

Laboratory Risk Management and Assessment, on ISO 17025 perspective

Speaker / Author: D. J. E. Rademeyer

Co-author(s): C.F. Botha

ISHECON

PO Box 320, Modderfontein, 1645, South Africa

e-mail: rademeyerd@ishecon.co.za or bothad@ishecon.co.za

Telephone no.: 011 997 7945

1 Abstract

ISO 17025, in its most basic form, encompasses a management system for laboratories to ensure competence and continued improvement through risk management. A successful laboratory business therefore needs to manage operational, business and technical risks to facilitate secure, safe, healthy and environmentally acceptable operations. This ensures business continuity, competence and quality.

Risk management, risk assessment, risk identification, analysis and mitigation are phrases used by many institutions and applied in a wide spectrum of industries and organisations such as chemical, mining, banking and insurance, as well as business management and accreditation.

Risk management, based on experience and perception of risk levels, is carried out by everybody on a daily basis in everything they do, e.g. driving a car, crossing the street, even having a meal. However, the complexities when considering the risks and accreditation of a business in laboratories can be overwhelming and needs to be addressed methodically to prevent confusion.

An understanding of the concepts, methods and tools involved, as well as what the requirements are to establish objectivity in a risk assessment, is essential to assess and manage risks effectively. It is also important to understand when risk is not acceptable and whether reduction of the risk is practical and cost effective. The risk assessment will also identify possible opportunities for improvement and new business.

This paper will endeavour to introduce laboratory management, analysts and technicians to the basic concepts of risk management and assessment within a laboratory business.

2 Introduction

Work carried out in a laboratory can be of a research, analytical or testing nature. It may involve chemicals, biological agents, mechanical equipment, electrical systems or operational aspects. In any laboratory certain objectives need to be achieved to sustain the business, to meet client's needs or to comply with accreditation or legal requirements. In non-ideal circumstances, there is a chance that these objectives may not be met, in which case there could be negative consequences, which ultimately will lead to some form of loss. Losses could be financial,

economic, human, material, or even company image. When there is a chance of a loss, it is termed a risk.

A laboratory and a business face risks on a daily basis. The international standard ISO/IEC17025 [1] dealing with requirements for the competence of testing and calibration laboratories, requires laboratories to address risk. Specific mention is made of non-conforming work. This can be seen as including work that is unsafe, unhealthy; that is damaging to the environment, that can cause damage to assets, produce incorrect results, result in dissatisfied clients, lead to loss of business, produce a financial loss, revoke accreditation and create a negative laboratory organisation image.

If these risks are not well managed, they could eventually lead to various losses and penalties. Complying with the standard requires a laboratory to manage risk, i.e. a risk management system must be in place.

3 Risk Management

In order to manage risk in any environment, the risks must be known, only then can something be done to avoid or minimise the risk.

In a laboratory there may be small or large risks; avoiding or minimising them always involves effort, resources and money. Spending large amounts of money and resources on small risks would be counterproductive and a wastage, whereas inadequate allocation of money and resources to large risks, will allow the risks to proliferate to eventually end up in losses. This implies that to effectively manage risk, the risks must not only be identified, but the magnitude of the risks must also be estimated, e.g. whether they are small or large.

Therefore, risk needs to be evaluated regularly in terms of the likelihood of the unwanted occurrence and the seriousness of the effects. Small risks can sometimes be tolerated, without solving them. Larger risks may need immediate and strong action. In order for management to

decide when and how much should be done about the risks, they must judge the risks against some target of acceptability.

In essence, risk management entails knowing the risk, knowing the magnitude of the risk and allocating suitable resources, as well as judging the risk. In this process an effective risk assessment is critical.

Apart from the risk assessment, which is the focus in this paper, a complete risk management system should, in addition, include.....

- risk management system documentation;
- control of risk management system documents;
- control of records;
- actions to address risks and opportunities;
- a continuous improvement mind-set;
- corrective actions;
- internal audits;
- management reviews.

4 Risk Assessment

The South African National Standard [2] deals with risk assessment in detail and can serve as a reference. We will only deal with the basic principles in this paper.

Risk is the probability of a loss and is a function of the probability of an occurrence and the seriousness of its effects..

