

Privacy Information Management System (PIMS) ISO 27701:2019

If your organization acts as either a **data controller** or a **data processor** (or both), this standard extends the context of your organization within an information security management system (ISMS) under ISO 27001 with additional requirements and controls. Through a privacy impact analysis, the organization identifies its risks to an individual's data privacy and data protection of personally identifiable information (PII). Personal data is information that relates to an identified or identifiable individual.

ISO 27701:2019: Privacy Information Management System (PIMS) provides a framework which supports an organization's ability to protect personally identifiable information (PII) and meet ever-evolving regulatory requirements. ISO 27701 alone is not able to receive an ISO certification. An organization can add to an existing or implement concurrently with an ISO 27001 system for a "dual" mark certification.

Why Implement and ISMS and PIMS?

- ✓ The basis of a functional PIMS is balanced between **data protection** and **data privacy**.
 - Data protection means keeping data safe from unauthorized access.
 - Data privacy means empowering individuals to make their own decisions about who can process their data and for what purpose.
- ✓ PIMS are systems that help give individuals more control over their personal data.
- ✓ PIMS allow individuals to manage their personal data in secure, local or online/hardcopy environments and share these details when and with whom the individual chooses. **Personal data is information that relates to an identified or identifiable individual.**
- ✓ The requirement for a privacy impact analysis allows an organization to identify its risks to an individual's data privacy and data protection.
- ✓ Specific Annex controls in ISO 27701 are added to the ISMS and managed as part of a larger **information and privacy management system**.
- ✓ PIMS helps to ensure compliance to growing global privacy requirements



ABOUT RADIAN COMPLIANCE, LLC

COMPANY INFO

www.RadianCompliance.com
Info@RadianCompliance.com
630-305-7100

LOCATIONS

Chicago and Washington D.C. Metro

SUPPLIER CODES

DUNS: 964813237
CAGE: 75B51

CONTACT

Sally Smoczynski, CISSP
Managing Partner / Owner
SSmoczynski@RadianCompliance.com
630-728-7181

Lisa DuBrock, CPA, CPP, CBCP
Managing Partner / Owner
LDuBrock@RadianCompliance.com
847-997-2032

CERTIFICATIONS ACCREDITATIONS



Radian Compliance, LLC applies its 100% successful methodology to assist clients with ISO management systems standards and regulatory frameworks to maintain compliance or obtain certification. Radian supports its clients with ongoing knowledge and consulting with evolving legal, regulatory and contractual compliance requirements. Radian is a **WBENC certified Women Business Enterprise and Woman Owned Small Business, a CMMC-AB Registered Provider Organization™ and an ASIS Preferred CPE Provider.**

The Radian Team supports and are recognized as subject matter experts in the following standards and frameworks:

Solution	Formats Supported
Management Systems	ISO 9001 ▪ ISO 22301 ▪ ISO 31000 ▪ ISO 28000 ▪ ISO 14001
Information Security, Cybersecurity & Privacy	ISO 27001 ▪ ISO 27701 ▪ CMMC ▪ NIST ▪ HIPAA
IT Service Management	ISO 20000-1 ▪ ITIL
Private Security Companies – Land & Marine	ISO 18788 ▪ ANSI/ASIS PSC.1
Compliance Assessment & Program Development	Workplace violence prevention programs ▪ Physical security assessments ▪ ITAR/EAR

PIMS Differentiators

The Radian team's experiences are deeply rooted in information security and data privacy. Not only are we experts in the ISO process, but we have knowledge of GDPR and the continued addition of state privacy laws such as those in California, Ohio, Illinois, Massachusetts and now Virginia. Our team is constantly learning and providing relevant information to our customers of this ever-changing privacy landscape. We are active in security organizations such as ASIS, (ISC)2 and IAPP.