SIE 2015
6th International Symposium on Industrial Engineering
24th-25th September 2015
FACULTY OF MECHANICAL ENGINEERING
STEINBEIS ADVANCED RISK TECHNOLOGIES
INNOVATION CENTER FME

RISK BASED AUDIT OF MANAGEMENT SYSTEMS

Srđan Vulanović[1], Vojislav Vulanović[1], Vladan Radlovački[1], Milan Delić[1]
[1]Faculty of Technical Sciences, University of Novi Sad, Serbia

Abstract. *Obligation of periodical internal and external audits is common for all management systems. Standard ISO 19011 provides guidance on auditing of management systems including the principles for auditing, managing an audit programme and conducting the management system audits. ISO 19011:2011 introduces the concept of risk in management system audits but it does not give specific guidance for the risk assessment and risk management process of the organization. This paper proposes a model for management system auditing based on risk assessment. The adopted model refers to the risks concerning the achievement of audit goals, together with risks of the audit to interfere with audited activities and processes of the organization.*

Key words: *Management systems, audit, risk management, risk assessment*

1. INTRODUCTION

It can be established that the purpose of implementation of international management standards is the reduction or elimination of certain risk groups, such as [1]:

- risks related to the process quality - ISO 9001,
- risks related to the environment - ISO 14001,
- risks related to the occupational health and safety - OHSAS 18001,
- risks related to the food safety - ISO/IEC 22000, etc.

All listed standards are subject to periodical internal and external audits, which are carried out in accordance with the requirements of ISO 19011 [2]. This international standard sets no requirements, but provides guidelines for the management of audit programs, planning and carrying out the process of management system audit, together with guidelines for competences of auditors and evaluation criteria for audit team.

The reliance on numerous principles is characteristic for auditing. These principles should be harmonized with the management system policy, and should help the management to conduct an effective and reliable audit, which provides information needed for the improvement of organizations performance.

Adherence to these principles is a prerequisite that the conclusions of an audit are relevant and sufficient, allowing auditors to come to similar conclusions in similar circumstances even if they work independently.

Six principles are listed below [2]:

- Integrity - the foundation of professionalism
- Correct presentation - the obligation to report truthfully and accurately
- Professional attention – required attention and judgment in audit
- Confidentiality - Information security
- Independence - the basis for the impartiality and objectivity of the conclusions
- Evidence-based approach - the rational method of achieving reliable and reproducible conclusions of systematic audit process

The authors of this paper argue that the risk management should also be one of the core principles of an audit, because risk management must be embedded in all the organization's practices and processes in order to be relevant, effective and efficient [3]. One more reason for this claim is the explicit requirement of standard ISO 19011:2011 for obligatory risk assessment of every conducted audit.

2. METHODOLOGY

Second edition of ISO/IEC 17021:2011 [4] that sets guidelines for auditing management systems, accepted the approach to perform simultaneous audit of two or more management systems *(combined audit)* so there is a need for establishing a universal method for assessing the risks of combined audit.

The process flow for the audit programme management, embedded in the PDCA (PLAN-DO-CHECK-AKT) cycle of continual improvement is shown in Figure 1 [2].

