Accedere's *Integrated Audit Approach* for SOC 2 Attestation and ISO/IEC Certification

Background

Accedere's Integrated Audit Approach

Simultaneously conducting audits for two different standards or frameworks is an integrated audit. By conducting integrated audits, clients can reduce their costs and time by using the existing policies, procedures, and governance documentation and leveraging the available evidence for different standards or frameworks that meet both requirements and reduce Auditor's onsite audit time. In addition, Accedere's integrated approach to audits can significantly reduce the burden on internal resources; for example, integrating an ISO/IEC 27001 certification audit with a SOC 2 reporting assessment allows for performing the audit more efficiently.

ISO/IEC 27001:2013 certification

ISO/IEC 27001 is an International Standard that provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Adoption of an ISMS is a strategic decision of an organization that is influenced by the organization's needs and objectives, security requirements, the organizational processes used, and the size and structure of the organization. An ISMS preserves information confidentiality, integrity, and availability by applying a risk management process. It gives confidence to interested parties that risks are adequately managed.

SOC Reports

A SOC 2 is a report on controls of a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. SOC 2 reports are intended to meet the needs of a broad range of users that require detailed information and assurance about the controls at a service organization relevant to the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. SOC 2 compliance reports are part of AICPA's SSAE 18 Attest Standard for the SOC 1, SOC 2, and SOC 3 reports.

Accedere Inc.

Accedere Inc. is a global provider of Assurance services for cybersecurity compliance. Accedere Inc. is a Colorado CPA firm registered with PCAOB focusing on Cloud Security and Privacy and empaneled Cloud Security Alliance (CSA) auditors for conducting assessments for CSA STAR Level attestation and certification requirements. Additionally, as an ISO/IEC certification body, Accedere Inc has the relevant expertise to support ISO/IEC 27001 and the STAR certification process.

Ashwin Chaudhary is the CEO of Accedere. He is a CPA from Colorado, MBA, CITP, CISA, CISM, CGEIT, CRISC, CISSP, CDPSE, CCSK, PMP, ISO27001 LA, ITILv3 certified cybersecurity professional with about 20 years of cybersecurity/privacy and 40 years of industry experience. He has managed many cybersecurity projects covering SOC reporting, Privacy, IoT, Governance Risk, and Compliance. Accedere.io

Sifflet Inc.

Founded in 2021, Sifflet is a software company headquartered in Paris, France. Sifflet is a Data Observability platform that helps organizations achieve more trust in their data and fasten the adoption of a data-driven culture.

Sifflet was founded by Salma Bakouk, Wajdi Fathallah, and Wissem Fathallah based on the principle “data must be mastered so that enterprises can innovate.” Through their anomaly detection algorithm, the company's mission is to provide a Data Observability platform to help organizations achieve more trust in their data and fasten the adoption of a data-driven culture. Sifflet’s data quality monitoring technology serves enterprise customers. Siffletdata.com

Problem

Striving for cybersecurity assurance

Cybersecurity frameworks, standards, and certifications can be complicated to understand, making it difficult for a company to identify which framework/standard/certification they should aim to achieve to be cyber secure.

Sifflet wants to assure its clients of their data security and confidentiality. This is when they approached Accedere Inc. and engaged in understanding their options and timelines for conducting an audit.

Accedere analyzed Sifflet's requirements and suggested getting attested for SOC 2 Type 1 and ISO/IEC certification through an integrated audit approach, which would eventually help them achieve SOC 2 and ISO compliance during the same period.

Solution

Accedere's Proposal

Accedere evaluated Sifflet's SaaS (Software as a Service) and suggested a plan to help them achieve the SOC 2 attestation and ISO/IEC 27001 certification with an Integrated Audit.

Performing a Gap Assessment

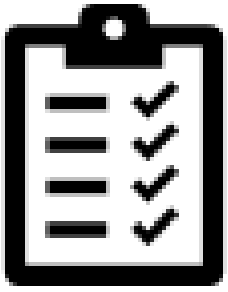
Accedere conducted a thorough analysis of Sifflet and identified the critical gaps in their organization with reference to SOC 2 Type 1 assessment for the applicable Trust Services Criteria 2017 (Security, Availability, and Confidentiality) and ISO/IEC 27001 standard.

Integrated Audit Preparation

For Sifflet to be adequately prepared for the Integrated Audit, they had to perform the following:

- ✓ Determine the scope and context of their Information Security Management System
- ✓ Prepare a System Description
- ✓ Conduct a company-wide analysis to document Information Assets
- ✓ Conduct a Risk Assessment based on the identified Information Assets
- ✓ Define Control Objectives and determine appropriate Controls to mitigate risks
- ✓ Complete a Statement of Applicability (SoA) and justify controls deemed not applicable
- ✓ Prepare and approve relevant Policies, Procedures, and Governance documents
- ✓ Gather appropriate Evidence to ensure the controls were suitably designed to meet the applicable Trust Services Criteria

Performing the Integrated Audit



Accedere conducted the ISO 27001 Stage 1 documentation review audit and provided areas of opportunity for Sifflet to update the policies, procedures, and governance documentation, the SoA, and the System Description. This also meets the policies and procedures review process for SOC 2 requirements.

Sifflet updated its documentation to close all areas of concern identified in the Stage 1 documentation review audit.

Sifflet implemented their controls per their SoA and System Description.

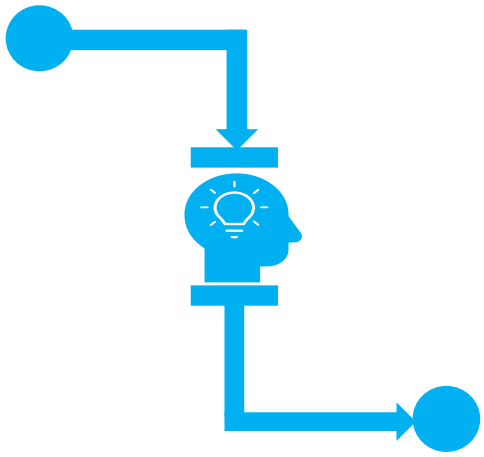
Accedere also conducted document, process, and evidence review walkthroughs of Sifflet's Risk Management program, Incident Response management, HR operations, Change Control management, and Business Continuity management, which meets ISO 27001 Stage 2 implementation audit and SOC 2 controls audit.

During Accedere's integrated approach to auditing, all Sifflet ISO 27001 and SOC 2 controls were evaluated.

Results

Primary Benefits of Accedere's Integrated Approach

- ✓ Tremendous cost savings
- ✓ Reduced effort for customers and the auditors
- ✓ Confirms customer trust
- ✓ Increases market share
- ✓ Improves competitive advantage
- ✓ Enables organizations to secure their information and reduce their risk



With Accedere's Integrated Audit approach, Sifflet achieved SOC 2 Type 1 Attestation, ISO/IEC 27001:2013 Certification, and good cybersecurity maturity.

Congratulations to Sifflet on their incredible success!

For more details on achieving the SOC 2 attestation, ISO/IEC certification, and CSA STAR Level 2, please get in touch with Accedere at info@accedere.io

You can also visit our website to know about our services https://accedere.io