ISO/IEC 29134
Privacy Impact Assessment

Frank Fransen | 4 oktober 2016

NEN informatiemiddag *'De toekomst van privacy en normen'*

Agenda

- Introduction to Privacy Impact Assessment
- ISO/IEC 29134 - Privacy Impact Assessment
- Summary

Privacy Impact Assessment
What is a PIA?

Privacy Impact Assessment (PIA)

Wilt u als organisatie privacyrisico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen? Dan kunt u een privacy impact assessment (PIA) (laten) uitvoeren.

https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia

Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst

"Een Privacy Impact Assessment (PIA) is een hulpmiddel om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacyrisico's op gestructureerde en heldere wijze in kaart te brengen."

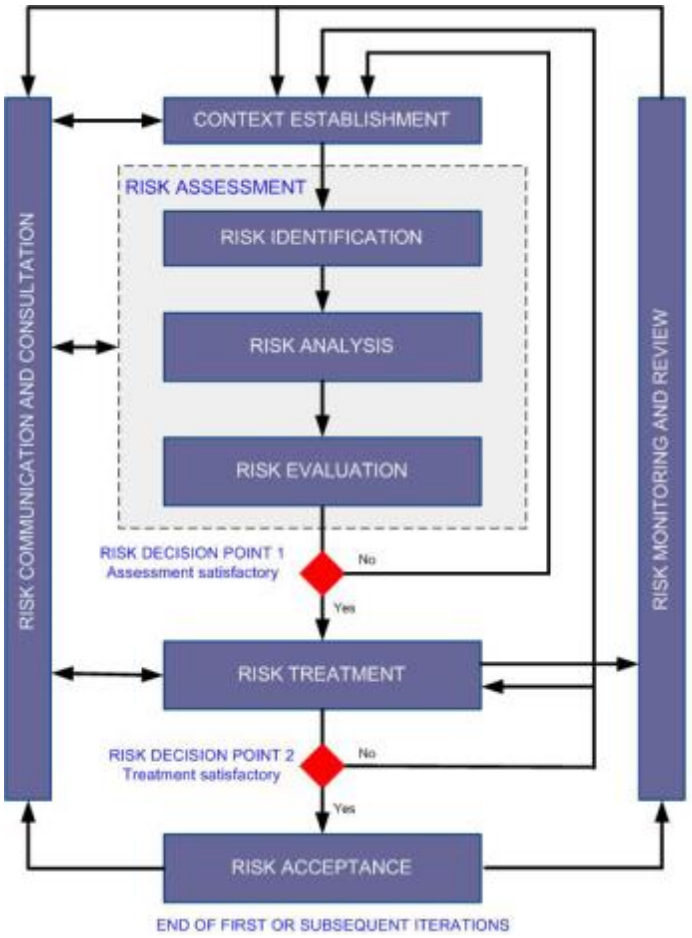
Process for identifying *Privacy related risks*

NEN TNO

Privacy Impact Assessment

What is a PIA?

The risk management process from ISO/IEC 27005 -



Privacy Impact Assessment

Privacy Impact Assessment

What is a PIA?