4.1 Principles

A risk assessment entails the identification of threats, dangers or hazards, followed by determining its likelihood and its severity. A combination of the likelihood and the severity allows the risk to be estimated, which is then compared to a target in order to make a decision

or judgement about its acceptability. Thus, a risk assessment may include the following elements:

- Selecting a system, a process, an operation, or an activity;
- Setting some risk targets which must not be exceeded or transgressed;
- Identifying the hazards, dangers or threats;
- Generation of causes for the hazards, dangers or threats;
- Estimating the likelihood of the hazards, dangers or threats occurring. This is often dependent on the causes;
- Determining the severity or seriousness of the hazards, dangers or threats. This is normally expressed in terms of harm to personnel, environmental impact, business or financial losses, legal and regulatory penalties and negative reputation;
- Combining the likelihood and the severity to obtain a risk result;
- Finally carrying out an assessment, meaning making a value judgement against the target to decide whether the risk is acceptable or not;
- Based on the assessment, improvements must be made to the system, process, operation, or activity to achieve an acceptable risk.

The approach is illustrated by the diagram in the Figure 4-1 below

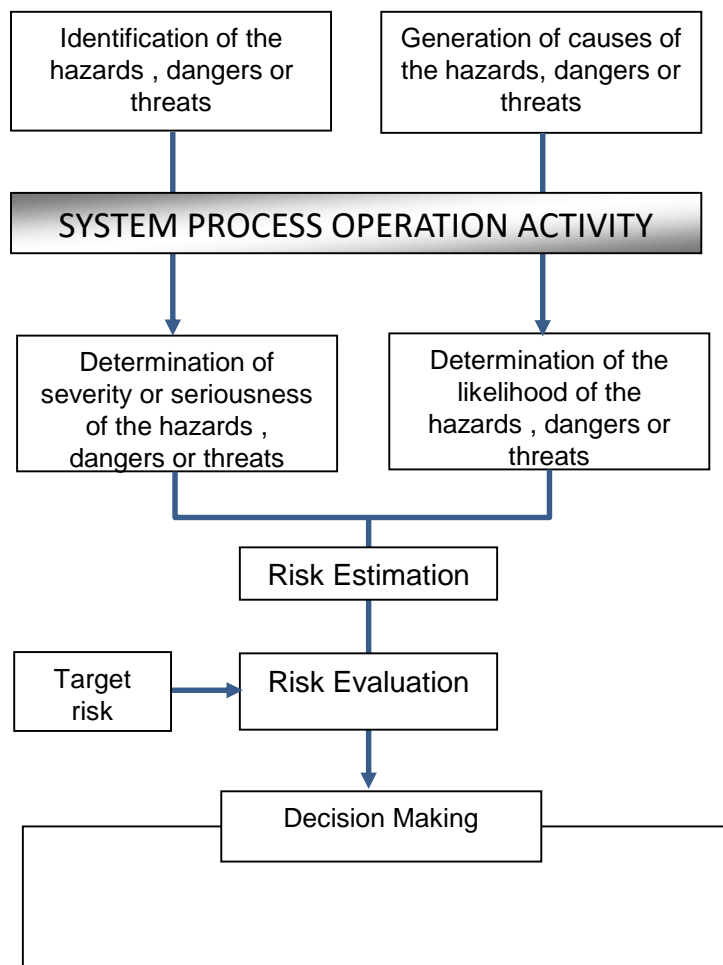


Figure 4-1 The risk assessment process

4.2 Scope

Risk assessment in laboratories must address risks posed by the laboratory operations to

- Personnel
- Assets, equipment
- Methods, procedures and processes
- Resources
- Business
- Clients

4.3 Procedure

4.3.1 Defining the System

The first step in assessing the risks is to define the boundaries of the system under consideration. This could for example be the bench work, methods, calibration of instruments and results, activities in the building, client's procedures, accounting or accreditation.

4.3.2 Risk Identification

As mentioned already, one cannot analyse risks without first identifying what risks could actually exist in a given situation. This entails identifying risks and the means by which they can occur.

Some technique is required to systematically identify risk. The word 'systematic' is crucial. One risk that is not identified can result in an entire risk assessment being meaningless. One of the ways to ensure that this does not happen is to have a logical, thorough and step-by-step approach to identifying risks.

There are several systematic techniques, but most appropriate for a laboratory is a guide word method that will prompt management and personnel to think what could possibly go wrong, similar to the established Hazard and Operability Study technique, focusing on the equipment with which the tests and analyses are carried out, and the personnel/humans involved.

Normally, the aim is to avoid exposure of personnel, assets, operations, business and organisation to threats. Thus, a laboratory is designed to contain the risks (e.g. use of calibrated instruments, proper safe methods, correct results, client satisfaction, return on investment, good organisational image and maintenance of accreditation). Only in abnormal circumstances will threats then occur, for example, an analyst that short-cuts a procedure, an instrument or a reference that performs outside its control limits without detection, a sample that deteriorates and becomes mouldy. Thus, when identifying threats one is actually looking for situations that can lead to the threat (loss of calibration) and how it will affect results, ultimately causing harm or loss.

