위험관리체계의 기록관리표준 적용방안 연구

A Study on the Application of Records Management Standards to Risk Management Framework

정 기 애(Ki-Ae Jeong)*
이 정 훈(Jeong-Hoon Lee)**
남 영 준(Young-Joon Nam)***

목 차

〈초 록〉

업무환경의 변화와 불확실성의 증대로 인해 위험관리의 중요성이 날로 부각되는 상황에서 업무의 정당성 확보와 정보적 가치 제고를 위해 기록관리 측면의 위험관리 역시 매우 중요해지고 있다. 기존의 전통적인 기록관리의 위험성이 주로 보존기능에 집중되어 있었다면 IT기반에서는 업무와 기록의 연관성이 높아짐에 따라 기록의 생산, 유통, 활용 단계 즉 업무과정의 위험성이 기록관리의 위험성으로 직결되고 있다. 본 연구는 ISO 31000의 조직 전반의 위험관리 프레임웍을 토대로 기록관리의 위험관리 요소와 대응 전략을 제시하였다. 특히 기록관리 위험관리 프로세스를 ARMA에서 제시하는 업무영역과 NIST에서 제시한 시스템영역으로 구분하고, 각 영역의 프로세스별 점검요소는 ISO의 기록관리표준 중에서 업무과정에 대한 표준(ISO TR 26122)와 기록의 생산 맥락에 대한 표준(ISO 16175-3)에서 해당 요소를 추출하였다.

주제어: 기록관리체계의 위험관리, 기록관리의 위험관리요소, 기록관리표준

<ABSTRACT>

Owing to changing work environment and increasing uncertainty, risk management in records management area is becoming more important to secure work legitimacy and to increase the value of information for future. While risk factors in traditional records management were mainly focused on the preservation function, those in current records management were directly coupled with those of overall work processes which produce, distribute, and utilize records because information technologies make the relationship between works and records closer. This study proposes a set of risk management factors and strategies in records management based on the overall risk management framework of ISO 31000. Moreover, ARMA's works areas and NIST's systems areas were applied to form the risk management processes in records management, and ISO's records management standards were used to suggest the checklists for the processes in both areas, especially with ISO TR 26122 for work processes, and ISO 16175-3 for the context of records.

Keywords: risk management of RMS, risk factors of RM, records management standards

* 한국전력기술(주) 정보자료팀장(jka@kepco-enc.com) (제1저자)
** 전남대학교 경영전문대학원 교수(jhoon.lee@chonnam.ac.kr) (공동저자)
*** 중앙대학교 일반대학원 기록관리학과 교수(namyj@cau.ac.kr) (교신저자)
■ 접수일: 2011년 11월 20일 ■ 최초심사일: 2011년 11월 28일 ■ 게재확정일: 2011년 12월 23일

1. 서 론

1.1 연구의 필요성 및 목적

IT기술의 급속한 발전은 조직의 업무 프로세스와 영역의 급격한 변화를 유발하고 있으며, 시장과 고객의 요구 변화와 함께 조직 전체의 전략변화를 촉진하고 있다. 이러한 다각적인 변화는 그 방향과 파급효과를 예측하기가 매우 어려워 조직의 불확실성을 더욱 증대시키고, 이익의 기회보다는 큰 위험요소로 작용할 가능성이 크다. 오늘날 많은 조직이 위험관리체계(Risk Management System)를 도입하는 배경에는 이러한 불확실성의 증가라는 시대적 변화에 기초를 두고 있다.

기록관리 영역도 IT기술의 발전에 힘입어 아날로그 매체에서 디지털 기록으로 옮겨가면서 기존의 보존 중심의 아카이브 기능에서 기록의 라이프사이클에 기반을 둔 프로세스 관리 기능으로 전환되고 있다. 즉, 기존의 기록관리 업무는 업무 과정이 종료된 이후 보존을 위해 기록관으로 이관된 시점부터 시작되었지만, 디지털 기록으로 전환되면서 기록의 생산과 유통 단계인 업무 과정 전반에 대한 기록요건의 적절한 반영과 통제가 필요하게 되었다.

특히 디지털 기록의 형식과 내용이 다양화됨으로서 기록의 품질 유지와 장기 보존은 갈수록 복잡해지고 있으며, 시장과 기술 환경의 변화는 업무영역의 통합과 분리를 가져오고, 그에 따라 업무과정의 결과물인 기록의 평가, 분류체계, 메타데이터 설계, 보존 정책 등 기록관리 영역이 큰 영향을 받게 된다. 따라서 업무환경의 변화가 기록관리시스템에 즉시 반영되고 그 결과를 피드백할 수 있는 효과적인 대응 체계가 필요하다.

사실상 기존 기록관리 영역의 위험관리는 주로 보존단계에 영향을 미치는 이벤트적 위협요소 즉 재난관리 측면에 초점을 맞추어 다루어져 왔다. 그러나 디지털 기록관리 환경에서는 업무 과정의 위협 요소가 기록의 관리와 보존 전반에 영향을 미치게 된다. 이는 업무영역의 변화와 IT기술 발전에 기인한 업무환경의 불확실성과 위험이 기록관리 영역에까지 영향을 주기 때문이다. 따라서 기록관리의 위험이 기록이관 이후의 천재지변이나 인재(人災)에 의한 단발적 사건에 한정되지 않고, 기록의 생산과 유통 즉, 업무과정 전체 영역으로 확대되었다. 이는 기록관리의 위험관리가 조직 전반의 통합 위험관리 체계와 상호 연계 혹은 통합되어야 함을 의미한다.

확대된 기록관리의 위험관리 목적은 크게 두 가지 측면으로 나누어 고려할 수 있는데, 첫째는 조직의 정당성 확보 측면, 둘째는 지식자원의 축적 측면이다. 오늘날 글로벌 환경에서 기업간 또는 조직간 협업관계의 확대와 기업의 사회적 책임 요구의 증대는 조직의 윤리성과 투명성을 더욱 요구하고 있다. 상호 이해관계가 다른 조직간의 책임을 명확히 밝히기 위해서는 각 조직이 수행한 업무 결과물의 증거력에 기반한 정당성 확보가 매우 중요하다. 또한 선행 경험 축적을 통한 지식자원의 확보는 후속 업무의 불확실성을 최소화하는데 기여한다. 따라서 기록관리의 실패는 곧 해당 조직의 업무영역에 큰 위협요인이 되고, 업무 수행과정에 내포된 문제점이 기록의 관리와 보존에도 악영향을 주는 상호 불가분적 관계로 전환되면

서 보다 전문적이고 체계적인 기록관리의 위험관리정책이 필요하게 되었다.

그러나 기록관리 분야의 현실을 살펴보면, 기록관리 기능이 대부분 조직의 총무부서 산하 행정수발 기능에 위치하고 있기 때문에, 조직의 경영전략이나 위험관리체계에 대한 기록관리 요건의 적용이 어려운 상황이다. 특히 민간영역으로 갈수록 기록관리 기능은 더욱 유명무실하다. 이로 인해 대부분의 기업이나 공공기관에서 기록관리의 위험요소를 조직의 위험관리체계에 연계하여 관리하고 있지 않기 때문에 예측하지 못했던 위험이 발생했을 때 이에 대한 대응이 적절히 이루어지지 못해 조직이 전체적으로 위기에 처하는 경우도 있다.

따라서 조직의 위험요소에 대해 기록관리 측면에서의 대응 전략을 수립하여 기록관리의 조직 기여도를 증대하기 위한 전략이 필요하다. 이를 위해서는 우선 기록관리 영역의 위험관리 요소를 추출하고 조직 전반의 위험관리체계에 대한 기록관리 요건을 적용할 수 있는 구체적인 방법론이 요구된다. 본 연구는 위험관리표준인 ISO 31000에서 제시하는 위험관리 프레임웍과 프로세스를 토대로 기록관리표준에서 제시하고 있는 주요 요건을 대입함으로써 기록관리와 위험관리의 상호연계 방법론을 제시하고자 하였다.