ISO/IEC DIS 29134

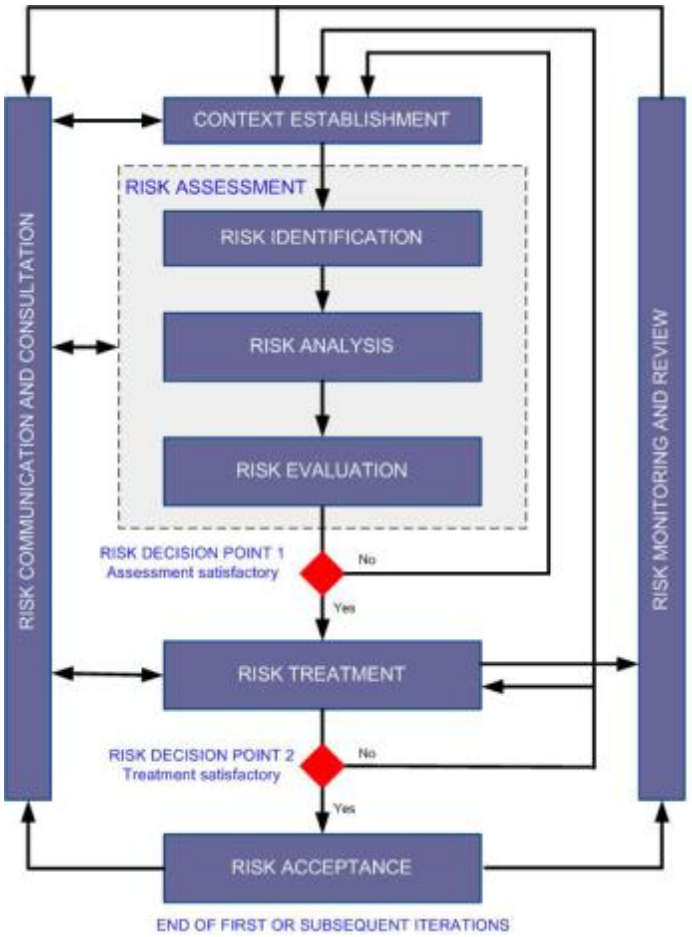
Privacy Impact Assessment – systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing privacy risk

Seems more like *"Privacy Risk Management"*

Privacy Impact Assessment

What is a PIA?

The risk management process from ISO/IEC 27005 -



Privacy Impact Assessment

(Source: Authoriteit Persoonsgegevens)

ISO/IEC 29134 - Privacy impact assessment -- Methodology

Privacy Impact Assessment
Why?

- Better insight into privacy risks
- Privacy by Design
- Basis for informing *PII principals*
- Less impact from oversight by regulator
- Show *compliance* with data protection acts

Privacy Impact Assessment
Why? … Mandate

General Data Protection Regulation (Regulation (EU) 2016/679)

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

DPIA

- GDPR enters into application 25 May 2018

Source: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Privacy Impact Assessment
Why? … Mandate *GDPR*

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

- Description of envisaged *processing & purpose;*
- *Necessity & proportionality* to the purpose;
- Assessment of the *risks*; and
- *Measures* to address the risks.

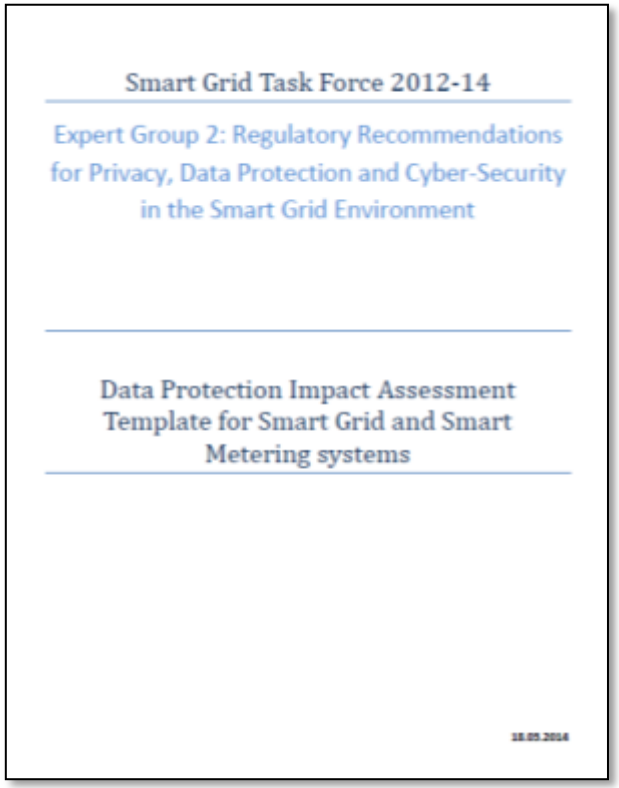
Privacy Impact Assessment
Why? … *Dutch Mandates*

