Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
National Metrology Institute

Data-based Metrological Support Services

Progress Report on Work Package 4

Dr.-Ing. Marko Esche

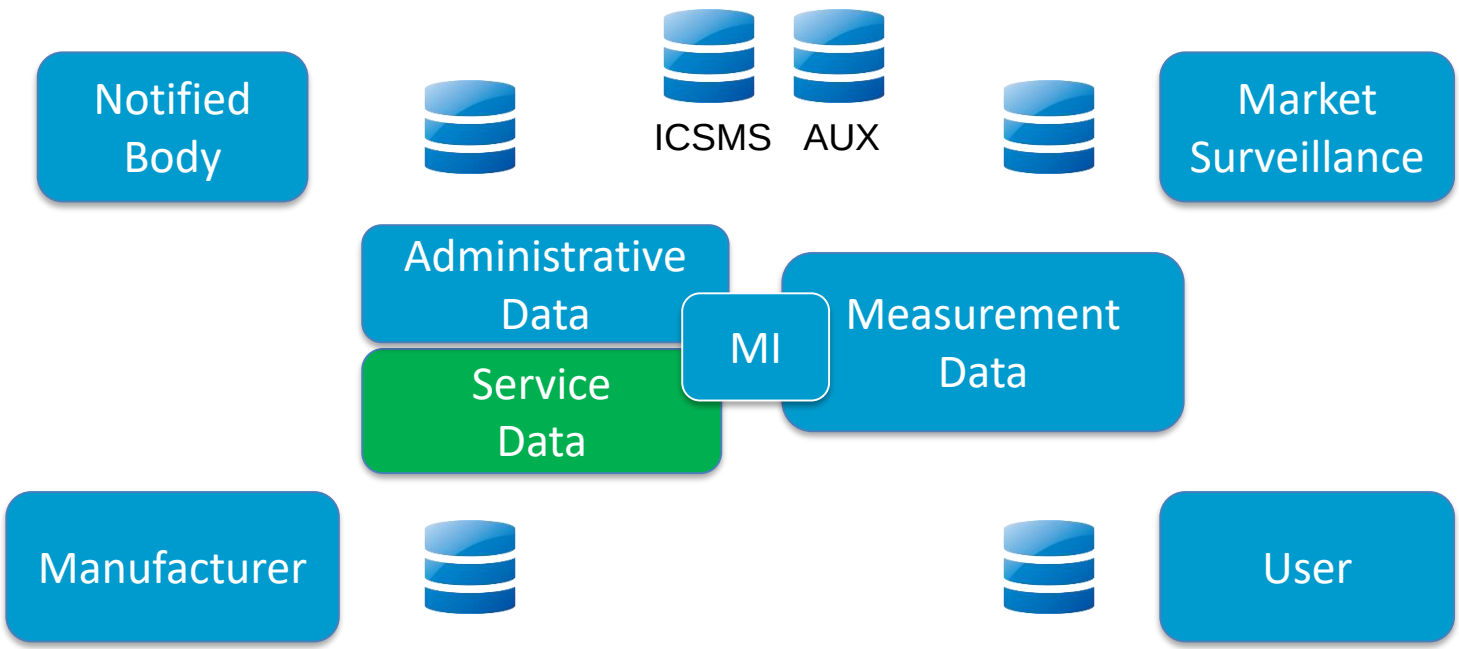
Overview

- Objectives of Work Package 4
- Exemplary support service: risk assessment
- Report on task 1: Inter-institutional comparison
- Report on task 2: Closing the risk assessment looü
- Summary
- Further work

WP 4: Data-based Metrological Support Services

- Objectives
  - Use data volumes created by measuring instruments employed in the EU single market
  - Based on connected databases, develop **new data-driven metrological services** such as methods for closing the risk assessment loop.
- Exemplary support service: **software risk assessment**

Connect separate databases



Within individual "Data Shells"

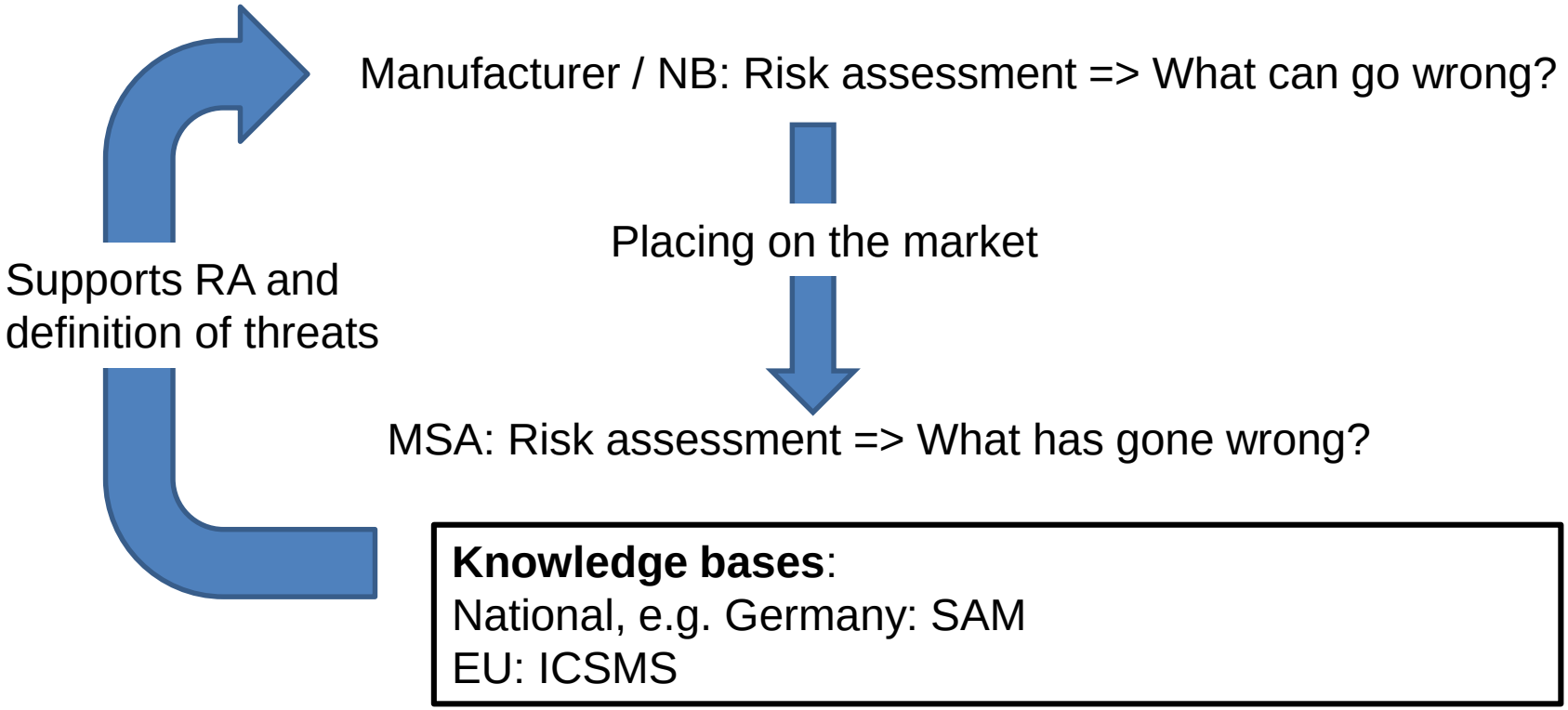
Within joint "Data Shells"

