armanino

armanino.com

WELCOME

Learn How to Get ISO Certified

Webinar: June 9, 2021

bsi. By Royal Charter

What You Will Learn Today

Learn New ISO Standards & How You Can Get Certified

- Determine how to achieve ISO 27001 and ISO 27701 certifications
- Examine the importance of implementing these standards in your organization
- Identify changes in ISO certifications and data privacy laws

Panel

MODERATOR
Mirena Taskova
Managing Director | Armanino Advisory LLC
Mirena.Taskova@armanino.com

Brian Petersen
Director | Armanino Advisory LLC
Brian.Petersen@armanino.com

Willy Fabritius
BSI Group
Global Head InfoSec | Privacy and Business Continuity
Willibert.Fabritius@bsigroup.com

Nick Meyer
Manager| Armanino Advisory LLC
Nick.Meyer@armanino.com

What is ISO?

Global 165 Member countries

- Members of various national standards organizations come together to develop universal standards
- Helps to facilitate world trade

Diverse Broad range of standards

- Technical – ISO 27000, ISO 22301
- Environmental – ISO 14000
- Manufacturing – ISO 9000

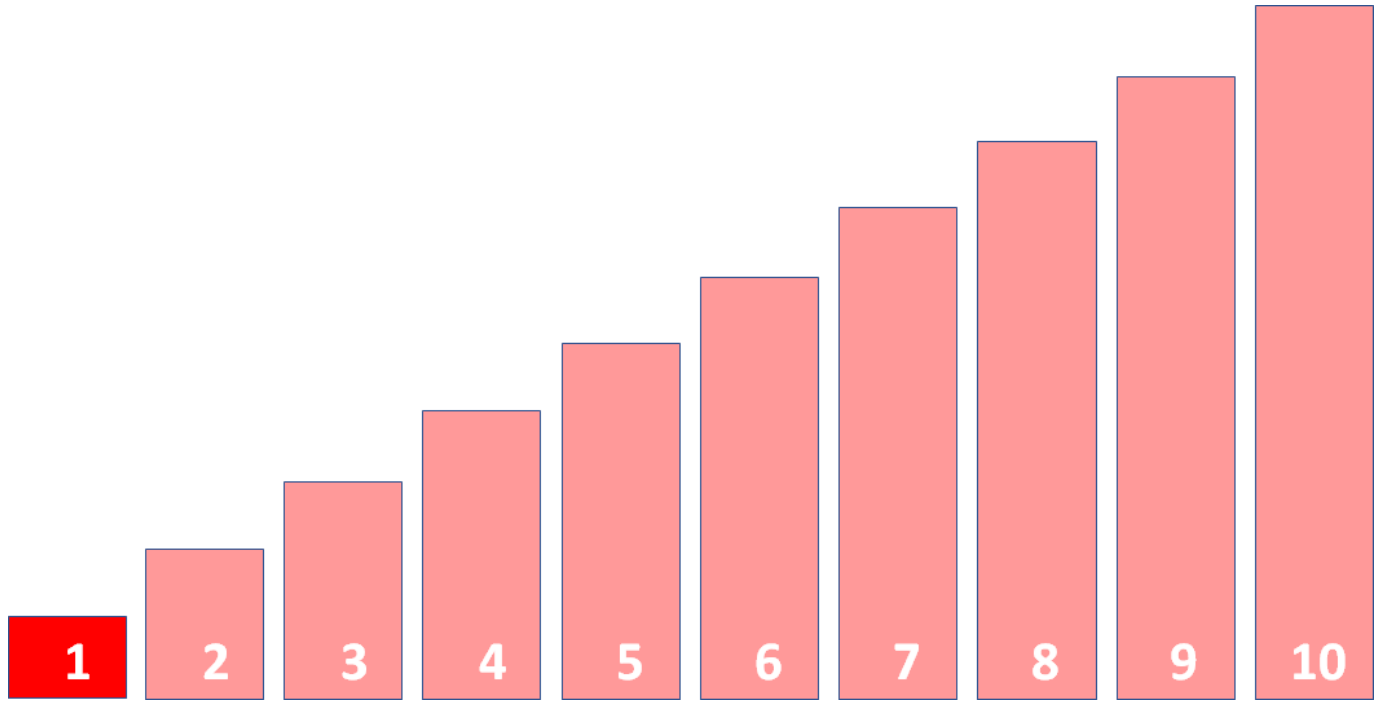
Independent ISO develops and publishes standards

- ISO does not certify compliance against the standard
- Other accredited bodies perform certifications