- Since September 2013, Dutch government agencies have to conduct a PIA when developing new laws and regulations for which the development of new ICT-systems or establishment of a database is anticipated.
  - Using: *Toetsmodel Privacy Impact Assessment Rijksdienst*

Source: https://www.rijksoverheid.nl/documenten/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst

Privacy Impact Assessment

Manny methods available



ISO/IEC 29134 - Privacy Impact Assessment
International Standard

- ISO/IEC 29134 – Information technology – Security techniques – Privacy impact assessment – Guidelines

- **Status:** DIS
  - Target publication date: 2017-05-30

- **Scope**

  This International Standard gives guidelines for:
  - a process on privacy impact assessments;
  - a structure and content of a PIA report.

  It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

ISO/IEC 29134 - Privacy Impact Assessment
Outline

Chapter 5 - Preparing the grounds for PIA

- 5.1 Benefits to carry out a PIA
- 5.2 Objectives of PIA reporting
- 5.3 Accountability to conduct a PIA
- 5.4 Scale of a PIA

Chapter 6 - Guidance on the process for conducting a PIA

Chapter 7 - PIA report

ISO/IEC 29134 - Privacy Impact Assessment
Guidelines for a process

- The process for conducting a PIA consists of 21 steps

Section	Title	# steps
6.2	Determine whether a PIA is necessary	1
6.3	Preparation of the PIA	6
6.4	Perform the PIA	
6.4.1	Identify information flows of PII	1
6.4.2	Analyse the implications of the use case	1
6.4.3	Determine the relevant privacy safeguarding req.	1
6.4.4	Assess privacy risk	3
6.4.5	Prepare for treating privacy risks	3
6.5	Follow up of the PIA	5
		21

ISO/IEC 29134 - Privacy Impact Assessment
Guidelines for a process – structure

- Each step is structured as follows:
  - "Objective" – something that should be achieved;
  - "Input" – guidance about what information may be needed to achieve the "Objective";
  - "Expected output" – the recommended target for the "Actions"
  - "Actions" – guidance on activities that may need to be carried out to achieve the "Objective" and create the recommended "Expected output"; and
  - "Implementation Guidance" – provides more details of matters that may need to be considered in performing the "Actions".

ISO/IEC 29134 - Privacy Impact Assessment
Guidelines for a process – structure

- Each step is structured as follows:

6.4.4.3 Privacy risk evaluation

Objective: To prioritize the identified privacy risks

Input: Identified privacy risks, privacy risk analysis

Expected output: Privacy risk map

Actions:

A privacy risk evaluation should be produced.

Output in terms of the privacy risk map should be documented in the PIA report (see clause 7.5.4).

