J. Soc. Korea Ind. Syst. Eng Vol. 40, No. 3 : 38-48, September 2017
https://doi.org/10.11627/jkise.2017.40.3.038
ISSN : 2005-0461(print)
ISSN : 2287-7975(online)

A Fundamental Concept of Risk-Based Thinking and Risk Management for ISO 9001:2015 Certification

Ho Gyun Kim* · Byung Hwan Kang** · Dong Joon Park***†

*Department of Production and Information Technology Engineering, Dong-Eui University
**LRQA, Korea Ltd.
***Department of Statistics, Pukyong National University

ISO 9001:2015 인증을 위한 리스크 기반 사고의 개념과 리스크 관리

김호균* · 강병환** · 박동준***†

*동의대학교 생산정보기술공학과
**LRQA, Korea Ltd.
***부경대학교 통계학과

ISO 9001 Quality Management Systems-Requirements has been revised in 2015. It has been updated four times since its publication in 1987. It is the most widely used International Standard in the world. There are over one million companies and organizations in over 170 countries certified to ISO 9001 from an ISO survey. Organizations are supposed to be certified to this new version by late 2018. The key changes in ISO 9001:2015 are to establish a High Level Structure (HLS) and focus on Risk-Based Thinking (RBT). Risk-Based Thinking means the process approach to decide how risk is addressed in establishing the processes to improve process outputs and prevent undesirable results. It pursues process planning and controls based on risks so that organizations can improve the effectiveness of the quality management system. It maintains and manages a Quality Management System that inherently addresses risks and meets objectives.

In this article we firstly attempt to explain how to understand the fundamental concept of Risk-Based Thinking which is a systematic approach to consider risks rather than treating prevention as a separate component of a Quality Management System. We comment on the detailed requirements that contain risks in ISO 9001:2015 clauses. We also summarize recent advances on the risk assessment and management in line with ISO 31000:2009 Risk Management-Principles and Guidelines. We finally propose the practical risk management procedures for implementing ISO 9001:2015 with an emphasis on RBT. This article would contribute to help quality managers and practitioners convert to ISO 9001:2015.

Keywords : ISO 9001:2015, Quality Management System(QMS), Risk Management, Risk Assessment, Risk-Based Thinking(RBT)

Received 16 August 2017; Finally Revised 21 September 2017;
Accepted 22 September 2017
† Corresponding Author : djpark@pknu.ac.kr

1. 서 론

기업경쟁력의 원천은 고객만족에 있으며 제품 또는 서비스의 품질은 고객만족의 중요 요소 중 하나이다. 기업은 제품 또는 서비스가 고객들의 품질 요구사항을 충족하는 것을 확신시키기 위하여 체계적인 품질보증 활동을 하고 있다. 품질보증 활동의 객관성과 효율성을 높이기 위해 제 3자의 객관적인 평가가 필요하게 되었고 품질경영시스템(QMS : Quality Management System) 인증제도가 도입 확산되었다. 기업에서는 기업의 특성에 따라 품질경영시스템 뿐만 아니라 환경경영시스템(EMS : Environmental Management System)과 안전 보건 경영시스템(OHSAS : Occupational Health and Safety Management System) 등 다양한 경영시스템의 인증 획득을 위해 노력하고 있다[13].

국제표준화기구(ISO : International Organization for Standardization)에서는 1987년에 최초로 품질경영시스템 ISO 9000시리즈를 제정하였으며, 변화하는 시장요구에 대응할 수 있도록 약 5년마다 규격의 적절성을 검토해왔다. 이후 ISO 9000 패밀리(현재는 시리즈 대신 사용됨)는 1994년, 2000년, 2008년, 2015년에 네 차례 개정되었다. 최근 국내외 기업 경영환경의 급격한 변화에 따라 국내 대기업에서는 2017년까지 조기 전환인증을 추진하고 있으며, 협력업체 및 이해관계자들은 개정 규격에 따라 품질방침을 변경하고 실행함으로써 규격의 전환인증을 획득하여야 하는 실정이다.

Kim et al.[13]은 ISO 9001의 2008년과 2015년 규격에 대한 차이점 분석(gap analysis)을 실행하고, 동남권 지역 제조업체를 중심으로 제조업체의 특성과 2015년 개정 규격과의 관련성을 통계적으로 분석하여 시사점을 찾고자 하였다. 2015년 개정 규격은 리스크(risk) 파악 및 기업 내·외부 경영환경을 고려한 위기관리 프로세스 구축과 운영 개선 및 조직, 인적자원들의 지식 공유·관리가 가장 핵심적인 변화임을 강조하였다. ISO 9001:2015 개정 규격의 주요변화 가운데 가장 큰 특징은 다음 두 가지로 요약할 수 있다[12].

- "리스크 기반 사고(RBT : Risk-Based Thinking)"에 근거한 규격이다.
- 여러 가지 ISO 경영시스템 규격을 조직에 쉽게 적용하기 위해서 동일한 핵심언어(identical core text)와 공통용어(common terms and definitions)와 상위구조(HLS : High Level Structure)를 갖춘 Annex SL(부록 SL이란 의미)을 사용한 규격으로서 10개의 절(Clauses)로 구성되어 있다-일반 사항 3개의 절(1. 적용범위, 2. 인용표준, 3. 용어와 정의)과 조직적용을 위하여 구체화한 7개의 절(4. 조직 상황, 5. 리더십, 6. 기획, 7. 자원, 8. 운영, 9. 성과평가, 10. 개선).

위에서 언급하는 리스크는 연구 분야에 따라 다양한 개념과 정의가 있으나 QMS와 관련된 리스크의 정의는 다음과 같다 :

- ISO 3100:2009(리스크 관리 규격) : 목표에 대한 불확실성의 영향
- ISO 9001:2015 서문(Foreword) : 긍정 또는 부정의 효과를 가지는 불확실성의 효과(the effect of uncertainty and any such uncertainty can have positive or negative effects).