1.2 연구방법 및 선행연구

앞에서 기술한 바와 같이 기록관리의 위험관리는 주로 기록의 아카이브 기능 측면에서 기록의 위해가 될 만한 사건 즉, 재난관리 측면에서 주로 연구가 이루어져 왔다. 사실 위험관리는 그동안 경영학이나 사업관리 영역에서 다루어져 왔고, 기록관리 영역에서는 업무과정과 연계한 위험관리 연구가 부진한 것이 사실이다. 최근에 IT 기술분야에서 디지털 기록의 위험관리가 어느 정도 이루어졌는데, 예를 들면 DRAMBORA (Digital Repository Audit Method Based on Risk Assessment)[1]와 NIST(National Institute of Standards and Technology)[2]에서 제시한 IT 정보자원의 위험관리지침이 있다. 하지만 주로 디지털 기록 관리 측면보다는 IT 중심의 관리요소에 주로 초점이 맞추어져 있다. 반면에 ARMA(American Records Management Association)[3]에서는 기록관리의 위험관리를 단발성 이벤트적 관리 측면과 기록관리 프로세스 관리 측면으로 구분하고 각각의 특성을 설명하고 구체적인 사례를 통해 기존에 없던 새로운 위험관리 방법론을 제시하고 있다.

먼저 DRAMBORA는 디지털 리포지터리에 대한 위험평가와 감사절차에 대한 내용을 담고 있다. DRAMBORA는 디지털 파일의 장기보

1) DRAMBORA는 DCC(Digital Curation Center)와 DPE(Digital Preservation Europe)가 '위험평가에 기초한 디지털 저장소 감사 방법'으로 공동 작성한 것이다. 기관이 디지털객체의 장기보존에 적합한 기관인지 여부를 스스로 감사하고 인증하는 도구로 개발된 것으로 우리나라 국가기록원, 영국 British Library 등의 기관에서 참조 활용하고 있다(임진희 2010).

2) NIST는 미국상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소로 1901년 설립되었고 산업현장에서 필요로 하는 각종 기술과 측정 분야에 국가 기준이 되는 표준을 선정하고 개발, 적용하는 연구소이다(http://www.nist.gov/index.html 〈2011.12.19〉).

3) 미국 기록관리의 법률 및 표준 제.개정과 교육, 기술개발 및 자료발간을 통해 기록관리의 발전을 도모하는 기록관리전문가협회로서 비영리단체이다(http://www.arma.org/about/overview/index.cfm 〈2011.12.19〉).

존에 대한 적합성을 평가하고 감사하는 도구로서 자체 감사를 위한 조직의 기능과 의무, 업무활동 및 주요 자산을 정의하도록 하며 6단계로 이루어져 있다. 첫 번째 단계는 업무맥락과 배경을 확인 하는 단계이고 두 번째 단계는 조직의 정책과 규정에 대한 프레임웍을 문서화한다. 세 번째 단계는 업무활동, 자산 및 그 소유권자를 확인하고, 4단계부터 본격적으로 위험요소를 설정하고 5단계는 각 위험요소에 대한 평가를 거쳐 마지막 6단계에서 평가 확인된 위험 평가 내용에 기반하여 위험관리 대응 전략을 수립하는 단계를 제시하고 있다(임진희 2011).

그리고 NIST에서 제시하는 정보관리시스템에 대한 위험관리 가이드가 있다. NIST에서는 IT정보관리시스템 측면에서의 위험관리의 특성과 역할을 제시하고 있으며 시스템 구축 단계(System Development Life Cycle 이하 SDLC)에 기반하여 위험관리 요소에 대한 평가를 5개의 단계, 즉 기획단계(Initiation), 프로그램 개발단계(Development or Acquisition), 실행단계(Implementation), 운영 및 유지보수 단계(Operation or Maintenance), 처분단계(Disposal)로 구분하여 각 단계별로 위험관리의 개념과 범위를 설정하고, 구체적인 위험관리 활동은 다시 9단계로 나누어 제시하고 있다(NIST, Special Publication 800-30).

ARMA에서는 기록관리 측면에서의 위험관리 방안을 제시하였다. ARMA는 기록관리영역의 위험관리를 업무과정에 대한 위험관리와 기록의 보존기능에 대한 위협 사건으로 구분하고, 다시 각 영역을 다시 9단계로 구분하여 위험관리에 대한 세부적인 전략을 제시하고 있다. 9단계를 소개하면 먼저 첫째 단계는 조직의 정책 및 전략을 수립하고, 둘째 단계에서 업무 프로세스에 대한 분석을 실시한다. 이를 토대로 셋째 단계에서는 기록과 정보자원의 유형과 요건에 따른 중요도를 설정하며, 넷째 단계는 규정이나 표준과의 차이점을 분석하고, 다섯째 단계에서 위험요소에 따른 영향과 파급효과를 분석한다. 또한 여섯째 단계는 각 위험요소별로 발생가능성과 영향의 정도에 따라 우선순위를 설정하고, 일곱째 단계는 품질 요건의 수준과 위험요소에 대한 분석을 실시하며, 여덟째 단계는 전체 통합관리 측면에서의 위험관리 목록을 제시하고, 마지막 아홉째 단계에서 분석결과에 따른 대응 전략을 수립하도록 하고 있다(Lemieux 2004).

기록관리표준에서 제시하고 있는 원칙과 기준들은 사실상 기록관리의 위험을 전제로 한다. 즉, 기록관리의 실패로 인한 위험 요소를 사전에 대비하여 업무의 실패 확률을 최소화 하고 궁극적으로 조직의 성과에 기여하는 것이다. 따라서 기록관리표준의 개념과 목적은 위험관리표준의 목적과 맥락을 같이한다. 본 연구는 위험관리 표준의 프레임웍과 기록관리의 표준에서 제시하고 있는 요건을 상호 대응, 연계함으로써 조직 전반의 위험관리 정책 수립과 시스템 구축에 필요한 요소를 추출하고, 위험관리 정책 및 프레임웍에 대한 기록관리 요건 적용의 구체적인 방법론과 전략을 제시하였다.

구체적으로 기록관리 정책 및 개념 측면에서는 ISO 15489의 요건을 적용하였고, 업무과정과 기록의 생산 맥락에 대한 위험관리 요소는 ISO 16175-3 및 ISO TR 26122의 요건을 토대로 연구를 진행하였다. 문제는 기존의 기록관리표준에서 제시하는 기준들은 기록관리의 실

무적 요건과 위험요소를 추출 하는데는 유용하나 조직의 정책과 경영의 차원에서 기록관리의 위험관리가 적용되도록 하는데는 미흡하다는 점이다. 기록관리가 조직 전반의 위험관리 정책에 쉽게 반영되도록 하는 도구는 기존의 기록관리표준의 요건으로는 불충분하다. 따라서 지난 11월 15일자로 공식 발행된 기록경영시스템(ISO 30301)의 개념 적용이 필수적으로 요구된다.

2. 이론적 배경

2.1 위험관리의 일반 이론

일반적으로 위험은 여러 가지 의미로 해석되고 사람과 조직의 상황에 따라 달리 정의된다. 경영학 이론에서는 위험은 불확실한 상황이나 사건으로 정의하고 불확실한 상황이 항상 손실이나 실패의 결과를 초래하는 것은 아니라고 설명한다. 불확실성은 때로 새로운 기회를 가져다 줄 수도 있기 때문이다. 하지만 일반적으로 위험은 부정적인 결과가 초래될 가능성이 있을 때에 사용하며, 때로는 예상과의 편차나 안전과 관련된 다른 현안을 의미할 때도 있다.[4)]