ISO Certification Process

Buy a standard

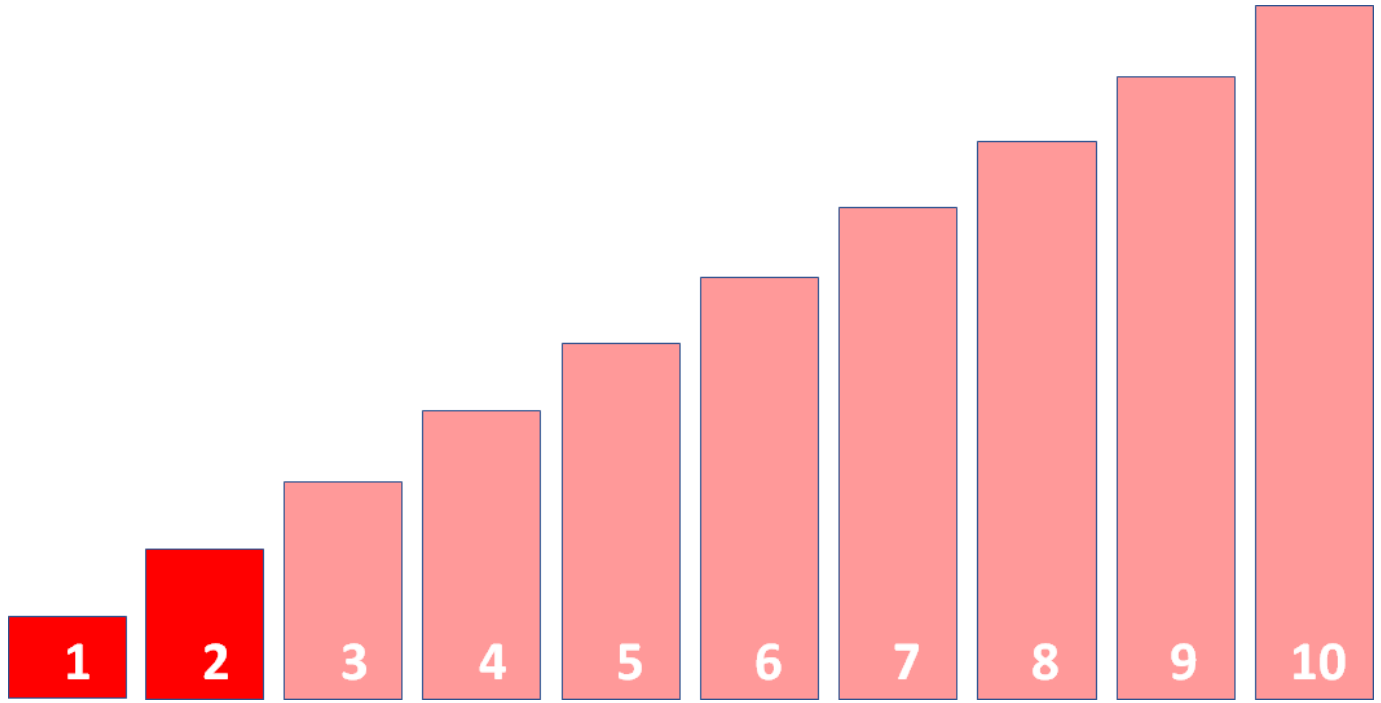
- To understand what is required from your organization and begin preparing for implementation, you'll need a copy of the standard.



ISO Certification Process

Contact a Partner

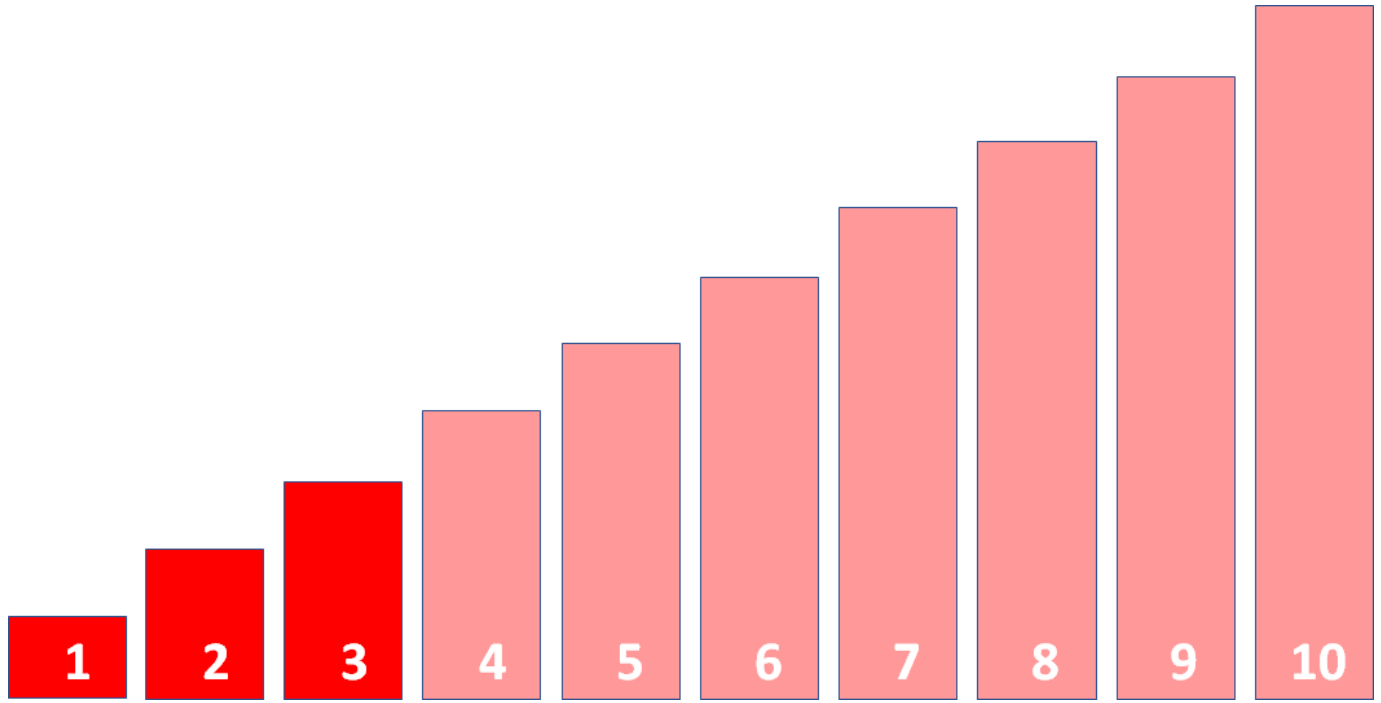
- To discuss what you need and recommend the best course for implementation and certification for you.