한편 국제 표준화 기구의 기술위원회인 ISO TC/176/SC2 (www.iso.org/tc176/sc02/public)에서는 RBT를 언급한 후, RBT가 프로세스 접근법을 대체하며 예방조치에 대한 별도의 절이 없음을 밝혔다. 현재까지 2015년에 개정된 ISO 9001의 규격과 관련된 학술적 연구는 문헌에서 찾아보기가 어렵다. 이에 따라 본 논문에서는 ISO 9001:2015에서 강조한 RBT의 의미와 함께 리스크 평가 및 관리의 개념을 검토하고 리스크 관리의 실행 전략을 제시하여 2015년 개정 규격으로 전환 인증을 추진하는 기업의 품질경영 실무자 및 연구자들의 이해를 증진시키고자 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 RBT의 기본적인 개념과 함께 리스크 기반의 QMS 도입 시 기대효과를 예측하고 ISO 9001:2015 규격에서 리스크를 명시한 절(Clauses)의 의미를 서술한 후, 조직의 현실적인 예를 들어 리스크 기반 사고의 6단계를 기술한다. 제 3장에서는 위기분석학회(SRA; Society for Risk Analysis)와 리스크 관리 규격 ISO 31000:2009와 연구문헌을 중심으로 리스크의 평가, 척도화, 불확실성, 관리 전략, 프로세스, 분석을 요약한다. 제 4장에서는 조직의 현실적 업무에서 발생 가능한 구체적인 리스크를 열거한 후, 품질경영 실무자들이 리스크 기반의 ISO 9001:2015를 실제 업무에 도입할 수 있도록 체계적인 리스크 관리 절차를 제안한다. 마지막으로 제 5장에서는 연구 결과를 종합하고 향후 연구방향을 서술한다.

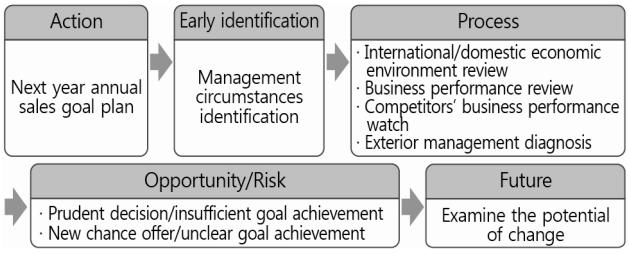
2. 리스크 기반 사고(RBT)

2.1 리스크 기반 사고 개요

전술한 바와 같이 ISO 9001:2015 개정 규격에서 가장 큰 특징 가운데 하나는 RBT를 강조한 것이다. 2008년 규격과 달리 개정 규격에서는 품질경영시스템의 요소들을 "예방조치(prevention)"가 아닌 "리스크(risk)"의 개념으로 고려하여 PDCA 사이클 속에 내재하는 품질경영시스템의 요소들을 체계적으로 관리(systematic approach to risk)한다는 의미이다. 예를 들어 경영활동에서 일어나는 상황을 RBT를 고려하지 않는 과정으로 적으면 <Figure 1>과 같다 :

<Figure 1> Routine Process

RBT는 품질의 경영을 시작하는 설계부터 운용 후, 개선하는 마지막 단계까지 시스템 전체 내부의 리스크를 식별하여 고려하는 것을 의미한다. 시스템 내 모든 프로세스의 리스크 수준이 동일하지 않으므로 각각의 프로세스에 대한 리스크를 고려하여 세심한 주의와 체계적인 계획과 관리가 필요하다. 또한 리스크의 결과는 부정과 긍정의 양면성을 갖고 있다. 즉, RBT는 바람직하지 않은 결과를 예방(prevent)하거나 감소(reduce)시키기 위하여 반응(reactive)하는 것보다는 초기에 식별하고 조치함으로써 선행하여 조치(proactive)하는 것이다. 위에서 언급한 신년 매출 목표 수립에 대하여 RBT를 고려한 상황의 프로세스는 <Figure 2>와 같다 :



<Figure 2> Process Based on RBT

그러므로 리스크 기반으로 QMS가 정립되었을 때는 예방조치는 이미 자동적으로 장착(built-in)되어 수행되고 있다는 것을 의미한다. RBT를 기반으로 한 QMS가 정착되면 조직과 이해관계자들에게 다음의 기대효과를 예상할 수 있다 :

• 조직
  - 수립 목표의 달성 가능성 증가
  - 변화하는 법 및 규제에 능동적인 대처
  - 경영환경 변화에 선행하는 조직문화
  - 위기대응능력이 향상된 조직경영
• 이해관계자
  - 제품 및 서비스 품질의 일치
  - 고객의 신뢰 및 만족 향상
  - 조직에 대한 신뢰 보증.

2.2 ISO 9001:2015에 언급된 리스크 기반 사고

본 절에서는 리스크가 직접적으로 명시된 2015년 규격의 각 절을 구체적으로 살펴본다. 가장 먼저 리스크가 나타나는 곳은 ISO 9001:2015 각 절에 대한 설명이 시작되기 전 단계인 Introduction의 0.3 Process approach의 0.3.3 Risk-Based thinking 제목으로 명문화되어 있고 "조직은 위기와 기회를 다루기 위한 조치를 계획하고 도입해야 한다"라고 설명이 되어 있다.

다음으로는 4절부터 10절까지 리스크에 대하여 언급되고 있는데 각 절에서 나타나는 리스크에 대한 설명을 기술하면 다음과 같다 :

4. Context of the organization(4절 조직상황)에서 조직은 QMS 운용에 요구되는 프로세스를 결정하고 리스크 및 기회를 다루어야 한다.

5. Leadership(5절 리더십)에서는 최고 경영자는 RBT의 식을 촉진하고 제품 및 서비스의 적합성에 영향을 미칠 수 있는 리스크 및 기회 그리고 고객만족을 증진시키는 능력을 결정하고 다루어야 한다.

6. Planning(6절 기획)에서는 조직은 QMS를 기획할 때, 조직상황(4절)을 고려하여야 하며,
   1) QMS가 의도된 결과를 달성할 수 있음을 보증,
   2) 바람직한 영향의 증진,
   3) 바람직하지 않은 영향의 예방 또는 감소,
   4) 개선달성을 처리하는데 필요한 리스크 및 기회를 결정하여야 한다.

   또한 조직은
   1) 리스크 및 기회를 다루기 위한 조직,
   2) QMS의 프로세스에 조치를 통합하고 실행 및 이러한 조치의 효과성을 평가하는 방법을 기획하여야 한다.

7. Support(7절 지원)에서는 조직은 필요한 자원을 결정하고 제공하여야 한다. 이 절에서는 리스크가 명시적으로 언급되어 있지 않는데 절의 설명 가운데 '적절히(suitable or appropriate)'라는 표현이 있을 때는 리스크가 암시적(implicit)으로 표현된 것을 의미한다.