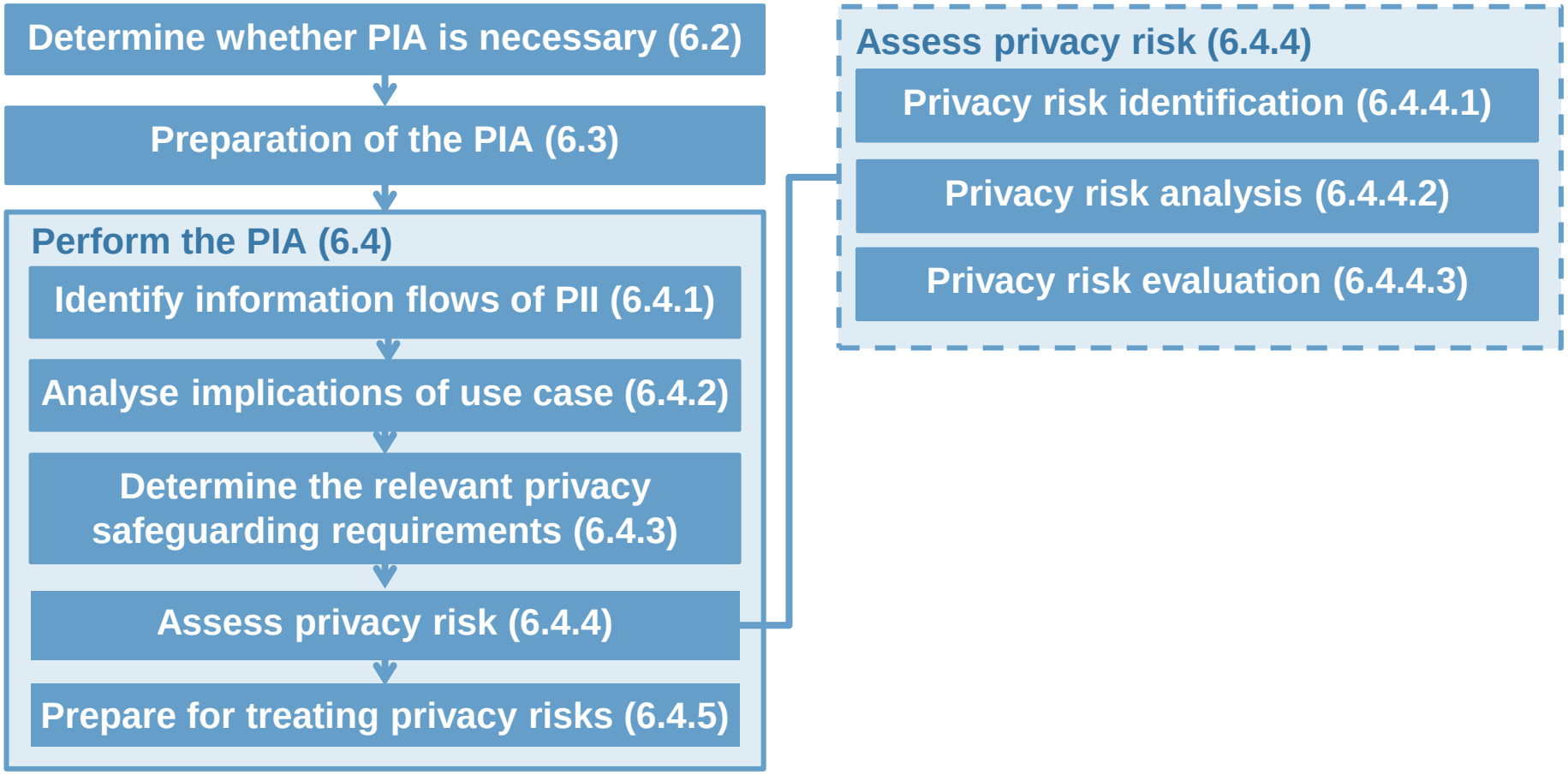
Implementation Guidance:

Producing a privacy risk evaluation should involve the relative prioritization of privacy risk, based on the severity of privacy impact on PII principals as well as the overall impact to the organization.

The treatment of identified privacy risks may require more resources than are available to the organization. Prioritizing the identified risks will help the organization prioritize the allocation of resources for their treatment.

ISO/IEC 29134 - Privacy Impact Assessment

Guidelines for a process – steps



ISO/IEC 29134 - Privacy Impact Assessment

Privacy risk identification (6.4.4.1)

Implementation Guidance:

Privacy risks include, but are not limited to:

