Sensiba

Certified B Corporation

WEBINAR | EXTERNAL

ISO 27001 vs SOC 2: Do I Need Both?

Risk Assurance Services

Introductions

Jeffery R. Stark

Audit Partner

- With over 25 years of entrepreneur experience, Audit Partner Jeff Stark is dedicated to quality financial reporting. He specializes in revenue recognition, complex debt/equity transactions, mergers and acquisitions, accounting for income taxes, and purchase accounting for technology companies. Jeff is also a co-lead partner in our risk assurance services group and has deep expertise in SOC 1 & SOC 2 reporting as well as ISO 27001.
- As the Firm's Technology practice leader, Jeff has extensive experience advising clients on exit strategies. As a one-time entrepreneur that founded, built, and sold his own company, Jeff is extremely passionate about applying his experience to help his clients do things right and solve their business challenges. He works extensively with professionally managed venture-backed companies seeking to grow and ultimately be acquired or pursue an IPO path. He works with clients in enterprise software, cloud/SaaS, network equipment, cybersecurity, development stage enterprises, healthcare, internet advertising, and med-tech.

Scott Dritz

ISO Practice Leader

- With more than 30 years of technology expertise, ISO Practice Leader Scott Dritz helps clients achieve their business objectives and address their information security needs by helping them implement and optimize ISO 270001 compliance programs. Scott leads a team helping clients of all sizes enhance their information security management system and its processes based on the ISO 27001 framework, as well as the intersection of various cyber security systems.
- A certified ISO 27701 Lead Auditor, Scott also holds the Certified Information Systems Security Professional (CISSP) designation and Certified Information System Auditor (CISA). He is also certified in ISO 19011:2018 Leading Management Systems Audit Teams and ISO 19011:2018 Management Systems Auditing and holds the ISO 27001:2022 Lead Auditor - Information Security Certification. He also has numerous cloud and cyber security designations.

- 40+ Years in Business
- Serving 8,000+ United States & International Clients
- Thousands of Community Service Hours Each Year
- Six Locations With Professionals Across the Country

Tax

Business, International, Private Wealth, Research & Development (R&D) Tax Credit, State & Local, Estate & Trust

Audit & Assurance

Financial Statement Audits, Reviews & Compilations, Internal Audit, Sarbanes-Oxley Compliance (SOX), Employee Benefit Plans