8. Operation(8절 운영)에서는 조직은 6절 기획에서 결정된 리스크 및 기회를 프로세스의 실행에 적용하여야 한다.

9. Performance evaluation(9절 성과평가)에서는 조직은 리스크 및 기회를 다루기 위하여 취해진 조치의 효과성을 모니터링, 측정, 분석 및 평가하여야 한다.

10. Improvement(10절 개선)에서는 조직은 바람직하지 않은 영향을 시정, 예방 또는 감소하여야 하고 QMS를 개선하며 필요한 경우 리스크 및 기회를 계속적으로 갱신하여야 한다.

<Table 1> The Places where Risk is Addressed in ISO 9001:2015 and Remarks

ISO 9001:2015	Remarks
Introduction	• The concept of RBT is explained
4. Context of the organization 4.4 QMS and its processes	• **Risks** and opportunities, and plans to implement the appropriate actions to address them? → To determine its QMS processes and to address its risks and opportunities
5. Leadership 5.1.2 Customer focus	• **Risks** and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed? → To promote awareness of RBT and to determine and address risks and opportunities that can affect product/service conformity
6. Planning for QMS 6.1 Actions to address **risks** and opportunities	6.1.1 When planning for the QMS does your company consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the **risks** and opportunities that need to be addressed? 6.1.2 Do you take actions to address **risks** and opportunities that are proportionate to the potential impact on the conformity of products and services? → To identity risks and opportunities related to QMS performance and take appropriate actions to address them
7. Support	• To determine and provide necessary resources(**risk** is implicit whenever 'suitable' or 'appropriate' is mentioned)
8. Operation 8.1 Operational planning and control	• Does your company plan, implement, and control the processes to meet requirements for the provision of products and services and to implement the action to address **risks** and opportunities by : → To manage its operational processes
9. Performance evaluation 9.1.3 Analysis and evaluation 9.3 Management review	• Effectiveness of action taken to address **risks** and opportunities? • Does the management review include the review of the effectiveness of actions taken to address **risks** and opportunities? → To monitor, measure, analyze and evaluate effectiveness of actions taken to address the risks and opportunities
10. Improvement 10.2 Nonconformity and corrective action	• Update **risks** and opportunities identified during the planning? → To correct, prevent or reduce undesired effects and improve the QMS and update risks and opportunities

*__risks__ referred to in ISO 9001:2015 are boldfaced.

위에서 언급한 리스크의 설명에 이어 ISO 9001:2015의 요구사항에서 "리스크(risk)"라는 용어가 직접 명시된 곳을 모두 열거하면 <Table 1>과 같고 표 안에 진한 글씨로 **risk**를 나타냈다.

2.3 리스크 기반 사고의 6단계

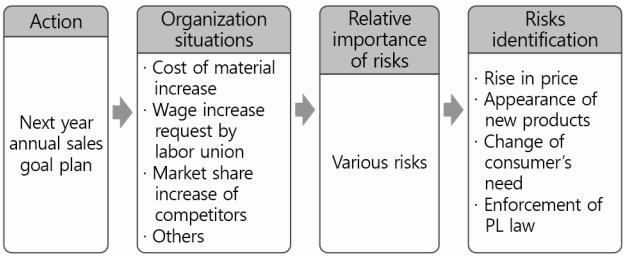
ISO 9001:2015 규격은 조직에게 공식적인 리스크 관리를 요구하지는 않는다. 그러나 ISO 31000:2009와 ISO 31010:2010 규격을 활용하면 리스크 사고를 기반으로 한 QMS 및 프로세스를 훨씬 더 체계적으로 구축할 수 있다 [10, 11]. 리스크 기반 사고는 일반적으로 다음의 IUPICL 6단계로 구분할 수 있다 :

- 리스크 식별(Identify)
- 리스크 이해(Understand)
- 리스크 처리 계획(Plan)
- 계획의 실행(Implement)
- 효과성의 확인(Check)
- 학습 및 개선(Learn)

위의 6단계에 따른 리스크 기반 사고를 예를 들어 설명한다.

2.3.1 조직상황에 따른 리스크의 식별

식별 단계에서는 리스크는 조직에서 발생하는 상황에 따라 각각 다르게 다룰 수 있다. 앞의 예와 같이 신년 매출 목표 수립에 대한 리스크는 상황에 따라 다르게 나타나지만 예견할 수 있는 리스크를 <Figure 3>과 같이 정리할 수 있다 :

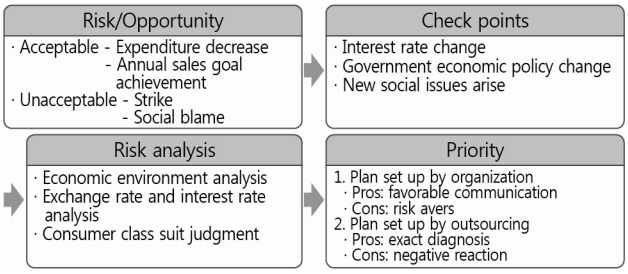


<Figure 3> Risk Identification

2.3.2 리스크의 이해 : 리스크 및 기회 간 균형, 리스크 분석 및 우선순위 설정

이해 단계에서는 리스크를 용인여부(acceptable or unacceptable)로 분류하고 장단점(advantage, disadvantage)을 비교하여 이해한 다음, 목표를 정하고 우선순위를 부여한다. 예를 들면 <Figure 4>와 같다 :

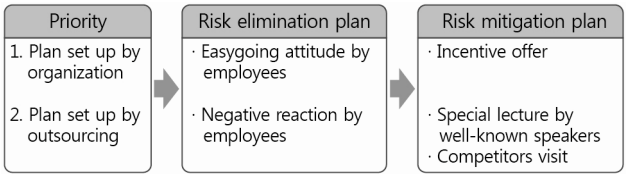
- 목표 : 국내외 경제 환경 및 유동성과 리스크를 고려한 신년 매출 목표를 수립한다.



<Figure 4> Risk Understanding

2.3.3 리스크 처리 계획

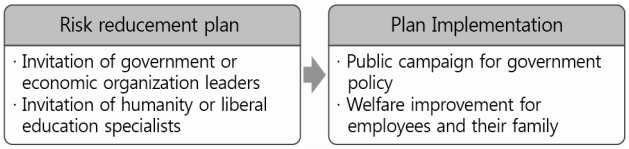
처리 계획 단계에서는 어떻게 리스크를 피하거나 제거할 것인가? 또는 어떻게 리스크를 완화할 것인가? 등의 계획을 수립한다. 예는 <Figure 5>와 같다 :



<Figure 5> Risk Planning

2.3.4 계획의 실행

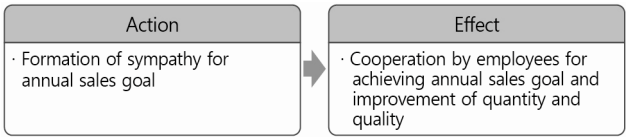
실행 단계에서는 리스크를 처리하기 위하여 수립된 계획에 따라 실행한다. 예는 <Figure 6>과 같다 :