Information security

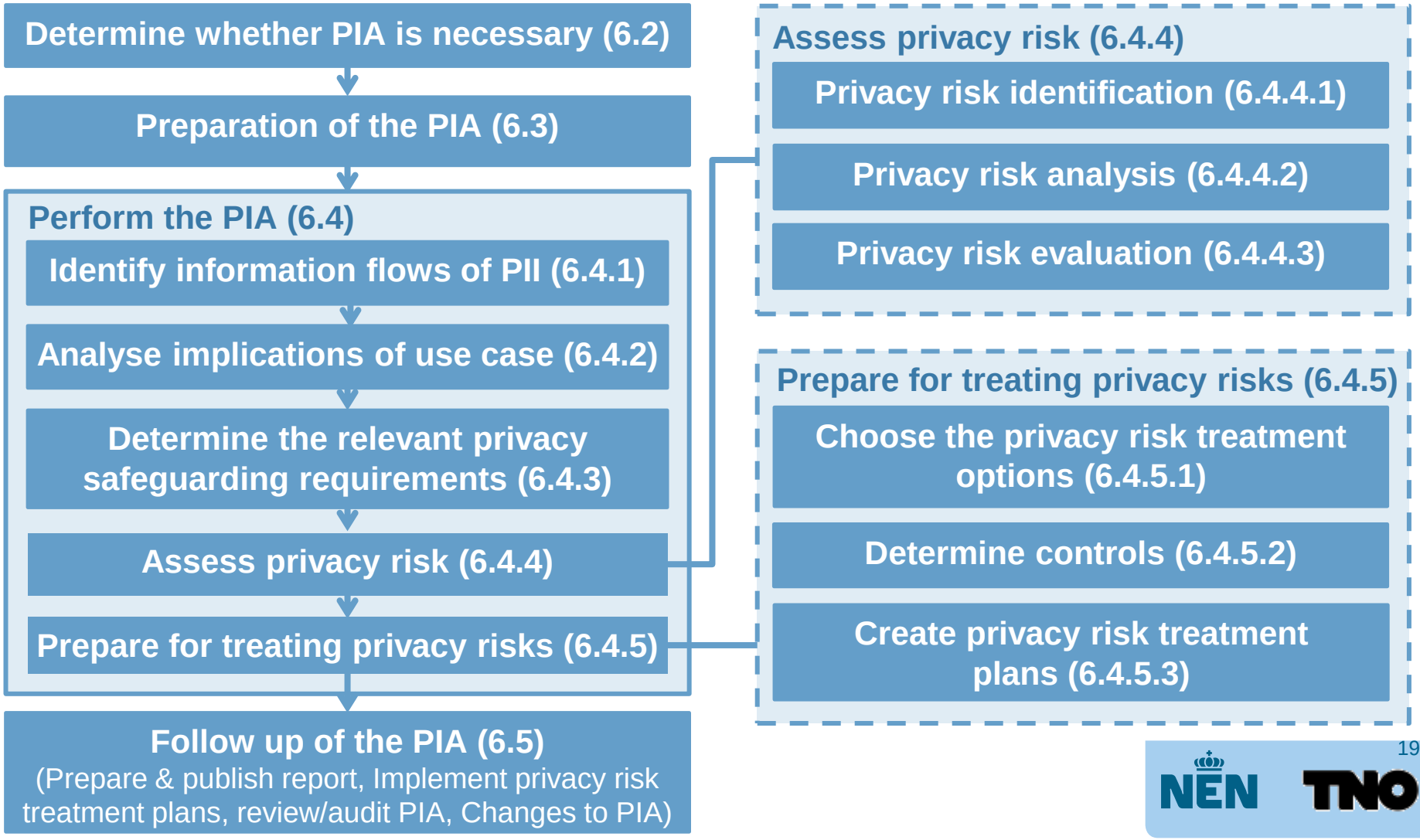
- unauthorized access to PII (loss of confidentiality);
- unauthorized modification of the PII (loss of integrity);
- loss, theft or unauthorized removal of the PII (loss of availability);

It is possible to consider other aspects like the following ones:

- excessive collection of PII (loss of operational control);
- unauthorized or inappropriate linking of PII;
- insufficient information concerning the purpose for processing the PII (lack of transparency);
- failure to consider the rights of the PII principal (e.g. loss of the right of access);
- processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation);
- sharing or re-purposing PII with third parties without the consent of the PII principal; and
- unnecessarily prolonged retention of PII.

