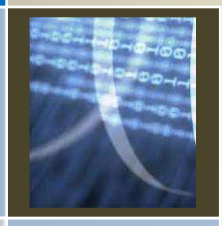
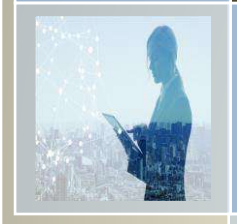
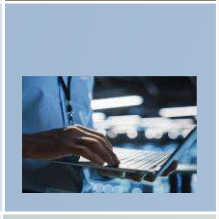
**Deming Certification & Rating Pvt. Ltd.**
Email: - info@demingcert.com
Contact: - 02502341257/9322728183
Website: - www.demingcert.com
No. 108, Mehta Chambers, Station Road, Novghar, Behind Tungareswar Sweet,
Vasai West, Thane District, Mumbai- 401202, Maharashtra, India







# ISO 27018:2019 Code of practice for protection of personally identifiable information (PII) in public clouds

What is ISO 27018:2019 Code of practice for protection of personally identifiable information (PII) in public clouds ?

**ISO/IEC 27018** is a security standard part of the ISO/IEC 27000 family of standards. It was the first international standard about the privacy in cloud computing services which was promoted by the industry. It was created in 2014 as an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. It helps cloud service providers who process personally identifiable information (PII) to assess risk and implement controls for protecting PII.[1] It was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27.

## Structure of the standard

The official title of the standard is "Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors". ISO/IEC 27018:2019 has eighteen sections, plus a long annex, which cover:

1. Scope
2. Normative References
3. Terms and definitions
4. Overview
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communications security
14. System acquisition, development and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management

# Objectives

The objective of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. It has the following objectives:

- Help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract.
- Enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services.
- Assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement.
- Provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multiparty, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place.

# Advantages

Using this standard has the following advantages:

- It provides a higher security to customer data and information.
- It makes the platform more reliable to the customer, achieving a higher level than the competition.
- Faster enablement of global operations.
- Streamlined contracts.
- It provides legal protections for cloud providers and users.

## List of International Organization for Standardization standards

This is a list of published International Organization for Standardization (ISO) standards and other deliverables. For a complete and up-to-date list of all the ISO standards, see the ISO catalogue.

The standards are protected by copyright and most of them must be purchased. However, about 300 of the standards produced by ISO and IEC's Joint Technical Committee 1 (JTC 1) have been made freely and publicly available.

ISO Brand

This is a dynamic list and may never be able to satisfy particular standards for completeness. You can help by adding missing items with reliable sources.

.

## Background

Organizations of all types and sizes increasingly want to reduce the amount of energy they consume. This is driven by the need or desire to:

- reduce costs,
- reduce the impact of rising costs,
- meet legislative or self-imposed carbon targets,
- reduce reliance on fossil fuels, and
- enhance the entity's reputation as a socially responsible organization.

In tandem, governments increasingly want to reduce the Greenhouse Gas Emissions of their citizens and industries, and are imposing legislative mechanisms to compel carbon reduction more and more frequently.

In response, a range of energy management standards, specifications and regulations were developed in Australia, China, Denmark, France, Germany, Ireland, Japan, Republic of Korea, Netherlands, Singapore, Sweden, Taiwan, Thailand, New Zealand and the USA.

Subsequently, the European Committee for Standardization (CEN) developed EN 16001:2009 *Energy management systems. Requirements with guidance for use* as a first international energy management standard. This was published in July 2009 and withdrawn in April 2012 as it had been superseded by ISO 50001.

## Development

The United Nations Industrial Development Organization (UNIDO) recognized that industry around the world needed to mount an effective response to climate change.[1] It also noted a proliferation of national energy management standards that were emerging as a response to market demand for help with energy efficiency.

In April 2007, a UNIDO stakeholders meeting decided to ask ISO to develop an international energy management standard.

ISO for its part had identified energy management as one of its top five areas for the development of International Standards and, in 2008, created a project committee, ISO/PC 242, *Energy management*, to carry out the work.

ISO/PC 242 was led by ISO members for the United States (ANSI) and Brazil (ABNT). In addition, its leadership included the ISO members for China (SAC) and the United Kingdom (BSI Group) to ensure that developed and developing economies participated together in the project committee.

