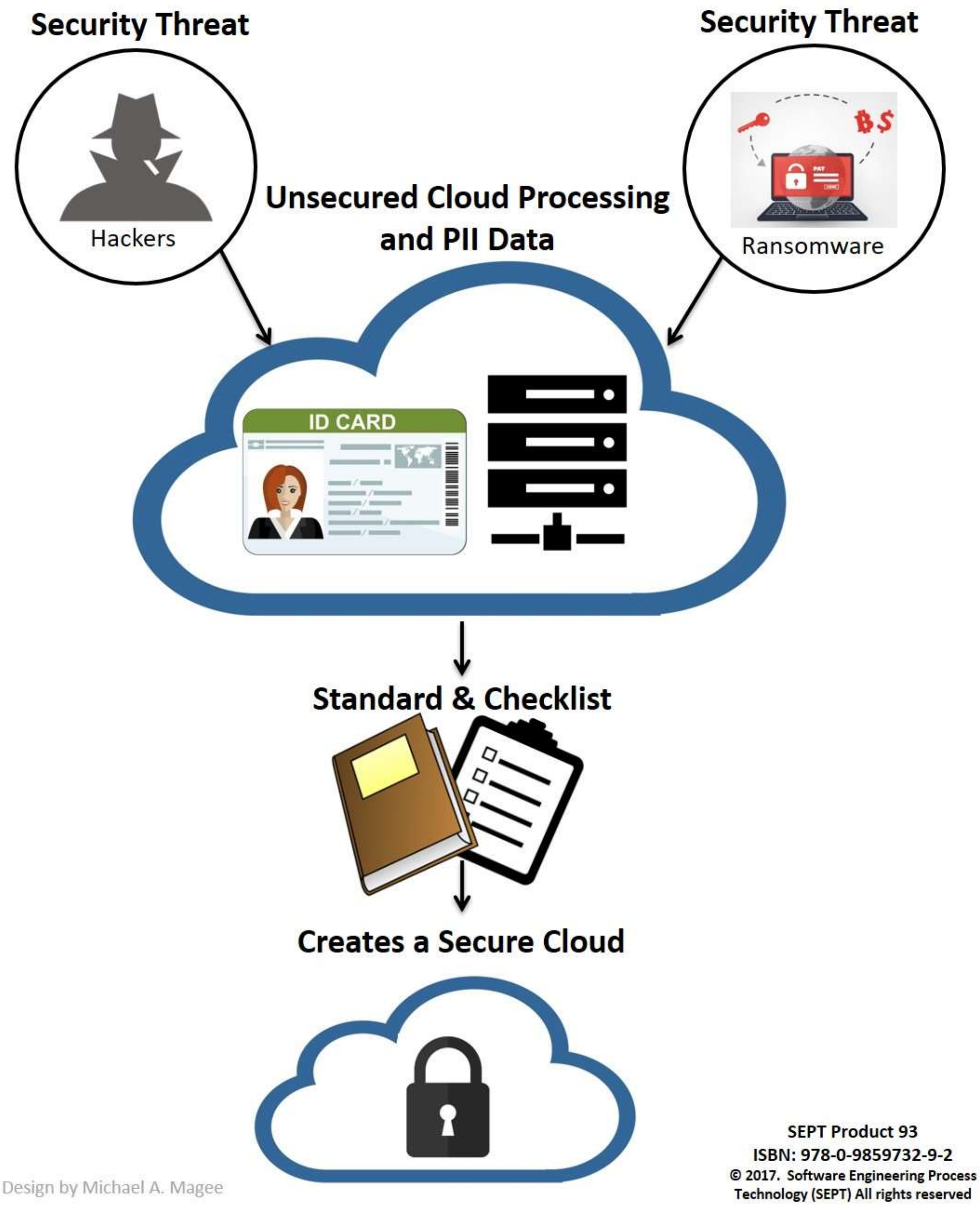
SEPT
In Business
since 1992

Checklist ☑ for Standard ISO/IEC 27018:2014 Information Security - Protection of Personally Identifiable Information (PII)