=> **Trustworthy** information exchange

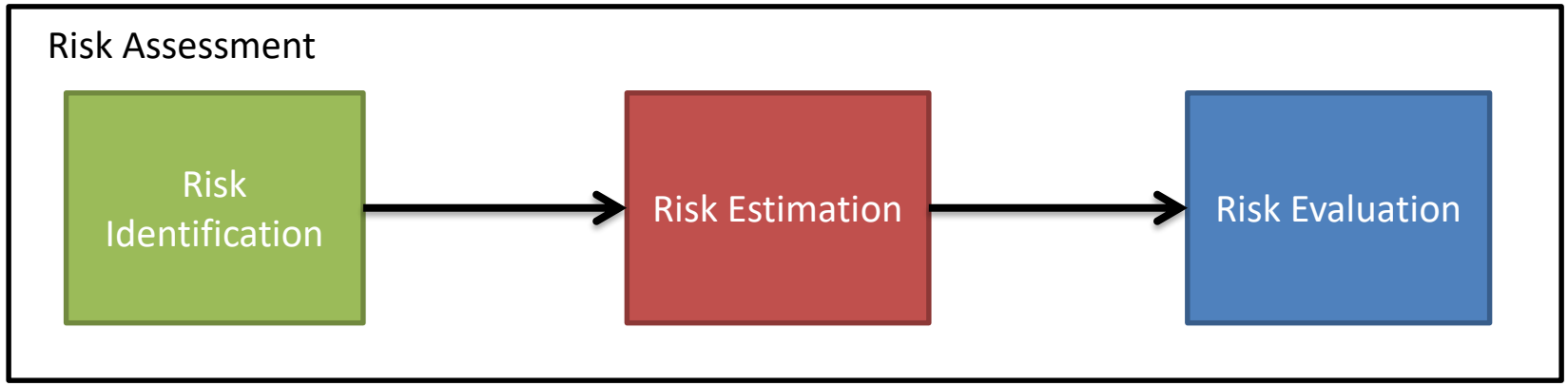
Exemplary support service

- MID (Directive 2014/32/EU) requires an **“analysis and assessment of the risks”** to be part of the documentation submitted for conformity assessment.
- Within the Metrology Cloud, **a framework for risk assessment** is investigated which has been **accepted by WELMEC WG 7** and can be used by manufacturers and Notified Bodies.
- The structure of ISO/IEC 27005 is used for the analysis.
- Methods from ISO/IEC 15408 and 18045 are employed to **provide reproducible numerical risk scores**.