<Figure 6> Risk Implementation

2.3.5 효과성의 확인

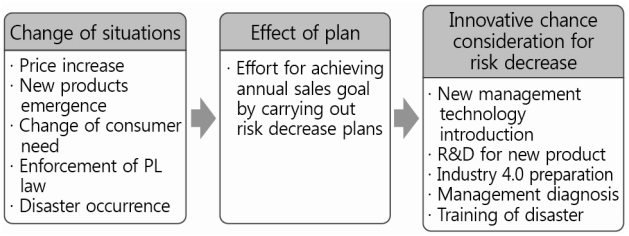
확인 단계에서는 리스크를 처리한 조치에 대하여 효과의 유무를 확인한다. 예를 들면 <Figure 7>과 같다:



<Figure 7> Effect Checking

2.3.6 학습 및 개선

마지막 단계에서는 예상치 못한 다른 경제 사회적 환경 변화에 따라 리스크 처리를 위한 계획을 수립하여 지속적으로 혁신적인 기회를 고려한다. 예를 들면 <Figure 8>과 같다 :



<Figure 8> Learning and improvement

• 개선 : 상황변화에 따라 달성하지 못할 가능성이 증가됨에 따라 목표달성이 가능한 혁신적인 기회를 고려한다.

3. 리스크의 관리

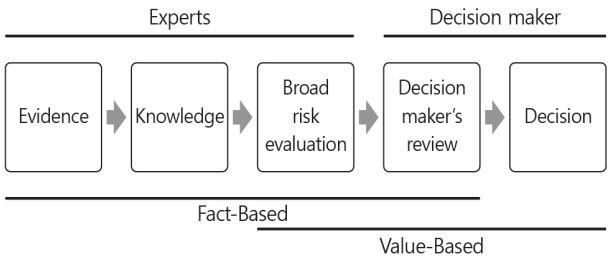
3.1 리스크 평가와 의사결정과학

리스크 평가와 관리는 1970년대 및 1980년대 이후 등장하여 활발히 연구되고 있고 다양한 연구 분야에서 리스크 분석의 접근 방법이 적용되고 있다. 대표적인 전문가 그룹으로서는 “Society for Risk Analysis”가 있다[20]. 리스크의 중요한 연구 분야는 크게 다음 두 가지로 분류된다 :

• 특정 활동의 리스크 평가와 리스크 관리 연구
• 리스크의 이해, 평가, 특성화, 의사소통 및 관리를 위한 개념, 이론, 프레임워크, 접근법 및 모형과 관련된 포괄적인 리스크의 연구.

Aven[5, 6]에서 위의 두 번째 포괄적인 리스크의 연구는 첫 번째 연구인 특정 활동의 리스크 평가 및 관리에 사용되는 도구들을 포함하고 있음을 강조하였다.

Hansson and Aven[9]은 <Figure 9>의 사실과 가치 간의 연관성 모형을 통하여 리스크의 평가와 의사결정의 관계를 설명하였다. 먼저, 어떤 현상에 관하여 실험 및 분석으로 수집된 데이터와 정보는 증거로 활용된다. 관련 전문가 및 과학자는 증거를 연구와 분석과정을 통하여 지식으로 축적한다. 다음으로 증거와 지식을 활용한 심도 있는 연구를 거쳐서 리스크 평가 단계에 도달한다. 의사결정자는 리스크와 불확실성에 관한 가치를 고려하고 여러 가지 다른 주제의 정보를 종합하여 최종 검토와 결정 단계에 이른다. 위의 단계적 절차를 따라서 리스크에 대한 사실과 가치에 근거를 둔 최종적인 의사결정을 할 수 있다.



<Figure 9> A Model for Linking the Various Stages in the Risk Informed Decision Making

3.2 리스크의 정의와 척도화

SRA[18, 20]에서 발간한 전문용어집에는 다양한 기본

개념과 함께 전문용어의 질적 정의와 양적 측정을 분리하여 수록하고 있다. 그 책자에는 리스크 개념에 초점을 맞추어 확률, 취약성(vulnerability), 강건성(robustness) 및 탄력성(resilience) 등의 용어로서 해설하고 있다. 또한 SRA에서는 인간 가치의 관점에서 자연 현상을 포함한 시스템 운영 결과와 관련된 리스크를 정의하였다. 예를 들어 리스크의 질적 정의를 사건 및 결과에 불확실성의 차원을 추가하여 다음의 일곱 가지로 표현하였다 :

- 불행 발생 가능성
- 원하지 않는 부정적 사건 결과의 실현 잠재성
- 불확실한 상황에 노출되어 손실 발생
- 활동의 결과와 관련된 불확실성
- 인간 가치의 관점에서 활동의 결과에 대한 불확실성과 심각성
- 활동의 특정한 결과의 발생과 관련된 불확실성
- 기준 가치로부터의 편차와 관련된 불확실성.

국제표준화기구에서 발행한 리스크 관리에 관한 규격인 ISO 31000:2009 Risk Management-Principles and Guidelines에서는 리스크를 "목표에 대한 불확실성의 영향"으로 정의하고 있는데 이것은 위의 네 번째와 다섯 번째 정의의 좁은 의미로 볼 수 있다.

Aven[3, 6]는 리스크의 크기를 판단하기 위하여 리스크를 측정하고 기술하기 위한 척도로서 다음의 두 가지 예를 제시하였다 :

- 리스크 기술의 3차원 척도(s_i, p_i, c_i)
  여기서 s_i : i번째 시나리오,
  p_i : i번째 발생가능 확률,
  c_i : i번째 결과
- 리스크 기술의 3차원 척도(C, Q, K)
  여기서 C : 특정한 결과,
  Q : C와 관련된 불확실성의 척도(확률),
  K : 지식의 강도를 포함하는 C와 Q의 배경 지식.

Aven[6]은 리스크 정의를 다양하게 범주화하고 기술하여 분석하였다. 대부분의 경우에 분석 방식이 의사결정자를 잘못 판단하게 할 수 있으므로 기대 손실을 포함한 의사결정 방법과 불확실성을 충분히 반영한 순수 확률을 기반으로 한 의사결정을 제안하고 있다.

3.3 리스크 평가에서 불확실성의 연구

불확실성의 변동 속에 내재된 우연 또는 불확실성에 대한 지식의 부족으로 인하여 리스크 분석에는 확률적 분석이 가장 많이 사용된다. Flage et al.[7]은 리스크를 평가할 때 불확실성을 표현하는 기술과 방향에 관한 연구를 하였다. 여러 가지 확률적 접근 방법 가운데 불확실성을 해결하는 방법으로 베이지안 방법이 가장 보편적으로 사용되고 구간 확률, 가능성 척도 및 질적 방법 등 다양한 대안이 연구되고 있다[1, 2, 4, 15]. Lindley[15]는 임의의 리스크 A의 발생의 불확실성에 평가자의 주관적인 확률을 부여하여 불확실성을 평가하는 직접 비교법을 사용하였다. 예를 들면 통계학 교재에 나타나듯이 $P(A) = 0.3$로 표현하였다. 이와 같이 불확실성에 대한 평가로서 전문가들은 주관적인 확률 또는 구간 확률을 활용하여 리스크를 평가한다.

