Service Description:
CISO and Advisory Services

1. Service Overview

eSentire's CISO and Advisory Services (the "**Service**") is a flexible engagement offering which provides Client access to an eSentire Executive Consultant who can assist Client with the designing, developing, enhancing, and communicating aspects of Client's cybersecurity program and initiatives.

The general parameters and deliverables of the Service are described below. The specific operating cadence and support required will be discussed during the welcome meeting between Client and the Executive Consultant, refined at regular service touchpoints, and maintained in a mutually agreed-upon strategic roadmap.

2. Service Definitions

Any capitalized terms contained in this Service Description are as defined in the Order Form, below or herein:

"**Executive Consultant**" is an eSentire security consultant who will provide security leadership tailored to Client's organizational needs. This resource will be available to assist Client with the development of Client's cybersecurity strategy, risk management practices, compliance efforts, and overall security posture enhancement.

"**Insight Portal**" means the eSentire maintained Client interface used for secure document exchange and collaboration. Client may be provided access to the Insight Portal depending on other eSentire Services Client has purchased.

3. Service Capabilities

The Service includes the following:

3.1. Engagement Initiation. During Contract Year 1 only, the Service will begin with a welcome call (held remotely) between Client and the Executive Consultant, to enable the Executive Consultant to gain a high-level understanding of Client's security environment, team, operations, and priorities. During this call eSentire will introduce the Executive Consultant and exchange contact information. eSentire will also assist Client with access to the Insight Portal so that during the Service the parties can use it for secure document exchange and collaboration. The time used to provide the Welcome Call is included as part of the Service and therefore Hours are not consumed from the contracted allotment of Hours in Clients Service Tier.

3.2. Security Gap Analysis ("**Gap Analysis**"). During or following the welcome call, and annually thereafter, the Executive Consultant will schedule and conduct workshops with Client, to gather information required by the Executive Consultant to carry out the initial Gap Analysis. This analysis will be aligned with the NIST (National Institute of Standards and Technology) cyber security framework and/or other industry frameworks applicable to Client (as applicable and if agreed to). Artifacts may be requested by eSentire from Client, as evidence to validate the analysis.

Upon completion of the Gap Analysis, the Executive Consultant will provide Client a comprehensive report and strategic roadmap ("**Roadmap**"), by posting it to the Insight Portal. A formal review meeting between the Executive Consultant and Client will occur to align the Roadmap to Client budget requirements, resources, and timelines and will be reviewed to determine which initiatives to prioritize. In the event the Service renews, this process is repeated during each Contract Year. Both the Engagement Initiation Process (described in 3.1), and the Gap Analysis completed by the Executive Consultant and reviewed with Client, must occur within the first 90 days of each Contract Year (as applicable). The time used to perform the Gap Analysis and create the Roadmap, is included as part of the Service and therefore Hours are not consumed from the contracted allotment of Hours in Clients Service Tier.

3.3. Consulting Hours. Client may utilize Hours, to request support of Roadmap initiatives, or other security initiatives agreed to, up to the number of Hours allocated in Client's Service Tier (defined in section 4). In some cases, the level of effort required to deliver Client's desired outcomes may exceed Hours allocated in the Service Tier ordered by Client. Client may purchase additional Hours or upgrade to a higher Service Tier at the next Renewal Term, as described below. At the end of a Contract Year, any Hours that have not been used by Client will be deemed forfeited by Client, and the Executive Consultant has no further obligation with respect to such Hours. Hours do not roll over and will reset at the beginning of each Contract Year. As such, no refund, credit, or other form of reimbursement will be due by eSentire to Client.

3.4. Ongoing Consultation. Prior to performing a project in alignment with prioritized Roadmap initiatives or other security support services requested and agreed to (each a "Project"), the Executive Consultant will provide Client with an Engagement Letter (a sample of which may be provided upon request) defining the high-level scope of work, deliverables, and high-level timelines. Client must execute an Engagement Letter before any Project can commence. The activities associated with each Project, as defined in an Engagement Letter, will consume Hours from the contracted allotment of Hours in Clients Service Tier. All Projects will be delivered remotely unless otherwise agreed upon by Client and the Executive Consultant. A Project may consist of one or more of the following types of services:

3.4.1 Strategic Services. Examples of strategic services that may be requested include, but are not limited to:

- Board Communications, Presentations, and Training – includes providing board communications, guidance, and presentation assistance aimed at providing Client's leadership or board of directors with a clear understanding of Clients cybersecurity risks and strategies.
- Executive Briefings – includes an executive briefing provided by the Executive Consultant to Client on a cadence agreed upon by both parties, up to a monthly frequency, covering content and materials relevant to the Roadmap and prioritized initiatives.
- Participation in IT (Information Technology) Governance/Risk Committees - includes providing strategic guidance and advice, insights into emerging threats, and recommendations on risk management practices to guide Client's security governance.
- Security Policy Guidance - includes providing guidance on security policy development and updates, reviewing cybersecurity policies against applicable regulations, and confirming such policies are aligned with current industry requirements/recommendations.
- Vendor Risk Management - assistance with development of a program to evaluate and monitor Client's third-party security practices, and confirming that vendor-related risks are identified, assessed, and mitigated to align with Client's cybersecurity standards.

3.4.2 Assessment Services. Examples of assessment services that may be requested include, but are not limited to:

- Incident Response (IR) Plan and Execution Testing – a tabletop exercise that uses a mock incident to test Clients existing processes and procedures for responding to cyber-security emergencies, to validate the IR plan's effectiveness, and to confirm Client's readiness for managing and mitigating potential cybersecurity incidents.

