armanino

armanino.com

WEBINAR

# From Local to Global: Scaling Your Information Security & Data Privacy Practices

KNOWLEDGE

# Learning Objectives

**Discuss** the importance of having and improving an ISMS & PIMS

**Explore** methods to protect your clients' data (PII) in line with GDPR privacy regulations.

**Verify** your business is following regulations during international business integrations.

WELCOME

# Today's Presenters

**Arti Lalwani**
Managing Director
Armanino Advisory LLC

**Danny Vega**
Supervising Senior
Armanino Advisory LLC

**Chris Reilly**
Supervising Senior
Armanino Advisory LLC

# Agenda

- Information Security Background & Examples
- Data Privacy Background & Examples
- ISO Certifications Overview
- First AI Certification
- Why are ISO Certifications Useful
- Scoping
- Certification Process
- Recommendations
- Q&A

WHAT IS IT?

# Information Security/Cloud Security

The practice of **protecting information from unauthorized access**, disclosure, disruption, modification, or destruction. It involves implementing measures and controls to ensure the confidentiality, integrity, and availability of data. These three key principles are often referred to as the CIA triad:

**Confidentiality:**
**Ensuring** that information is only accessible to those who are authorized to view it.

**Integrity:**
**Protecting** information from being altered or tampered with in an unauthorized manner.

**Availability:**
**Ensuring** that information and resources are available to authorized users when needed.

**Risk management, incident response, and the implementation of security policies, procedures, and controls are necessities for every organization.**

INFORMATION SECURITY

# Man in the Middle Attack Examples

## Cash App

- Malicious activity performed by former disgruntled employee
- Improper termination procedure
- More than 8 million users could be affected

## Tesla

- Two former employees responsible for leaking 100GB of company data (i.e., social securities)
- More than 75,000 employees effected

**These types of breaches can lead to losing clients and reputational damage**

**Recommendation: Security Awareness trainings**

WHAT IS IT?

# Data Privacy

Focuses on **the rights of individuals to control how their personal information is collected, used, shared, and stored**. It is governed by various laws and regulations, such as the **General Data Protection Regulation** (GDPR) in Europe, the **California Privacy Rights Act** (CPRA) in the United States, and other regional and industry-specific regulations. These laws are designed to protect individuals' privacy and give them control over their personal information. Key concepts include:

- **Consent:** Individuals should have control over how their data is collected and used.
- **Data Minimization:** Collecting only the data that is necessary for a specific purpose, and no more.
- **Transparency:** Organizations should be transparent about their data collection and processing practices.
- **Data Security:** Protecting personal data from unauthorized access, breaches, or leaks.
- **Data Subject Rights:** Individuals have specific rights concerning their data, such as the right to access their data, correct inaccuracies, request deletion (also known as the "right to be forgotten"), and object to certain types of data processing.

DATA PRIVACY

# Breach Examples

### Equifax

- Private records of 147.9 million Americans, 15.2 million British citizens and 19,000 Canadian citizens were exposed
- One of the largest cybercrimes related to identity theft
- Equifax will pay $575 million and potentially up to $700 million as part of a global settlement with the FTC, the Consumer Financial Protection Bureau and 50 US states and territories

### Pegasus Airlines

- Vulnerability in software left 6.5 terabytes of data exposed
- Compromised 23 million files
- Originated from a misconfigured “bucket” on Amazon’s cloud service AWS

These types of breaches can lead to losing clients, reputational damage, and hefty fines

**Recommendation: Security Awareness trainings**

ISO CERTIFICATIONS OVERVIEW

# What is it?

**Developed by the International Organization for Standardization, ISO/IEC 27001:2022 is an international information security standard providing requirements for an Information Security Management System (ISMS).**

- It is an **all-encompassing framework for protecting all types of digital information**, including employee data, financial data, customer data, corporate IP, third-party entrusted information, personally identifiable information "PII"

|

ISO CERTIFICATIONS OVERVIEW

# What is it? cont'd...

## ISO 27001:

Provides a framework & methodology for design, monitoring & continuous improvement of an **Information Security Management System** (ISMS)