한편, SRA[18]에서는 오늘날 불확실성에 대하여 비확률적 표현이 많이 사용되고 있다는 점을 지적하였다. 신뢰성 있는 확률을 쉽게 결정할 수 없을 때 또는 불확실성이 지나치게 큰 상황에서는 확률외의 다른 방법을 시도한다. Avan and Nokland[1]는 불확실성 척도의 논리적 근거로서 전통적인 중요도 척도와 개선 잠재성 및 Birmbaum 척도를 비교하는 새로운 형태 방법을 소개하였다. Aven and Zio[2]는 리스크를 나타내는 모형에서 불확실성을 오류에 관한 불확실성으로 정의하고 함수의 형태로 $g(x)-y$로 표현하였다. 여기서 $g(x)$는 파라미터 x를 갖는 y의 모형, y는 평가하는 양을 의미한다. 이와 같이 불확실성을 평가하기 위한 다양한 연구를 진행하였다.

3.4 리스크 관리 전략과 프로세스

리스크 관리는 크게 두 범주인 리스크 관리 전략과 리스크 관리 프로세스로 분류한다[18, 20]. 리스크를 관리하기 위한 전략으로서 다음의 세 가지 전략을 주로 사용하고 대부분의 경우 세 가지 전략을 혼합하여 사용한다 :

- 리스크 정보 활용(risk-informed) 전략
  리스크 평가를 통해 리스크를 회피, 감소, 전달 및 보유하여 리스크를 취급하는 전략
- 경계/예방(cautionary/precaution) 전략
  대체품 개발, 안전 요인, 안전장치의 중복설계, 수단의 다양화 등의 대안을 갖는 시스템 설계와 비상 경영 등 적응을 위한 전략
- 광범위한(discursive) 전략
  불확실성 및 모호성의 감소, 사실의 명확화, 영향을 받는 사람들의 참여 등을 통해 신뢰를 구축하는 전략.

리스크 관리 프로세스는 대부분의 리스크 분석 교재나 ISO 31000:2009에서 확인할 수 있는데 일반적으로 다음의 6단계로 구분한다 :

- 리스크 관리 활동 목적의 정의와 목표기준의 특정화
- 고려한 활동 및 정의한 목적에 영향을 주는 상황과 사

건의 식별-체크리스트, HAZOP(hazard and operability), FMEA(failure mode and effects analysis) 등의 방법 활용
- 사건의 원인과 결과의 분석-FTA(fault tree analysis), ETA(event tree analysis), 베이지안 네트워크의 사용
- 사건과 결과의 가능성 판단과 리스크의 기술
- 리스크 중요도 판단을 위한 리스크의 평가
- 리스크의 취급

3.5 리스크 분석

리스크 분석의 일반적인 방법을 고려한다면 의사결정 분석의 도구인 C/B 분석, 비용과 효과성 분석, 다변량 분석 등을 사용하여 리스크의 정보를 생성할 수 있다. 이 방법들은 의사결정 대안의 장단점을 조직화하는 시스템 접근방법이지만, 명시적으로 비교문제에 어떤 요인들의 포함여부에 따라 다르게 나타날 수 있다. 그리고 리스크 분석 결과, 분석에서 누락된 문제들을 추가적으로 경영검토와 판단하는 것이 필요하다.

신뢰성 공학의 교재[16, 17]나 ISO 31010:2009를 활용하여 보다 과학적인 리스크 분석과 평가를 할 수 있다. 외국의 연구자들이 제안한 분석 방법으로서 Gilboa and Marinacci[8]는 의사 분석 접근법으로 리스크를 분석하였는데 베이지안 기반의 불확실성하에서 의사결정에 대한 기대효용을 고려하였다. Klinke and Renn[14]은 리스크 형태와 관리 전략을 제시하면서 지연 효과, 피해의 분산, 리스크 이동의 잠재성 등을 고려한 불확실성과 피해의 측면에서 설명하였다. 각 리스크의 형태에 대하여 리스크 관리 전략과 리스크를 관리하기 위하여 전술한 세 가지 주요 전략을 통합하였다.

4. 리스크 관리의 실행

4.1 리스크 관리를 위한 준비

리스크 관리 전략은 각각의 조직의 상황에 적합하게 작성되고 효과적으로 리스크 관리를 실행하기 위하여 지속적으로 반복하여 보완하고 수정되어야 한다. 체계적인 리스크 관리의 국제적 규격인 ISO 31000:2009는 리스크 관리의 프로세스가 조직의 지배구조, 전략 및 기획, 정책, 가치와 문화에 맞도록 프레임워크를 개발하고 실행하여 지속적으로 개선하도록 명시하고 있다.

리스크 관리를 조직에서 효율적으로 실행하기 위한 다양한 양식이 있지만, <Figure 10>에 리스크 관리에 지침이 될 만한 영국의 글로벌 인증기관인 APMG International에서 사용하는 리스크 관리 전략 양식을 제시한다. 주요 항목을 설명하면 다음과 같다 :

4.1.1 목적(Purpose)

리스크 관리 기법 및 규격과 효과적인 리스크 관리 절차를 얻기 위한 책임을 기술한다.

4.1.2 주의사항(Advice)

다음의 기준에 맞도록 프로젝트 개요, 업무 사례, 관리층의 리스크 관리 가이드에서 도출한 리스크 관리 전략을 명시한다 :

① 고객과 공급자가 이해할 수 있는 책임명시
② 이해가능한 리스크 관리 절차의 문서화
③ 명확한 척도, 기댓값, 접근성을 정의
④ 관리 수준을 위해 적절한 척도의 선택
⑤ 리스크 보고 요건의 정의.

4.1.3 개요(Introduction)

목적, 적용범위, 책임 및 권한을 명시한다.

① 목적
- 조직의 품질경영시스템의 계획된 결과에 영향을 미치는 불확실한 요인을 파악하여 리스크 영향을 최소화하고 기회로 활용하기 위함

② 적용범위
- 조직의 경영전략, 방침, 목표 및 품질경영시스템의 모든 분야에 적용

③ 책임 및 권한
- 최고경영자 : 리스크 파악 결과 도출된 대응방 안의 승인과 실행 책임
- 운영지원책임자 : 도출된 경영환경 이슈 및 이해관계자의 요구사항을 근거로 리스크 파악, 발생원인 및 영향분석, 수준평가와 대응방안의 수립, 실행 모니터링, 관리의 책임
- 각 부서책임자 : 리스크 파악 및 분석, 대응방안 실시의 책임.