- Security Technology Evaluation – an evaluation of security technologies, tools and systems for their efficacy, alignment with organizational security requirements, and capacity to enhance the existing security infrastructure.
- Regulatory Compliance Readiness – an evaluation of Client's preparedness for adhering to applicable regulatory requirements (i.e. HIPAA, PCI, SOC2, SEC, etc.), assistance in identifying the complexities of compliance with such regulatory obligations,

3.4.3 Continuity Services. Examples of continuity services that may be requested include but are not limited to:

- Incident Response (IR) Plan Creation – assisting Client in the creation of an IR plan, designed to document the handling of security incidents and incident recovery process.
- Continuous Security Metrics and Key Performance Indicators *(*"KPIs") - assisting Client in the establishment of metrics and KPIs that provide for ongoing, measurable performance evaluation of Client's cybersecurity posture for sustained security management and improvement.

3.5. Touchpoints. The Executive Consultant will conduct regular meetings remotely with Client at a mutually agreed upon cadence ("**Touchpoints**"). The purpose of the Touchpoints will be to prioritize initiatives, provide updates on Project progress, timelines, and remaining Hours, and to update and refine the Roadmap which may include adding or removing prioritized initiatives. Touchpoints will occur at a minimum cadence of one time every four weeks and will be 30 to 90 minutes in duration. Actual cadence and duration will vary and will be agreed upon between the Executive Consultant and Client. Touchpoints will consume Hours from the contracted allotment of Hours in Clients Service Tier.

4. Service Tiers

The Service offers three service delivery options ("**Service Tiers**"): Small, Medium, and Large. Each Service Tier includes up to a defined number of Hours per Contract Year as outlined in table 1 below (used towards Service Elements as applicable and described above). Hours do not roll over, expire at the end of each Contract Year, and reset at the beginning of each Renewal Term. New Projects cannot be initiated within 60 days of the end of each Contract Year unless agreed upon by the Executive Consultant. Material changes to the Roadmap may require new time and scope allocations and will be mutually agreed upon by the Executive Consultant and Client. All Hours will be consumed and tracked in 30 minute increments.

Table 1.

Service Tiers	Contracted Allotment (Hours)
Small	60 hours
Medium	120 hours
Large	240 hours

During the current Service Term, Client may add Hours to their Service Tier contracted allotment, in five hour increments pursuant to a signed amendment. Upgrading to the next Service Tier, may be requested for an upcoming Contract Year in advance, and will require a signed order. Unless otherwise stated on Order Form, all Services leverage English-speaking resources, are delivered remotely, and will be provided during eSentire standard business hours (unless otherwise agreed to in writing). Client may request on-site services, and if approved by eSentire, Client shall be responsible for fees associated with such travel and related expenses.

5. Responsibilities and Assumptions

Client acknowledges that the ability for eSentire to deliver the Service is dependent upon Client's compliance with the responsibilities hereunder and understanding of the assumptions. In the event Client fails to perform its responsibilities herein, in the time and manner specified or contemplated below, or should any obligation set out herein with respect to the Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

5.1. Client Responsibilities:

- Knowledge Baseline: Client must have a foundational understanding of cybersecurity concepts and the importance of a proactive approach to reducing risk and building resilience.
- Data Accessibility: Client will provide necessary access to their systems and data in order for eSentire to conduct assessments and analyses.
- Feedback Loop: Client is willing to actively participate in feedback sessions, ensuring the continuous refinement and improvement of the Service.
- Collaborative Mindset: Client is expected to work collaboratively with eSentire.
- Dynamic Landscape: Client must understand that the threat landscape is continually evolving, and recommendations and strategies may need to be adjusted over time.
- Scope of Service: Each Project delivered by eSentire is delivered based on agreed-upon scope as documented in an Engagement Letter or otherwise discussed, and do not include aspects beyond this scope unless explicitly stated.
- Infrastructure: Client has the necessary infrastructure in place to support the implementation of recommended security solutions and practices.
- Response Time: Client will respond in a timely manner to urgent alerts or recommendations to ensure the efficacy of the proactive engagement.
- Continuous Engagement: Client is expected to maintain regular touchpoints with the Executive Consultant.

5.2. Constraints. The constraints outlined below provide a foundational understanding of the collaborative framework between the Executive Consultant and Client. These factors help set clear expectations and delineate operational boundaries, fostering a transparent and productive partnership. Constraints include:

- Regulatory Requirements: The Executive Consultant can perform Assessment Services to help prepare Client for a certification but does not perform the compliance certification itself.
- Solution Implementation: While the Executive Consultant provides recommendations and guidance on security essential practices, they do not implement security solutions or technical fixes.
- Dependency on Client Data: The quality and accuracy of the Service is contingent on the accuracy and completeness of the data and information provided by Client.
- Technology Constraints: The Executive Consultant's recommendations are based on existing technologies and methodologies known at the time of Service. They do not account for future technological advancements.
- Non-binding Recommendations: While the Executive Consultant provides recommendations based on assessments and analyses, these are suggestive in nature. Final decisions and implementations are the responsibility of Client.
- External Factors: The Services do not account for unpredictable external factors such as global cyber threats, geopolitical changes, or unforeseen industry shifts.
- Financial Limitations: Any recommendations provided by the Executive Consultant are based on cybersecurity essential practices and do not consider Client's financial constraints or budgetary restrictions unless specified.