ISO Certification Process

The application

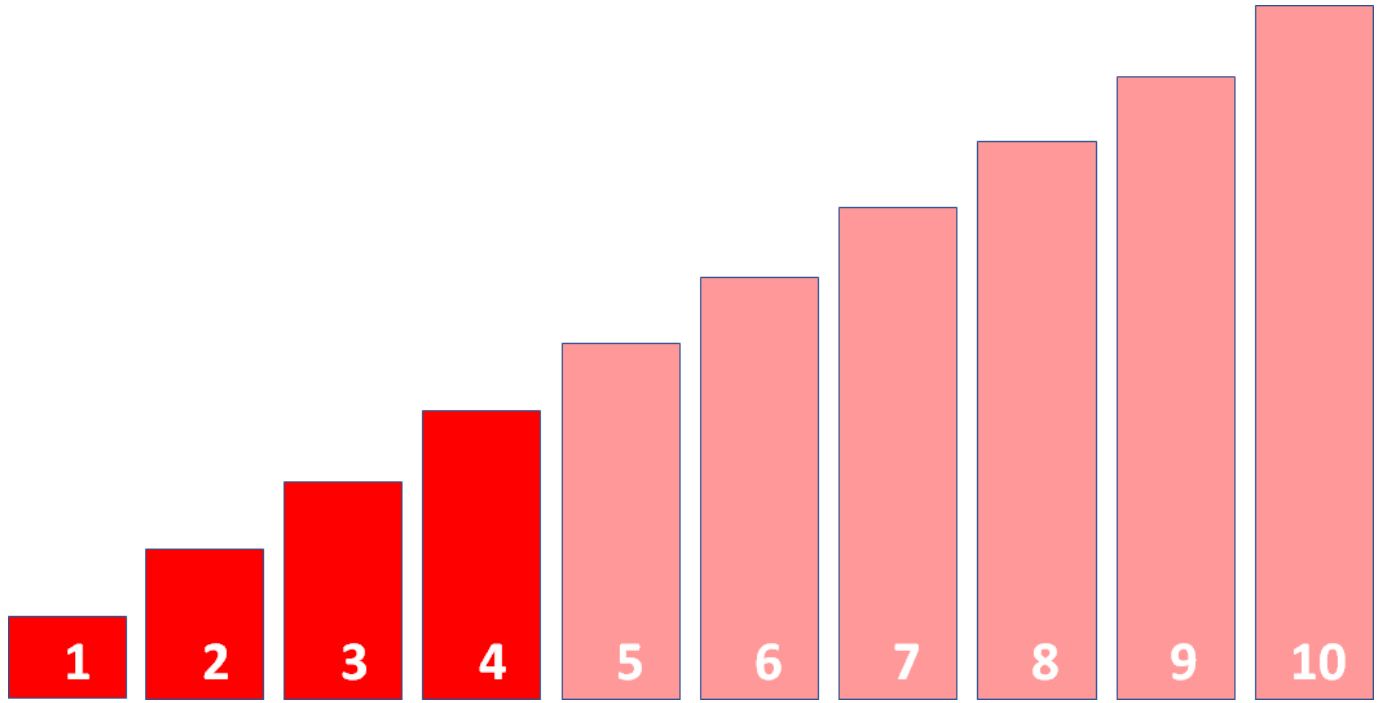
- Completing the application is a formal recognition of your organization applying for certification.



ISO Certification Process

Make sure you have the necessary skills and tools

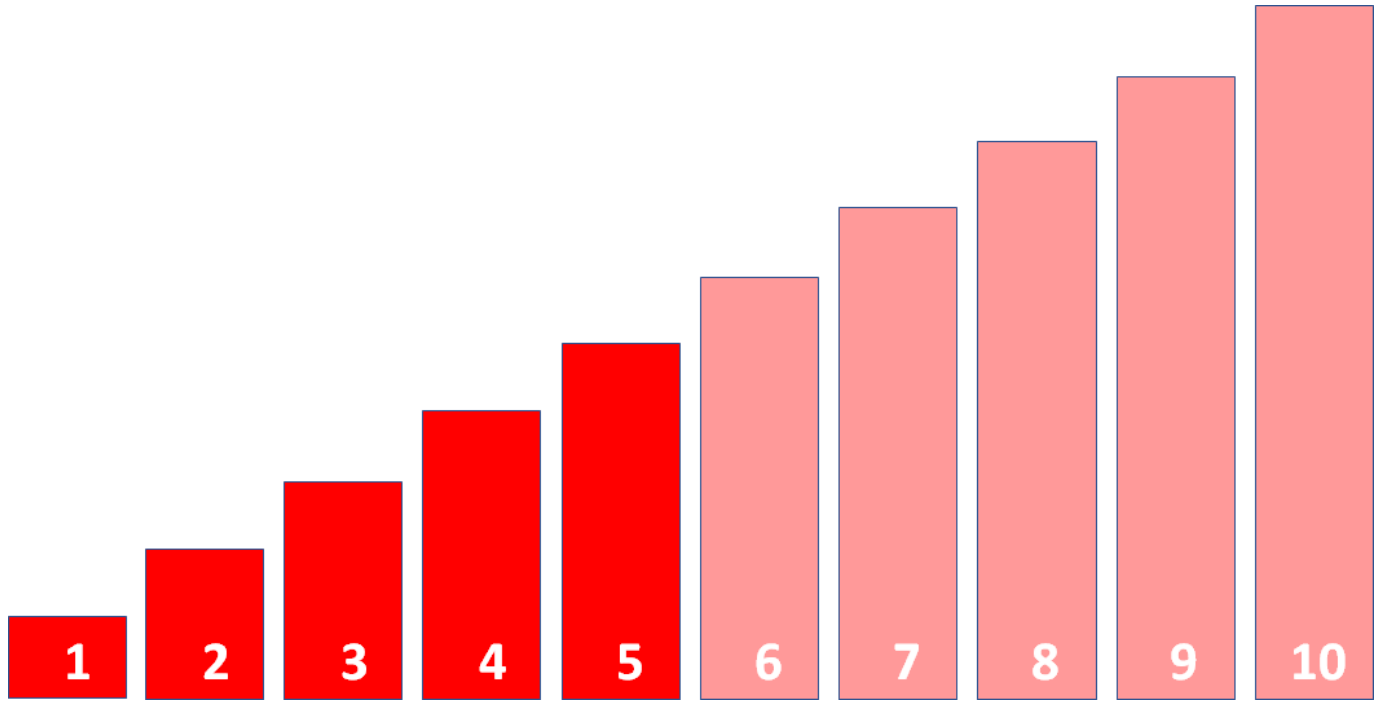
- Our range of workshops, seminars and training courses will help your staff understand your objectives and the roles necessary.



