



This Fixed Price-Fixed Scope Service Description describes the **Information Visibility Assessment Service** (the "Service"). This Service Description is part of any Services Instrument that incorporates this Service Description by reference (collectively, the "Agreement"). **"Services Instrument"** means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Veritas certificate, or a written statement of work or similar document, between Customer and Veritas with associated terms and conditions, that references this Service Description.

Service Overview

This Service is a Fixed Price-Fixed Scope Service engagement to assess a Customer's data and make recommendations on Information Governance and Storage Reduction strategies. During the engagement, Veritas shall leverage both Information Map and Data Insight ("DI"). Veritas shall provide a set of recommendations based upon its findings. During the Service, Veritas shall scan with DI the following:

- A maximum capacity of up to twenty-five (25) Terabytes in total for scanning
- A maximum capacity of up to one (1) Terabyte in total of data for classification

Veritas will analyze the combined technical and business findings and make recommendations made through an Information Visibility Executive Summary report. A follow up analysis of Customer's environment and a second Executive Summary Report shall be provided approximately six (6) months after the performance of Phase 1 and 2 of the Service.

Delivery Details

Scope of Service

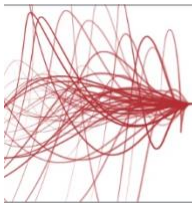
NOTE: Prior to commencement of Services, Veritas will schedule a thirty (30) minute Information Visibility Assessment Service kick-off meeting to discuss objectives, requirements, and project timelines.

The following tasks shall be performed for this Service using a phased approach:

- | | |
|----------------|--|
| Phase 1 | Analysis of Information Map Environment |
| Phase 2 | DI Implementation, Scanning, Classification, and Summary of findings |
| Phase 3 | Follow-up Analysis of Information Map and Summary of findings |

PHASE 1 ANALYSIS OF INFORMATION MAP ENVIRONMENT

As part of this phase, Veritas shall analyze Customer's Information Map Environment. Prior to the commencement of Phase 1, Customer must have Information Map installed configured, and populated with current data.



November 2018

Veritas shall:

- Review roles and responsibilities, scope of Service, Customer readiness, and resource / schedule requirements
- Review and assess current data management environment, using Information Map (Note: Data captured in the form of screenshots and .csv exports shall be collected)
- Host a WebEx to create reports to include an analysis of:
 - Stale and orphaned data
 - Non-business data (e.g. audio and video files)
 - Email files
 - Database files
 - Compressed and archived files
 - Virtual machine files
 - Over and underutilized content sources
 - Most and least active content sources
 - Large and small files
 - Unknown files
 - Ransomware detection

PHASE 2 DI IMPLEMENTATION, SCANNING, CLASSIFICATION, AND SUMMARY OF FINDINGS

As part of this phase, Veritas shall implement and configure DI as well as prepare and present findings to Customer.

Veritas shall:

- Perform DI installation, configuration, and scanning of target sources up to twenty-five (25) TB
- Configure and classify up to one (1) TB of data for both Low and High Risk PII
- Perform analysis of data based on scanning and classification
- Execute ROI calculator
- Execute DI aging and permissions reports

PHASE 3 FOLLOW-UP ANALYSIS OF INFORMATION MAP AND SUMMARY OF FINDINGS

Approximately six (6) months following the completion of Phase 2, Veritas shall reengage with Customer in order to reassess Customer's Information Map environment. (Note: DI reporting and classification shall not be included as part of Phase 3).

Veritas shall:

- Review and assess current data management environment, using Information Map. *(Note: Data captured in the form of screenshots and .csv exports shall be collected)*
- Host a WebEx to create reports to include an analysis of:



November 2018

- Stale and orphaned data
- Non-business data (e.g. audio and video files)
- Email files
- Database files
- Compressed and archived files
- Virtual machine files
- Over and underutilized content sources
- Most and least active content sources
- Large and small files
- Unknown files
- Ransomware detection

Deliverable

Phase 2 Deliverable

- Prepare and deliver the Executive Summary Report with data gathered in Phase 1 and 2

Phase 3 Deliverable

- Prepare and deliver an Executive Summary Report with data from Phase 3

Key Dependencies & Customer Responsibilities

- All tasks shall be performed remotely from a Veritas facility. If Customer requires Veritas to perform the Service onsite, the parties will mutually agree on travel and expense fees.
- Work is conducted during Normal Work Hours.
- Customer shall provide Veritas resource(s) with reasonable access to data centers, systems, tools, equipment, and documentation necessary to carry out the work
- No changes to systems or networks shall be made as part of the Service

Customer Responsibilities. Veritas can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following prerequisites, assumptions, or dependencies, Veritas' performance of the Service may be delayed, impaired or prevented:

- Prior to commencement of the Service, Customer shall, in (1) physical site, prepare:
 - One (1) Windows Server prepped for the DI installation. Hardware/Software pre-requisites are detailed in the Veritas DI Software Compatibility List: https://www.veritas.com/support/en_US/doc/127841202-127841205-0/index
 - Up to two (2) filers or servers (Windows, NetApp or EMC) for scanning. Targets scanned must be on the same physical network within the same physical site as the DI Server. Hardware/Software requirements for the targets are detailed in the Veritas DI Software Compatibility List referenced above.



November 2018

- Veritas recommends Customer consider the following for the source filers or servers:
 - Avoid duplicative shares (Note: do not opt to scan multiple paths which point to the same data)
 - If Windows deduplication is enabled be aware this can impact reporting results
 - Avoid DFS
 - To avoid permission issues, ensure the DI server, AD server, and source targets reside in the same domain
- Prior to commencement of Phase 1 Customer shall create an account for Veritas to connect remotely to Customer's Information Map environment
- During Phase 2:
 - Ensure that server resources and appropriate permissions is available for the DI installation.
 - Complete ROI questionnaire before the commencement of the Service
- For Phase 3:
 - Customer shall host a WebEx or create an account for Veritas to connect remotely to Customer's Information Map environment
- Veritas strongly recommends that the Customer back up all critical hosts in Customer's environment before Service commencement. Veritas does not accept responsibility or liability for any loss of data incurred by Customer during the delivery of this Service
- Provide the necessary staffing resources (e.g., LAN, SAN, OS Platforms, DBA, etc.) to enable the Service to be performed.
- Allocate any necessary space, power, cooling, networking, security measures, and wire/cable management for the Service.
- Provide any necessary network access for Veritas, SNMP and email address requirements for alert notifications, and open the necessary network ports to enable the Service to be performed.
- Provision a contiguous range of physical IP addresses and a contiguous range of virtual IP addresses. All IP addresses (both physical and virtual) must be part of the same subnet and use the same netmask as the node's access IP.
- Any additional Customer Responsibilities set forth in this Services Description and the Services Instrument.

Acceptance Schedule

Acceptance conditions are set forth in the Services Instrument. The milestone percentage below indicates (1) the percentage of the Service to be completed for each milestone and (2) for any Service which is not pre-paid, the percentage of the Service to be invoiced upon acceptance.

Payment Milestone	Acceptance Schedule	Milestone Percentage
Milestone #1:	Upon acceptance of the Service and Deliverable listed herein Phase 1&2	84%
Milestone #2:	Upon acceptance of the Service and Deliverable listed herein Phase 3	16%