

Service Attachment for Managed Compliance Services

Effective May 22, 2026. This Service Attachment for Managed Compliance Services supersedes and replaces all prior versions.

This Service Attachment is between Methodology IT ("Provider") and the Client identified on the applicable Order. Together with the Master Services Agreement, the Order, the Schedule of Services, the Service Attachment for Managed Services, the Schedule of Third-Party Services, and any other applicable Service Attachments, it forms the Agreement between the parties. Capitalized terms not defined here have the meanings given in the Master Services Agreement.

This Attachment governs Provider's delivery of compliance services — risk assessment, written information security program development, control alignment, continuous monitoring, evidence collection, vendor risk management, incident response support, and audit support — for one or more named regulatory frameworks identified on the Order.

1. Scope and applicability

Managed Compliance Services are delivered in support of one or more specific regulatory frameworks named on the Order. The frameworks Provider currently supports include:

- **HIPAA** — Health Insurance Portability and Accountability Act (Security Rule, Privacy Rule, Breach Notification Rule)
- **PCI-DSS** — Payment Card Industry Data Security Standard
- **SOC 2** — System and Organization Controls 2 (Trust Services Criteria)
- **CMMC** — Cybersecurity Maturity Model Certification (Levels 1 and 2)
- **NIST CSF / NIST 800-171** — National Institute of Standards and Technology Cybersecurity Framework and SP 800-171 controls
- **GLBA / FTC Safeguards Rule** — Gramm-Leach-Bliley Act and FTC Standards for Safeguarding Customer Information
- **CCPA / CPRA** — California Consumer Privacy Act and California Privacy Rights Act

- **New York DFS Part 500** — New York State Department of Financial Services cybersecurity regulations
- **State data-protection laws** — including state breach-notification statutes applicable to Client

Each Order identifies the specific framework(s) in scope. Services delivered under this Attachment are scoped to the named framework(s); compliance with other frameworks is not included unless added by a subsequent Order.

For purposes of this Attachment, "**Protected Information**" means any data Client handles that is regulated under a framework named on the Order, including but not limited to: protected health information (PHI); cardholder data (CHD) and sensitive authentication data (SAD); nonpublic personal information (NPI); controlled unclassified information (CUI); federal contract information (FCI); personal information (PI) under state privacy laws; and other data classes identified on the Order.

2. Services

Provider will deliver the services identified on the Order. The available services under this Attachment include those described in this section. Additional services may be added by entering into a new Order.

2.1 Risk assessment

Provider will conduct an initial risk assessment to identify and evaluate risks to the confidentiality, integrity, and availability of Protected Information, including risks associated with collection, storage, processing, transmission, and disposal. The assessment will produce a risk register and a remediation roadmap prioritized by likelihood and impact. The risk assessment will be refreshed at least annually or whenever Client's business undergoes a material change.

2.2 Written Information Security Program (WISP) and policy development

Provider will assist Client in developing, implementing, and maintaining a Written Information Security Program tailored to Client's size, complexity, and regulatory scope. The WISP will incorporate administrative, technical, and physical safeguards and will include supporting policies appropriate to the framework(s) in scope — including access control, acceptable use, data classification, incident response, business continuity, vendor management, secure disposal, and others. Policies are reviewed at least annually and revised as required.

2.3 Security baseline and control alignment

Provider will implement and maintain a security baseline configuration aligned to the framework(s) in scope and to the CIS Critical Security Controls. Controls cover identity, endpoint, network, email, cloud, logging, and other domains as applicable to the framework. Provider will maintain control mappings showing how implemented controls satisfy framework requirements.

2.4 Continuous compliance monitoring

Provider will monitor in-scope systems for drift from the established baseline, monitor identity and access events for anomalies, monitor logging and alerting infrastructure, and respond to detected compliance gaps. The cadence and depth of monitoring depend on the framework and the service tier on Client's Order.

2.5 Evidence collection and documentation

Provider will maintain documentation supporting Client's compliance posture, including policies, procedures, risk assessments, training records, vendor reviews, control implementation records, change records, and incident records. Documentation is retained in Provider's documentation platform for the retention period required by the applicable framework or for the duration of the Service Term, whichever is greater. Evidence collection is designed to support, not replace, formal audit activities undertaken by qualified third parties.

2.6 Vendor and third-party risk management

Provider will assist Client in establishing and maintaining a vendor risk management process: maintaining a vendor inventory, classifying vendors by risk, reviewing vendor security posture on a defined cadence, reviewing and tracking required vendor agreements (Business Associate Agreements, Data Processing Addenda, similar instruments), and monitoring vendors with access to Protected Information for material changes in posture.

2.7 Security awareness training and policy attestation

Provider will assign and track security awareness training and policy attestation for Client Users on a schedule appropriate to the framework. Training topics and frequency are tailored to the framework in scope. Completion records are maintained for audit purposes.

2.8 Incident response and breach notification support

Provider will assist Client in developing and maintaining an incident response plan tailored to the framework(s) in scope. In the event of a confirmed or suspected incident involving Protected Information, Provider will assist in detection, initial containment, evidence preservation, and the first phase of investigation. Breach notification support — including assistance with regulatory and customer notification timelines, content, and methods — is included as set forth in the Order; substantial breach-response engagements (extended forensic investigation, regulator interactions, litigation support) are quoted separately under the Master Services Agreement.