ISO Certification Process

Your assessment team is appointed

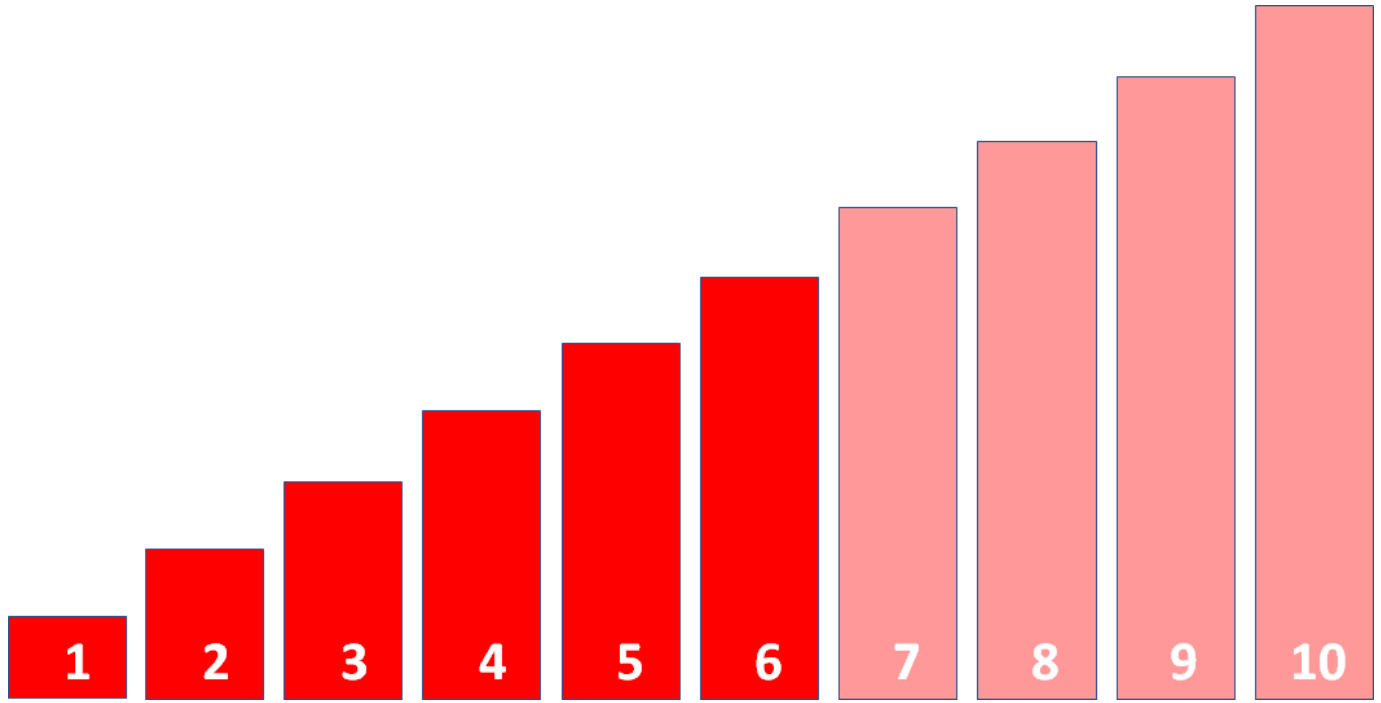
- Your ISO Certifying Auditor will be appointed a Client Manager with appropriate industry experience to ensure you are always getting the most from your certification.