4.4 Risk Analysis

As previously stated, risk is the likelihood of an event actually happening (sometimes referred to as the chance, probability or frequency) and the consequences (sometimes referred to as the severity or seriousness).

$\text{RISK} = \text{LIKELIHOOD} \times \text{SEVERITY}$
--

An analysis of risk, associated with certain threats, therefore requires some consideration of both likelihood and consequence. That consideration can range from qualitative judgements based on experience through semi-quantitative estimates to detailed calculated predictions based on statistical data.

4.4.1 Qualitative

Using qualitative judgement of probability and severity, for example, operating staff may decide that if a certain reagent is spilled, no one would be harmed and as this has never happened in all their combined working lives, they consider it virtually impossible to happen and therefore not a significant risk.

4.4.2 Quantitative

Involves the detailed calculation of both the probability and the consequence elements and is more time consuming.

4.4.3 Semi-quantitative

This uses qualitative judgement of probability and severity, but assigns numbers to the probability and severity to express the magnitude of each risk numerically. These two numbers are then combined to give an indication of the risk and are judged according to a predetermined acceptability target.

A semi-quantitative risk analysis method is regarded most suitable for laboratory risk assessments.

4.4.4 Cause analysis

Threat identification techniques identify what can cause the potential risk to occur, i.e. what aspect has to fail to go wrong. The chance of the risk occurring depends on a combination of the chances of the different causal events occurring, i.e. the chance of the failures coinciding. Chance is expressed as a probability between 0 and 1. Instead of chance one may use likelihood expressed as a frequency, e.g. number per time unit, usually a year, which is the criterion that will be used for laboratories

So in a qualitative analysis one may say 'there is a small chance that it will happen' or 'it will happen once in my lifetime', while quantitatively one may say 'there is a 50% chance it may happen' or 'the frequency of the event is less than once in 70 years'.

4.5 Consequence analysis

Consequences are the results of a risk event taking place. In laboratories the consequences of concern from analytic and test work could be injuries, illnesses, pollution, customer claims, court case, loss of accreditation, loss of business and poor organisational image. The severity of the consequence of the risk depends again on a combination of the different effects occurring, i.e. the degree of seriousness in terms of injuries, illnesses, clients that are dissatisfied, financial loss or degradation of organisational image.

So, in a qualitative analysis one may say 'little money is lost', while quantitatively one may say the result was 'one disabling injury', 'temporary illness', 'two clients dissatisfied', 'R50 000 lost income', etc.

4.6 Risk Estimation

Since risk is composed of both consequences and likelihood, these two entities need to be combined into a single number that represents both simultaneously.

Thus, if one multiplies a 10% chance of the calibration becoming inaccurate by harsh handling and this results in two customers being lost, then the risk will be:

Risk = 0,1 (Chance) * 2 (Severity) = 0,2 chance of losing customer.

4.7 Risk Assessment

Determination of the risk is of no use on its own. The risk level has to be compared to a target to make a judgement. If no judgement about the risk can be made, nothing can be done with the information, i.e. risk assessment is undertaken to facilitate decision-making. A decision is needed about whether the risk is too high or low enough, is it acceptable or unacceptable.

Thus, a valued judgement of risk is the 'assessment'.

4.8 Risk Treatment

If the risks are too high, the assumptions must be reviewed, or changes must be made to the design of the equipment or procedures to mitigate or reduce the risk. Risks can then be re-estimated in terms of the likelihood and severity with these modifications in place. The risks are re-calculated and re-assessed until they are acceptably low.

4.9 Risk Matrix

A convenient technique to analyse risk in a laboratory semi-quantitatively is to use a risk matrix. This comprises a grid where, in graph format, consequences are assigned to the x-axis and likelihood to the y-axis. A 5 by 5 matrix is typical, where likelihood is expressed as a frequency (number of times per year) and the consequences are expressed in terms of harm to

people, environmental impact, business interruption, material damage, legal and regulatory and impairment of reputation. The intersection on the grid denotes the risk. In order to facilitate risk assessment the grid is filled in with different colours, from which the required action is proposed. See Figure 4-2 below for a standard risk matrix recommended for laboratories.