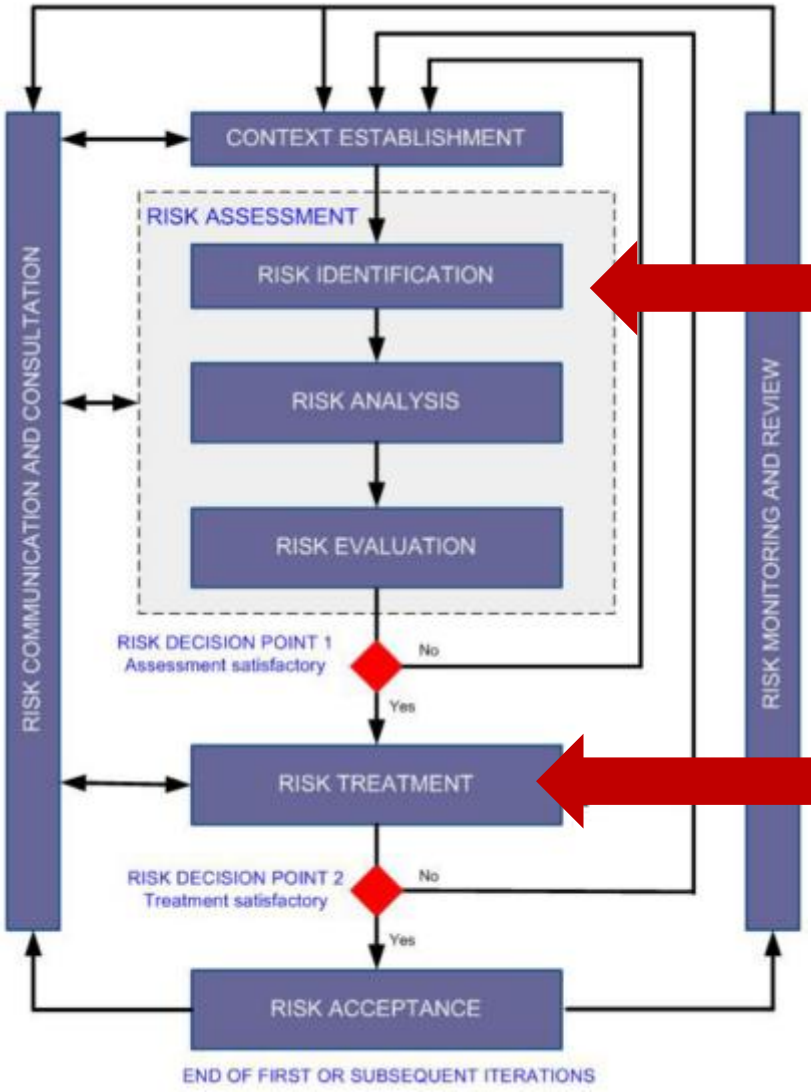
ISO/IEC 29134 - Privacy Impact Assessment

Guidelines for a process – steps



ISO/IEC 29134 - Privacy Impact Assessment

Mapping to ISO/IEC 27005



Assess privacy risk (6.4.4)

- Privacy risk identification (6.4.4.1)
- Privacy risk analysis (6.4.4.2)
- Privacy risk evaluation (6.4.4.3)

Prepare for treating privacy risks (6.4.5)

- Choose the privacy risk treatment options (6.4.5.1)
- Determine controls (6.4.5.2)
- Create privacy risk treatment plans (6.4.5.3)

ISO/IEC 29134 - Privacy Impact Assessment
PIA report

- Guidelines on the content of a PIA Report
  - The style is ***"the PIA report should …"***

- Defines requirements on:
  - the report structure (Clause 7.2);
  - the scope of the assessment (Clause 7.3);
  - the privacy requirements (Clause 7.4);
  - the risk assessment (Clause 7.5);
  - the risk treatment (Clause 7.6); and
  - the conclusion and decisions (Clause 7.7)
  - the PIA public summary (Clause 7.8).

Summary

- Term PIA is used to refer both to *privacy risk assessment & privacy risk management*

- GPDR mandates Data Protection Impact Assessment
  - > requires: *privacy risk management (risk treatment)*

- ISO/IEC 29134 – Privacy Impact Assessment
  - Expected publication date: **May 2017**
  - Gives guidelines for a process on privacy impact assessments *(incl. risk treatment steps)*.
  - Specifies the structure and content of a PIA report.

Questions

Frank Fransen
+31 (0)88 866 7729
frank.fransen@tno.nl