Risk Assurance

HIPAA, SOC Reports, ISO Certification, NIST

Consulting

Outsourced Accounting, Lease Accounting, Family Office

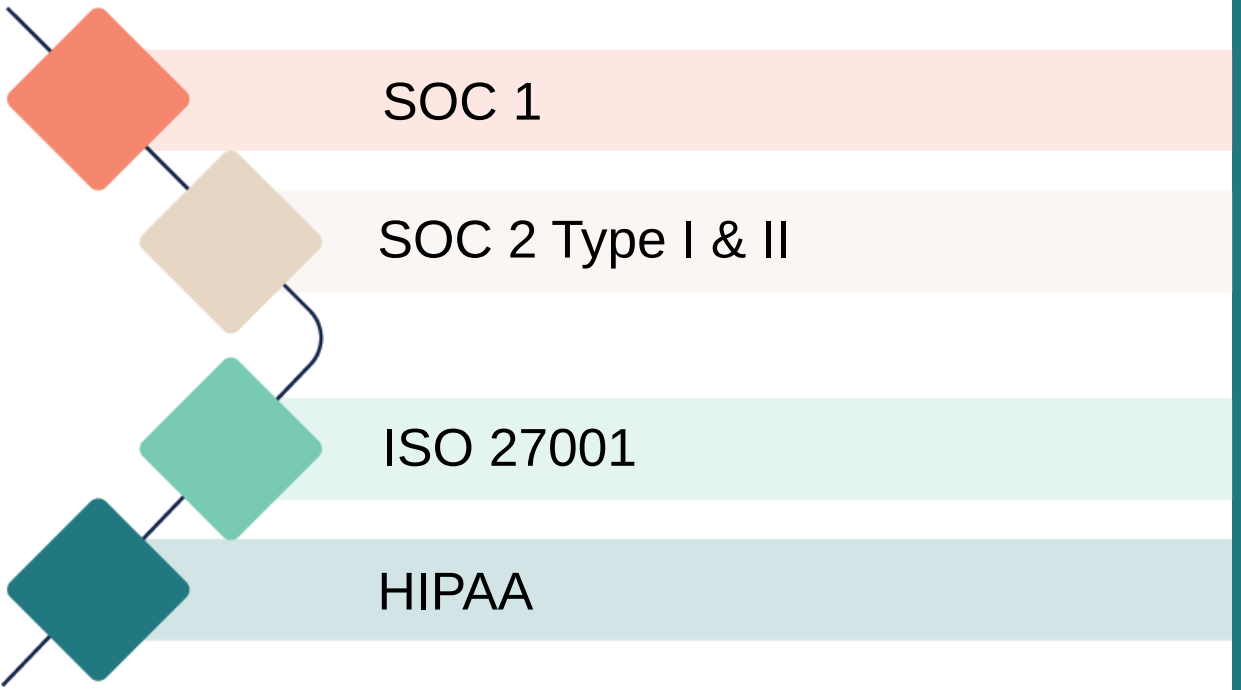
Technology

Sage Intacct, ERP, BlackLine, Limelight, Finance Automations

Sustainability

B Corp Certification, SASB Standards & CDP, Impact IQ ESG Assessment, Climate Neutral Certification

Risk Assurance Services



Auditing Standards

- AICPA SOC
- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- HIPAA
- NIST

Platform Partner

- Drata
- Vanta
- Sprinto
- Tugboat
- SecureFrame
- Others

Sensiba

What is ISO 27001?

Certified B Corporation

What is ISO?

International Organization for Standardization

- Founded in 1947 by
  - International Federation of the National Standardizing Associations
  - United Nations Standards Coordinating Committee

Popular Standards

- 9001 – Quality Management
- 14001 – Environmental Management
- 45001 – Occupational Health and Safety
- 27001 – Information Security
- 27701 – Privacy

ISO Certification Body

Standards Covered

- ISO 27001 – Information Security Management Systems
- ISO 27701 – Privacy Information Management Systems*
- ISO 27017 – Cloud Services
- ISO 27018 – Personally Identifiable Information (PII)

* Maps very closely to GDPR

ISO 27001 Requirements

Fully implemented Information Security Management System (ISMS) Includes:

- Statement of Applicability
- Risk Assessment
- Internal Audit
- Management Review

Headcount	Audit Days
1-10	5
11-15	6
16-25	7
26-45	8.5
46-65	10
66-85	11
86-125	12
126-175	13
176-275	14
276-425	15
426-625	16.5
626-875	17.5
876-1175	18.5
1176-1550	19.5
1551-2025	21
2026-2675	22
2676-3450	23
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27
8501-10700	28
10701+	Contact SME
Reference	ISO 27006

Source ISO 27006 – Annex B

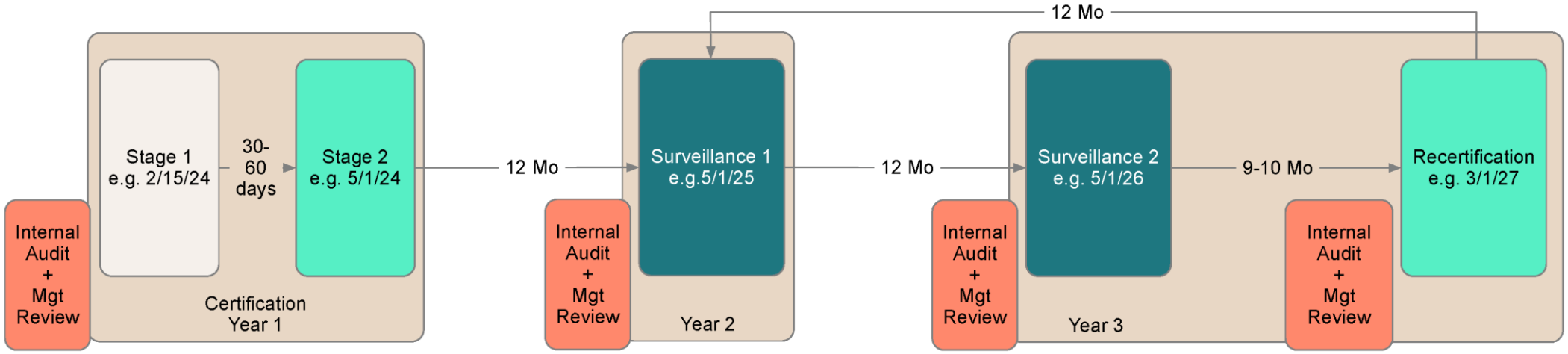
Audit Days

Can be reduced by a maximum of 30%

Can be increased up to 100%

Depending on Client's Risk Factors

3-year ISO Certification Cycle



Who needs ISO 27001

Every company that

- Supports international customers
- Wants to grow into international markets
- Has sensitive information

Types of Companies

- SaaS Providers
- Financial Institutions
- Healthcare Providers
- Government Agencies
- Professional Services Firms
- Managed Service Providers

Sensiba

What is SOC 2?