Aspects of Directive 2014/32/EU



Method description

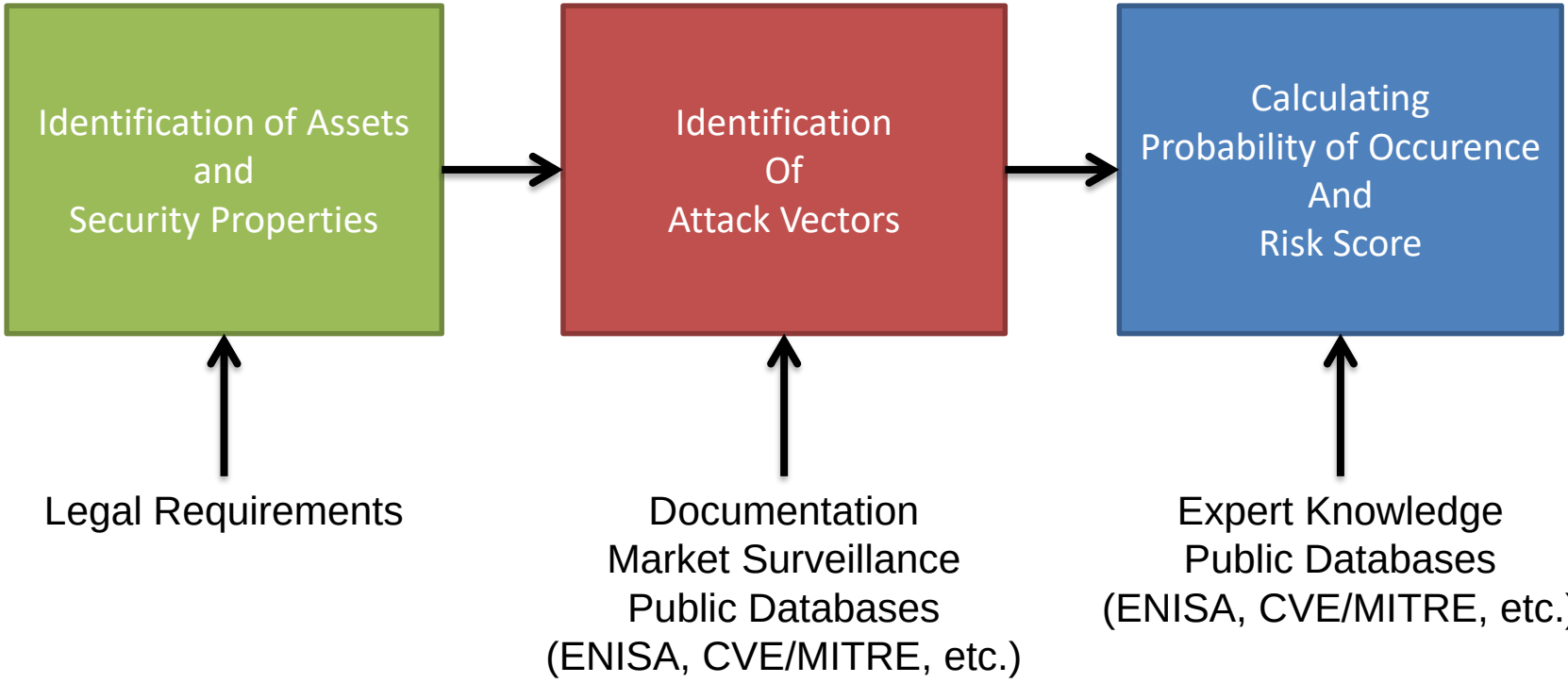


- ISO/IEC 27005: **“Risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event.”**
- Needed components:
  - threats to assets
  - impact/hazard/consequence
  - probability/likelihood

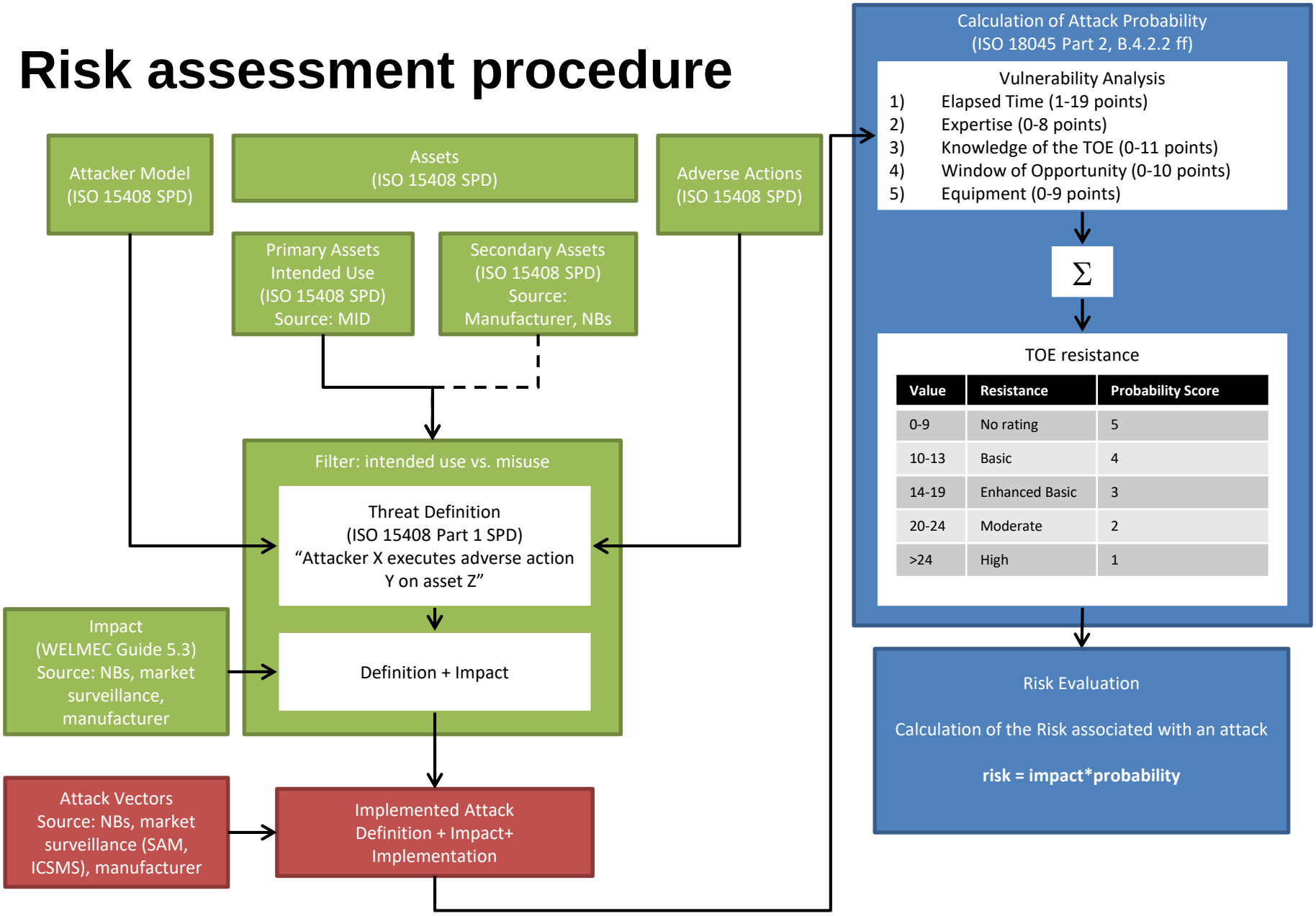
Software requirements in the MID

Assets derived from the MID		
Number	Asset	Security Property
A1	metrological software	integrity, authenticity
A2	evidence of an intervention	availability, integrity
A3	measurement data	integrity, authenticity
A4	metrological parameters	integrity
A5	inadmissible influence on the software	unavailability
A6	indication of the result	availability, integrity

Risk assessment procedure (ISO/IEC 27005)