위험은 대부분의 경우 예측하기 어려운 시기에 매우 다양한 형태로 일어날 수 있으며, 이로 인해 최근에 각 기관이나 조직들은 각자의 목적과 환경에 적합한 위험관리 프로세스를 수립하여 시행하고 있다. 위험관리를 효율적으로 하기 위해서는 우선 위험에 대한 명확한 구분과 분류가 필요하다. 이를 위해 일반적으로 아래의 3가지 방식으로 위험을 구분한다(김선규 2010, 15-16). 첫째 유형분류는 경영 위험(Business Risk)과 투기적 위험(Speculative Risk), 순수위험(Pure Risk)과 보험가능 위험(Insurable Risk)으로 구분한다. 경영 위험과 투기적 위험은 재무적으로 이익과 손실의 가능성이 모두 포함된 유형으로 경제적, 정치적 상황에서 오는 위험이나 타 조직과의 계약관계 혹은 내부 운영상에서 발생할 수 있는 위험이다. 반면에 순수 위험 혹은 보험가능 위험은 재무적 이익의 가능성은 전혀 없고 위험 발생시 재무적 손실 가능성만 존재하는 것으로 자동차 사고, 화재, 도난, 자연재해 등의 사건으로부터 오는 위험이다. 둘째 유형분류는 위험에 대한 인지여부와 결과에 대한 추정의 정도를 통해 위험의 유형을 구분하며, 알려진 위험(Knowns), 모르는 위험(Known-Unknowns), 전혀 알 수 없는 위험(Unknowns)이 있다. 알려진 위험은 잠재된 위험을 인지할 수 있고 인지된 위험의 발생 가능성과 손실의 범위를 추정할 수 있는 위험을 말하며, 모르는 위험은 잠재된 위험을 인지할 수는 있으나 인지된 위험의 발생가능성과 손실의 범위 추정이 어려운 위험, 즉 지진, 태풍과 같은 자연재해로 인한 위험과 같은 것이다. 그리고 전혀 알 수 없는 위험은 위험의 인지 자체를 가늠할 수 없는 예측 불가능한 위험을 말한다. 셋째 유형분류는 위험의 발생 위치나 소스가 어디인가에 따라 구분하는 것으로 내부 위험(Internal Risk)과 외부 위험(External Risk)이 있다. 내부 위험은 사업이나 조직

4) KS A ISO/IEC Guide 73 : 2002 3.1.1항.

자체에 존재하는 위험으로 대부분 통제 가능한 범주로서 품질 위험, 관리 위험, 기술 위험, 안전 위험 등이 이에 속한다. 또한 외부 위험은 사업이나 조직의 외부에 존재하는 위험으로 대부분 통제가 어려운 특성을 가지고 있으며, 정부 정책의 변동, 법규 및 규제요건의 변동, 사회적 혼란, 환경오염, 환율 등에 의한 위험이 포함된다.

업무영역 측면에서 좀 더 세부적으로 위험을 구분하면 재정적 위험(Financial Risk)과 전략적 위험(Strategic Risk), 운영 위험(Operational Risk), 돌발 상황에 의한 위험(Hazard Risk)으로 구분한다. 다음의 표는 영국 위험관리표준에서 제시하고 있는 위험관리영역이다(Lemieux 2004, 12).

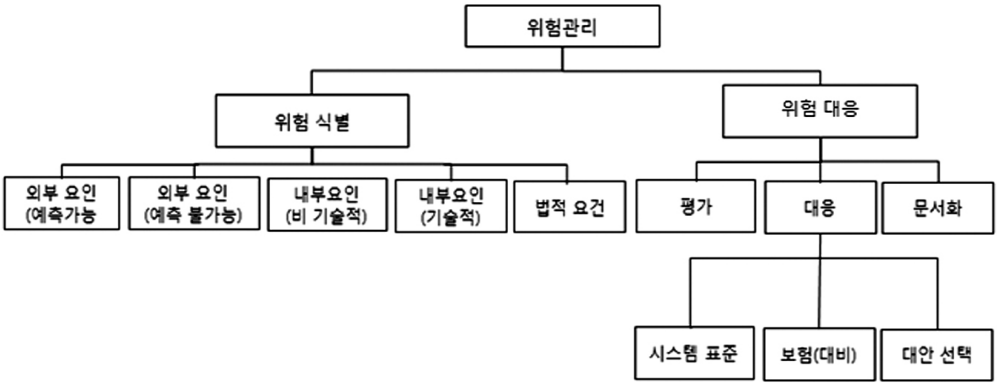
〈표 1〉에서 재정적 위험, 정책적 위험, 운영 위험은 내부에서 발생할 소지가 있지만 돌발 위험은 거의 없으며, 외부적 상황 및 환경은 조직의 재정, 전략, 운영 및 돌발 상황의 위험이 모두 존재한다. 이는 외부 환경의 변화 예측이 내부보다 어렵기 때문이다.

지금까지는 위험의 발생 특성에 따른 유형 구분 측면에서 기술하였다. 일반적으로 위험관리 기능은 크게 위험의 식별 과정과 대응 과정으로 구분한다. 위험의 식별은 외부적 환경의 예측 불가 영역과 예측 가능 영역, 내부의 비기술적 영역과 기술적 영역, 또한 조직 공통의 규제요건이나 법률에 대한 법적 영역으로 총 5개의 영역으로 구분한다. 한편 위험 대응 과정은 먼저 위험의 평가, 평가에 따른 대응, 문서화 과정으로 다시 구분하며, 특히 위험의 대응 전략은 조직체계의 표준화, 보험 등의 사후 대비, 대응전략 선택 과정으로 세분화된다. 위험관리의 식별과 대응과정을 간단히 정리하면 다음의 〈그림 1〉과 같다.

먼저 위험의 유형별로 기록관리 업무와의 연관성 측면에서 살펴볼 필요가 있다. 일반적으로 경영위험 혹은 투기적 위험 중에서 타 기관과의 관계에서 오는 위험일 경우 특히 기록관리 업무와의 연관성이 높다. 예를 들어 계약상의 조건 이행 여부 혹은 규제요건에 대한 이행 여부는 기록의 증거력을 바탕으로 하는 정당성 확보의 문제와 직결된다. 또한 위험 가능성은 해당 분야의 지식이나 정보가 없을 때 증가한다는 특성을 감안해야 한다. 따라서 조직의 위험관리 측면에서 가장 효율적인 위험 대응 전략은 해당

〈표 1〉 위험의 유형 구분

구분	재정적 위험 (Financial Risks)	전략적 위험 (Strategic Risks)	운영 위험 (Operational Risks)	돌발 위험 (Hazard Risks)
내부요인	- 자금유동성 - 현금흐름	- 연구개발 - 지적 자산	- 회계관리 - 정보시스템	-
내·외부 공통요인	-	- M&A	- 인사채용 - 공급자사슬	- 공공 접근 - 종업원 - 자산 - 제품과 서비스
외부요인	- 이자율 - 외환변동 - 신용보증변동	- 경쟁 - 고객의 변화 - 산업구조의 변화 - 고객요구	- 규제요건 및 절차 - 문화 - 위원회 구성	- 계약 - 자연재해 - 공급자 문제 - 환경변화



〈그림 1〉 위험관리체계의 기능구분

조직의 핵심 지식자원 즉 선행 경험자원의 축적이다.

다음은 기록관리의 위험 발생이 조직의 위험에 영향을 미치는 것이다. 특히 운영 위험에서 정보시스템과 전략적 위험의 지적 자산에 대한 위험은 기록관리체계와 직접적으로 연관되어 있다. 또한 대부분의 기록관리 위험은 잠재된 위험의 인지가 가능한 위험으로 분류된다. 왜냐 하면 기록관리는 해당 조직의 경험 지식의 축적을 지원하고, 정당성 확보에 영향을 미치므로 기록관리의 위험이 바로 조직의 손실과 연결되는 것은 당연하다.

이상과 같이 기록관리와 위험관리의 연관성을 위험 유형에 따라 구분하면 첫 번째 유형 그룹 중에 기록관리 위험은 경영 위험에 속하며, 두 번째 유형 그룹 중에서는 위험 발생 가능성에 대한 인지가 어느 정도는 가능하고 문제 발생 시 손실에 대한 예측도 가능하다는 특성을 가진다. 또한 발생 영역이 주로 내부에 있어서 위험 식별과 대응 전략을 보다 효율적으로 수립할 수 있다.

2.2 기록관리 영역의 위험요인 증대

기록관리의 궁극적인 목적은 해당 조직의 비전과 미션에 기반한 기록의 정보적 가치, 증거적 가치, 역사적 가치 측면에서의 보존과 활용의 효율화이다. 따라서 기록관리 측면에서의 조직의 위험은 이 세 가지 요소의 실패에서 기인된다. 삼성경제연구소는 경영자가 최근 주시해야 할 4대 위험으로 기업생태계 위험, 소통 위험, 사회적 책임 위험, 원자재 위험을 제시하였다(삼성경제연구소 2011). 이중에서 기록관리와 깊은 연관성이 있는 영역은 기업생태계 위험, 소통 위험, 사회적 책임 위험이다.