ISO Certification Process

Gap Analysis

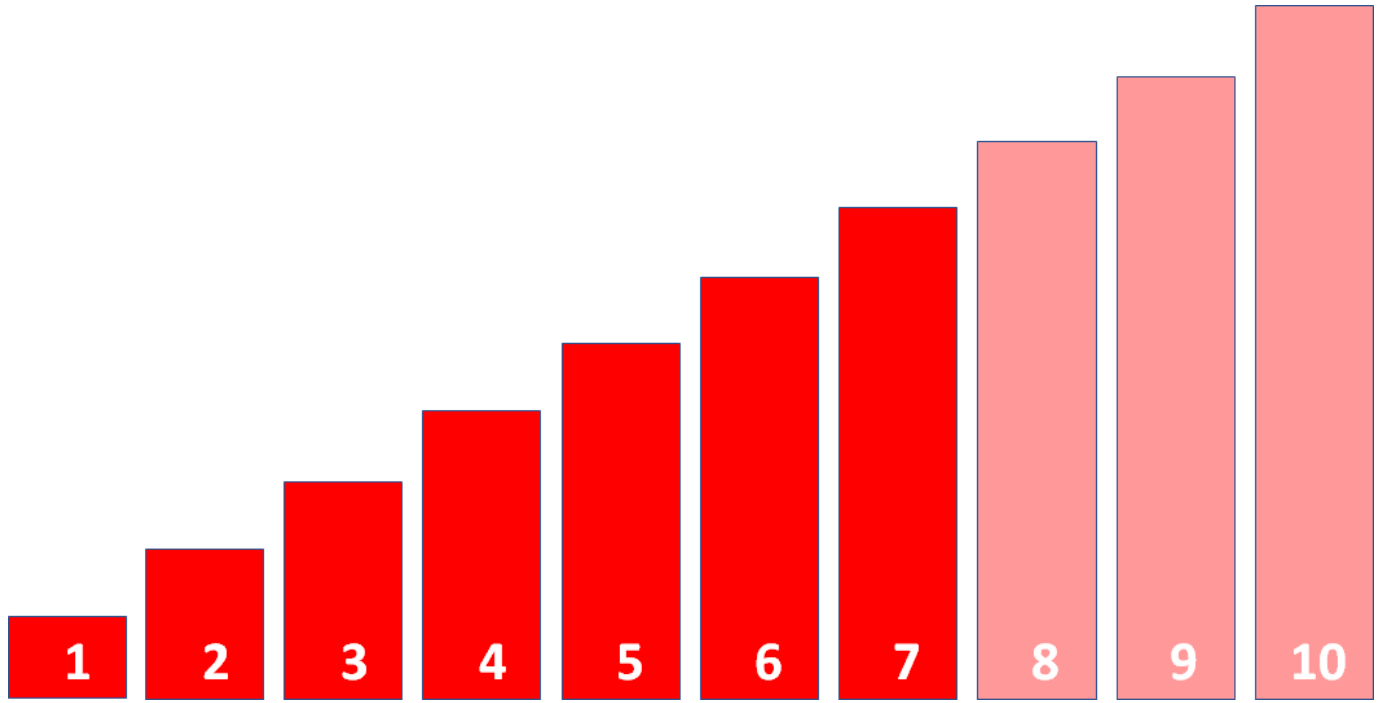
- The GAP assessment will look at the existing processes and procedures and compares these with the requirements of the standard. This will help you identify any areas that to be resolved.



ISO Certification Process

Assessment – Stage 1

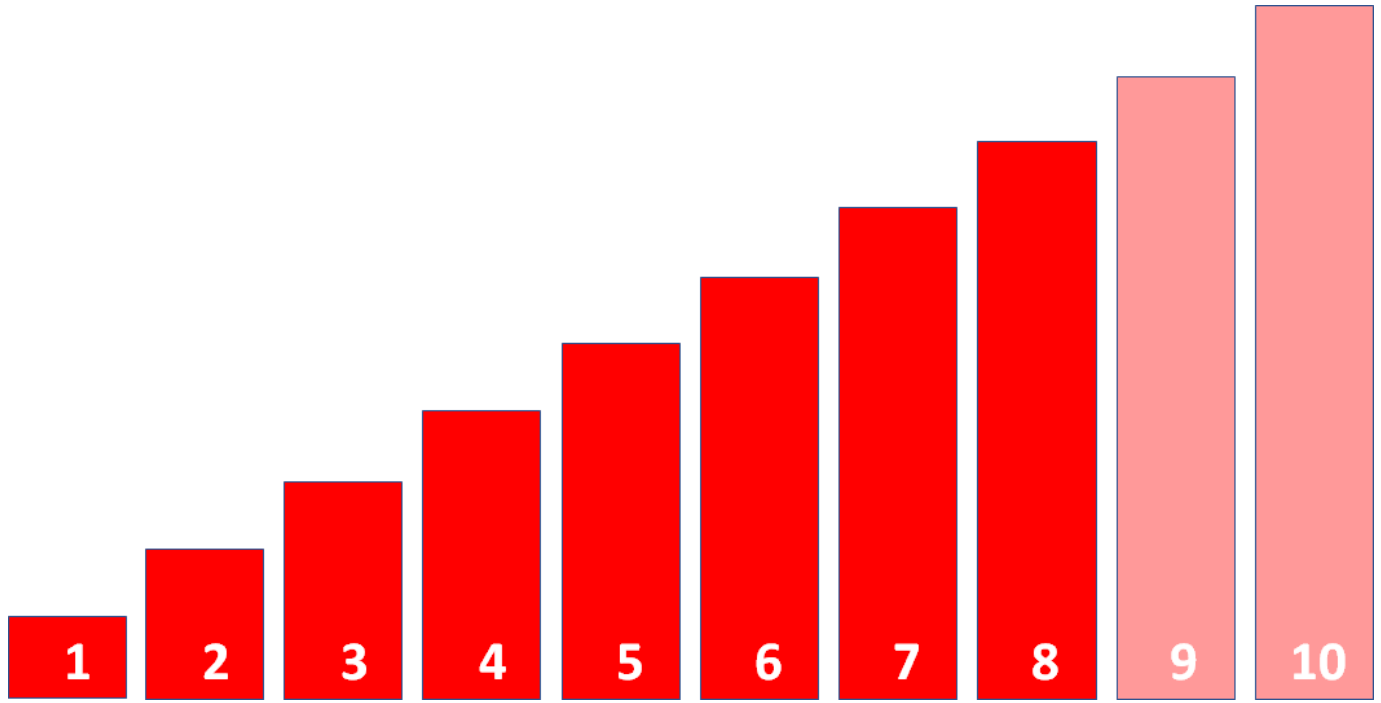
- We'll help you identify ways to improve your business performance. We'll then give you a proposal detailing the cost and time involved.