Risk assessment procedure



M. Esche and F. Thiel, "Software risk assessment for measuring instruments in legal metrology", FedCSIS 2015

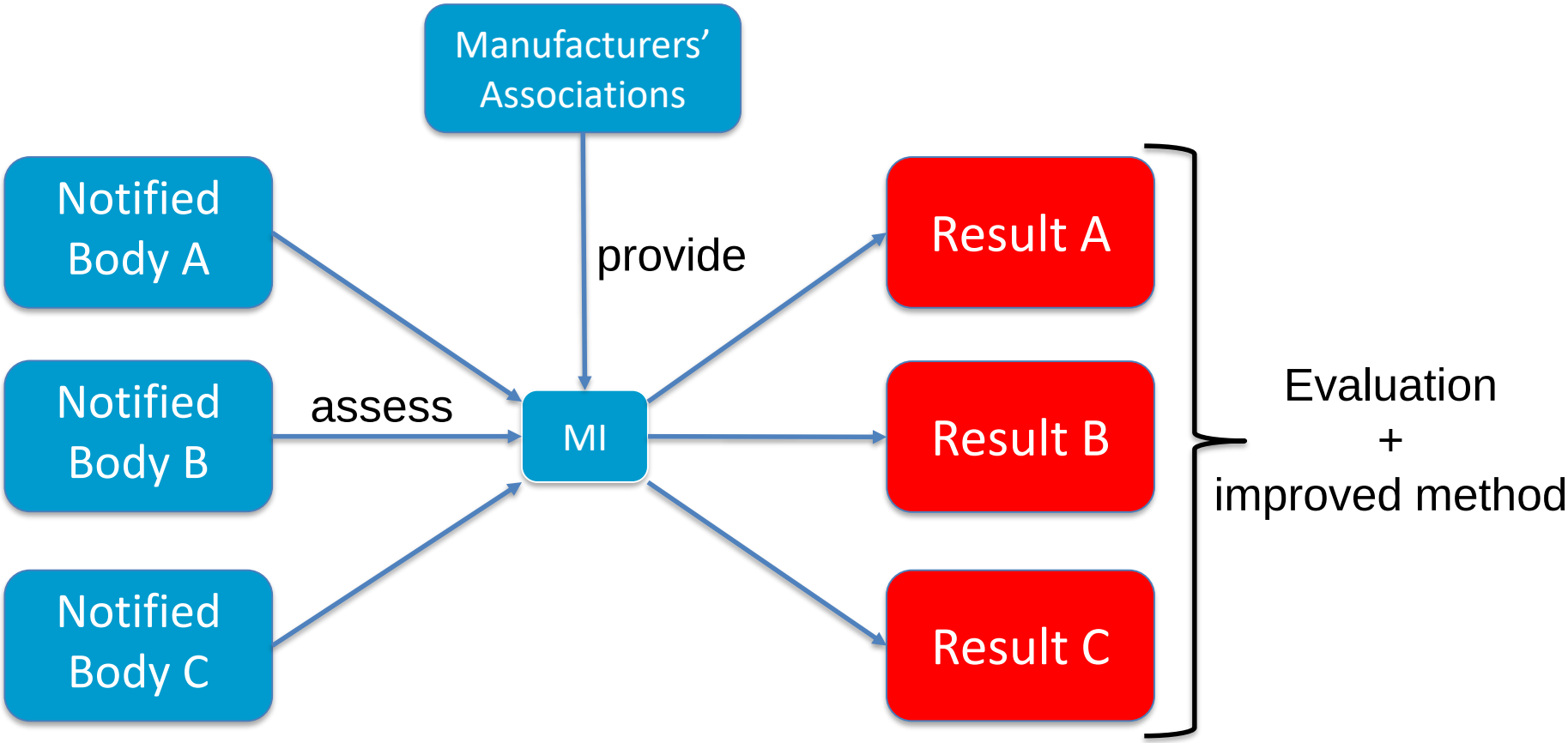
Challenges

- No link between probability of occurrence and incident information from the field
- Accuracy depends on the assessor’s skill and knowledge about the measuring instrument.
- No objective way to quantify attacker motivation in current method
- Parties involved consider risk to be a theoretical concept.
- Data available within the Metrology Cloud may help to solve these issues.

Tasks of Work Package 4

- **Task 1: Inter-institutional comparison**
  - Test and evaluate existing risk assessment method.
  - Different market actors (notified bodies, manufacturers market surveillance) assess generic instruments to investigate objectiveness of the method.
  - Goal: Suggestions for the improvement of the method
- **Task 2: Closing the risk assessment loop**
  - Investigate strategies for the inclusion of incident data.
  - Investigate data sources made available via the Metrology Cloud.
  - Develop and test a concept for incident data inclusion.