첫째, 기업생태계 위험은 오늘날의 글로벌 경제 구조에 기인한다. 단일 목표 혹은 단일 제품을 생산하기 위해 서로 다른 목적과 구조를 가진 조직들이 연계하여 협업을 통해 수행한다. 기업 생태계는 공동의 노력으로 경쟁력을 창출하는 한편, 위험을 공유하는 단위라는 양면성이 있다. 기업은 자신이 속한 생태계가 경쟁에서 패배하거나 생태계 내부에서 사건, 사고가 발생했을 때 연쇄적으로 위험에 노출될 수 있

다. 기업 생태계 위험이 증대 하는 이유는 우선 기술과 지식의 융복합화와 IT의 발달 등을 통해 자원과 역량의 공유와 교환이 활성화되고, 다음으로는 조직간의 공급사슬 범위가 전세계로 확산되면서 돌발 상황 발생 지역이 대폭 확대되었기 때문이다. 이로 인해 조직 상호간의 책임 문제가 수반되며 상호 개방형 정보 채널이 만들어진다. 그러나 사후에 문제가 발생했을 때 해당 문제 발생 프로세스를 담당했던 조직들은 각자의 입장에서 논리와 증거를 제시해야 한다. 특히 건설사업과 같은 목표물의 수명기간이 수십년 이상의 장기간이 소요되므로 해당 책임 주관 조직 및 업무수행조직의 증거력 확보가 중요하게 된다.

둘째, 소통 위험 영역이다. 최근에 소셜 미디어의 확산으로 기업의 소통 위험이 증폭되고 있다. TV, 신문, 라디오, 잡지 등 대중 매체가 주도하던 사회적 매체 환경이 페이스북, 트위터 등 소셜 미디어의 부상으로 다변화되고 있으며, 정보의 사실 여부, 기업의 책임 유무와 무관하게 검증되지 않은 정보로 인한 위험성이 높아져 가고 있다. 이러한 위험성은 조직의 외부에서만 형성되지 않고, 조직 내부에서도 유사한 상황을 초래할 수 있다. 과거에 한정된 범위에서만 이루어지던 소통 체계가 더 이상 경계선이나 장벽 없이 보다 넓은 범위에서 보다 빠르게 확산되는 것이다. 따라서 기록의 중요성은 더욱 커지고 있다. 무작위로 확산되는 정보의 소통체계에서 결국 검증된 증거력만이 조직을 지켜낼 수 있기 때문이다. 조직이 수행한 업무의 정당성 확보는 결국 기록의 증거력을 제대로 보존하고 관리할 때 유지될 수 있기 때문이다.

셋째, 사회적 책임 위험 영역이다. 오늘날 기업들은 사회적 책임에 대한 요구를 강하게 받고 있다. 즉 지속가능한 기업으로의 성장을 목표로 사회, 환경적 책임과 경제적 책임을 이행해야 하며, 이는 기업의 지속가능경영, 사회적 책임, 기업윤리 등의 용어와 혼용되어 사용되고 있다. 따라서 기업의 사회적 책임 영역은 법률과 규정의 엄격한 준수는 물론이고 환경보존, 사회공헌 활동 등의 모범적인 기업시민의 역할을 요구하는 데서 비롯된 위험이 수반된다. 기업에 대한 사회의 기대 수준이 높아지고 책임 범위가 확대됨에 따라 요구수준에 미치지 못하는 경영활동을 할 경우 재무적 손실이나 명성이 훼손되는 위험이 증가되고 있기 때문이다. 따라서 법과 규정의 준수는 기업 경영의 필수요건이며 이는 기록관리의 주요 목적인 컴플라이언스와 맥락을 같이 하며, 기록관리의 실패는 결국 해당 조직의 위험 관리의 실패와 직결된다.

이상에서 기술한 바와 같이 오늘날 정부조직이든 기업조직이든 해당 조직의 위험 관리 영역 중 상당 부분이 기록관리와 연계되어 있다. 특히 기록의 디지털화로 인한 기록의 속성 변화가 위험을 더욱 증가시키고 있다. 즉 디지털 기록의 시스템 의존성은 장기보존 능력의 약화를 초래하고, 복본성은 진본성 확보와 정보 유출 문제를 대두시키고 있으며 접근성과 가독성 유지를 위해 기록관리요건은 갈수록 강화되어 가고 있다. 또한 IT 거버넌스에 의한 업무 영역 및 프로세스 간의 통합화 현상에 따라 기록의 생애주기 관리가 요구되면서 문서관리와 기록관리의 구분이 모호해 지고 있고, 업무 과정의 트랜잭션 정보를 보존할 필요성이 증대되고 있

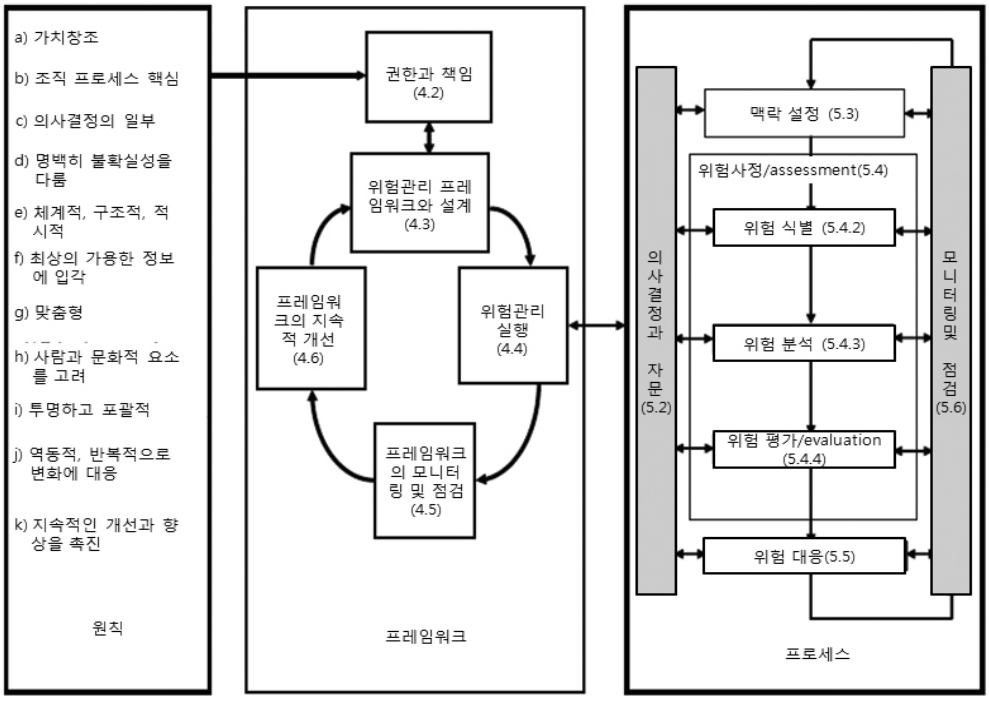
다. 이는 기록관리가 기존의 단순한 기록의 물리적 기능적 관리에서 벗어나 기록의 생산, 유통 단계에 대한 통제와 기준 제시의 역할을 요구하고 있음을 의미한다. 따라서 기록관리의 위험관리가 단순히 기록의 보존 단계에서의 재난관리 수준에서 벗어나 조직 전체의 경영 및 위험관리체계와 연동되어야 하고, 기록관리가 조직 전체의 위험관리체계에서 검토되고 통제되어야 한다.

2.3 ISO 31000에 기반한 위험관리 프레임워크와 프로세스

ISO 31000(이하 위험관리표준)은 ISO에서 위험관리를 보다 체계적으로 조직의 정책과 시스템 차원에서 관리되도록 제시된 위험관리체계에 대한 경영 표준이다. 위험관리표준에서 제시하는 위험관리표준은 크게 위험관리 프레임워크와 위험관리 프로세스로 구분하여 다음의 〈그림 2〉와 같이 제시하고 있다.