ISO Certification Process

Assessment – Stage 2

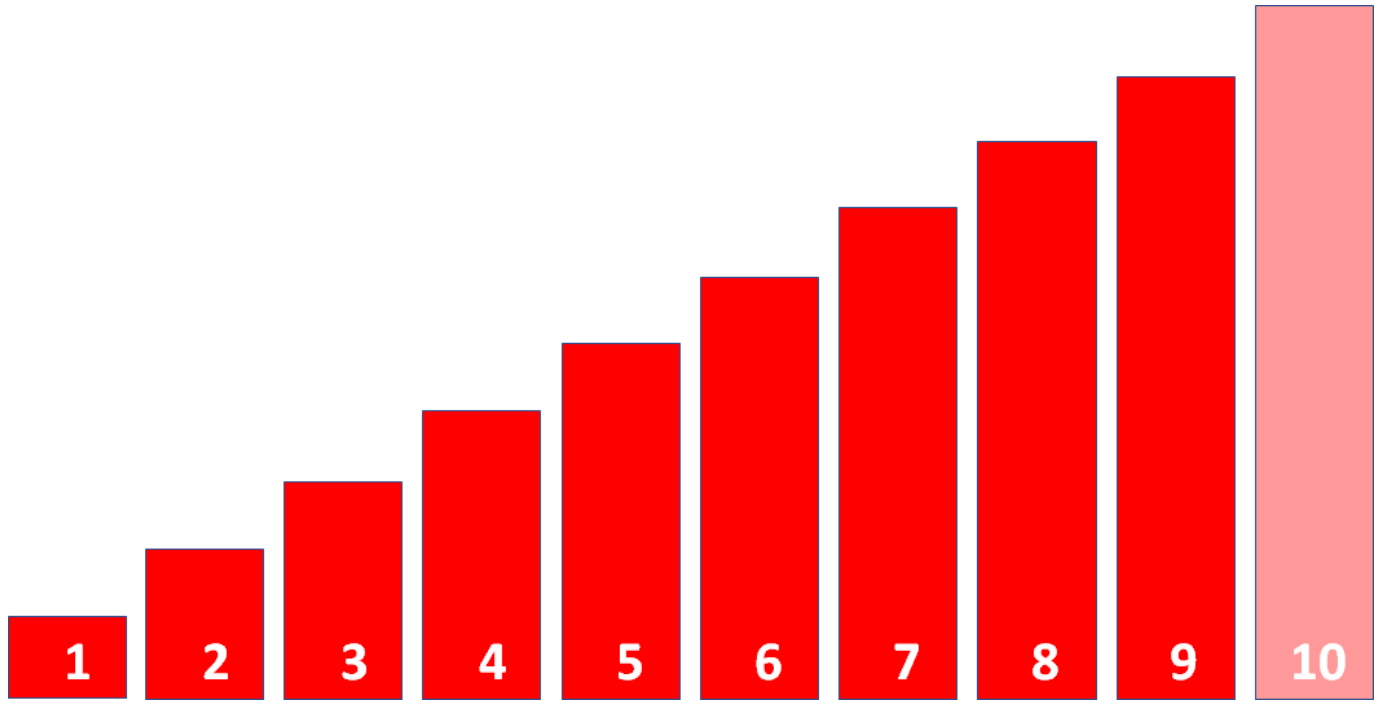
- This is the final assessment. Stage 2 confirms your management system is fully aligned to the standard and is fully operational within your organization.



ISO Certification Process

Achieving your certification

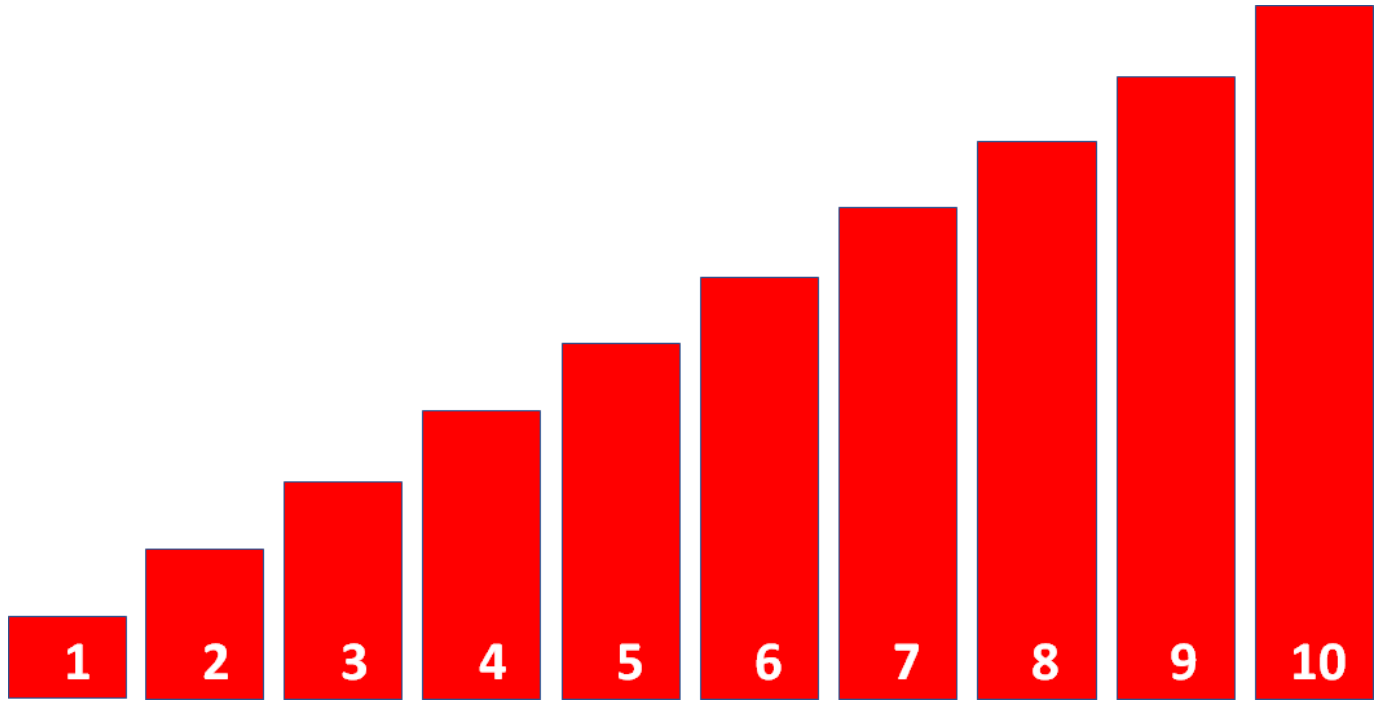
- Once you have certification, it's essentialthat you promote your achievement. Use your new BSI Assurance Mark as a valuable marketing tool to promote your certification.