Overview
Purpose
Contents
Advice
Introduction
(States the purpose, objectives and scope, and identifies who is responsible for the strategy)

Risk Management Procedure
The procedure should cover activities such as :
Identify
Assess
Plan
Implement
Communicate

Tools and Techniques	Records
Reporting	Timing of Risk Management Activities
Scales	Proximity
Risk Categories	Risk Response Categories
Early-warning Indicators	Risk Tolerance
Risk Budget	

<Figure 10> Example of a Risk Management Strategy Worksheet

4.2 맞춤형 리스크 관리 절차의 제안

조직에서 리스크 관리 절차를 전개하기 위해서는 리스크 관리 업무 절차를 기술하고 조직의 관리에서 발생하는 변동을 충분히 반영해야 한다. ISO 9001:2015 해설의 품질리스크경영과정의 개요에서는 일반적인 리스크 관리 절차를 다음과 같이 서술하고 있다:

- 리스크의 평가 : 리스크의 확인, 분석, 평가
- 리스크의 제어 : 리스크의 감소, 수용
- 품질 리스크 경영 과정의 결과
- 리스크의 검토

위의 개요에는 각 항목에 대한 일반적인 설명과 함께 각 조직에 맞는 관리 방안을 실현하도록 명시만 하고, 구체적인 절차는 제시되어 있지 않다. 현재까지 연구 문헌에도 구체적인 실현 방법은 찾아보기 어렵고 다음의 일반 사항만 나타난다 :

- 리스크와 기회의 분석과 우선순위 부여
- 리스크의 대처 행동과 계획
- 계획의 도입 또는 조치
- 대처 행동의 효과성 검토
- 경험으로부터 교훈과 지속적 개선.

따라서 본 절에서는 RBT 기반의 ISO9001:2015를 효과적으로 도입할 수 있도록 조직의 업무에 따른 구체적인 리스크들을 나열하고, 제 2.3절의 리스크 기반 사고 IUPICL 6단계를 근거로 다음과 같이 맞춤형의 실제적인 업무와 절차를 단계적으로 제안한다.

4.2.1 리스크의 식별(Identify)

리스크 식별 단계에서는 운영지원 책임자가 「조직상황 분석」 규정의 경영환경분석, 내・외부이슈 파악 절차로부터 도출 가능한 중요 이슈와 이해관계자의 요구 및 기대사항을 토대로 리스크를 파악해야 한다. 리스크 파악 대상은 조직의 업무 프로세스에서 수립 목표에 미달되거나 고객 불만족, 효율성의 저하, 자산/이익 측면의 손실 발생, 직원 안전 보건 또는 사기저하 등을 유발할 수 있는 모든 불완전한 활동이 포함된다. 각 업무 별로 발생할 수 있는 중요 리스크의 구체적인 예를 <Table 2>에 제시하였다.

조직의 경영활동 중에 사업목표 달성 및 제품 및 서비스, 프로세스 등 품질경영시스템에 중대한 영향을 미치는 변경사항 등이 발생할 경우에는 운영지원 책임자는 관련 업무의 책임자와 함께 리스크를 파악하여야 한다. 운영지원 책임자는 파악된 리스크에 대하여 각 업무별 리스크 내용에 따라 발생 원인과 영향을 구분하여 정리하여야 한다.

<Table 2> Examples of Key Risk List in Business Sectors

Task	Main risks examples
Management/ Planning	Strategy error and failure(future forecasting, Overseas expansion, M&A, Investment), Environment analysis failure(Competitor, New technology, New products, New customer)
Human Resource	Labor union, Strike, Corruption, Embezzlement, Sexual harrassment, Overseas business trip accident, Core manager accident
Capital/ Accounting	Raw material price sudden rise, Oil price sudden rise, Interest rate rise, Tax investigation, Foreign exchange fluctuation, Finance, Credit, Liquidity, Money flow
Business	Delivery price down(excessive competition, customer request), Customer secession, Revocation of contract, Contract mistake(product cost error), Customer key complaint
Design / Development	New technology/product development and design error, PL/PS measure failure, Technology drain, Design and development capability down, Intellectual property lawsuit
Purchase	Subcontractor discontinue supply, Bankruptcy, Closure, Labor dispute, Quality defect of materials and parts, Order mistake, Transport strike
Production	Production suspension, Facility failure, Damage during delivery, Electricity/Gas discontinue, Water pollution, Building collapse, Ground subsidence
Quality	Customer's key claim, Quality accident, PL lawsuit, Inspection device damage, Inspection inaccuracy, Judgment failure
Safety/ Environment/ Health	Lae enforcement, Spill of toxic chemicals, Worker poisoning from toxic material, Worker death, Civil complaint
IT/Security	Personal information spill, Server system down, DDoS, Virus infection, Internet disorder, Secret spill
Disaster	Fire, Explosion, Natural disaster(typhoon, earthquake, heavy snow, landslide), Infrastructure damage, Infectious disease
Law Observance	Terror or kidnap of workers, Closure of overseas factory(political anxiety, riot, civil war), Violence of laws(tax evasion, unfair trade, secret fund), Image down(mass com, SNS)
New Technology	Industry 4.0, AI, Big Data, IoT, Robotics, Drone, Autonomous vehicle, 3D printing, Nano new materials, VR, Bio new medicine

4.2.2 리스크의 평가(Assess)

리스크 평가 단계에서는 발생되는 리스크에 대하여 리스크의 발생원인 및 영향을 분석하고 리스크의 수준을 평가한다.

① 리스크 발생원인 및 영향분석

운영지원 책임자와 각 부서 책임자는 리스크 항목별로 리스크가 발생하거나 전개되는 과정(mechanism)을 파악한다. 또는 발생 원인을 규명하기 위해서 5W1H, 계통도 등의 방식을 이용하여 발생 과정과 원인의 연계성을 쉽게 파악할 수 있도록 한다. 리스크에 따른 영향과 결과에 다음을 포함하고 발생원인 및 영향에 대한 내용을 "위험"과 "기회"로 분류하여 「리스크 관리대장」에 등록한다 :

- 고객에게 미치는 영향
- 회사의 손익, 수익성에 미치는 영향
- 내외부 이해관계자에게 미치는 영향
- 제품 품질 및 납기에 미치는 영향
- 회사 이미지, 평판에 미치는 영향

② 리스크 수준의 평가

운영지원 책임자와 해당 부서의 책임자는 리스크의 영향과 발생 빈도에 대한 원활한 의사소통과 합리적 수준 평가로서 보편적으로 활용되는 비즈니스 리스크 행렬인 <Table 3>과 같은 리스크 심각성의 점수기준에 따라 수준 등급을 정하고 점수를 부여한다.