Certified B Corporation

What is SOC 2?

System and Organization Controls

- AICPA Standards
  - SOC 2 – Trust Services Criteria
    - Security (and the rest)
  - One of the suite of SOC offerings
- Tremendous growth
  - Cloud
  - Default Vendor Risk Management Request List Item

SOC 2 Report

- Audit (actually, Attest) Opinion
- Reasonableness Standard
- 4 (sometimes 5) Sections of the Report
- Type 1 and Type 2 Reports
  - Reporting Periods and Cycle
- SOC 2+
- SOC 2 Platforms

Who needs SOC 2 Type II and ISO 27001

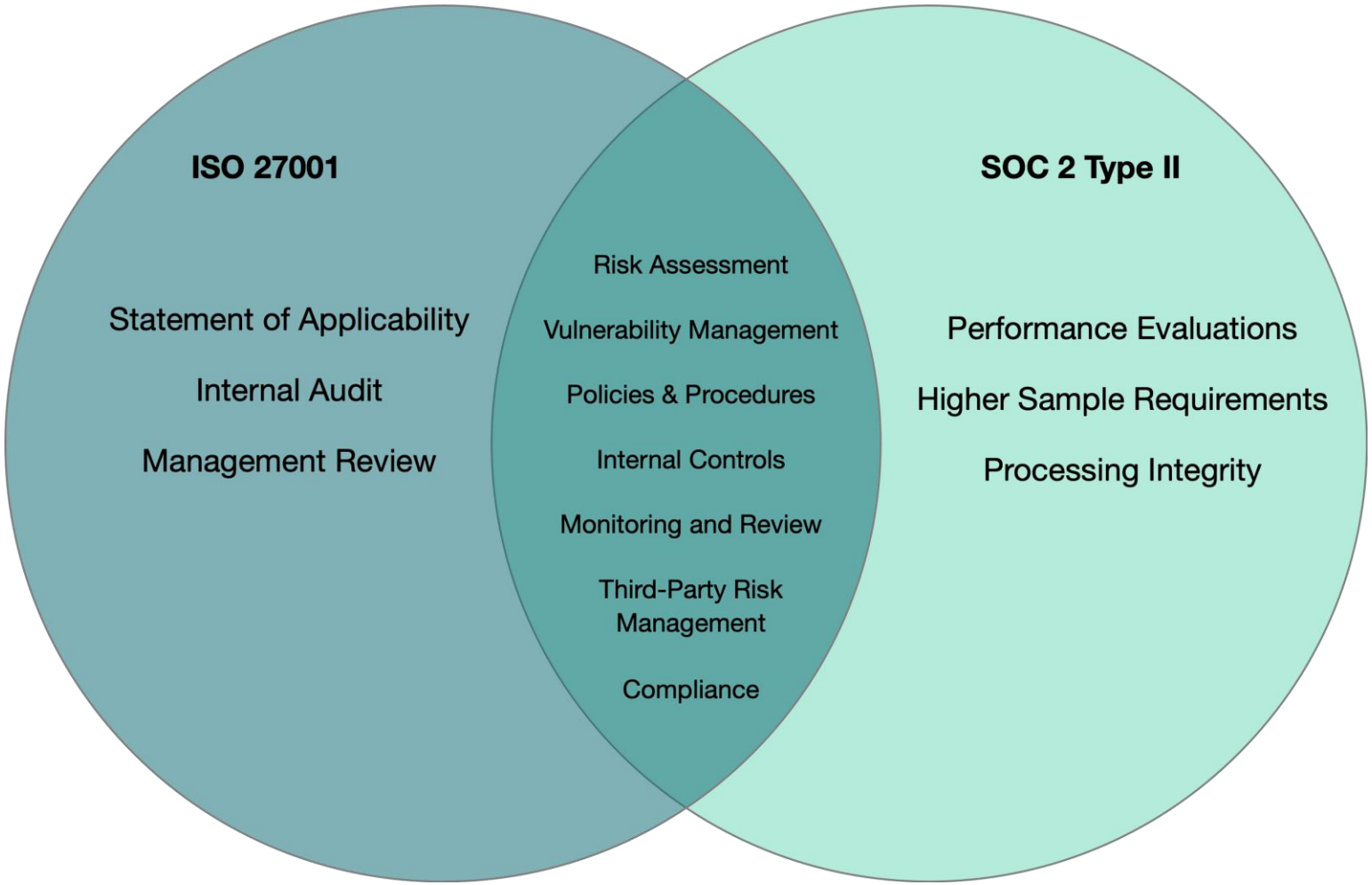
- Global company
  - North America
  - International
- Companies who want to demonstrate their security against multiple standards