〈그림 2〉에서 제시된 바와 같이 위험관리표준의 주요내용은 위험관리의 기본 원칙(4장)과 위험관리 프레임워크의 개요 및 일반사항(5장) 및 위험관리 프로세스(6장)로 구성되어 있고, 표준에서 제시하는 위험관리 기본 원칙은 다음과 같다.

- 위험관리는 가치를 창조하고 보존한다.
- 위험관리는 모든 조직 프로세스의 핵심부분이다.
- 위험관리는 의사결정의 일부이다.

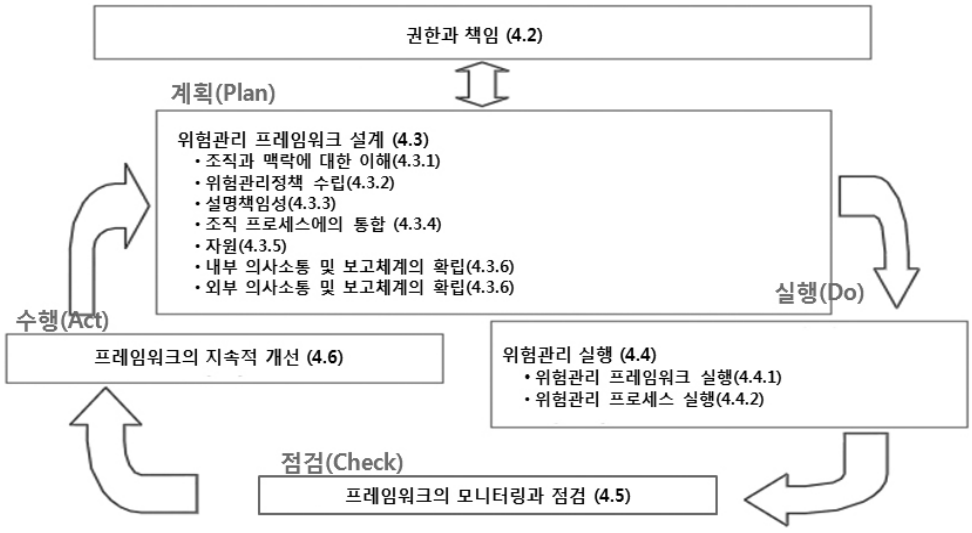


〈그림 2〉 위험관리 프레임워크와 프로세스 구조

- 위험관리는 명백하게 불확실성을 다룬다.
- 위험관리는 체계적이고 구조화되며 적시적이어야 한다.
- 위험관리는 최상의 가용한 정보에 토대를 둔다.
- 위험관리는 맞춤형이다.
- 위험관리는 사람과 문화적 요소를 고려한다.
- 위험관리는 투명하고 포괄적이어야 한다.
- 위험관리는 역동적이고, 반복적으로 변화에 대응한다.
- 위험관리는 조직의 지속적인 개선을 촉진한다.

다음은 위험관리 프레임워크의 구조[5]이다. 위험관리 프레임워크는 다른 ISO 표준에서 공통적으로 적용하는 계획수립-실행-점검-수정(Plan-Do-Check_Act; PDCA)의 프레임으로 제시되고 있다. 위험관리는 그 특성상 현행 프로세스 과정에서 기준을 어떻게 적용할 것인가의 측면보다는 미래에 일어날 수 있는 위험요소를 사전에 예측하고 이를 대비하고자 하는 목적이 강하다. 아래의 〈그림 3〉과 같이 위험관리 프레임워크에서도 계획수립(P) 부분이 다른 실행(D), 점검(C), 수정(A)의 영역보다 비중이 크다. 따라서 기록관리 업무에서도 가장 집중적으로 고려할 부분은 위험관리의 계획 수립 부분이다.

〈그림 3〉에서 제시된 바와 같이 위험관리 프레임워크 구조는 첫째, 권한과 책임, 둘째, 위험관리 프레임워크 설계, 셋째, 위험관리의 실행, 넷째, 위험관리 프레임워크에 대한 모니터링과 점검, 다섯째, 프레임워크의 지속적인 개선으로 구분할 수 있다. 먼저 첫째, 권한과 책임 영역은 위험관리를 수행하기 위한 조직과 개인에 대한



〈그림 3〉 위험관리 프레임워크의 구조와 내용

5) ISO 31000 Risk Management - Principles and Guidelines. 2009. 3항.

책임과 권한사항을 규정화하고 명시한다. 이는 조직의 위험관리 기본 계획을 수립하기 위해 가장 기본적으로 갖추어야 할 영역으로서 기록관리 측면에서는 기록관리 영역에서의 위험관리 책임과 위험관리 영역에서의 기록관리 책임으로 구분되며, 기록관리와 위험관리의 목적, 전략이 같아야 하고 각 절차간의 정렬성이 요구된다. 둘째 영역인 위험관리 프레임워크 설계영역은 위험관리 프레임워크에서 가장 핵심이 되는 내용으로서 조직의 맥락 이해, 위험관리 정책 수립, 설명 책임성, 조직내 프로세스 통합, 필요 자원, 내부와 외부 소통 기반의 수립을 수행한다. 각 활동 내역별로 정리하면 다음과 같다.

첫째, 위험요소의 정의와 대응 방안의 수립은 먼저 조직과 조직의 맥락(Context) 이해에서 출발한다. 따라서 위험관리 프레임워크의 첫 번째 영역인 조직의 맥락 이해는 가장 먼저 검토되고 정의되어야 할 영역으로서 사회적, 문화적, 경제적, 법적, 기술적 환경을 고려하여 설정되어야 한다. 조직의 목표에 영향을 주는 요소가 무엇인지와 외부 이해관계자간의 관계가 명확하게 검토되고 정의되어야 한다.

둘째, 위험관리 정책 수립이다. 위험관리 정책은 조직의 맥락에 근거해야 한다. 조직의 목적과 연계된 갈등요소와 그에 대한 해결 방안이 고려되어야 하며 위험관리에 대한 조직의 총괄적 책임과 필요자원의 확보가 필요하다. 기록관리 영역에서는 조직의 맥락에 의거한 기록관리 측면의 위험요소가 정의되고 그에 대한 관리 정책이 수립되어야 하며 이를 위해서는 해당 조직의 주요 기록 혹은 핵심 기록의 정의가 전제되어야 한다. 또한 핵심기록에 대한 위험요소와 대응방안이 함께 고려되어야 한다.

셋째, 설명 책임성(Accountability)이다. 위험관리 프레임웍의 개발, 실행, 유지 책임에 대한 영역으로 조직의 계층별로 상세한 책임사항의 지정과 할당이 필요하며 성과 측정 기준과 내부와 외부 보고체계가 수립되어야 한다. 기록관리 측면에서는 기록관리의 계층별 책임사항이 정의되어야 한다.

넷째, 프로세스 통합 측면에서의 요건이다. 위험관리는 조직 전체를 망라하는 업무 프로세스를 기반으로 수립되어야 한다. 특히 기록의 생산, 유통, 저장, 활용, 보존의 단계가 기록을 생산하고 유통시키는 업무 영역의 프로세스와 동적으로 연계되어 분석되어야 한다. 이를 위해서는 기록의 생산, 유통, 저장, 활용 단계를 담당하는 시스템과 보존을 담당하는 시스템간의 구분과 역할 정의가 필요하고, 각 단계별로 기록관리 관점의 위험요소가 정의되어야 한다.

다섯째, 필요 자원의 확보이다. 기록관리 영역에서의 위험관리를 위한 소요자원은 다른 영역과 같이 인력, 기술, 경험자원으로 구분하며 위험관리 각 프로세스에 따라 단계별로 필요자원이 사전에 배정되어야 한다. 필요 자원의 배정은 위험관리의 수단, 방법론, 프로세스 설정에 따라 이루어져야 한다. 기록관리 영역의 위험관리를 위한 자원 배정과 그 기준은 사전에 정의된 절차에 따라 이루어져야 하며 특히 경험자원의 확보를 위해 정보 및 지식관리시스템의 운영 기준을 정하고 또한 해당 역무 담당자에 대한 교육 프로그램도 갖추어야 한다.