## ISO 27701:

An extension to ISO 27001 that provides requirements for the design & implementation of the **Privacy Information Management System** (PIMS)

## ISO 42001*:

Provides a framework & methodology for design, monitoring & continuous improvement of an **Artificial Intelligent Management System** (AIMS)

**Armanino Certified, LLC is an ANAB: ANSI National Accreditation Board accredited certification body for ISO 27001 & ISO 27701.*

ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEM

# ISO 42001*: First AI Certification

The AI Act is a European Union regulation on artificial intelligence. It is the **first-ever comprehensive legal framework on AI worldwide**. It aims to establish a common regulatory and legal framework for AI. The Act assigns applications of AI to 3 risk categories:

- ○ **High Risk:** critical infrastructure, education, employment, law enforcement & healthcare
- ○ **Limited Risk:** Chatbots
- ○ **Minimal / No Risk**

- Increasing popularity and the speed of use of AI plays a role in the lack of regulation of it
- This ISO framework is for AI users, producers, developers and multiuse
  - ○ **This framework is to make sure we have an outlined management system in place so that there's security behind the use of AI**
  - ○ Carve out scope, similar to ISO 27701

**Armanino Certified, LLC is an ANAB: ANSI National Accreditation Board accredited certification body for ISO 27001 & ISO 27701.*

WHY IS THIS USEFUL?

# Global Expansion

If your company has an international presence or is planning on expanding globally:

- EU presence company needs to be compliant with GDPR… This is not something you can just say you're compliant with.
- ISO 27001 and ISO 27701 Certifications are the first time you can say you're compliant.
- Why? Because you have the ISO certifications, and they map back to GDRP
- Business Continuity for any location that is in-scope: ISO 27001 can cover that

WHY IS THIS USEFUL?

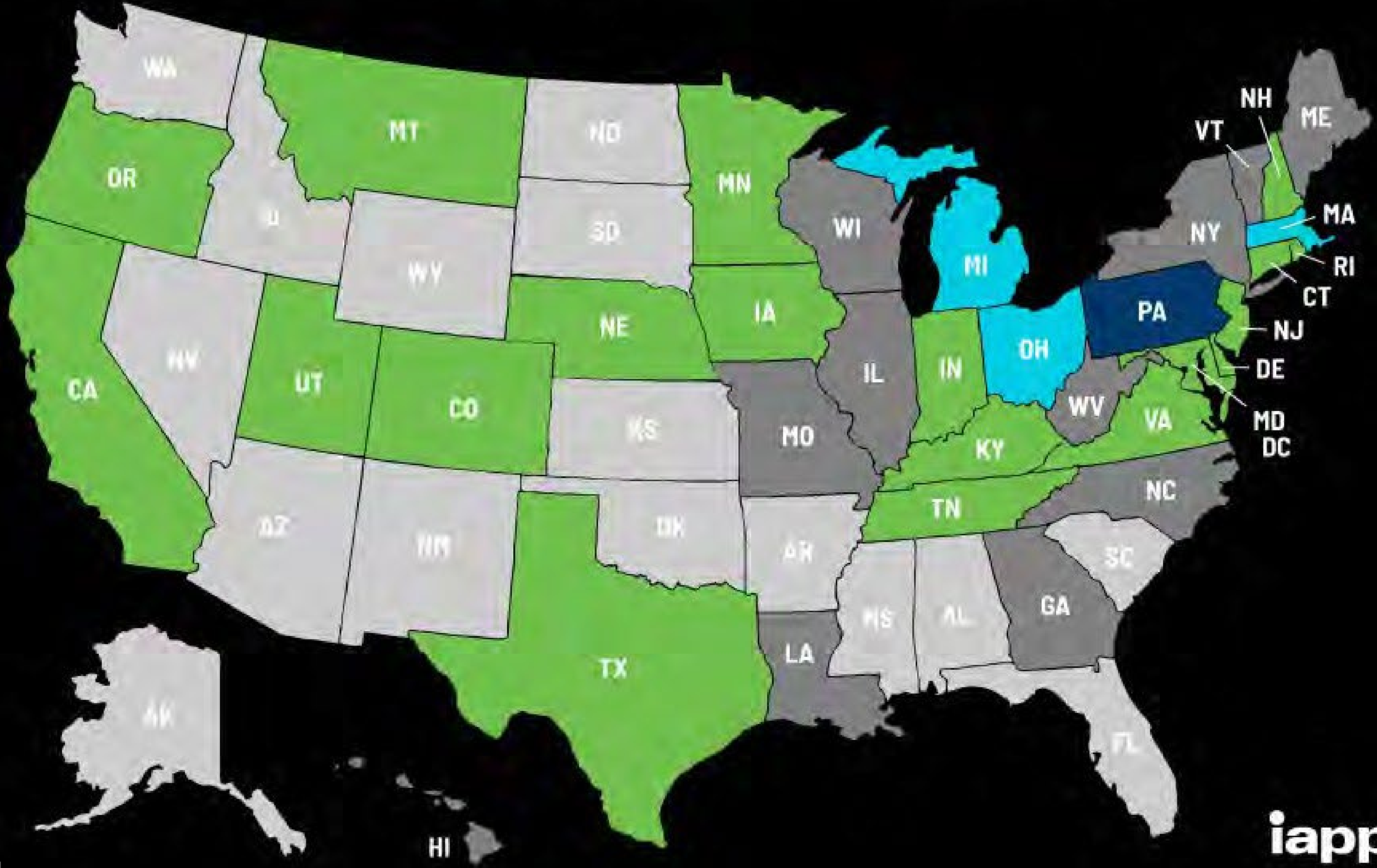
# Increasing Privacy Policies & Requirements