Security Threat

Hackers

Security Threat

Ransomware

Unsecured Cloud Processing and PII Data

Standard & Checklist

Creates a Secure Cloud

Cover Design by Michael A. Magee

SEPT Product 93
ISBN: 978-0-9859732-9-2

Checklist for Standard ISO/IEC 27018:2014 - Information Technology – Security Techniques

Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

SEPT Product 93

ISBN 978-0-9859732-9-2

Authors: **Andy Coster CQI and Stan Magee CCP (Ret.)**

Produced by Software Engineering Process Technology (SEPT)
1705 16th Lane NE Suite P203
Issaquah WA 98029
Tel. 425-391-2344
E-mail: stanmagee@smartwire.net
Web Site: www.12207.com

Change Page History

Date	Change	Reason
7/18/2017	First Version	

Checklist for Standard ISO/IEC 27018:2014 - Information Technology – Security Techniques

Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

SEPT Product 93

Components of the Checklist

This checklist is composed of 9 sections:

- Section 1. Introduction
- Section 2. Composites of all required and suggested "ISO/IEC 27018:2014 artifacts.
- Sections 3-8. Individual checklists for each evidence type.
- Sections 9. About the authors

Purpose of this standard

More companies are going to the cloud each day. The "cloud" offers organizations a variety of benefits: cost savings, flexibility, and mobile access to information. However, it also raises concerns about data protection and privacy; particularly around personally identifiable information (PII). PII includes any piece of information that can identify a specific user. The more obvious examples include names and contact details or your mother's maiden name. The cloud processor also has high risk. Security must be extremely high especially if you have a subcontractor doing part of the work. If this data is compromised it could cost a company customers, money, and reputation

Overview of the base standard ISO/IEC 27018:2014

ISO/IEC 27018 establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

ISO/IEC 27018 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

ISO/IEC 27018 is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in ISO/IEC 27018 might also be relevant to organizations acting as PII controllers; however, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. ISO/IEC 27018 is not intended to cover such additional obligations

Annex A to ISO/IEC 27018:2014 specifies new controls and associated implementation guidance which, in combination with the augmented controls and guidance in ISO/IEC 27002, make up an extended control set to meet the requirements for PII protection which apply to public cloud service providers acting as PII processors. These additional controls are classified according to the 11 privacy principles of ISO/IEC 29100.

Relationship to other 27000 Standards

If a PII processor wants to become certified to ISO/IEC 27001 – Information Security – Requirements then it should assess its practices using ISO/IEC 27002 – Information Security – Code of Practice.

In addition, there are specific controls specified in ISO/IEC 27018 that need to be addressed. If a PII processor is not interested in certification, the requirements and guidelines in these three standards should be an important part of business considerations.

SEPT provides checklists for all three standards to assist in understanding the requirements and related practices.

Purpose of the SEPT checklist

The task of getting information security under control is daunting. The last thing an organization wants in its security management operation is to call in a Notified Body for certification and to find out that the organization is lacking the correct records or documents for the auditor to examine. If you do not read the standard correctly it could cause a security problem or could increase the cost to become certified. That is why we believe a checklist is important.

For 20 + years Software Engineering Process Technology (SEPT) has been producing checklists for standards that address software issues. To reduce the fog surrounding these types of standards SEPT has been producing checklists for standards since 1994. This is another checklist related to standards for the IT industry that will aid an organization's compliance with an international information security code of practice.

The first step that an organization has in meeting the guidance of an information security management standard such as Standard ISO/IEC 27018:2014 is to determine what is *required* and what is *suggested*. Often these systems and technical standards are confusing and laborious because the directions contained in the standards are unclear to a lay person. The checklists lift this fog around a standard and state what is required and suggested by the standard in a clear and concise manner.

