Data Discovery Assessment

Our Securiti Data Discovery Assessment is a targeted assessment that aims to address several common challenges related to data and AI model security, including how to identify and protect sensitive data at scale, how this data flows into your AI tools and who has visibility of outputs, highlighting and addressing compliance gaps.

Prevent risk from becoming reality by uncovering and fixing your blind spots before they are amplified by AI tools or bad actors.

The Securiti Data Assessment Report will cover two main categories of outcomes:

High-Level Key Findings:

Findings will provide insights into:

- Your sensitive data catalogue and Data Risk score.
- Analysis of ROT (Redundant, Obsolete, Trivial) data.
- Sensitive Data Intelligence across the in-scope system.
- Mapping of data to relevant compliance and regulatory requirements.

High-Level Recommendations:

Actionable recommendations based on the findings, including:

- Strategies for data risk remediation and classification,
- Approaches for ROT remediation,
- AI policy guardrails for appropriate, dynamic governance,
- Other relevant suggestions for improving data security, compliance and AI governance.

Scope + Prerequisites for the Assessment:

This Data Discovery Assessment involves scanning one data system, with a limit of up to 500GB of data content. Video, audio, and image files are generally out of scope unless specifically required.

To ensure a successful assessment, the following prerequisites must be met:

- Deployment of POD hardware infrastructure and networking (details provided in separate document)
- Provision of access to the data store(s) (details to be provided in a separate document).
- Necessary approvals from stakeholders.
- Completion of any required change requests.

Success Criteria:

The success of the Securiti assessment will be measured by the following criteria:

- Successful deployment of the **securiti.ai** pod within the client's environment.
- Connection to the designated data store.
- Effective performance of data scanning, leading to the identification of potential Personally Identifiable Information (PII) findings metadata.
- Generation of a report detailing the findings from scanning the in-scope files.
- Identification of Redundant, Obsolete, and Trivial (ROT) files (as per agreed customer requirements).

Following successful completion of targeted assessment, Somerford are able to support implementation and expansion of Securiti to deliver the recommendations and realise your desired business outcomes.

Outline Timescales & Process Flow

Day -4	Day 0	Day 2	Day 3	Day 7	Day 10	Day 14
Scoping Call: Remote session to understand both technical scope and business requirements.	**Pre-Requisite Check:** ~30-60 mins technical call to validate all pre-requisites are completed.	**Deployment & Configuration:** ~4 hr technical call to deploy Securiti & configure identifiers.	**Health Check:** ~30-60 mins technical call to validate Securiti is functioning and meeting both technical and business expectations.	**Interim Review:** ~1 hr review call to discuss initial findings, goals & alignment to data priorities.	**Data Discovery Presentation:** Presentation to review outputs and evaluate the value achieved.	**Final Review:** Executive review of the final report with bespoke recommendations aligned to the original scope and business requirements.

Contact us: *info@somerfordassociates.com* *somerfordassociates.com/contact-us/*