- A response to more demand.
- Every state is starting to adopt a privacy policy or privacy requirements: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

# US State Privacy Legislation Tracker 2024

## Statute/bill in legislative process

- 🟨 Introduced
- 🟦 In committee
- 🟦 In cross chamber
- 🟦 In cross committee
- 🟩 Passed
- 🟩 Signed
- ▨ Inactive bills
- ⬜ No comprehensive bills introduced



Last updated 22 July 2024

WHY IS THIS USEFUL?

# Contractual Obligations & Vendor Questionnaires

- **Client contracts**
  - Microsoft SSPA: Microsoft requires you to fill out their SSPA... ISO 27001 can replace this assessment
  - SSPA AI – ISO 42001
- **Vendor obligations**
  - Larger companies (like Walmart) are requiring startups to be ISO 27001 certified
  - Vendor Questionnaires: ISO cuts them down

SCOPING

## How to Carve Out Your Scope

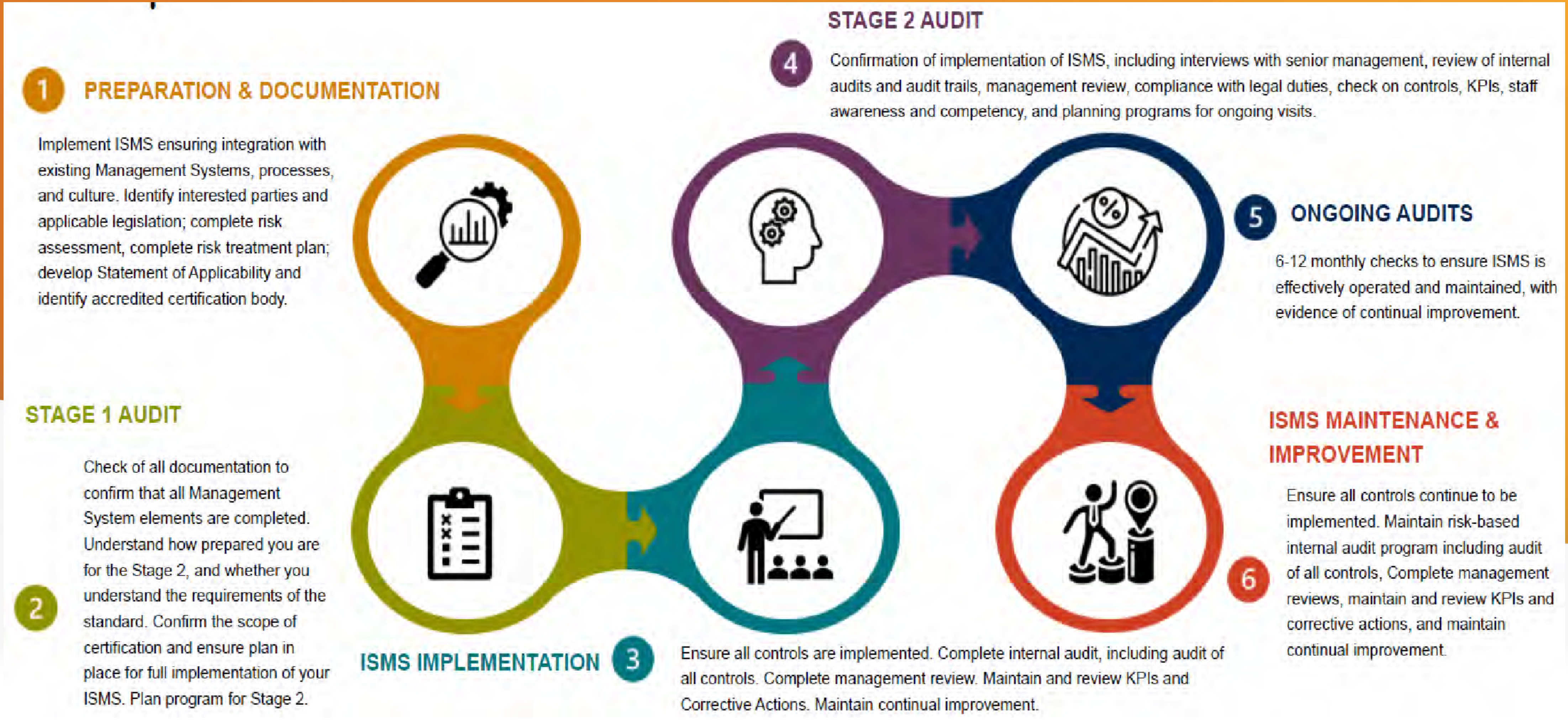
ISO 27001 scope is based on the organization's **headcount, locations, applications & dependencies.**

## How to Carve Out Your Scope/ PII Processor or Controller

ISO 27701 scope is based on the organization being a **controller, processor or both.**

- ISO 27701 scope can be the same or a carve out of your ISO 27001 scope.

# Certification Process



## 1 PREPARATION & DOCUMENTATION

Implement ISMS ensuring integration with existing Management Systems, processes, and culture. Identify interested parties and applicable legislation; complete risk assessment, complete risk treatment plan; develop Statement of Applicability and identify accredited certification body.

## 2 STAGE 1 AUDIT

Check of all documentation to confirm that all Management System elements are completed. Understand how prepared you are for the Stage 2, and whether you understand the requirements of the standard. Confirm the scope of certification and ensure plan in place for full implementation of your ISMS. Plan program for Stage 2.

## 3 ISMS IMPLEMENTATION

Ensure all controls are implemented. Complete internal audit, including audit of all controls. Complete management review. Maintain and review KPIs and Corrective Actions. Maintain continual improvement.

## 4 STAGE 2 AUDIT

Confirmation of implementation of ISMS, including interviews with senior management, review of internal audits and audit trails, management review, compliance with legal duties, check on controls, KPIs, staff awareness and competency, and planning programs for ongoing visits.

## 5 ONGOING AUDITS

6-12 monthly checks to ensure ISMS is effectively operated and maintained, with evidence of continual improvement.