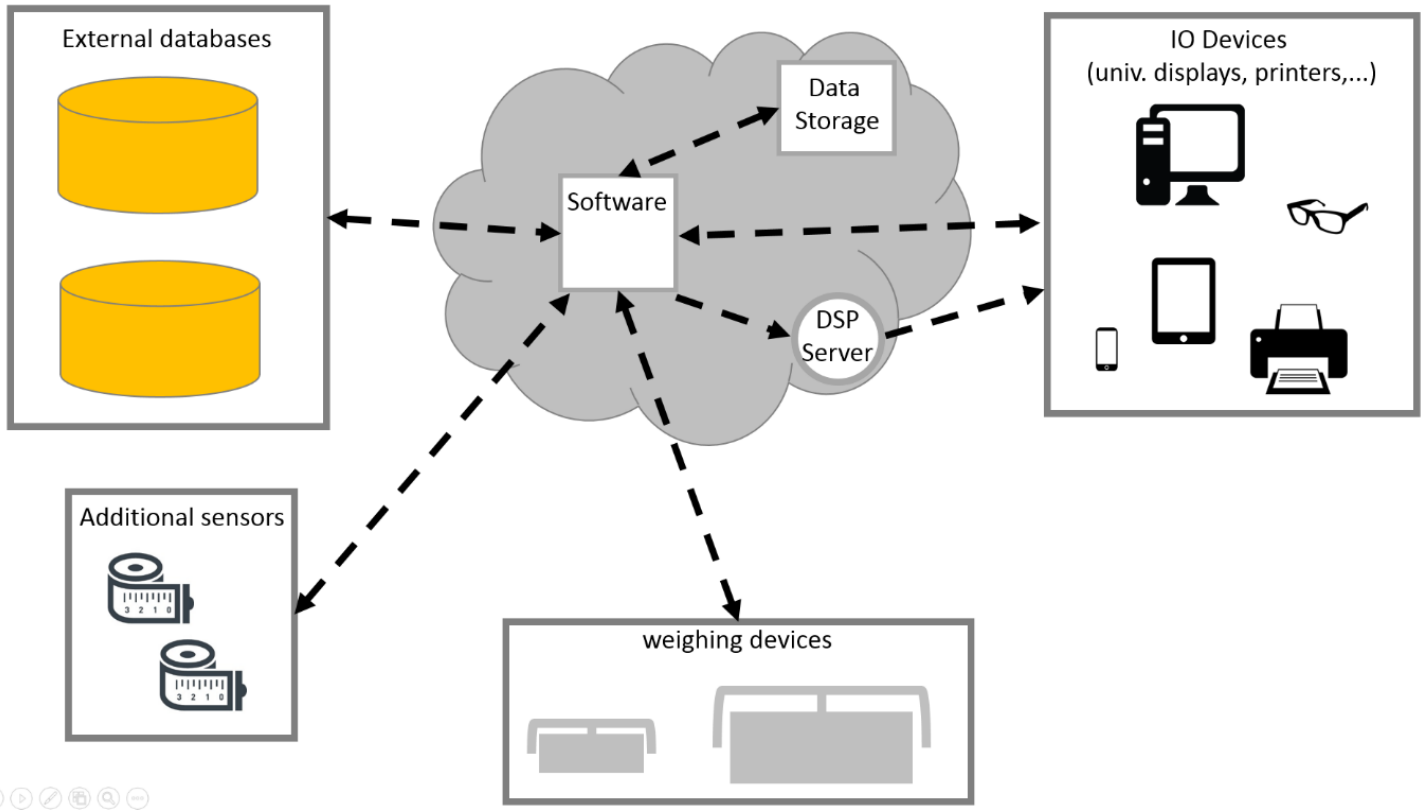
Task 1: Inter-institutional comparison



Report on task 1

- March 2018: Joint training session with WELMEC WG7 Subgroup Risk Assessment.
- June – August 2018: Proposal and development of an abstract measuring instrument by CECIP as a reference point.
- September 2018 – January 2019: Assessment of the abstract measuring instrument by five notified bodies
- February 2019: Collection and evaluation of results, proposal of a formalized risk assessment template
- **Threat 1:** introduction of false measurement results
- **Threat 2:** modification or replacement of software

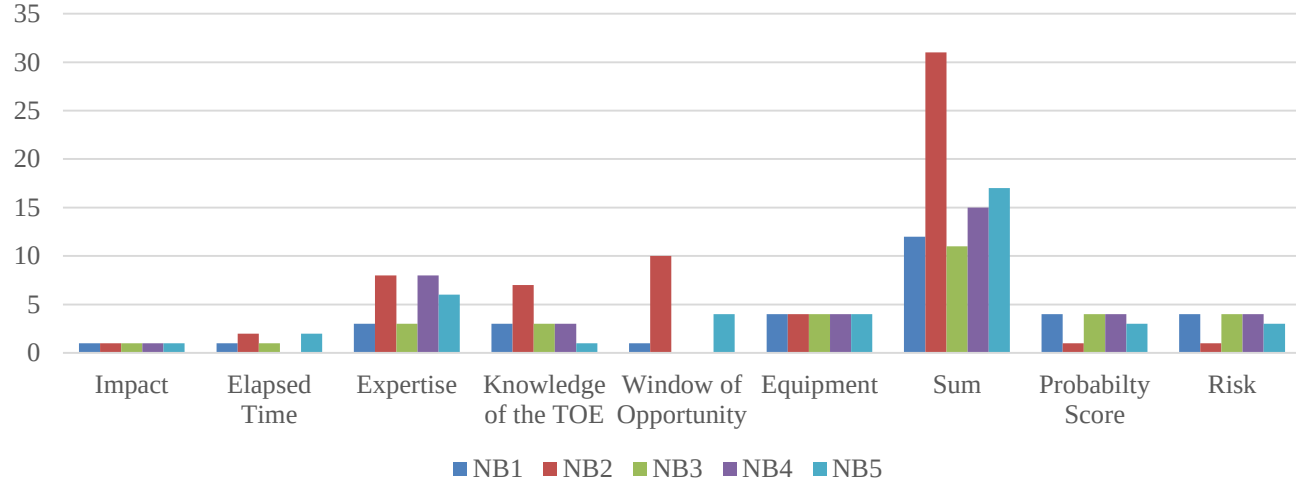
Cloud-based measuring instrument



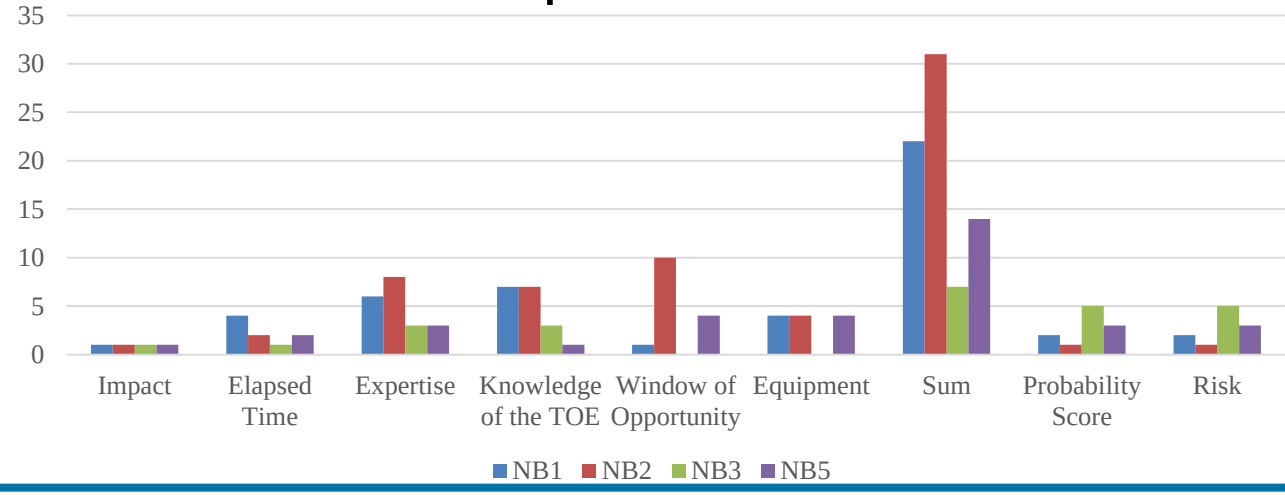
- two categories of display devices (full control, receive only)
- communication between separate components via Wi-Fi with WPA encryption
- Cloud offers data storage and display server (DSP).

