analysis
- Prepare evidence for external audits
- Engage with third-party auditors if needed