Maria Sklodowska-Curie
National Research
Institute of Oncology

TWELFTH INTERNATIONAL CONFERENCE OF RADIATION,
NATURAL SCIENCES, MEDICINE, ENGINEERING, TECHNOLOGY AND ECOLOGY
RAD CONFERENCE
JUNE 17-21, 2024
HUNGUEST HOTEL SUN RESORT, HERCEG NOVI, MONTENEGRO

Risk management in a calibration laboratory accredited for compliance with the ISO/IEC 17025 standard - practical examples

Iwona Grabska, Wioletta Ślusarczyk-Kacprzyk, Marcin Szymański

**The Secondary Standards Dosimetry Laboratory, Department of Medical Physics,
Maria Sklodowska-Curie National Research Institute of Oncology, Warsaw, Poland**

Laboratory accredited by the Polish Centre for Accreditation, accreditation No. AP 155*

* an actual scope of accreditation No. AP 155 is available on the PCA website: www.pca.gov.pl

Introduction

The Secondary Standards Dosimetry Laboratory (SSDL) in Warsaw in Poland has been accredited by the Polish Centre of Accreditation for the conformity with the **ISO/IEC 17025 standard „General requirements for the competence of testing and calibration laboratories”** [1].

The accreditation No. AP 155 granted on 28 May, 2014 covers the calibration of ionization chambers together with electrometers in a ^{60}Co gamma ray beam in terms of dose absorbed to water and calibration of well chambers with a ^{192}Ir source in terms of air kerma.

The Polish SSDL performs its laboratory activities in the aforementioned accreditation scope for radiotherapy centers in Poland.

Introduction

In this work, the ways of implementing requirements of the ISO/IEC 17025:2017 standard [1] regarding **actions to address risk and opportunities associated with the laboratory activities** are presented.

These requirements (see section 8.5 of the ISO/IEC 17025:2017 standard) are as follows:

a. consideration of risks and opportunities associated with laboratory activities;

b. planning and taking actions in relation to risks and opportunities and assessing the effectiveness of these actions.

Methods

Risk can be defined as **effect of uncertainty on objectives** [2].

This effect is a deviation from the expected and it **can be positive**, **negative** or **both**, and can address, create or result in **opportunities** and **threats** [2].

Managing risk considers the **external and internal context of the organization**, including human behaviour an cultural factor [2].

Methods

Due to the fact that the ISO/IEC 17025:2017 standard does not recommend the use of specific risk management methods, **each laboratory can define its own methodology**.

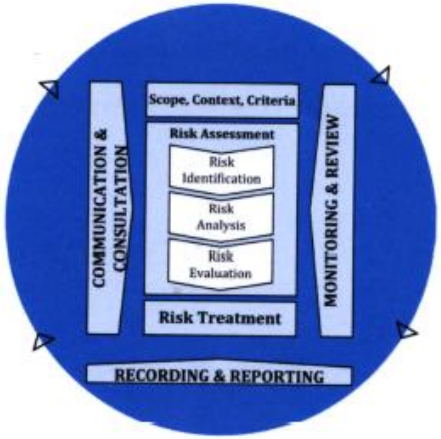
ISO 31000:2018 *Risk management – Guidelines* **can be a helpful standard in this regard**.

At the Polish SSDL,
it was assumed that **risk management is the overall process**,
as shown in the ISO 31000:2018 standard Risk management – Guidelines [2]
which standard can be applied to any organization and its context or activity.

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

Methods

Risk assessment is the overal process of **risk identification**, **risk analysis** and **risk evaluation** [2].



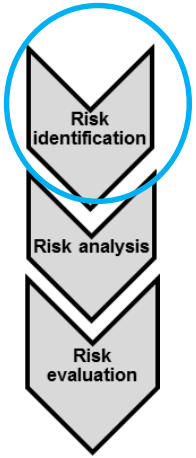
Risk identification
- **is conducted to find, recognize and describe risks that might help or prevent the Polish SSDL achieving its objectives.**

Risk analysis
- **is an activity aimed at determining the level of risk, taking into account the effectiveness of existing risk controls.**

Risk evaluation
- **involves comparing the results of the risk analysis with the criteria established at the Polish SSDL to determine where additional action is required.**

Note:
Risk assessment is conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders of the Polish SSDL.

Methods



Risk identification in practice:

Subject of risk identification: goals and objectives (processes).

Main areas of risk identification: staff, equipment.

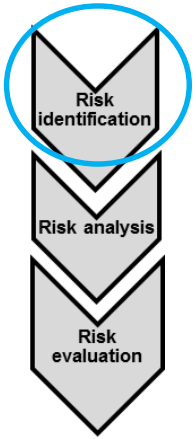
Risks are identified:
- during work planning - when goals are set, necessary resources are determined;
- on an ongoing basis - when the conditions for the performance of tasks change.

Risks are identified by:
- the same people who are involved in achieving goals and objectives;
- all levels of the organization (management and lower-level employees).

Main techniques for risk identification:
- "brainstorming„
- event lists;
- process analysis;
- threat scenarios ("black scenarios").