Results for the cloud-based instrument

Threat 1: introduction of false measurement results

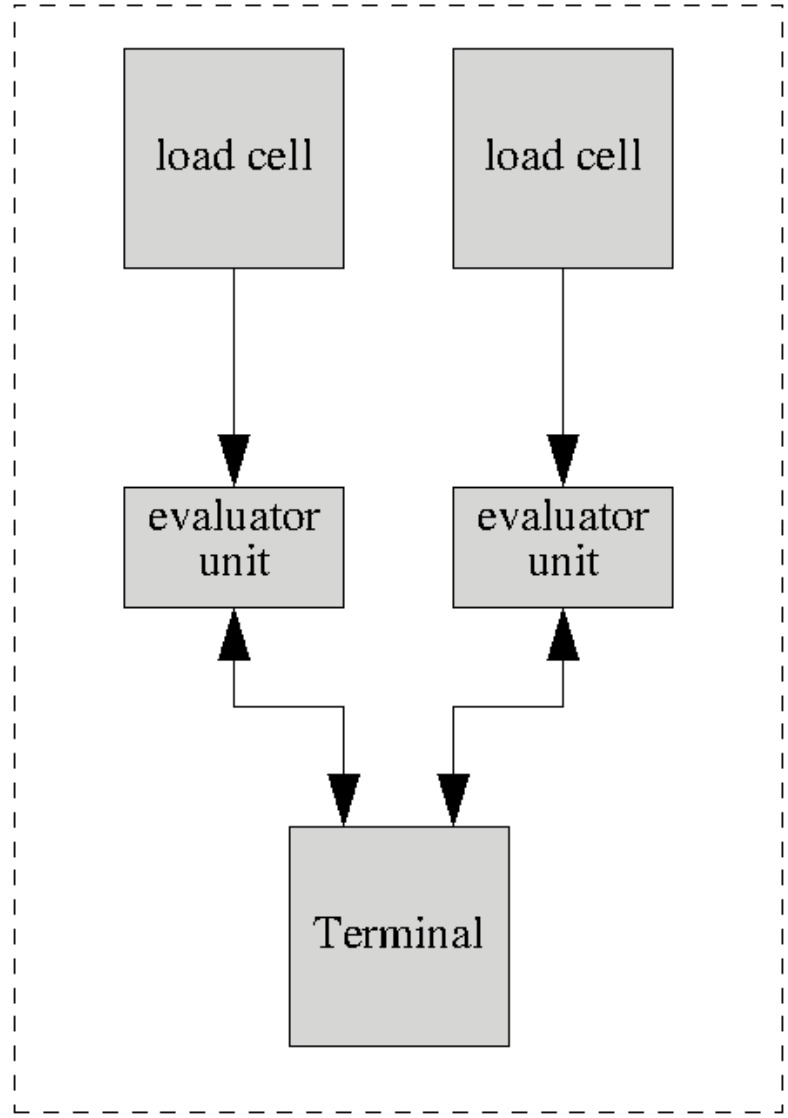


Threat 2: modification or replacement of software



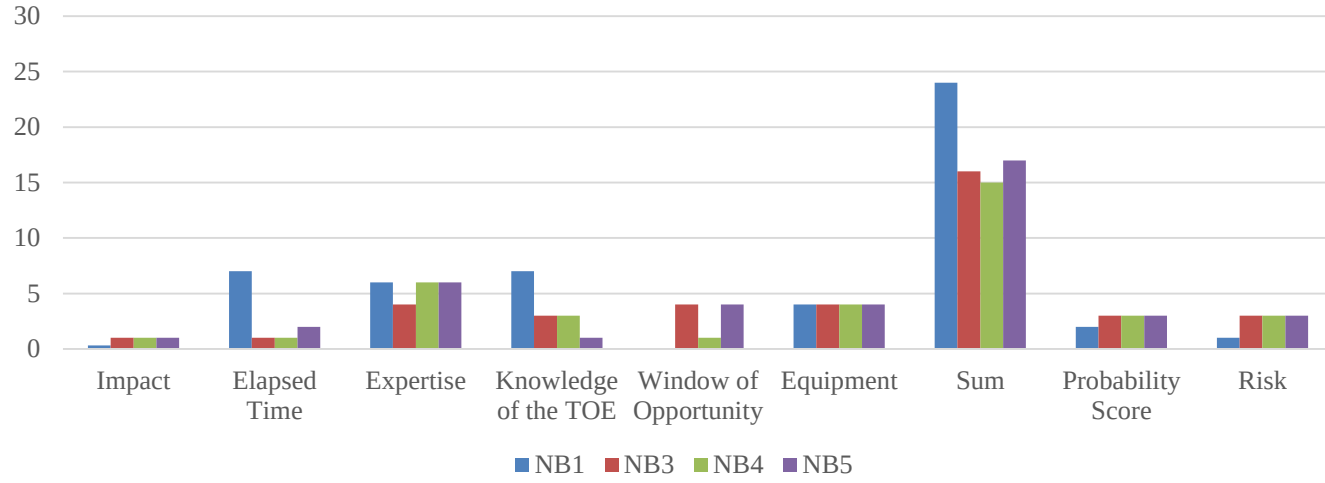
Simple weighbridge

- Sealed communication path from load cell to terminal
- Evaluator units and terminal are based on the same microprocessor.
- Data can be read from the terminal via RS 485 or can be written to a USB stick.
- Terminal checks the authenticity of all other units at startup.
- Flash memory for parameters and software is protected by a hardware switch.
- Legally relevant log is stored on an SD-card.