여섯째, 내부와 외부 소통기반의 수립이다. 위험관리에서 소통은 매우 중요한 역할을 한다. 특히 위험관리 프레임워크에 대한 핵심요소의

설정과 적정한 효과 분석 수준 및 내부 이해관계자의 자문 프로세스를 수립하고 있어야 한다. 외부적으로는 사전에 정의된 이해관계자의 참여 정도와 정보 교환체계가 중요하다. 또한 위험 발생 시 법적, 절차적 소통 요건을 사전에 검토하고, 외부 의견에 대한 적절한 피드백과 유사시 의사소통 절차를 사전에 수립하고 있어야 한다. 기록관리 영역에서도 기록관리와 관련된 외부 이해관계자의 정의와 범위 설정이 필요하다. 기록의 증거적 가치 측면에서의 고려가 필요하며 위험요소와 위험의 정도를 파악할 수 있는 기준 수립이 매우 중요하며 문제 발생 가능성과 그에 따라 적절한 의사소통 절차의 수립이 요구된다.

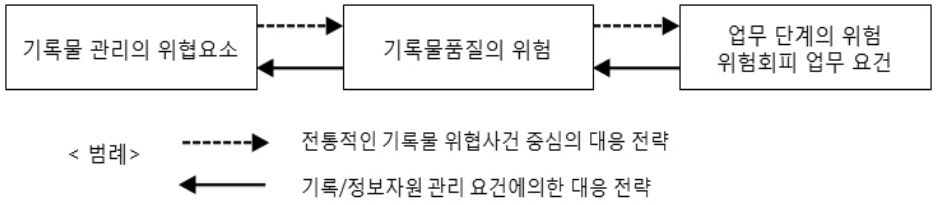
위험관리 프레임워크의 실행은 결국 위험관리 프로세스의 각 단계에서 이루어진다. 위험관리 프로세스는 앞의 〈그림 2〉에서 제시된 바와 같이 크게 맥락 수립과 위험 사정, 위험 대응의 3단계로 구분하며, 그중에서 위험 사정 단계는 다시 위험요소 식별, 위험 분석, 위험 평가 단계로 구분한다. 본 연구는 이러한 위험관리 표준에서 제시하는 프레임워크 체계와 프로세스 단계별로 기록관리 영역에서 고려해야 할 기준 및 요소들을 기록관리표준을 통해 제시하고자 하는 것이다.

3. 기록관리와 위험관리의 관계

3.1 기록관리 위험의 특성과 대응

전통적으로 기록관리영역의 위험은 주로 기록에 대한 위협 유발 사건(Trigger Event) 측면에서 고려되었다. 기록관리 영역의 위협적 사건은 시스템 고장, 컴퓨터 사기, 도난, 분실, 상해 및 적절치 못한 보존연한 설정 등 주로 자연 혹은 인적 재해, 인간의 실수에 의한 것으로서 그에 대한 대응전략 역시 재해방지 혹은 복구정책, 시스템 백업, IT 보안, 문서화 및 보존에 대한 절차를 통해 수립되었다. 반면에 오늘날 대부분의 업무 프로세스가 IT기반으로 전환되고 디지털 형식의 기록으로 바뀌면서 기존의 위협 유발 사건에 의거한 위험요소 이외에 디지털 기록의 품질 문제로 인한 위험요소가 높아지게 되었다. 따라서 기록관리 영역의 위험관리는 아래의 〈그림 4〉와 같이 아날로그 기록에 대한 전통적인 위험과 디지털 기록의 업무과정 측면의 위험에 대한 고려가 모두 필요하다(Lemieux 2004, 46).

〈그림 4〉에서 기록관리의 위험은 위협적 사건에 의한 기록관리 위험과 업무 과정에서 생성된 기록관리 위험으로 구분한다. 기록 관리의 실패는 곧 기록 품질의 위험을 초래하고 이

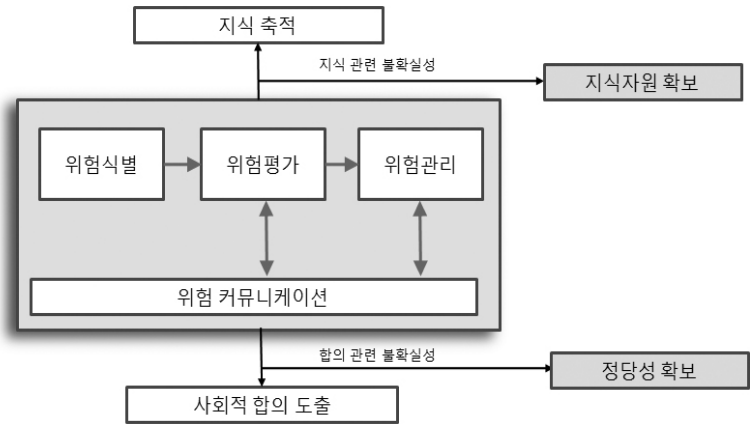


〈그림 4〉 기록관리 위험의 2가지 유형과 대응 전략

는 다시 업무 과정의 위험을 초래하며, 반면에 업무 과정에서의 기록관리 요건 적용의 실패는 기록 품질의 위험 요소로 작용한다. 이는 결국 해당 조직의 기록관리의 실패와 연결된다. 디지털 기록의 품질은 정확성, 완전성, 적시성, 보존성, 타당성, 이해성, 적절성, 신뢰성, 보증성, 공유성, 접근성, 검색성, 소통성 등 다양한 요소에 의해 결정된다. 따라서 기록관리 영역의 위험관리는 이러한 기록의 품질을 유지, 보존하는데 목적을 둔다.

또한 디지털 기록 관리의 위험은 IT 기술발전에 의한 급속한 변화와 불확실성에 기인한다. 기술 집약적인 분야일수록 그 위험의 폭은 커지며 디지털 기록의 위험성은 기록 자체의 문제이기보다는 디지털 기록을 생산, 유통, 활용하는 업무과정 전반의 문제에 기인한다. 즉 IT 거버넌스에 의거한 업무환경의 변화는 조직의 분리와 통합을 가져오고, 프로세스를 변경한다. 이러한 불안정한 환경에서 기록관리의 위험성은 지식자원의 축적과 사회적 합의 도출을 위한 정당성 확보, 두 가지 측면에서 검토되어야 한다. 따라서 지식자원 확보의 문제는 기록의 정보적 가치 측면에서, 정당성 확보의 문제는 기록의 증거적 가치 측면에서 고려되어야 한다. 위험관리는 곧 불확실성에 대한 예측과 관리라는 점에서 기록관리 위험의 특성은 다음의 〈그림 5〉와 같이 기록의 증거적 가치 측면과 정보적 가치 측면에 집중하여 전략이 수립되어야 한다(성지은 외 2007, 210).

또한 기록관리 위험은 다른 위험과 달리 사후 보험이나 사후 복구가 어렵다는 특징을 가진다. 특히 증거적 가치 보존의 실패는 조직에 큰 손실을 초래할 수 있고, 이에 따라 조직의 존립여부를 결정할 만큼의 치명적인 결과를 가져올 수 있다. 따라서 기록관리의 위험관리는 사전 예방 차원에 집중하여 이루어져야 한다. 기록의 정보적 가치 측면에서도 예방 차원의 전략은 매우 중요하다. 왜냐 하면 디지털 기록으로 전환되면서 기록의 품질 유지가 예전의 아날로그 매체보다 훨씬 더 복잡해졌기 때문이다. 특히 디지털 기록의 품질 비용은 초기 예방 비용보다 평가 비용과 실패 비용이 기하급수적



〈그림 5〉 기록자원의 위험관리 목적

으로 증가되는 특징을 가진다. 또한 기록의 정보적 가치 측면에서 중요하게 고려되어야 할 부분은 보안성 측면이다. 디지털 기록의 편집, 복사의 용이성은 보안 측면에서 매우 취약하다는 것을 의미한다. 이러한 취약성을 어떻게 보완하고 방어할 것인가는 IT분야에서 이미 많은 방법론이 제시되어 있고, 기록관리 측면에서는 주로 기록의 중요도와 활용도 차원에서 보안성을 고려해야 한다. 기록관리 위험의 유형을 구분하면 〈표 2〉와 같이 요약할 수 있다.