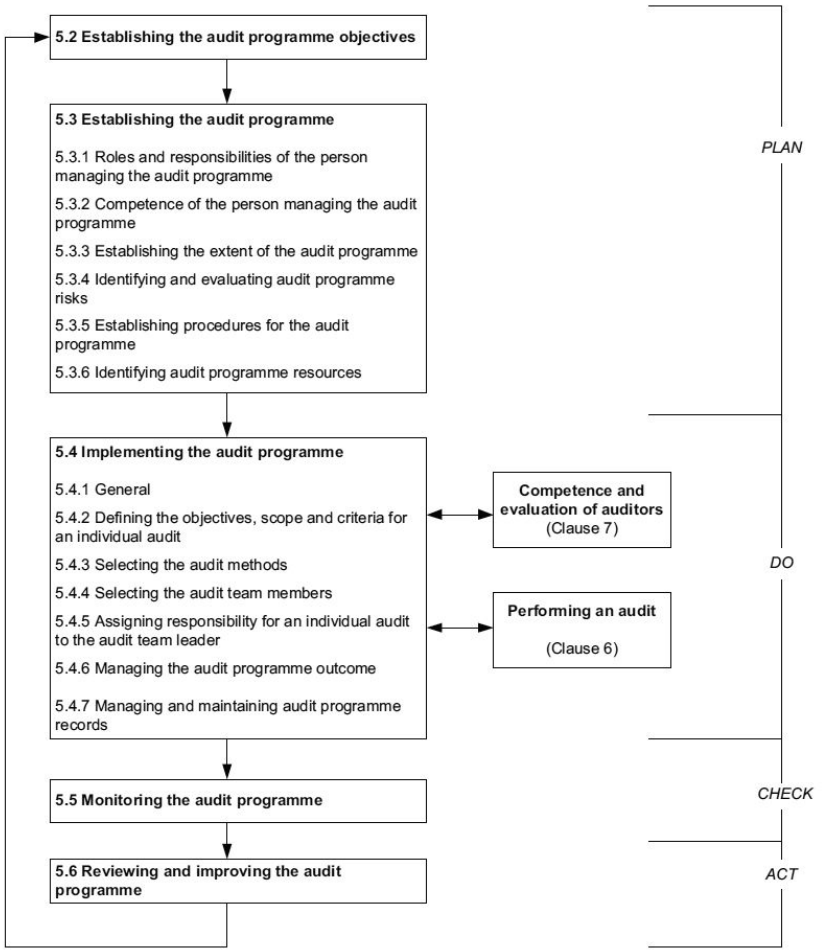

Figure 1: Process flow for the management of an audit programme

2.1 The audit programme objectives

According to the ISO 19011 [2] top management should ensure that the audit programme objectives are established to direct planning and conducting of an audit. Management should also ensure that the audit programme is implemented effectively. These objectives can be based on following:

- management priorities;
- commercial and other business intentions;
- characteristics of processes, products and projects, and any changes to them;
- management system requirements;
- legal, contractual and other requirements to which the organization is committed;
- need for supplier evaluation;
- needs and expectations of interested parties, including customers;
- auditee's level of performance, as reflected in the occurrence of failures or incidents or customer complaints;
- risks to the auditee;
- results of previous audits;
- level of maturity of the management system being audited.

2.2 Identification of audit risks

There are various risks associated with the planning, implementation, monitoring and review of audit programme that may affect:

- achievement of the objectives of an audit,
- audit results,
- effectiveness of the system and
- evaluation of the system ability.

When creating a program of an internal audit, one should consider the risks that may be associated with the following:

1. risks of inconsistency of the audit programme with the audit objectives,
2. risks in planning the insufficient time for audit programme realization,
3. risks of incompetence of the audit team for the effective audit realization,
4. risks of audit program realization (the absence of auditees, ineffective communication, etc.),
5. risks in disclosure of records during the audit,
6. risks in reviewing, monitoring and improving of the audit programme.

Other risks can be added to the list if management identifies them as relevant.

2.3 Assessment of audit risks

According to ISO 31000 [3] and ISO 31010 [5], almost all methods for risk assessment have two major criteria:

1. the likelihood of occurrence and
2. the significance of consequence

The authors of this paper adopted listed criteria and suggested a universal method for audit risk assessment that follows.

Six possible audit risks were identified in previous chapter. Each risk which is present in the particular organization should be assessed in terms of likelihood of occurrence. Each of the identified risks can cause a consequence with significance that also should be assessed.

Table 1 shows the criteria for evaluating the likelihood of occurrence and Table 2 shows the criteria for the assessment of significance of consequence.

Table 1

The likelihood of occurrence	Probability value	Grade 1
Almost impossible	< 0,001	1
Not likely	0,001 ÷ 0,03	2
Probably	0,03 ÷ 0,1	3
Quite likely	0,1 ÷ 0,3	4
Highly likely	> 0,3	5

Table 2

The significance of consequence	Consequence description	Grade 2
Slight	No impact on system functioning	1
Eligible	It does not affect the essential elements of system functioning	2
Unacceptable	Endangers the system functioning	3

The risk level (RL) should be calculated by multiplying the assessed grades for the likelihood of occurrence and the significance of consequence.

RISK LEVEL = GRADE 1 x GRADE 2.

2.4 The risk level matrix

The basic matrix for the evaluation of risk levels is given in Table 3, which shows that risk levels can be in the range from 1 to 15. There are 15 possible values for risk level (7 without repeating).

The authors suggest that risk levels should be grouped into three categories, which is shown in Table 4. It is assumed that if the unacceptable risk is present in a particular organization, the management representative must initiate a corrective action.

Table 3

Risk level (1 ÷ 15)			The likelihood of occurrence				
			Almost impossible	Not likely	Probably	Quite likely	Highly likely
			1	*2*	*3*	*4*	*5*
The significance of consequence	Slight	*1*	**1**	**2**	**3**	**4**	**5**
	Eligible	*2*	**2**	**4**	**6**	**8**	**10**
	Unacceptable	*3*	**3**	**6**	**9**	**12**	**15**

Table 4

The range of grades for risk level	1 ÷ 3	4 ÷ 6	8 ÷ 15
Risk Level Category (RLC)	Insignificant risk RLC 1	Acceptable risk RLC 2	Unacceptable risk RLC 3

2.5 Overall risk level of an audit

After the assessment, evaluation and categorization of all identified audit risks, one should calculate Overall Risk Level of an audit (ORL).