Experts from the national standards bodies of 44 ISO member countries participated and another 14 countries sent observers. Development organizations including UNIDO and the World Energy Council (WEC) were also involved.

ISO 50001 also drew on existing national and regional energy management codes and standards, including ones developed in China, Denmark, Ireland, Japan, Republic of Korea, Netherlands, Sweden, Thailand, the US and the European Union.

ISO published a revised version of ISO 50001 in 2018. The revision reflects a desire to promote adoption of the standard among small and medium sized enterprises. It also incorporates ISO's "high level structure" for use where organizations wish to integrate a number of management system standards together.

There are ten major components to ISO 50001:2018:

- *1.*: Scope
- *2.*: Normative references
- *3.*: Terms and definitions
- *4.*: Context of the organization
- *5.*: Leadership
- *6.*: Planning
- *7.*: Support
- *8.*: Operation
- *9.*: Performance Evaluation
- *10.*: Improvement

## Method

ISO 50001 provides a framework of requirements that help organizations to:

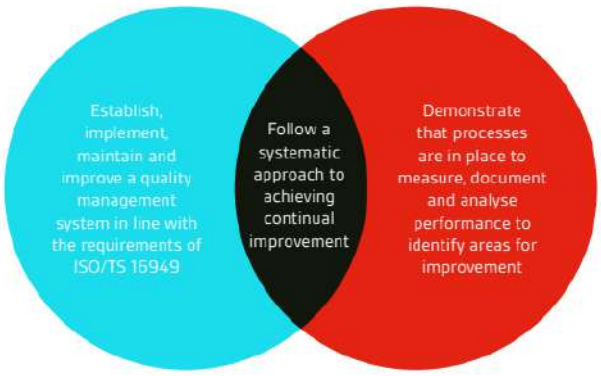
- develop a policy for more efficient use of energy
- fix targets and objectives to meet the policy
- use data to better understand and make decisions concerning energy use and consumption
- measure the results
- review the effectiveness of the policy and
- continually improve energy management.

ISO 50001 focuses on a continual improvement process to achieve the objectives related to the environmental performance of an organization (enterprise, service provider, administration, etc.). The process follows a plan – do – check – act approach.


The 4 phases of the PDCA circle

The overall responsibility for the installed energy management system must be located with the top management. An energy officer and an energy team should be appointed. Furthermore, the organization has to formulate the energy policy in form of a written statement which contains the intent and direction of energy policy. Energy policy must be communicated within the organization. The energy team is the connection between management and employees. In this phase the organization has to identify the significant energy uses and prioritize the opportunities for energy performance improvement.

## The principal requirements of the standard are illustrated below:

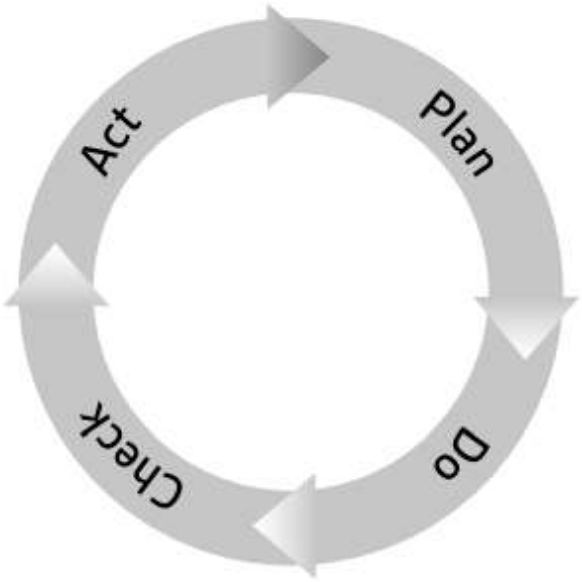



The next few pages of the guide takes you through the Plan-Do-Check-Act (PDCA) methodology, common in all ISO management systems and how DCS can help and support you on your ISO/TS 16949 journey.

## Understanding the principles of continual improvement

## Act

Correct and improve your plans to meet and exceed your planned results




## Plan

Establish objectives and draft your plans (analyse your organization's current systems, establish overall objectives, set interim targets for review and develop plans to achieve them)

## Check

Measure and monitor your actual results against your planned objectives

## Do

Implement your plans within a structured management framework