기록관리의 위험요소 식별과 대응 전략을 별도로 구축하여 시행하고 있는 조직이나 기관은 많지 않다. 다만 IT 정보기술 및 시스템 측면에서는 NIST에서 위험관리에 대한 대응 지침을 구체적으로 제시하고 있는데, NIST 지침은 디지털 기록의 콘텐츠 측면보다는 IT시스템 측면에서 제시된 내용으로서 상당 부분은 기록관리 측면에서도 가이드로 적용할 수 있다. NIST의 위험관리 가이드는 시스템 개발주기(SDLC)의 단계별 위험관리 수행 전략을 제시하고 있어 기록관리시스템 개발 및 구축에 유용하다. NIST에서 제시하는 SDLC 기반의 통합 위험관리 전략은 다음의 〈표 3〉과 같다.

〈표 3〉에서 제시된 IT 정보시스템 측면에서 위험관리 전략과 기록관리 측면에서 가장 크게 고려할 부분은 '단계 1'의 시스템의 목적과 범

〈표 2〉 기록의 위험관리 영역 구분과 핵심 고려사항

위험 영역 구분		위험관리 핵심 고려 사항
증거적 가치 측면	기록의 품질	IT 기술 및 정보시스템 개발 요건 반영
	기록의 맥락	조직의 맥락 반영, 내.외부 규제요건 반영
정보적 가치 측면	기록의 품질	IT 기술 및 정보시스템 개발 요건 반영
	기록 보안	핵심 자원 선정, IT 기술, 업무프로세스 분석

〈표 3〉 SDLC와 위험관리의 통합

SDLC 단계	단계별 특징	위험관리 활동에 의한 지원
단계 1 착수	IT시스템에 대한 요구를 기술하고 목적과 범위를 문서화한다.	위험 식별을 통해 시스템요구사항 특히 보안요구사항과 운영상 보안전략의 개발을 지원한다.
단계 2 개발 또는 인수	IT시스템을 설계, 구매, 프로그램화, 개발 또는 구축한다.	식별한 위험요소를 활용하여 IT시스템의 개발과정에서 구조와 설계를 가름하는 보안 분석을 지원한다.
단계 3 실행	시스템 보안요소를 규정, 실현, 시험 및 검증한다.	위험관리 프로세스를 통해 요구사항과 운용환경모델에 대한 시스템 실행 평가를 지원하며, 시스템 운용 이전에 위험 식별에 대한 의사결정이 이루어져야 한다.
단계 4 운용/유지보수	시스템 기능을 수행한다. H/W와 S/W의 추가, 조직 프로세스, 정책, 절차의 변경을 통해 시스템을 지속적으로 수정한다.	정기적 시스템 재인가시 또는 새로운 인터페이스 도입으로 IT시스템 운용 환경에 큰 변화가 있을 때 위험관리 활동을 수행한다.
단계 5 처분	정보, H/W, S/W의 처분을 포함하여 정보의 이동, 아카이브화, 폐기 등의 처분을 시행한다.	H/W와 S/W 폐기가 적절히 이루어지고 남은 데이터가 적절히 처리되는지, 시스템 전환이 안전하고 체계적으로 이루어지는지를 확인하기 위해 시스템 구성요소의 폐기 또는 교체시에 위험관리 활동을 수행한다.

위 설정과 '단계 2'의 시스템 개발 단계이다. '단계 1'에서는 대상 시스템에서 관리하는 기록의 범위와 유형 및 특성에 대한 요건을 상세히 검토하여 시스템 구축에 반영하여야 하기 때문이다. '단계 2'에서는 시스템의 본격적인 설계와 개발이 이루어지는 단계로서 메타데이터의 설계가 관건이 되며 기록의 사후 보존과 마이그레이션 등의 조치가 적절하게 이루어지기 위해서는 기록의 사전 평가에 의한 기록보존계획이 수립되고 메타데이터로 설정되어 있어야 한다. 조직의 맥락 정보는 일반적으로 기록의 메타데이터이고, 메타데이터는 결국 해당 조직의 업무과정의 분석과 깊이 연관되어 있다. 따라서 기록의 정보적 가치 측면에서의 위험관리 요소인 보안관리 역시 조직의 업무 과정 분석을 통한 핵심 업무 선정을 토대로 전략이 수립된다. '단계 3'과 '단계 4'는 시스템의 실행과 유지보수 단계로서 실제적인 수행과정에서 나오는 수정, 보완할 사항을 모니터링하고 보완하는 과정을 문서화하여야 한다. 마지막 '단계 5'에서 고려할 사항은 정보의 처분이 이루지는 단계로서 이 단계에서는 보존 대상과 폐기 대상의 구분이 명확해야 하며, 이를 위해서는 해당 조직의 기록보존일정표를 시스템에 반영하고 그에 따른 조치가 적절히 이루어지도록 해야 하나, 앞의 '단계 1과 2'에서 잘못 설정되었을 경우 기록의 품질 유지에 치명적 오류나 불필요한 과다 비용을 초래할 수 있다.

3.2 기록관리 정책 및 개념 측면의 위험관리 요소

기록의 디지털화로 인해 정보자원 측면에서의 활용성과 효율성은 획기적으로 발전하였으나 기록의 보존과 활용 측면에서의 불안전성은 오히려 더욱 증대되었다. 기록을 생산하는 과정 즉 업무 과정이 IT 기반에서 이루어짐에 따라 기존의 보존 측면에서만 고려되던 아날로그 기록 매체와 달리 디지털 기록은 기록의 생성, 유통, 활용의 전 과정에서 위험요소가 파악되고 관리되어야 한다. 즉 기록의 디지털화로 인해 기록관리와 위험관리의 상관성이 매우 높아졌다. 또한 위험관리가 사전 예방조치를 통해 위험발생 확률을 최소화하는 것인데, 기록관리 역시 기록의 증거적 가치, 정보적 가치의 훼손을 최소화하기 위해 사전 예방 차원의 업무 요건을 수립하고, 대부분의 관리업무는 이 요건에 맞게 수행하고 있는가에 초점을 둔다는 측면에서 공통점을 찾을 수 있다.

특히 기록관리의 보안 관리 영역은 기록의 정보의 자산적 가치 평가를 수행하고 그 결과를 토대로 한 기록의 기밀성, 무결성, 가용성에 영향을 주는 위험요소를 시스템 측면에서 파악하고 그에 대한 대응 전략을 수립한다는 측면에서 위험관리와 제도적, 시스템적 측면에서의 밀접한 연계가 이루어져야 한다. 이러한 두 분야의 상관 관계를 ISO 기록관리표준(ISO 15489-1)과 DRAMBORA의 단계별 프로세스 정의와 기술 내용 비교를 통해 정리하면 더 확실해진다(〈표 4〉 참조).

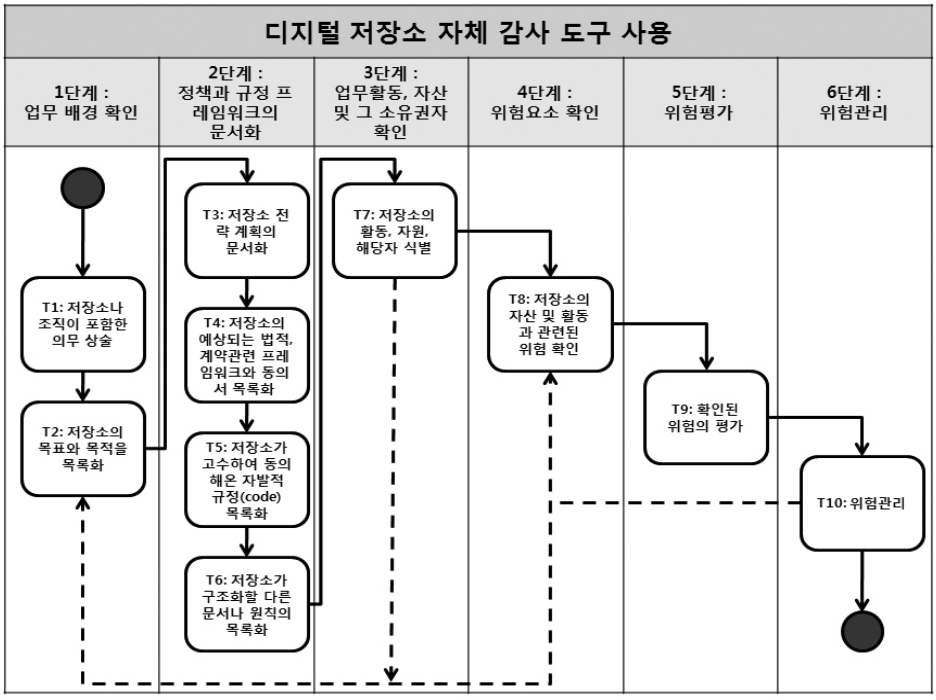
또한 DRAMBORA는 디지털 기록의 위험관리를 위한 직접적인 감사 도구에 대한 표준으로서 디지털 기록의 저장소에 대한 감사 프로세스를 구체화하여 6단계의 위험관리 프로세스를 다음의 〈그림 6〉과 같이 제시하고 있다(임진희 2011, 136).