Sensiba

Aligning ISO 27001 and SOC 2

Certified B Corporation

Overlap between SOC 2 Type II and ISO 27001



*~ 70% overlap

Key Differences between ISO 27001 and SOC 2

ISO 27001

- Certification of the Management System
- Well suited for organizations operating or doing business outside of North America
- Point in Time Audit
- 3-year cycle
- Requirements are more strict
  - Clauses are mandatory for every organization
- Internationally recognized

SOC 2

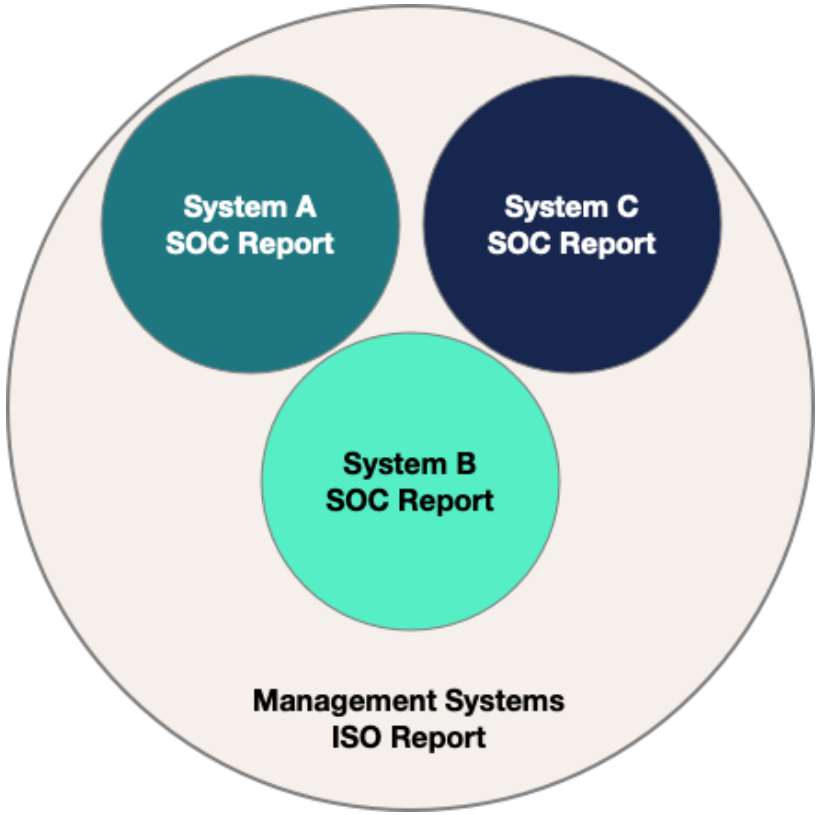
- Attestation (Audit) on the System
- Most prevalent for organizations doing business in North America, but international companies on the cloud are often seeking SOC 2
- Type 2 Reports, generally 1 year.
  - Initial SOC 2 can be shorter. Type 1 Option
- More tailored to the organization
  - Client chooses the TSCs and Controls
  - Client defines the System

System vs Management System

Each System needs a SOC report

An organization with multiple systems, but a single management system could conduct a single ISO audit for the management system instead of a SOC audit for each system