ISO Certification Process

Make excellence a habit

- Monitor your compliance. Maintain a focus on continual improvement by leveraging internal audit, management reviews, and other assessments.



ISO 27000

What is ISO/IEC 27000?

Family of Standards

Information Security based series of standards

- To help organizations improve their controls over information security
- 27001 (ISMS clauses), 27002 (Security control clauses), 27005 (InfoSec Risk Management), 27017 (Cloud service providers), 27018 (processing PII), 27701 (Privacy Info Management System, PIMS), etc.

ISO/IEC 27001

ISMS (Information Security Management System) requirements

- Originally created by BSI; adopted by ISO in 2005
- The fundamental requirements for an InfoSec program
- Focuses on “entity-level” controls (e.g., executive leadership)

ISO/IEC 27002

Security controls

- Controls noted in “Annex A” of ISO 27001
- Offers a wide selection of controls (technical and non-technical) to protect information assets
- A revision of this standard is currently under development

ISO/IEC 27001:2013

Organization-level requirements for establishing, implementing, maintaining, and continually improving an **information security management system (ISMS)**

Other ISO/IEC 27000 family standards are **complementary** to ISO/IEC 27001

The primary focus is on **continual improvement** of the ISMS

Organizations must **define a clear scope** for their ISMS

An ISMS requires a solid **tone-at-the-top** and **segregated roles and responsibilities**

ISO/IEC 27002:2013

Your **risk assessment** and risk management approach will determine the controls necessary for implementation (i.e., your risk treatment plan)

Your suite of controls is referred to as your **Statement of Applicability** or "**SOA**"

The 14 security control clauses are intended to provide a "**Defense in Depth**" strategy for any organization, but may **not** cover all necessary controls

ISO 27005 provides guidance on analyzing risk and selecting additional controls / risk treatment options

Risk assessments and risk treatments need to be **continuously** evaluated

ISO/IEC 27001 Growth

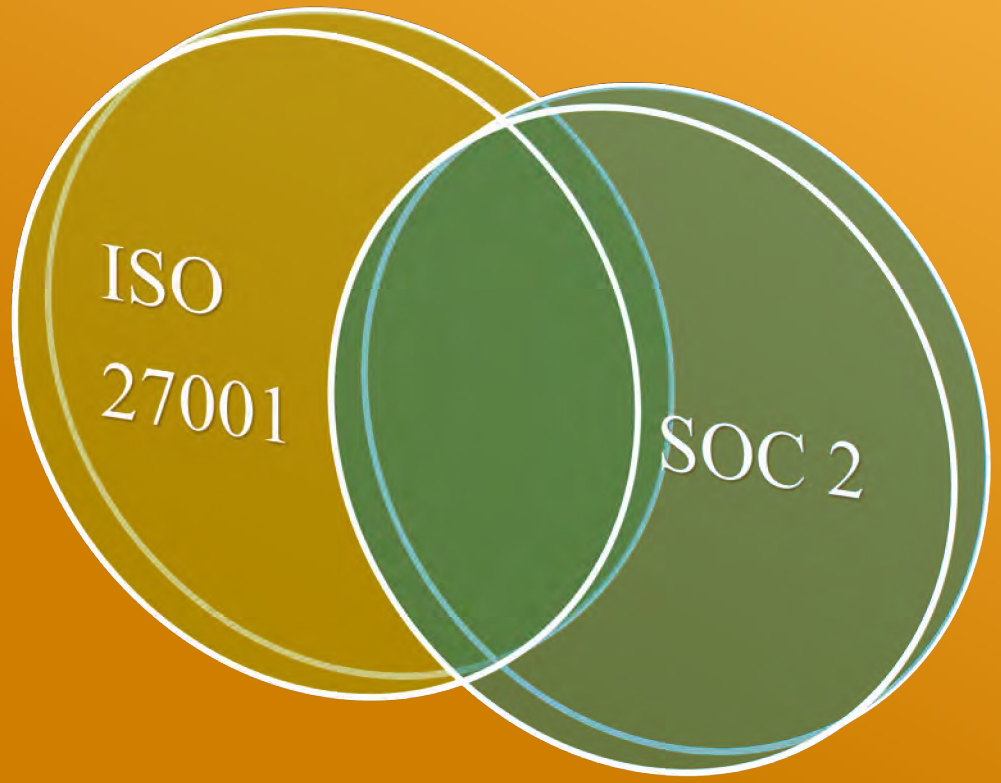
Parallel Frameworks

ISO & SOC 2 Similarities

- Similar information security controls
- Privacy component
- Require independent assessments
- Similar appeal to customers