If the audit risks are independent of each other, then the ORL can be calculated by following formula:

$$ORL = \sum_{i}^{n} RL_i$$

The number of evaluated risks can go from 1 to n.

If the identified risks have mutual influence, they should be multiplied (RL_1 x RL_2), and independent risks should be added. ORL is an indicator of a system and can be used for setting the audit objectives and improving the audit results, or for the reduction of risks in subsequent audits.

3. Model testing

The universal method for audit risk assessment was applied in industry of processing and production of metal products and steel plates, surface protection by galvanizing and painting.

The chosen organization had quality management system and environmental management system implemented and certified since 2013.

Identification and assessment of audit risks

All six potential risks from chapter 2.2 were identified and assessed in terms of likelihood and consequence, as shown in Table 5.

Table 5

Audit risks	Likelihood	Consequence	RL_i	RLC_i
1. Risks of inconsistency of the audit program with the audit objectives,	1	1	1	**1**
2. Risks in planning the insufficient time for audit programme realization,	2	1	2	**1**
3. Risks of incompetence of the audit team for the effective audit realization,	1	2	2	**1**
4. Risks of audit program realization (the absence of audited party, ineffective communication, etc.),	1	1	1	**1**
5. Risks in disclosure of records during the audit,	2	1	2	**1**
6. Risks in reviewing, monitoring and improving of the audit programme,	2	1	2	**1**

All risk level values in the Table 5 are in the range of insignificant risk and it can be concluded that corrective measures are not necessary.

In this case the overall risk level of an audit (ORL) is calculated as:

$ORL = (RL_1 + RL_2 + RL_4 + RL_5 + RL_6) \times RL_3$

It is estimated that RL_1, RL_2, RL_4, RL_5 and RL_6 are independent of each other, and they add up; but the RL_3 (auditors competence) has an impact on all identified risks, and it is multiplied by the sum of other risks. In this example the result of overall risk level of an audit is 16.

$ORL = (1 + 2 + 1 + 2 + 2) \times 2 = 16.$

The overall risk level is a value that indicates the potentiality for reduction of risks by improving the design, review and implementation of the audit program in the next cycle of audits.

4. CONCLUSIONS

The risk as a category is present in all management systems (in expected ISO 9001:2015 there is a new requirement for risk assessment of all identified processes), so the risk management system must be treated as an integral part of all processes in organizations.

Risk management supports the organization to achieve its objectives and avoid potential threats and unintended consequences. It can be stated that there are no "a-priori risky processes" but the risk varies in the context of its impact on the organization`s performance, so it should be treated in accordance to its context.

The audit of management systems is a process that cannot be excluded from other processes in organization and its risks should also be treated in accordance to ISO 19011:2011 requirements.

This paper shows a model for identification, assessment, evaluation and categorization of audit risks, which is flexible enough to be applied in organizations of all types and sizes. The proposed model is simple for application and is based on assessment of two crucial components of risk:

1. The likelihood of occurrence and
2. The significance of consequence

The greatest advantage of this model is based on a fact that every risk can be considered separately and also can be combined with other risks. According to the holistic approach, the overall audit risk should be calculated differently if single risks have mutual impact to each other (where the resulting risk level is much higher if there is some kind of inter-relationship between the assessed risks).

The model suggests that each identified audit risk should be treated in accordance to assessed risk level values, and the audit itself should be treated in accordance to calculated overall risk level.

The proposed model was successfully tested and validated in praxis so it can be concluded that it offers the possibility for effective and efficient audit risk management in organizations of various types and sizes.

REFERENCES

[1] Vulanović Srđan, Beker Ivan, Kesić Igor, Brkljač Nebojša, Vuković Milica: Possible Applications of ONR 49000 Standard Series in Risk Management in Organizations, International Convention on Quality – JUSK ICQ 2014, Belgrade, Serbia, 2014.

[2] ISO 19011:2011 - Guidelines for auditing management systems, International Organization for Standardization, Geneva, Switzerland, 2011.

[3] ISO 31000:2009 - Risk management – Principles and guidelines, International Organization for Standardization, Geneva, Switzerland, 2009.

[4] ISO/IEC 17021:2011 - Conformity assessment -- Requirements for bodies providing audit and certification of management systems, International Organization for Standardization, Geneva, Switzerland, 2011.

[5] IEC 31010:2009 - Risk management -- Risk assessment techniques, International Organization for Standardization, Geneva, Switzerland, 2009.