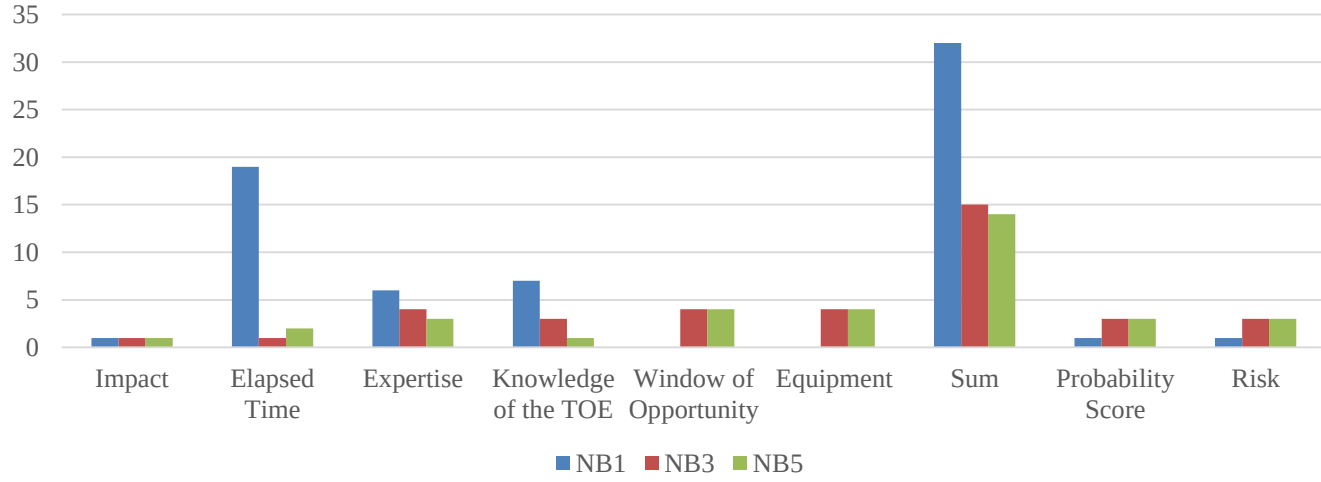


Results for the simple weighbridge

Threat 1: introduction of false measurement results



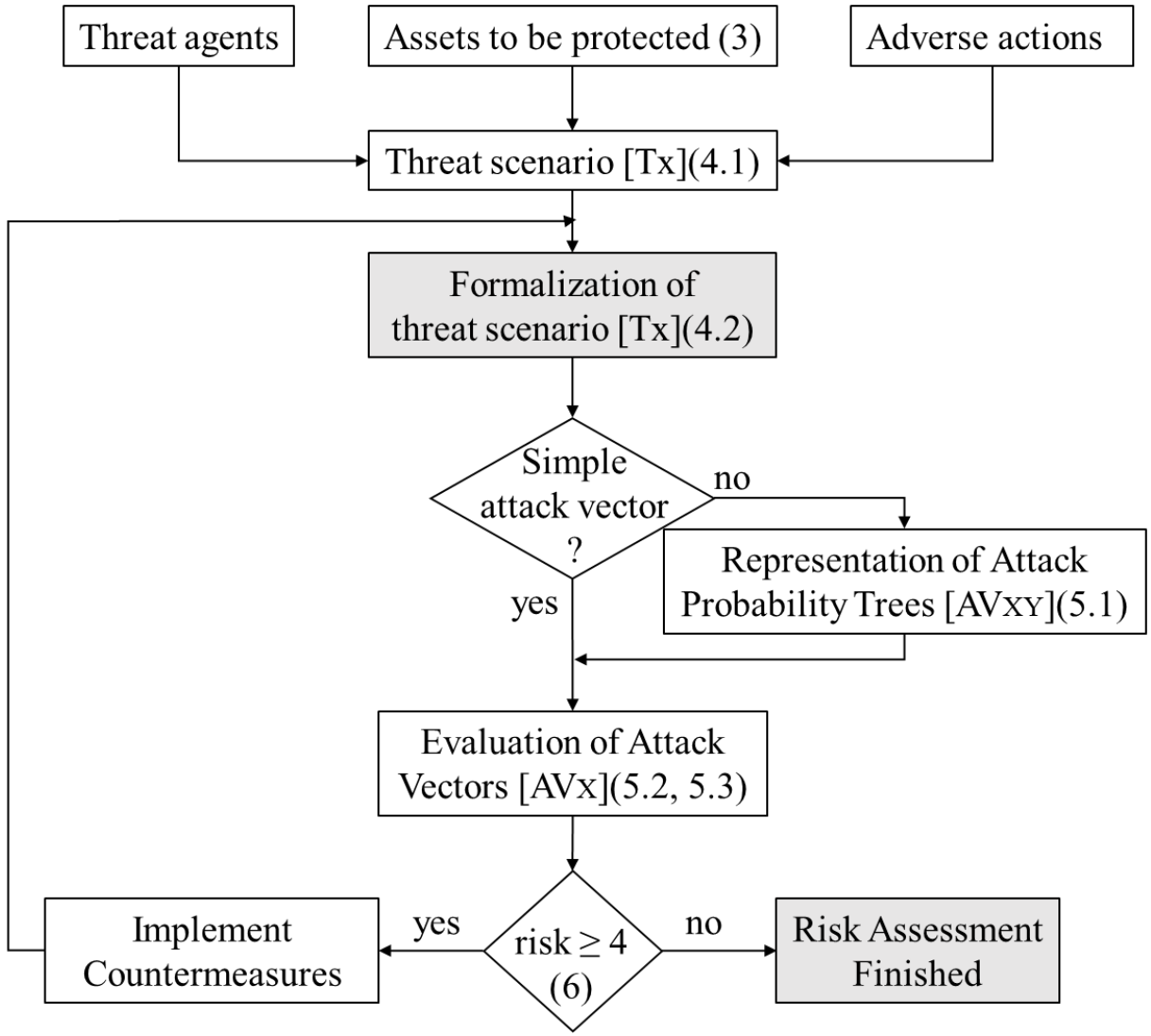
Threat 2: modification or replacement of software



Task 1: observations

- Objective comparison of risk assessment results for software is only possible if certain prerequisites are fulfilled.
- **Instructions for new evaluators** on how to perform the risk assessment according to ISO 18045 shall be readily available.
- **Examples for evaluation of common attack vectors** to reduce the workload for evaluators shall be supplied.
- **Proper documentation of the complete attack vector and justification** for the evaluation shall be required of all assessors to allow for better comparability of assessment results.