Recommended risk identification technique:
- mixed as a combination of all the techniques listed.

Methods



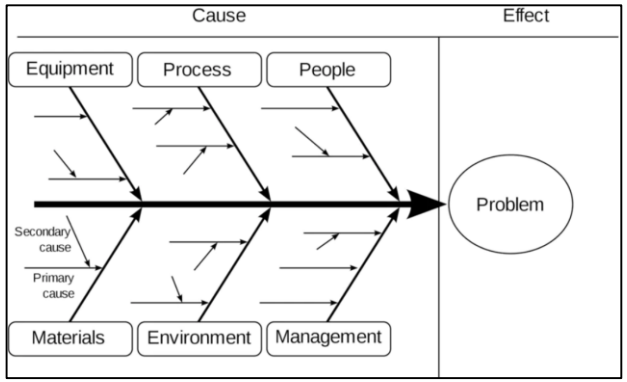
Risk identification in practice:

The next step in risk identification is <u>risk description</u>.

Description of the risk, i.e. indicating:

- the **source (cause)** of the potential risk;
- **effects (consequences)** that will occur after the risk materializes.

An example of a tool for determining the causes of potential risks:
the Ishikawa diagram.



Methods

Risk analysis in practice:

Risk analysis is an activity aimed at determining the level of risk, taking into account the effectiveness of existing risk controls.

The level of risk - the magnitude of risk (risk significance), combining the **likelihood of risk materialization** and **the effect of risk materialization**.

Risk control – measure that maintains and/or modifies risk.

The level of risk can be determined by following techniques, depending on the circumstances and intended use:

- **qualitative** - risks presented in a descriptive way, without using any numbers;
- **quantitative** - risks presented using numbers;
- **combination of aforementioned techniques**.

Methods

Evaluation of the effectiveness of existing risk controls

Risk control – measure that maintains and/or modifies risk.

Control completely eliminates or reduces risk sufficiently → a strong control

Control partially eliminates or partially reduces risk → a moderate control

Control does not eliminate risk or does not sufficiently reduces risk → a weak control

Examples of risk control evaluation criteria:
- adequacy;
- efficacy;
- cost effectiveness.

If, for a given risk, **all three criteria for assessing the control of that risk are met** (if reasonable) → **control of that risk is strong.**

Methods

Evaluation of the effectiveness of existing risk controls

Risk control – measure that maintains and/or modifies risk.

Criteria adopted by the Polish SSDL:

Criterion	Definition	Scope of evaluation
Adequacy	The applied risk responses are the appropriate / accurate response to a given risk.	Do the applied risk responses: • affect the sources (causes) or consequences of the risk, or both; • have been structured in such a way that their proper application will protect against the respective risk.
Efficacy	The applied risk responses effectively deal with the risks for which they were established, work as planned.	Do the applied risk responses: • reduce risks to the desired degree (to an acceptable level); • completely protect against a given source (cause) of risk or limit the consequences, without the need for other actions.
Cost effectiveness	The applied risk responses effectively affect risk with the least possible expense associated with the operation of these responses.	Whether: • the costs of implementing and operating the response do not exceed the damage that would be caused if the risk materialized; • the expenses of the applied response are lower than the effects obtained as a result of the response.

Methods

Risk evaluation in practice:

Estimated level of risk ≤ established acceptable level of risk → identified risk is acceptable

Estimated level of risk > established acceptable level of risk → identified risk is UNACCETABLE

If the identified risk is on UNACCEPTABLE level, actions are taken to bring the risk to an acceptable level.

Acceptable level of risk can be established as:

- **common for the entire organization** (all processes / tasks);
- **separate for individual processes / tasks**.

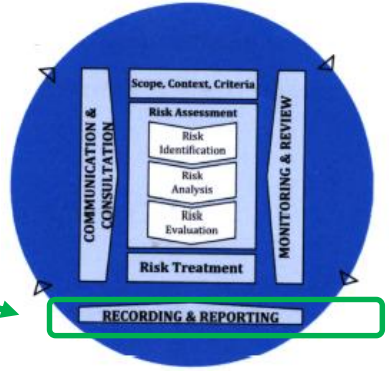
Example of risk evaluation:

Score (score 25 is the highest score)	**Level of risk**	
from 15 to 25	**UNACCETABLE**	**Risk requires actions and management decision (risk management plan)**
from 5 to 14	**medium acceptable**	Risk requires proceeding and ad hoc actions
from 1 to 4	**low acceptable**	Risk requires ongoing monitoring and ad hoc actions

Methods

Recording and reporting risk in practice:

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. [2]



At the Polish SSDL, meeting the requirements of the ISO/IEC 17025:2017 standard regarding activities related to risks and opportunities **is described in the established procedure:**
„Activities related to risks and opportunities in the Medical Physics Department".