STANDARD RISK MATRIX		Based on AS/NZ 4360 "Risk Management" and Anglo Platinum FROG No.A42:2006				
Hazard Consequence Severity		1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
Loss Type Where a risk event has more than one loss type, choose the one with the highest rating. Additional loss types may exist for a risk event, identify and rate accordingly.	Harm to People (Safety & Health)	First aid case / Exposure to minor health risk	Medical treatment case / Exposure to major health risk	Lost time injury / Reversible impact on health	Single fatality or loss of quality of life / Irreversible impact on health	Multiple fatalities / Impact on health ultimately fatal
	Environmental Impact	Minimal environmental harm	Material environmental harm – remediable short term	Serious environmental harm – remediable within life-of-facility	Major environmental harm – remediable post life-of-facility	Extreme environmental harm – irreversible
	Business Interruption/ Material Damage & other losses	No disruption to operation. R500k to < R5m	Brief disruption to operation. R5m to < R50m	Partial shutdown. R50m to < R500m	Partial loss of operation. R500m to < R5b	Substantial or total loss of operation. R5b and higher
	Legal & Regulatory	Low level legal issue	Minor legal issue; non-compliance and breach of the law	Serious breach of law; investigation, report to authority; prosecution and/or moderate penalty	Major breach of the law; considerable prosecution and penalties	Considerable penalties & prosecutions. Multiple law suits & jail terms
	Reputation/ Social/ Community	Slight impact - public awareness may exist but no public concern	Limited impact - local public concern	Considerable impact - regional public concern	National impact - national public concern	International impact - international public attention
Likelihood	Examples (Consider near miss and real events)	Risk Rating/ Assessment				
5 Almost certain	Unwanted event occurred frequently; 1 or more per year, likely to recur in 1 year	11 - M	16 - H	20 - H	23 - E	25 - E
4 Likely	Unwanted event occurs infrequently; less than 1 /year. Likely to recur in 5 years	7 - M	12 - M	17 - H	21 - E	24 - E
3 Possible	Event happened in the business at some time; or could within 10 years	4 - L	8 - M	13 - H	18 - H	22 - E
2 Unlikely	Event happened in business at some time; or could recur in 20 years	2 - L	5 - L	9 - M	14 - H	19 - H
1 Rare	Event not known to occur in business; or highly unlikely to occur in 20 years	1 - L	3 - L	6 - M	10 - M	15 - H
Interpretation of Risk Rating		Notes				
Risk Rating	Risk Assessment	Risk Evaluation – Management response required				
21 to 25	E – Excessive	Implement urgent and immediate corrective action			1 Qualitative risk matrices cannot deliver precise risk evaluation. They provide a ranking of risk, and indicate the extent of risk treatment response required from management.	
13 to 20	H – High	Implement corrective action			2 The Monetary Loss Type scale can be 'calibrated' for each study by sliding the scale along to the point where the R value is regarded as 'catastrophic' for the entity concerned.	
6 to 12	M – Medium	Review existing systems				
1 to 5	L – Low	Maintain existing systems				

Figure 4-2 A Standard Risk Matrix

4.10 Laboratory Threats

Below is a list of possible key threats in a laboratory with some cause factors in brackets that could be analysed in terms of the risks they pose to the organisation:

- Safety and health dangers (accidents, illnesses, diseases)
- Environmental effects (waste disposal, pollution, compensation)
- Substandard quality work (calibration, methods, procedures, auditing, skills scarcity, training, qualifications)
- Failures (breakdown of equipment, deterioration, mal-operation)
- Deficient management (leadership, technical signatories, succession, policies, supervision, corruption)
- Insufficient resources (staff, strikes, materials, equipment)
- Noncompliance (legal, standards, procedures, certification, claims)
- Unavailability (utilities, power, reagents)
- Unsustainability (competition BEE, new technology, accreditation loss)
- Un-maintainability (resources, tools, spares)
- Security breach (access, sabotage, theft, confidentiality, data, hacking)
- Financial strain (costs, productivity, profit, debt)

4.11 Risk Report

The results of an assessment must be recorded in the standard report format that is clear and logical to others. See Table 4-1 below for a typical record sheet for a risk assessment.