To aid in determining what is “required” by the document in the way of physical evidence of compliance, the experts at SEPT have produced this checklist. The SEPT checklists are constructed around a classification scheme of physical evidence comprised of policies, procedures, plans, records, documents, audits, and reviews. There must be an accompanying record of some type when an audit or review has been accomplished. This record would define the findings of the review or audit and any corrective action to be taken. For the sake of brevity this checklist does not call out a separate record for each review or audit. All procedures should be reviewed but the checklist does not call out a review for each procedure, unless the standard calls out the procedure review. In this checklist, “manuals, reports, scripts and specifications” are included in the document category. In the procedure category, guidelines are included when the subject standard references another standard for physical evidence. The checklist does not call out the requirements of the referenced standard.

Since ISO/IEC 27018 is a guidance standard we have departed from our usual practice by making “should” a requirement (R) of the guidelines (no “shall” is specified) and “may” a suggested (S) item. This enables a distinction to be made regarding the more important considerations (“should”).

The authors have carefully reviewed the Standard ISO/IEC 27018:2014 and defined the physical evidence required based upon this classification scheme. SEPT’s engineering department has conducted a second review of the complete list to ensure that the documents’ producers did not leave out a physical piece of evidence that a “reasonable person” would expect to find. It could certainly be argued that if the document did not call it out then it is not required; however, if the standard was used by an organization to improve its process, then it would make sense to recognize missing documents. Therefore, there are documents specified in this checklist that are implied by the standard, though not specifically called out by it, and they are designated by an asterisk (*) throughout this checklist. If a document is called out more than one time, only the first reference is stipulated.

There are occasional situations in which a procedure or document is not necessarily separate and could be contained within another document. For example, the "Security Monitoring Log Information Record" could be a part of the "Security Monitoring and Operational Diagnostics Log Information Record." The authors have called out these individual items separately to ensure that the organization does not overlook any facet of physical evidence. If the organization does not require a separate document, and an item can be a subset of another document or record, then this fact should be denoted in the detail section of the checklist for that item. This should be done in the form of a statement reflecting that the information for this document may be found in section XX of Document XYZ. If the organizational requirements do not call for this physical evidence for a project, this should also be denoted with a statement reflecting that this physical evidence is not required and why. The reasons for the evidence not being required should be clearly presented in this statement. Further details on this step are provided in the Detail Steps section of the introduction. The size of these documents could vary from paragraphs to volumes depending upon the size and complexity of the project or business requirements.

General Principles of the Checklist for ISO/IEC Standard 27018:2014

This checklist was prepared by analyzing each clause of this document for the key words that signify a:

- Policy
- Procedure (Including Guidelines)
- Plan
- Records
- Document (Including Manuals, Reports, Scripts and Specifications)
- Audit
- Review

This checklist specifies evidence that is unique. After reviewing the completed document, the second review was conducted from a common sense "reasonable person" approach. If a document or other piece of evidence appeared to be required, but was not called out in the document, then it is added with an asterisk (*) after its notation in the checklist. The information was transferred into checklist tables based on the type of product or evidence.

In total, there are 170 artefacts included in the SEPT ISO/IEC 27018:2014 checklist. These are in addition to those identified through analysis of the related standards.

Using the Checklist

When a company is planning to use ISO/IEC 27018:2014 standard, the company should review the evidence checklist. If the company's present process does not address an ISO/IEC 27018:2014 standard product, then the following question should be asked: "Is the evidence product required for the type of business of the organization?" If, in the view of the organization, the evidence is not required, the rationale should be documented and inserted in the checklist and quality manual. This rationale should pass the "reasonable person" rule. If the evidence is required, plans should be prepared to address the missing item(s).

Detail Steps

An organization should compare the proposed output of their organization against the checklist. In doing this, they will find one of five conditions that exist for each item listed in the checklist. The following five conditions and the actions required by these conditions are listed in the table below.