This procedure includes the following forms for documenting risk and opportunity activities:

- ✓ **Form No. 1:** ***Register of risks and opportunities in the year ……;***
- ✓ **Form No. 2:** ***Criteria for evaluating the strength of risk control;***
- ✓ **Form No. 3:** ***Risk analysis principles;***
- ✓ **Form No. 4:** ***Acceptable risk levels.***

Practical examples of risk management

- several selected threats important from the point of view of the Polish SSDL were identified;
- for each threat:
  - ✓ an assessment of the strength of the controls currently applied was made;
  - ✓ likelihood and effect of the risk materialization were determined using the following tables:

Likelihood of risk materialization	Descriptive assessment of the likelihood of risk materialization	Scoring of the likelihood of risk materialization
< 15%	low	1
16 % - 45 %	moderate	2
46 % - 60 %	high	3
> 60 %	very high	4

Effect of the risk materialization	Descriptive assessment of the effect of the risk materialization	Scoring of the effect of risk materialization
Materialization of the risk will insignificantly affect the implementation of the task to which it relates	low	1
Materialization of the risk will complicate the implementation of the task to which it relates	moderate	2
Materialization of the risk will make it impossible to carry out the task to which it relates	high	3
Materialization of risk will disable the SSDL from functioning	very high	4

Note: If the risk responses used are rated as strong, then the likelihood or effect of risk materialization or both the likelihood and effect of risk materialization are rated lower, respectively (depending on what the strong risk responses are directed at).

✓ the level of risk was further determined using the following table:

Scoring of risk level	Descreptive assessment of risk level
1 - 4	low
5 - 8	moderate
9 - 12	high
13 - 16	very high

✓ in the Polish SSDL for the task: "Obtaining a valid calibration factor result", a low level of risk is considered acceptable, and a moderate level for other tasks.

Practical examples of risk management

Identification of risk			Opis ryzyka lub szansy (potencjalna przyczyna i skutek)	Applied control and evaluation of its strength	Risk analysis		Risk level	Risk level is acceptable?	The planned reaction
Purpose / Subprocess number	Task	Risk			Likelihood of risk materialization	Effect of risk materialization		Yes / No	
Providing customers with valid calibration results / 22.5	Monitoring the validity of calibration results and preventing invalid results from being included in calibration certificate.	Low representativeness of confirmation of the validity of the results obtained throughout the scope of accreditation based on samples representing the PT programs selected and planned for participation.	Potential cause: limited access to PT. Effect: obtaining an invalid calibration result.	Control used: review of the participation plan by the SSDL Head and ongoing monitoring of opportunities to participate in various PTs appropriate to one's scope of accreditation. Strength evaluation: strong control.	1	3	3	Yes	No reaction is required.
Providing customers with valid calibration results / 22.5	Monitoring the validity of calibration results and preventing invalid results from being included in calibration certificate.	Low effectiveness of monitoring and control of the concrete calibration results.	Potential cause: incorrect determination of the calibration factor value. Effect: obtaining an invalid calibration result.	Control used: checking the calculation of the calibration performed by another SSDL employee, monitoring the currently obtained calibration results in relation to the results of the previous calibration. Strength evaluation: strong control.	1	3	3	Yes	No reaction is required.
Providing customers with valid calibration results obtained with impartiality / 22.5	Reliable preparation of calibration certificate.	Pressure on SSDL personnel carrying out laboratory activities regarding calibration results.	Potential cause: personal/family/professional relationships of personnel performing laboratory activities with the client's personnel. Effect: issuing an unreliable calibration certificate.	Control used: • commitment of the employee on the relevant Management System document to maintain impartiality, objectivity and independence from all pressures (commercial, financial and other) with regard to laboratory activities carried out by the employee; • control of proper assignment of tasks to employees. Strength evaluation: strong control.	1	2	2	Yes	No reaction is required.
Reliable preparation of calibration certificate / 22.5	Obtaining a valid calibration factor result.	Unexpected change in the calibration factor of the calibration chamber.	Potential cause: malfunction of the calibration chamber or damage to the electrometer. Effect: obtaining an invalid calibration result.	Control used: intermediate checks of the standard in accordance with the relevant procedure for the management of calibration equipment. Strength assessment: strong control.	1	3	3	Yes	No reaction is required.
Providing customers with valid calibration results / 22.5	Monitoring the validity of calibration results and preventing invalid results from being included in calibration certificate.	Setting too low frequency of participation in bilateral comparisons in the area of calibration.	Potential cause: failure to take into account fundamental changes in equipment, calibration method or personnel affecting the validity of calibration results. Effect: obtaining an invalid calibration result.	Control used: review by the Head of SSDL of the participation plan in bilateral comparisons and monitor the currently obtained calibration results in relation to the results of the previous calibration. Strength assessment: strong control.	1	2	2	Yes	No reaction is required.

Conclusions

Practical examples of risk management presented in this work may be helpful for calibration and testing laboratories that plan to join the process of obtaining accreditation for compliance with the requirements of the ISO/IEC 17025:2017 or for such laboratories that would like to improve their risk management.

References

1. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, General requirements for the competence of testing and calibration laboratories, ISO/IEC 17025:2017, ISO, Geneva (2017).

2. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Risk management – Guidelines, ISO 31000:2018, ISO, Geneva (2018)

Thank you for your attention.