2.9 Audit support

Provider will support formal third-party audits, examinations, and assessments of Client's compliance program by responding to evidence requests within the scope of the Services, attending working sessions, and providing reasonable explanation of implemented controls. Audit support is

included up to a defined number of hours per audit cycle as specified on the Order; additional support is billed at the rates in the Schedule of Services.

2.10 Reporting

Provider will deliver compliance reporting on a cadence aligned to Client's service tier as described in the Schedule of Services — typically quarterly for clients on the Complete tier and monthly for clients on the Total tier. Reports include risk register status, control status, monitoring summary, training completion, vendor review status, open findings, and recommended actions.

3. Client responsibilities

3.1 Ultimate responsibility for compliance

Client acknowledges and agrees that Client is ultimately responsible for its own compliance with all applicable laws, regulations, contractual obligations, and industry standards. Provider's services support, supplement, and inform Client's compliance program; they do not transfer compliance obligations to Provider. Provider is not a law firm, an accounting firm, an auditor, or a Qualified Security Assessor (QSA). Where Client requires legal opinions, certified audits, or attestation reports, Client will engage qualified independent third parties.

3.2 Cooperation, access, and information

Client will provide Provider with timely access to facilities, systems, networks, personnel, and documentation reasonably required to deliver the Services. Client will designate a primary and backup point of contact with authority to make decisions and authorize work on Client's behalf for matters relating to this Attachment.

3.3 Compliance with laws

Client will comply with all applicable laws, regulations, and industry standards relating to the protection of Protected Information. Client will obtain and maintain all permits, licenses, and approvals required for Provider to perform the Services.

3.4 Notification of changes

Client will promptly notify Provider of any material change to Client's business operations, systems, locations, scope of Protected Information handled, or regulatory exposure that could affect the Services or Client's compliance posture. This includes mergers and acquisitions, divestitures, new product lines, new processing flows, new regulatory regimes, and similar events.

3.5 Notification of issues

Client will promptly notify Provider of any known or suspected security incident, non-conforming service condition, compliance finding, regulatory inquiry, or customer complaint involving Protected Information.

3.6 Use and care of systems

Client will use and operate systems handling Protected Information in accordance with the policies, procedures, and recommendations Provider has put in place. Client will take reasonable precautions to prevent unauthorized access, misuse, damage, or alteration of those systems.

3.7 Data backup

Where Client has not subscribed to Provider's Backup Services for systems handling Protected Information, Client is responsible for maintaining appropriate backups and recovery capabilities aligned to the framework's requirements.

3.8 Insurance

In addition to the insurance required under the Master Services Agreement, Client will maintain commercially reasonable cyber liability and privacy liability insurance coverage appropriate to its scope of Protected Information and regulatory exposure.

4. Indemnification

In addition to the indemnification obligations in the Master Services Agreement, Client will indemnify and hold harmless Provider, its officers, directors, employees, and agents from and against any claim, fine, penalty, damage, or expense (including reasonable attorneys' fees) arising out of or related to:

- a regulatory investigation, inquiry, or enforcement action against Client, except to the extent caused by Provider's gross negligence or willful misconduct;
- Client's failure to comply with applicable laws or regulations;
- Client's failure to implement Provider's reasonable recommendations regarding compliance;
- Client's misrepresentation of its compliance posture to a third party, including auditors, regulators, customers, or insurers.

5. Disclaimers

Provider does not warrant that the Services will satisfy the specific requirements of any auditor, examiner, regulator, certification body, customer, insurer, or other third party reviewing Client's

compliance. Provider will not issue and is not authorized to issue a certification of compliance, an attestation report, an audit opinion, or a legal opinion regarding Client's compliance.

Provider's services are designed to materially improve Client's compliance posture and prepare Client for third-party audit and assessment. The outcome of any audit or assessment depends on factors beyond Provider's control, including but not limited to Client's adoption and operation of recommended controls, the practices and decisions of Client personnel, the judgment of the third-party assessor, and changes in the regulatory environment.

6. Exclusions

The following are excluded from this Attachment and may be quoted separately or performed by third parties at Client's election:

- Legal advice, legal opinions, regulatory advocacy, or legal representation
- Formal third-party audits, certifications, examinations, or attestation reports (these are performed by qualified independent third parties)
- Forensic investigation and breach-response work extending beyond the initial response support included in this Attachment
- Regulatory fines, penalties, settlement payments, or restitution
- Customer notification mailings, call-center support, and credit-monitoring services associated with a breach (these are typically arranged through a breach-response vendor)
- Implementation of physical security controls (locks, badge systems, surveillance) where physical infrastructure work is required
- Compliance with frameworks not named on the Order
- Penetration testing and red-team engagements (available as Project Services)
- Independent risk assessments performed by other firms

Provider is not responsible for failures to deliver Services caused by Client's failure to comply with its obligations, Client's misuse or unauthorized modification of systems, Client's failure to implement Provider's reasonable recommendations, third-party criminal activity not within Provider's control, Force Majeure events, or other causes outside Provider's reasonable control.

7. Fees and term

Fees for the Services are set forth in the Schedule of Services and on the applicable Order. Term, renewal, and termination of this Attachment are governed by the Master Services Agreement.

Provider may update this Service Attachment with at least sixty (60) days' written notice for material changes. Non-material updates (clarifications, framework citation updates as regulations evolve) may be made without notice provided they do not materially decrease Service functionality.