Condition	Action Required
1. The title of the documented evidence specified by the checklist (document, plan, etc.) *agrees* with the title of the evidence being planned by the organization.	Record in checklist that the organization is compliant.
2. The title of the documented evidence specified by the checklist (document, etc.) *disagrees* with the title of the evidence planned by the organization but the content is the same.	Record in the checklist the evidence title the organization uses and record that the organization is compliant, and the evidence is the same although the title is different.
3. The title of the documented evidence specified by the checklist (document, etc.) is *combined* with another piece of evidence.	Record in the checklist the title of the evidence (document, etc.) in which this information is contained.
4. The title of the documented evidence specified by the checklist (document, etc.) *is not planned* by the organization because it is not required.	Record in the checklist that the evidence is not required and the rationale for this decision.
5. The title of the documented evidence called out by the checklis*t* (document, etc.*) is not planned* by the organization and *should be* planned by it.	Record in the checklist when this evidence will be planned and reference a plan for accomplishing the task.

Product Support

All reasonable questions concerning this checklist or its use will be addressed by SEPT free of charge for 60 days from time of purchase, up to a maximum of 4 hours consultation time.

Note: Sept use Dropbox for "cloud" storage who are certified to ISO/IEC 27001 and 27018.

Guarantees and Liability

Software Engineering Process Technology (SEPT) makes no guarantees implied or stated with respect to this checklist, and it is provided on an "*as is*" basis. SEPT will have no liability for any indirect, incidental, special, or consequential damages or any loss of revenue or profits arising under, or with respect to the use of this document.

Section 2
ISO/IEC 27018:2014 Evidence Products Checklist by Clause

ISO /IEC 27018:2014 Clause Number and Name	**Policies** and Procedures	Plans	Records	Documents	**Audits** and Reviews
4.0 Overview					
4.1 Structure of this standard					
4.2 Control categories.	• Control Description Document Procedure*			• Control Description Document	• Control Description Document Review*
5 Information security policies					
5.1 Management direction for information security	• Applicable PII Protection Legislation Document Procedure* • **Compliance with Applicable PII Protection Legislation Policy** • Contractual Agreement Responsibilities Between PII Processor, Sub-Contractors and Cloud Service Customer Document			• Applicable PII Protection Legislation Document* • Contractual Agreement Responsibilities Between PII Processor, Sub-Contractors and Cloud Service Customer Document	• Applicable PII Protection Legislation Document Review* • Contractual Agreement Responsibilities Between PII Processor, Sub-Contractors and Cloud Service Customer Document Review* • **Independent PII Processor Compliance Audit**

* Suggested item PII – Personally Identifiable Information

Section 2
ISO/IEC 27018:2014 Evidence Products Checklist by Clause

ISO /IEC 27018:2014 Clause Number and Name	**Policies** and Procedures	Plans	Records	Documents	**Audits** and Reviews
6 Organization of information security					
6.1 Internal organization.	- PII Processor Pont of Contact for Cloud Service Customer Document Procedure*			- PII Processor Pont of Contact for Cloud Service Customer Document	- PII Processor Pont of Contact for Cloud Service Customer Document Review*
6.2 Mobile devices and teleworking.					
7 Human resource security					
7.1 Prior to employment.					
7.2 During employment.					
7.2.1 Management responsibilities					

* Suggested item PII – Personally Identifiable Information

Section 2
ISO/IEC 27018:2014 Evidence Products Checklist by Clause

ISO /IEC 27018:2014 Clause Number and Name	**Policies** and Procedures	Plans	Records	Documents	**Audits** and Reviews
7.2.2 Information security awareness, education and training	• Applicable Legal Sanctions for Breach of Security Rules and Procedures Document Procedure* • Consequences of Breach of Security Rules and Procedures Addressing Handling of PII Procedure			• Applicable Legal Sanctions for Breach of Security Rules and Procedures Document*	• Applicable Legal Sanctions for Breach of Security Rules and Procedures Document Review*
7.2.3 Disciplinary process					
7.3 Termination and change of employment					
8 Asset management					
9 Access control					
9.1 Business requirements of access control.					
9.2 User access management					

* Suggested item PII – Personally Identifiable Information