또한 운영지원 책임자와 각 부서 책임자는 리스크의 원인에 대하여 발생 가능성을 추정하고 <Table 4>의 리스크 빈도의 점수화 기준에 따라 점수화 한 다음, 리스크 수준 평가결과는 「리스크 관리대장」에 기록한다.

운영지원 책임자와 각 부서 책임자는 리스크 심각성과 발생가능성 등급을 기준으로 <Table 5>를 이용하여 리스크 등급을 결정한다. 등급 평가 결과 H 또는 S등급이거나 심각성 또는 발생 가능성 중 하나가 5등급인 경우 중점 관리 대상으로 분류하고 대응 방안을 수립하여 관리한다. 리스크 분석 결과는 「위험 관리대장」에 기록한다.

4.2.3 위험 대응방안의 수립(Plan)

위험 대응방안의 수립단계에서는 운영지원 책임자와 각 부서 책임자가 관리대상으로 등록된 리스크에 대하여 <Table 6>에 따라 대응방안을 수립한다. 운영지원 책임자와 각 부서 책임자는 위험에 대한 대응방안이 "통제"이거나 기회로서 대응이 필요한 경우, 구체적인 대응방안을 수립하고 사업계획에 반영한다. 대응방안 수립 시에는 적절한 기한 내에 완성되도록 하고 달성 가능한 방안으로서 목표달성 여부의 측정 가능한 것이 되도록 한다. 위험 대응방안 수립 결과는 「위험 관리대장」에 기록한다.

<Table 3> Classes of Risk Severity

Step	Intensity (Level)	Human loss	Liability of compensation	Recognition loss
1	Trivial (Very Low)	None	No	No
2	Slight(Low)	Minor wound (1)	No	No
3	Normal (Moderate)	Minor wound (more than 1)	Materials of explanation	Few persons concerned
4	Important (High)	Serious wound	Arbitration /lawsuit	Nearby area
5	Fatal (Catastrophic)	Death	Lawsuit	Nationwide influence

<Table 4> Classes of Risk Occurrence Likelihood

Step	Likelihood	Time (Occurrence period)	Frequency (Occurrence/ 1,000)	Reference
1	Remote	Over 3 years	Less than 0.1	Exceptional
2	Low	Within 3 years	Over 0.1	Sometime
3	Moderate	Within 1 year	Over 1	Possible
4	High	Within 3 months	Over 10	Most of time
5	Very High	Within 1 month	Over 50	Definitely

<Table 5> Risk Level Determination

Severity / Possibility	1 Trivial (Very Low)	2 Slight (Low)	3 Normal (Moderate)	4 Important (High)	5 Fatal (Catastro-phic)
1(Very low)	L	L	M	H	H
2(Low)	L	L	M	H	S
3(Moderate)	L	M	H	S	S
4(High)	M	H	H	S	S
5(Very high)	H	H	S	S	S

The letters in table, L, M, H, and S, respectively, represent Low, Moderate, High, and Significant. Severity and possibility in table are come, respectively, from the results of <Table 3> and <Table 4>.

<Table 6> Counter Plans to Risk

Counter-plan	Time of application	Method of application
Retention	• Low possibility of risk occurrence, low loss. (management cost > loss cost)	• Ignore risk and perform task
Transfer	• Low possibility of risk occurrence, high loss.	• Buy insurance and transfer risk to the third person
Reduction	• High possibility of risk occurrence, low loss. (management cost < loss cost)	• Reduce risk through PDCA cycle • Warning if necessary
Avoidance	• High possibility of risk occurrence, high loss, excess cost	• Risk versus profitability analysis and abandon the product/process or other planning

4.2.4 위험 대응방안의 실행(Implement)

위험 대응방안의 실행단계에서 운영지원 책임자와 각 부서 책임자는 다음을 포함하는 위험 대응방안을 실행한다.

① 관련 프로세스/시스템 개정 또는 개선
② 관련 물적 자원 확보 또는 변경
③ 관련 인원 훈련 및 이해 여부 확인
④ 대응방안 실행

운영지원 책임자와 각 부서 책임자는 대응방안의 실행과정 및 완료 여부를 모니터링하고 실행 결과를 최고경영자에게 보고한다.

4.2.5 유지 및 관리(Communicate)

유지 및 관리단계에서 운영지원 책임자와 각 부서 책임자는 대응방안 실행 이후 잔여 위험의 존재 여부와 수준을 파악하고 그 수준을 평가한다. 잔여 위험이 감내할 수준이 아닌 경우 리스크 분석 및 대응방안 수립 후, 다시 실행한다. 운영지원 책임자와 각 부서 책임자는 위험 항목별로 사후 관리 필요 여부를 판단한다. 사후관리가 필요한 경우 "위험 모니터링 포인트"를 수립하고 「위험 관리대장」에 등록하며, 다음의 점검 및 조치를 한다.

① 실무담당자 : 수시 점검, 보고 및 조치
② 부서책임자 : 최소 년 1회 정기점검 및 조치
③ 내부 심사원 : 심사항목과 함께 관리상태 점검

운영지원 책임자와 각 부서 책임자는 매년, 수시로 「위험 관리대장」의 위험 처리 상태를 확인하여 예측하지 못한 중대 사고의 발생을 최소화 되도록 하여야 한다. 리스크 처리 이후 잔여 위험의 수준이 감내할 수준인지 결정하여 감내할 수준이 아니면 감내할 만한 위험이 남을 때까지 신규위험 처리방안을 수립하여 관리하고, 처리의 효과를 확인하고 그 효과를 기초로 한 실행관리 사항을 해당 프로세스에 기입하여 지속적으로 개선한다.

4.2.6 기록(Records)

기록단계에서는 현재까지 발생한 리스크를 등록하고 기록한다. 관련된 모든 기록은 「품질기록관리」 규정에 의거하여 기록하고 유지한다.

지금까지 설명한 맞춤형 리스크 관리의 모든 전개 과정을 책임 및 권한, 설명과 함께 <Figure 11>에 리스크 관리 업무 흐름도를 요약하였다.