ISO & SOC 2 Differences

- ISO has more focus on ISMS controls
- Certification vs. Attestation
- 3-year vs. Annual



ISO 27701

ISO/IEC 27701

ISO/IEC 27701 is an extension to ISO/IEC 27001 for the management of Personally Identifiable Information (PII)

PIMS - Privacy Information Management System

Framework defines PIMS controls for both **PII Controllers** and **PII Processors**

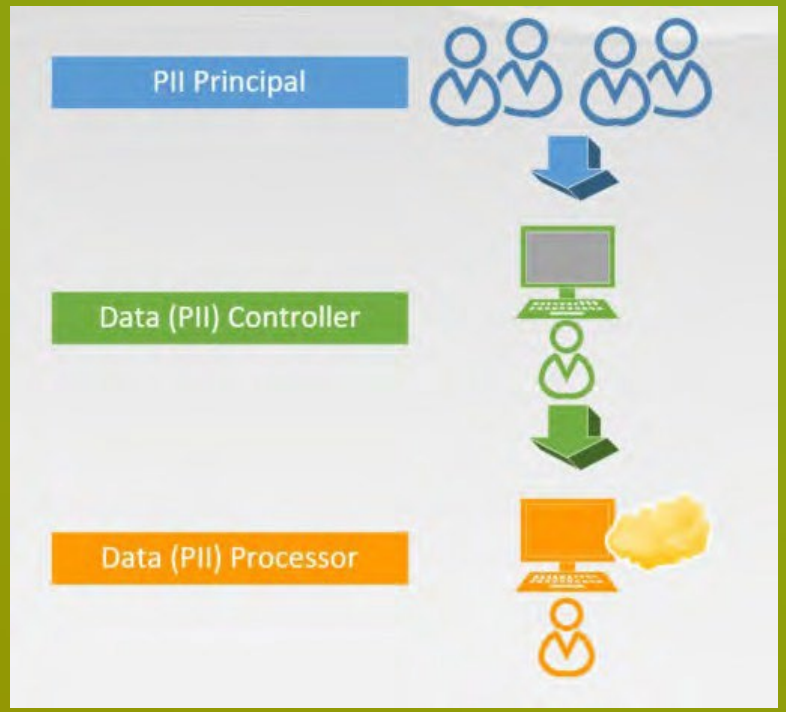
ISO/IEC 27701 contains an Annex (D) **mapping the standard to the GDPR**

Framework provides applicable guidance on managing PII for **companies of all types and sizes**

ISO/IEC 27701

Requirements for PII Controller (Clause 7) & PII Processor (Clause 8)

Conditions for collection and processing	Obligations to PII principals	Privacy by design and privacy by default	PII sharing, transfer, and disclosure



Changes in ISO Standards

Privacy Updates – Data Transfers from Europe

- On June 4, 2021, the European Commission published its final implementing decision adopting modernized standard contractual clauses ("New SCCs") under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR).

- The New SCCs will replace the old three sets that were adopted under the previous Data Protection Directive 95/46.

- The Implementing Decision will be effective on the 20th day following its publication in the Official Journal of the EU, meaning that **the New SCCs can be used from June 27, 2021**.

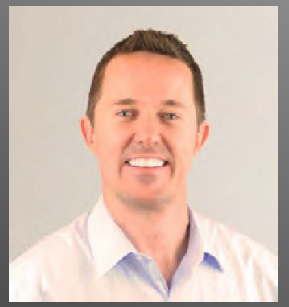
- You can continue signing the previous sets for another 3 months but **after September 27, 2021, no new contracts can be signed using the old set.**

- Transition period – **Until December 27, 2022** (I.e. 18 months from the effective date of the Implementing Decision) **you should revise your agreements (which incorporate the old sets) by replacing the old sets with the New SCCs - unless your processing operations change, in which case the new SCCs should be used from that moment.**

Thank You

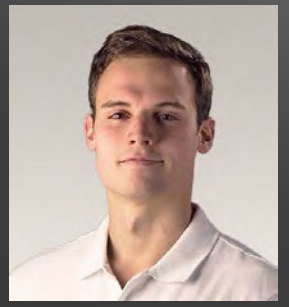
Contact Us

Mirena Taskova
Managing Director | Armanino Advisory LLC
Mirena.Taskova@armanino.com



Brian Petersen
Director | Armanino Advisory LLC
Brian.Petersen@armanino.com

Willy Fabritius
BSI Group
Global Head InfoSec | Privacy and Business Continuity
Willibert.Fabritius@bsigroup.com



Nick Meyer Manager|
Armanino Advisory LLC
Nick.Meyer@armanino.com

⌂ś › ŢăŢű÷Ç Ll ⌂› ┼ ┴ ═ăŢ⇒ Ţ÷ ő┼ ⌂Ţ› ┼ă╗┼ ÷ õ⌂› ˜ ┼ã˜ ł ÷¢┬⌂F˜ ┬F⌂l □