Solution: risk assessment template



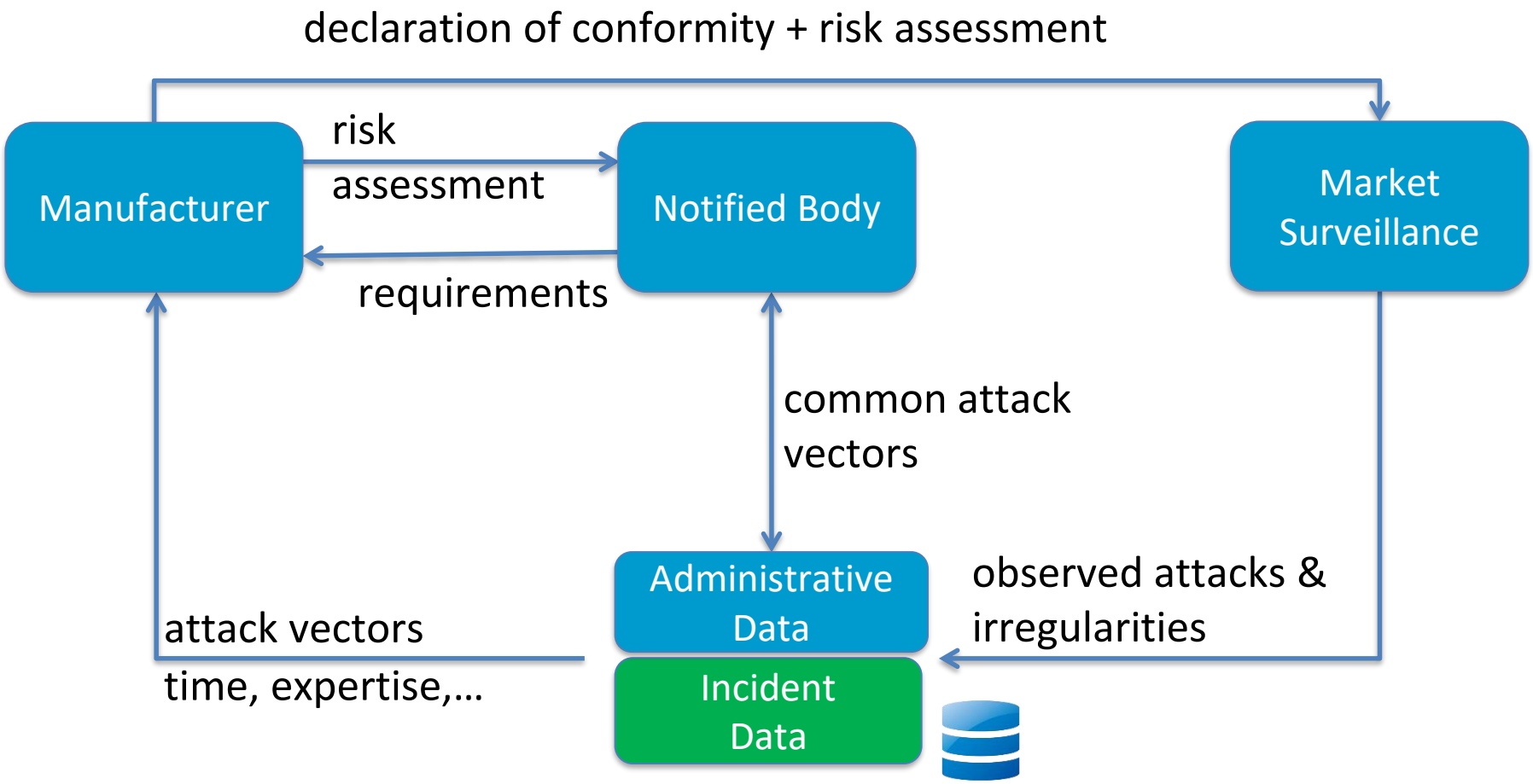
Report on task 2

- June – December 2018: Investigation of inclusion strategies for incident data in software risk assessment
- February 2019: Presentation of proposals by PTB and CECIP
- **Conclusions:**
  - Risk is an inherently theoretical concept.
  - Incident data is not available prior to putting the instrument on the market.
  - Incident data can be used to calculate risk scores during a second assessment round.
  - Attacker motivation should be reflected in the assessment.

Report on task 2

- Concerning the incident data:
  - Data available via the cloud would need to be very specific.
  - WP4 will need to make it clear to market surveillance/other WPs, which kind of data is needed for risk assessment.
  - PTB will update the proposal to close the loop.
- CECIP is currently developing an extended proposal to determine attacker motivation.
- The motivation (score) shall then be incorporated into the risk assessment result as well.

Task 2: target workflow



Summary

- Task 1 has progressed to the stage of publishing a first template for risk assessment formalization.
- The template will now be tested by the partners and modified where necessary.
- Task 2 will produce draft concept within the next two months.
- WP1 and market surveillance will be contacted once a precise definition of the needed data has been formulated.

Further work

- These results will be presented to WELMEC WG7 in September.
- WG7 will decide how to include the results in its work program.
- The applicability of a simplified risk assessment method for components/modules of a measuring instrument should be investigated as well.
- Intended outcome:
  - simplify the method
  - make results more easily reusable
  - pave the way towards risk-based evaluation of measuring instruments




Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
Abbestraße 2-12
10587 Berlin

Dr.-Ing. Marko Esche
Telefon: +49 30 3481-7975
E-Mail: marko.esche@ptb.de
www.ptb.de

Version: 05/19