ISO 27001 Certifies Management Systems



ISO 27001 Internal Audit

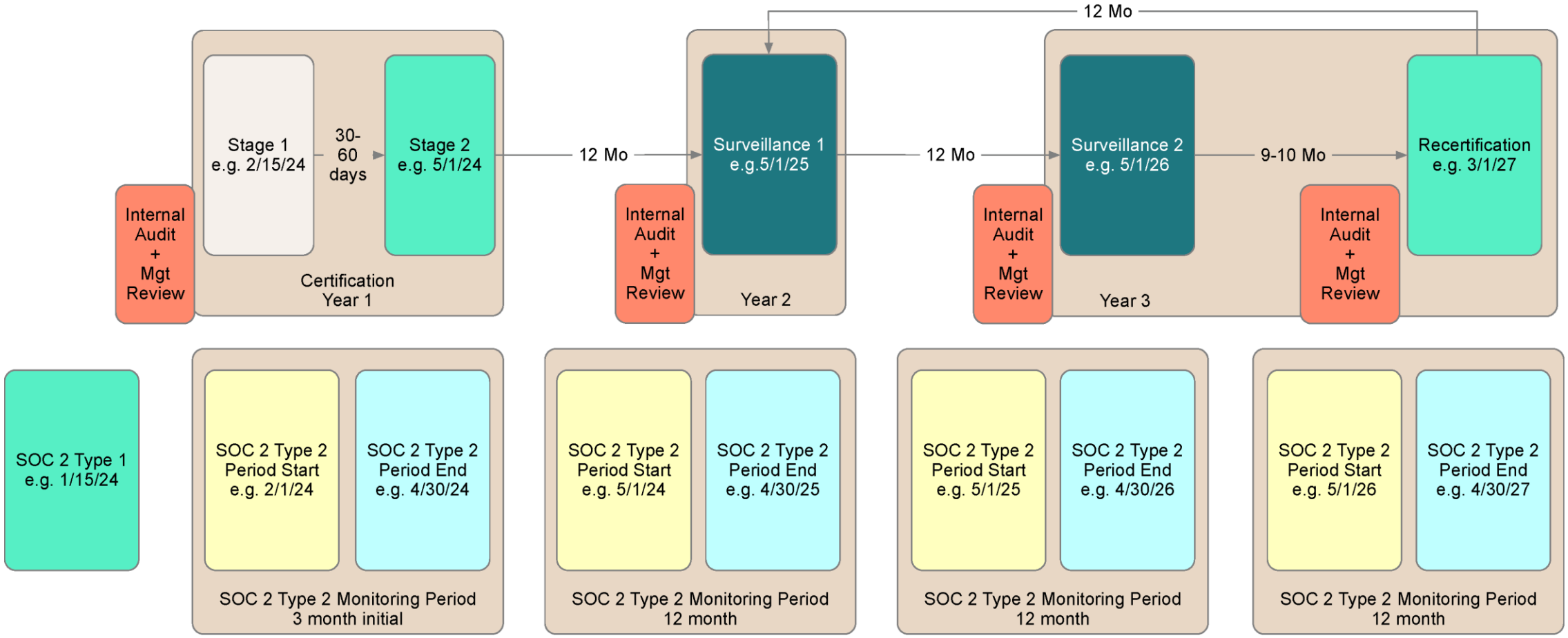
Required by the standard

- Two main components of who can conduct the Internal Audit
  - Competency with the ISO Standard
  - Independence / Impartiality from the ISMS
- Cannot be a report generated by a GRC Platform

What does this mean?

- Most organizations vend their internal audit to a third party because:
  - They don’t have the competence
  - If they have the competence, they’re usually involved with the ISMS
  - They want a more through evaluation of their management system

3-year ISO Certification Cycle + SOC



Collect Evidence Once, Audit Many

Aligning ISO 27001 and SOC 2

ISO 27001

- Mapping Controls
- Utilizing GRC tools / Readiness Platforms
- Timing Considerations / Conversations
- ISO Auditors can utilize the SOC sample selections

SOC 2

- Shift the type II period end to be slightly ahead of the desired ISO Certification / Surveillance audit
- Ideally shorten the period to line up ISO and SOC fieldwork
- Have SOC auditors select samples

Questions?

Contact:

Jeffery Stark, CPA, CISSP, CISA
Audit Partner
jstark@sensiba.com

Scott Dritz, CISSP, CISA
Senior Manager - Risk Assurance Services
sdritz@sensiba.com

Sensiba

Certified B Corporation

Thank you!