Responsibility and authority	Task flow	Remarks
• Department head : operating support manager	Identify risk	• when business plan starts
• Department head : operating support manager	↓ Analysis of risk cause	• when business plan changes
• Department head : operating support manager	↓ Assess risk level	• Severity, occurrence, and risk judgement
• Department head : operating support manager	↓ Plan countermeasure	• Level H or S or possibility level S
• Operating support manager : CEO	↓ Implement	• Residual risk
• Department head : operating support manager	↓ Communicate	• after implementation and follow-up management
• Internal auditor	↓ Records	• Periodical internal audit

<Figure 11> Flowchart of the Risk Management Implementation

5. 결 론

ISO 9001 품질경영시스템의 요구사항은 2015년에 개정되어 현재 많은 조직들이 전환 인증심사를 추진하고 있다. ISO 9001:2015 개정 규격의 주요변화 가운데 가장 큰 특징은 "리스크 기반 사고(RBT: risk-based thinking)"에 근거하며 모든 ISO 표준들을 상위구조(HLS : high level structure)로 병렬화 한 것이다. RBT는 품질경영시스템의 구성 요소들을 "예방조치(prevention)"의 대상으로 고려하지 않고 "리스크(risk)"의 개념으로 고려하여 PDCA 사이클 속에 내재하는 품질경영시스템의 요소들을 시스템적으로 선행적으로 관리한다는 의미이다.

ISO 9001:2015 개정 규격의 품질경영시스템을 도입하려는 조직들은 RBT에 근거를 둔 시스템을 갖추어야 한다. 본 논문에서는 개정 규격에서 리스크 단어가 나타나는 각 절을 구체적으로 제시하고 의미를 살펴보았다. RBT는 바람직하지 않은 결과를 예방하는 것이 아니라 QMS의 설계와 운용을 통해 처음부터 끝까지 통합적으로 리스크를 식별하고 관리하는 것이다. RBT의 기본적인 개념을 이해하기 위하여 신년 매출 목표를 수립하는 예를 들어 (1) 리스크 식별 → (2) 리스크 이해 → (3) 리스크 처리 계획 → (4) 계획의 실행 → (5) 효과성의 확인 → (6) 학습 및 개선의 리스크 기반 사고의 IUPICL 6단계에 맞추어 설명하였다.

리스크의 주요 주제인 리스크 평가와 의사결정과학, 리스크의 정의와 척도화, 리스크 평가에서 불확실성의 연구, 리스크 관리 전략과 프로세스, 리스크 분석에 관하여 간략하게 언급하였다. 참고로 영국의 글로벌 인증기관인 APMG-International에서 사용하는 리스크 관리 전략의 양식을 제시하였다. 마지막으로 RBT에 기반한 ISO 9001:2015 규격을 도입하려는 조직의 품질경영 실무자들이 실제로 활용 가능 하도록 발생 가능한 주요 리스크를 <Table 2>에 구체적으로 열거하고 <Table 3>~<Table 6>에 리스크 수준의 결정과 대처 방안 등 맞춤형 리스크 관리 전개 방법을 제안하였다.

본 논문은 품질경영 연구자와 실무자들에게 RBT의 개념을 확립시키고 리스크 관리를 적용할 수 있도록 ISO 9001:2015 규격의 (전환) 인증 사업에 직접적인 도움을 줄 것으로 기대한다. 향후연구를 위해서는 현장에서의 조직상황에 맞는 리스크 관리에 대한 실태 조사 및 분석이 이루어져야 할 것이다. 또한 개별 실행에서 리스크 평가 기법 및 도구들의 활용과 개발도 관심 있는 연구 주제가 될 것으로 기대한다.

References

[1] Aven, T. and Nokland, T.E., On the Use of Uncertainty Importance Measure in Reliability and Risk Analysis, *European Journal of Operational Research*, 2010, Vol. 95, pp. 127-133.

[2] Aven, T. and Zio, E., Model Output Uncertainty in Risk Assessment, *International Journal of Performability Engineering*, 2013, Vol. 9, No. 5, pp. 475-486.

[3] Aven, T., On the Allegations that Small Risks are Treated out of Proportion to the Importance, *European Journal of Operational Research*, 2015, Vol. 140, pp. 116-121.

[4] Aven, T., On the Need for Restricting the Probabilistic Analysis in Risk Assessments to Variability, *Risk Analysis*, 2010, Vol. 30 No. 3, pp. 354-360.

[5] Aven, T., Risk Assessment and Risk : Review of Recent Advances on their Foundation, *European Journal of Operational Research*, 2016, Vol. 253, pp. 1-13.

[6] Aven, T., The Risk Concept-Historical and Recent Development Trends, *European Journal of Operational Research*, 2012, Vol. 99, pp. 33-43.

[7] Flage, R., Aven, T., Baraldi, P., and Zio, E., Concerns, Challenges and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment, *Risk Analysis*, 2014, Vol. 34, No. 7, pp. 1196-1207.

[8] Gilboa, I. and Marinacci, M., *Ambiguity and Bayesian Paradigm, Advances in Economics and Econometrics : Theory and Application*, Cambridge University Press, 2013.

[9] Hansson, S.O. and Aven, T., Is Risk Analysis Scientific?, *Risk Analysis*, 2014, Vol. 34, No. 7, pp. 1173-1183.

[10] ISO 31000:2009 Risk Management-Principles and Guidelines, ISO, 2009.

[11] ISO 31010:2010 Risk Management-Risk Assessment Techniques, ISO, 2010.

[12] ISO 9001:2015 Quality Management Systems-Requirements, ISO, 2015.

[13] Kim, H.G., Kang, B.H., and Park, D.J., Counterplan of Manufacturers in Accordance with ISO 9001:2015 Revision Conversion, *Journal of Society of Korea Industrial and Systems Engineering*, 2016, Vol. 39, No. 3, pp. 71-82.

[14] Klinke, A. and Renn, O., A New Approach to Risk Evaluation and Management : Risk-Based, Precaution-Based, and Discourse-Based Strategies, *Risk Analysis*, 2002, Vol. 22, No. 6, pp. 1071-1094.

[15] Lindley, D.V., *Understanding Uncertainty*, Hoboken, NJ, Wiely, 2006.

[16] Rausand, M. and Hoyland, A., *System Reliability Theory : Models, Statistical Methods, and Application*, John Wiely & Sons, 2004.

[17] Seo, S.G., Kim, H.G., Kwon, H.M., Cha, M.S., and Yoon, W.Y., *Reliability Engineering*, 2nd Ed., Kyobomoongo, 2015.

[18] SRA, Glossary Society for Risk Analysis, www.sra.com/resources, 2015.

[19] www.iso.org/tc176/sc02/public

[20] www.sra.com.

ORCID

Ho Gyun Kim | https://orcid.org/0000-0002-7695-3348

Byung Hwan Kang | https://orcid.org/0000-0002-7423-0015

Dong Joon Park | https://orcid.org/0000-0003-0554-1378