Table 1 Example of a record sheet for a laboratory risk assessment

Table 1 – RISK ANALYSIS RECORD										
SYSTEM: Blood group determination						<i>Pr</i> ≡ reduced probability <i>Sm</i> ≡ Mitigated consequence ≡ Exposure, <i>Rfi</i> ≡ Risk Rating				
Operation, activity:										
No	Risk Event Threat	Causes	Prevention	Pr	Consequence	Protection	Sm	E	Rfi	Recommendation
1	Select wrong antigen	Wrong label	Procedure	2	Wrong type transfusion, jaundice	Blood ex-change	3	1	9 M	•Medium risk, review procedure
2	Other person blood tested	Doctor in correct enter name on sample (sample mixed up)	Re-quision sheet attached by nurse	2	Fatal potential for patient	Group 0 compatible with most persons Can do 'reverse' trans-fusion	4	1	14 H	•High risk, implement requisition receiver to check name on sample and requisition same and confirm n checklist

4.12 Risk Profile

The findings from a risk assessment can be display as a profile which can be easily visually interpreted by management. As an illustration, the risk events and threats identified and assessed can be grouped in key threats as listed in Section 4.11 above and then plotted on a graph as shown in Figure 4-3 below.

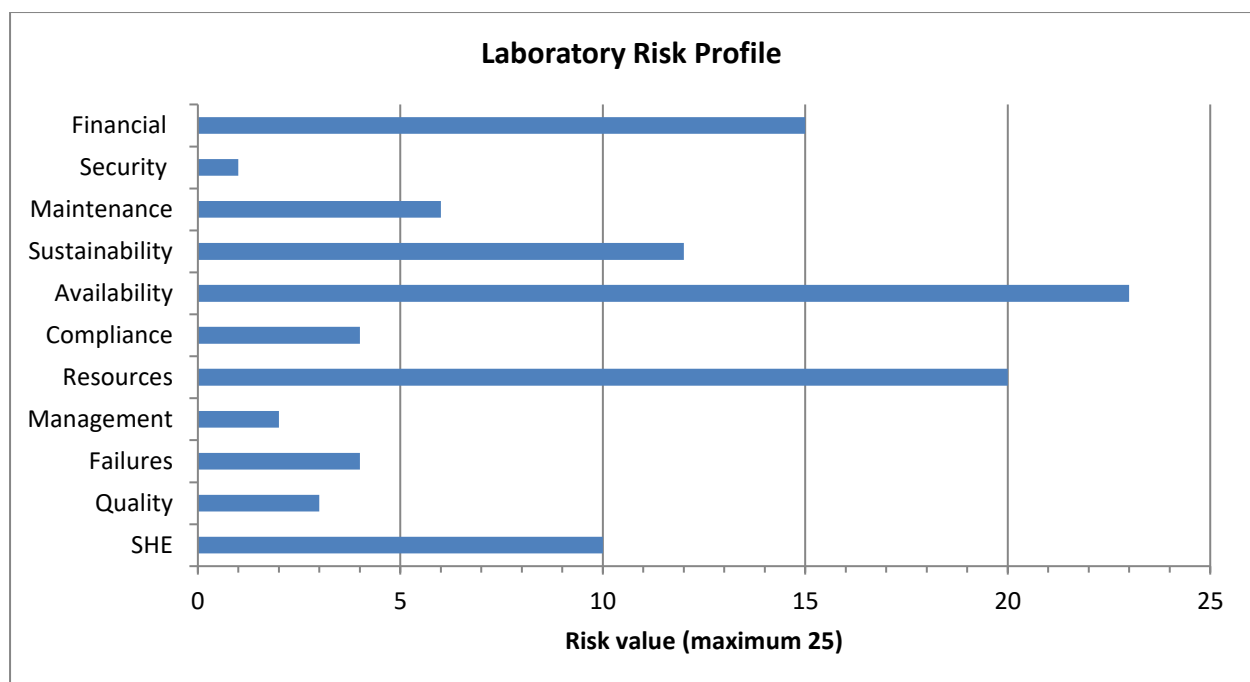


Figure 4-3 An example of a risk profile for a laboratory

The above risk profile can be updated every year and would be a useful aid for management and auditors to monitor progress in reducing risk or maintaining low risks.

5 Conclusion

In this paper we have attempted to explain the need for risk assessment specifically in laboratories in order to comply with the international standard ISO/IEC17025 [1] for laboratories. Principles pertaining to risk assessment were exemplified and a basic procedure has been proposed. This included a list of risks in a laboratory to be addressed and a means to record the risk together with a graphical presentation.

Laboratories will probably not be in a position to carry out these risk assessments on their own initially. Therefore further work will be done to do a practical risk assessment on a laboratory as a test case, where after the method can be refined. This will allow us to assist laboratories with their risk assessments.

6 References

1. SANS 17025:2018, General requirements for the competence of testing and calibration laboratories, Edition 3, May 2018.
2. SANS 31010:2010, Risk Management –Risk Assessment Techniques, Edition 1, January 2010.