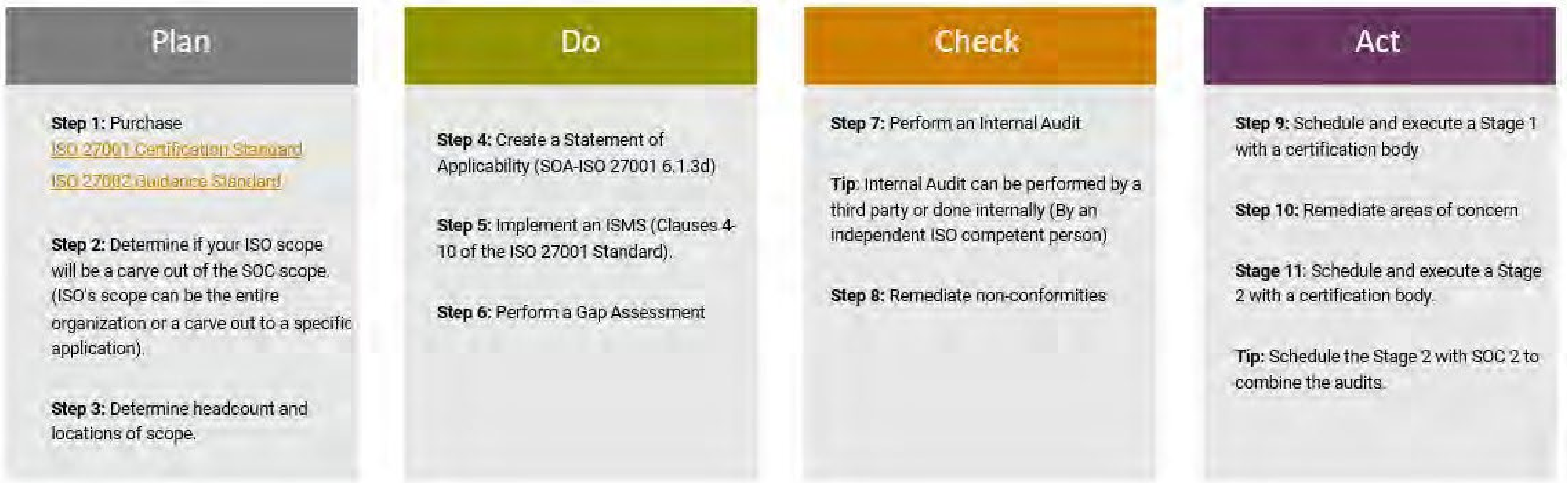
## 6 ISMS MAINTENANCE & IMPROVEMENT

Ensure all controls continue to be implemented. Maintain risk-based internal audit program including audit of all controls, Complete management reviews, maintain and review KPIs and corrective actions, and maintain continual improvement.

PROCESS

# How to add ISO after SOC 2

- SOC is an attestation, and ISO is a certification
- ISO certifications and SOC audits go hand in hand
    - 75% overlap… so a lot of clients that do a SOC Audit will want to include an ISO Certification as well because it is an international based standard.



**Plan**

**Step 1:** Purchase
ISO 27001 Certification Standard
ISO 27002 Guidance Standard

**Step 2:** Determine if your ISO scope will be a carve out of the SOC scope. (ISO's scope can be the entire organization or a carve out to a specific application).

