

COMPLIANCE ESSENTIALS SERVICE DESCRIPTION

This Service Description describes Coalfire's Compliance Essentials offering. All capitalized terms in this Service Description have the meaning defined in the Agreement or relevant Statement of Work under which the Service was purchased. This Service Description, with any attachments included by reference, is part of and incorporated into Client's manually or digitally-signed agreement with Coalfire which reasonably governs the use of the Service, or if no signed agreement exists, the Service Agreement found at: <https://www.coalfire.com/agreements/sa> (together, the "**Agreement**").

Summary: Coalfire's Compliance Essentials offering ("**Service**") is an internet based assessment, risk and compliance application designed to allow Clients to manage their data and evidence across multiple Information Security Framework Standards.

1. SERVICE OVERVIEW.

A. Service Description. Client can access the Service through a self-service online portal ("**Portal**") for use during Coalfire's performance of professional services with which this Service is included. Client may configure and manage the Service and view dashboards through the Portal. The Service is monitored for availability, service capacity and network resource utilization. Client may configure compliance programs, add assigned users, upload and manage documents and evidence, assign ownership of policy documentation, manage draft and publication status, and perform assessments against Compliance Essentials supported Information Security Framework Standards. Client may also create and modify custom security frameworks through the Portal. "**Programs**" means a service or group of services, applications or products that fall within a single compliance boundary. The Service includes up to five (5) Programs managed within the Portal.

(i). Included Modules. The following modules are included with the Service.

- (a). Continuous Compliance Module. This module supports compliance readiness by providing a centralized workflow enabled evidence collection repository that can be scoped to the Program. The cross-framework mapping of evidence allows a single request to be applied across multiple mapped frameworks.
- (b). Assessment Module. Assessment projects are created, scoped, and run in this module. Evidence is submitted for review and assessed against scoped frameworks. The module contains all documents associated with the assessment and supports the download of an audit package.
- (c). Policy. This module is a centralized Program level repository for policy documents. Workflow allows for the drafting, reviewing, and publishing of documents that can be used across the Portal when a specific policy is requested as evidence.
- (d). Dynamic Module. Customizable data tables can be created at the Program or assessment level to support the tracking of any custom data needed to supplement compliance or assessment activities.
- (e). Frameworks. Information Security framework standards are used to guide the collection of evidence and the assessment of those standards using the Platform.
- (f). Scoping Module. This module allows for the selection of information security standards that are to be applied to a Program or assessment.
- (g). Risk Management Module. This module enables Program level management of risks, tracking, quantification, and treatment plans.

(ii). Add-On Modules. The following are additional modules that may be separately purchased by Client.

- (a). Automation Module. This module enables automated collection and use of evidence from Client's cloud services.

B. Technical Support. During the Subscription Term Coalfire will provide technical support services for the Service, as detailed in this [Technical Support Terms and Conditions](#).

C. Maintenance.

- (i). Planned Maintenance. “Planned Maintenance” means scheduled maintenance of the Service during which access to the Service may be unavailable. For Planned Maintenance, Coalfire will provide five (5) calendar days’ notification of such planned event.
- (ii). Unplanned Maintenance. “Unplanned Maintenance” means scheduled maintenance of the Service during which access to the Service may be unavailable. For Unplanned Maintenance, Coalfire will provide prior notice of the unplanned event, if possible.
- (iii). Emergency Maintenance. “Emergency Maintenance” means maintenance of the Service that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as is practical.

D. AI Utilization and Transparency. Coalfire may utilize artificial intelligence (“AI”) tools and methodologies to enhance the provision of the Services. Coalfire commits to AI transparency and will provide details on the AI systems used in the Coalfire Transparency Statement, available at www.coalfire.com/legal. Coalfire will adhere to ethical AI practices and will comply with applicable laws and regulations governing the use of AI in the Services.

- 2. **LICENSE RESTRICTIONS.** Client shall not, and shall not permit any third party to: (i) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code, object code, or underlying structure, data mapping and relationships, ideas, or algorithms of the Service; (ii) modify, translate, or create derivative works based on the Service; (iii) copy, rent, lease, distribute, pledge, assign, or otherwise transfer or encumber rights to the Service; (iv) use the Service for the benefit of a third party; (v) remove or otherwise alter any proprietary notices or labels from the Service or any portion thereof; or (vi) use the Service to build a competitive product or service, or for any other competitive purposes.
- 3. **CLIENT RESPONSIBILITIES.** Coalfire can only perform the Service if Client provides required information or performs required actions, otherwise performance of the Service may be delayed, impaired, or prevented. Client must provide adequate personnel to assist Coalfire in delivery of the Service. Client may configure the features of the Service through the Portal or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Client chooses a setting.
- 4. **FRAMEWORK LICENSE REQUIREMENTS AND INDEMNIFICATION.** The Service provides functionality incorporating various Information Security Framework Standard texts which may be public domain or may be text licensed from third parties. These texts may only be displayed and/or enabled in the Service by validly licensed users according to their separately obtained license agreements with the licensing authority. Client agrees to only enable, display, or otherwise use Information Security Framework Standards and/or text for which Client has obtained the required rights. Client will indemnify, defend and hold Coalfire, its parents, subsidiaries, Affiliates, successors, and their directors, officers, employees, agents and representatives (collectively the “**Indemnified Parties**”) harmless, from and against any and all third party claims, demands, lawsuits, judgments, fines, and penalties (including interest thereon and court costs) caused by a claim that Client does not have sufficient rights and/or licenses to use the Information Security Framework Standards and/or text in connection with the Service.