**Step 3:** Determine headcount and locations of scope.

**Do**

**Step 4:** Create a Statement of Applicability (SOA-ISO 27001 6.1.3d)

**Step 5:** Implement an ISMS (Clauses 4-10 of the ISO 27001 Standard).

**Step 6:** Perform a Gap Assessment

**Check**

**Step 7:** Perform an Internal Audit

**Tip**: Internal Audit can be performed by a third party or done internally (By an independent ISO competent person)

**Step 8:** Remediate non-conformities

**Act**

**Step 9:** Schedule and execute a Stage 1 with a certification body

**Step 10:** Remediate areas of concern

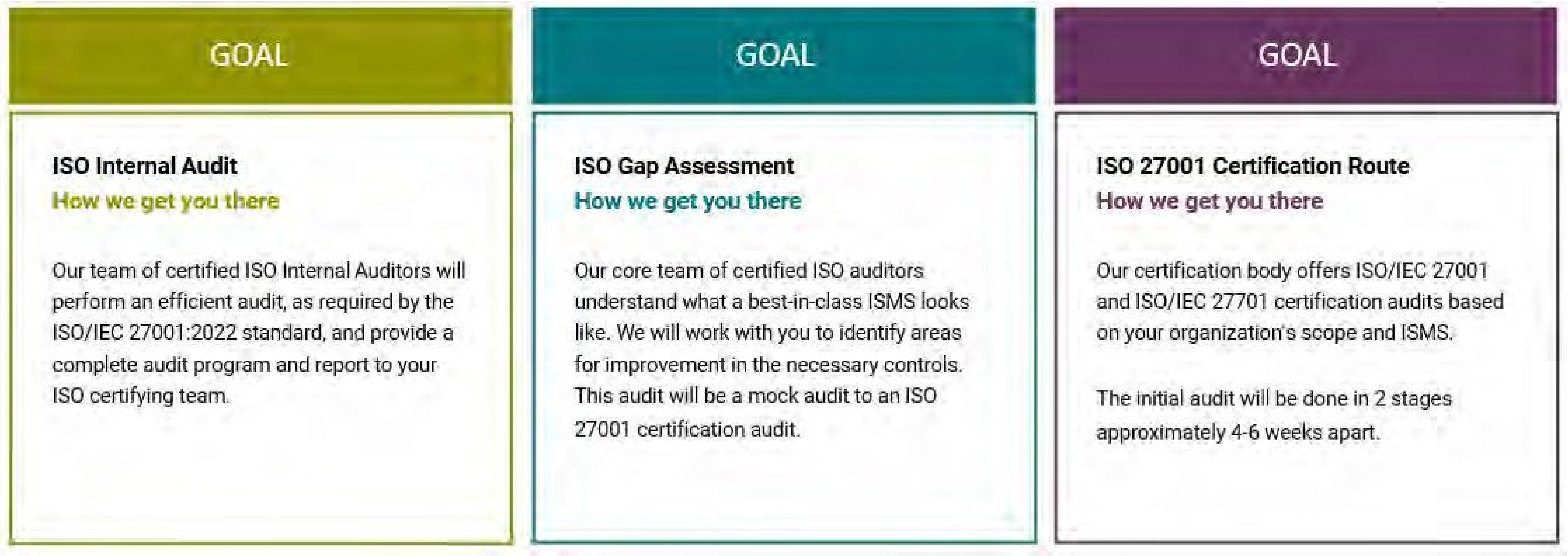
**Stage 11**: Schedule and execute a Stage 2 with a certification body.

**Tip:** Schedule the Stage 2 with SOC 2 to combine the audits.

PROCESS

# How to Get Started

- A plan of how we can work together to improve your ISMS/PIMS



GOAL

**ISO Internal Audit**

How we get you there

Our team of certified ISO Internal Auditors will perform an efficient audit, as required by the ISO/IEC 27001:2022 standard, and provide a complete audit program and report to your ISO certifying team.

GOAL

**ISO Gap Assessment**

How we get you there

Our core team of certified ISO auditors understand what a best-in-class ISMS looks like. We will work with you to identify areas for improvement in the necessary controls. This audit will be a mock audit to an ISO 27001 certification audit.

GOAL

**ISO 27001 Certification Route**

How we get you there

Our certification body offers ISO/IEC 27001 and ISO/IEC 27701 certification audits based on your organization's scope and ISMS.

The initial audit will be done in 2 stages approximately 4-6 weeks apart.

RECOMMENDATIONS

# Resources

- Should I be using a third-party?
  - Software companies
    - ✓ Risk Assessment
    - ✓ Templates
    - ✓ Monitoring
- Consultants
  - Everything customized for you
- Internal Audit
  - Done internally vs third-party

ISO CERTIFICATIONS

# Q&A

# Thank you for attending!

## Additional Questions?

Reach out to us at ISO@armanino.com

Possible (Re)Defined™

# [illegible]

“Armanino” is the brand name under which Armanino LLP, Armanino CPA LLP, and Armanino Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with law, regulations, and professional standards. Armanino LLP and Armanino CPA LLP are licensed independent CPA firms that provide attest services, and Armanino Advisory LLC and its subsidiary entities provide tax, advisory, and business consulting services. Armanino Advisory LLC and its subsidiary entities are not licensed CPA firms.