〈표 4〉 ISO 15489-1 위험관련 대비 항목 정리

구 분		위험 관련 항목의 내용 요약	위험관리 목표
4장	기록관리편익	▪ 기록관리 업무시스템 및 업무과정의 통합 ▪ 재난 발생시 업무 지속성 유지	- 업무 맥락정보유실방지 - 업무지속성 확보
5장	규제환경	▪ 업무환경을 관장하는 법령,판례,규정 제시 ▪ 규정 준수에 대한 충분한 증거 제시	- Compliance
6장	정책과 책임	▪ 정책의 성문화 및 정책 준수의 의무 보장 ▪ 기록관리 정책은 업무활동 분석 기반 수립 ▪ 현행 업무요구 반영을 위한 정기적인 정책 점검 ▪ 기록관리의 구체적인 책임사항 성문화	- 설명책임성 확보
7장	기록관리요건	▪ 기록은 업무활동을 수행하는 중에 생산, 접수, 이용됨. ▪ 기록의 진본성, 신뢰성, 이용성, 무결성 보호 ▪ 기록의 생산과정에서 메타데이터도 함께 생산, 연계관리 결정 ▪ 업무상 필요와 사회 기대치 충족 ▪ 보안이 유지되는 안전한 환경에서 기록유지 및 보존	- 정보적, 증거 적 가치 훼손 방지 - 조직 윤리성 확보 - 정보 보안성 확보
8장	기록시스템의 설계와 실행	▪ 기록시스템은 조직의 운영 목적에 부합하고 규제환경 충족 ▪ 기록시스템/기록처리 행위의 기록화 ▪ 기준에 대한 준수정도와 성과 측정 ▪ 핵심기록에 대한 의사결정과 보존기간 설정의 규제요건과의 부합화 ▪ 업무활동 영역의 모든 기록의 일상적 획득 ▪ 업무과정이 반영되도록 기록을 조직 ▪ 허가받지 않는 변경/처분으로부터 보호 ▪ 물리적 저장 매체 보호/분산관리/변환과 마이그레이션	- Compliance - 설명책임성 - 정보적 가치 훼손 방지 - 업무맥락 훼손 방지(무결성, 신뢰성 훼손 방지) - 재난 보호
9장	기록관리 과정과 제어	▪ 기록 획득 실패로 인해 발생할 수 있는 위험 분석 결과에 따라 획득 대상 문서 결정 ▪ 다양한 매체, 기술의 변화, 다수의 사용자와 환경을 고려한 기록관리 과정 제어 ▪ 의사결정 과정의 기록화 ▪ 내·외부 이해관계자들의 권리와 이해관계를 고려하여 기록의 보유기간 결정	- Compliance - 설명책임성 - 정보적 가치 훼손 방지 - 업무 맥락 훼손 방지
10장	모니터링과 감사	▪ 기록시스템의 절차와 과정이 조직의 정책과 요구에 따라 실행되고 있음을 보장하기 위해 기준의 준수 여부를 정기적으로 모니터링하고 그 결과를 업무에 반영 및 기록화	- 설명책임성 - 정보적 가치 훼손 방지 - 업무 맥락 훼손 방지

〈그림 6〉에서 1단계는 업무배경 및 맥락을 확인하는 단계로서 저장소의 의무와 조직의 존재 목적을 확인하고 이를 기반으로 위험분석의 범위와 요소를 설정한다. 또한 2단계는 조직의 정책과 해당 조직의 내부, 외부 규제요건을 확인하는 단계이다. 이 단계는 저장소의 전략 및 계획을 문서화하기 위해 해당 조직의 법적, 계약관련 요건 및 저장소에서 구조화할 문서와 원칙에 대한 목록화를 수행하는 단계이다. 3단계는 업무활동을 구분하고 각 업무활동에 대한 자원 및 소유권자를 확인하는 단계이다. 4단계는 각 업무활동 및 과정에 대한 위험요소를 확인하는 단계이고 5단계는 위험요소와 각 요소에 대한 위험의 정도를 평가하고 그에 따른 대응방안은 6단계에서 수행한다.

앞의 〈표 3〉에서 기술한 바와 같이 기록관리 표준은 이미 기록관리의 위험성을 전제로 위험의 최소화 측면에서 기준들을 제시하고 있고, DRAMBORA는 기록 저장소에 대한 위험관리 감사 도구와 절차를 제시하고 있다. 하지만



〈그림 6〉 DRAMBORA 위험관리 프로세스

이러한 기록관리의 위험요소를 조직의 정책이나 전사적 혹은 통합 위험관리체계에서 실제적으로 적용하고 있지 못한 것이 현실이다. 이는 아직 경영과 전략 차원에서의 기록관리의 동력이 미흡하기 때문이다.

3.3 위험관리체계의 기록관리표준 적용

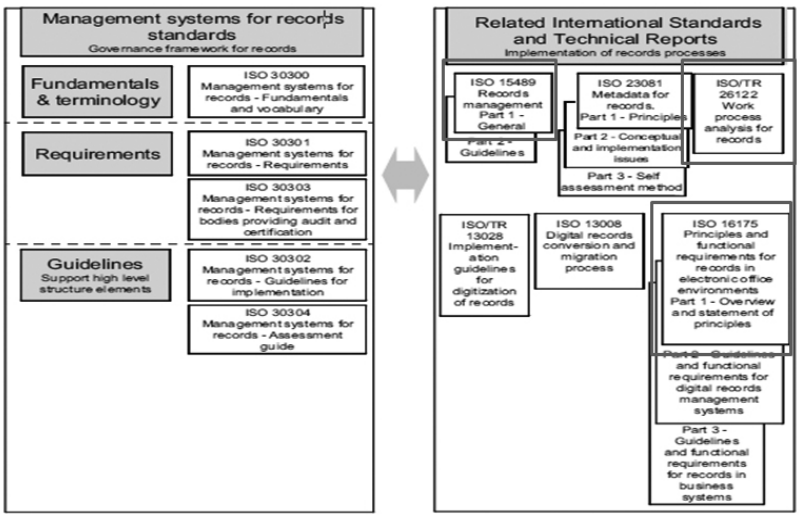
기록관리는 사실상 위험관리와 밀접한 관계를 갖고 있음에도 불구하고 위험관리 차원의 기록관리 대응방안을 별도로 운영하고 있는 곳이 많지 않다. 물론 IT자원의 보안 측면에서는 대부분의 기관이 개별 지침을 수립하고 시스템에 반영하고 있으나 정작 디지털 기록의 품질이나 보존 측면의 위험성에 대해서 인지하고 그에 대비하는 곳은 많지 않은 것이 현실이다. 그 이유는 기록관리에 대한 인식이 여전히 예전의 아카이브적 기능에서 크게 벗어나지 못하고 있고, 업무 과정에 연동되어 함께 수행되어야 할 프로세스 측면의 관리라는 인식이 부족하기 때문이다.

또 다른 이유는 기록관리를 경영정책이나 업무과정 관리에 연동 할 수 있는 툴이 마땅치 않다는 측면이 있다. 현실적으로 기록관리의 위험관리 연동은 조직의 경영정책 및 시스템 통합 차원에서 수행되어야 한다는 점에서 일반 기록관리 조직이 주도하기에는 역부족이고 경영기획 혹은 위험관리 조직은 기록관리의 중요성을 이해하지 못하고 있다. 이러한 차원에서 금년 말 즈음에 공식 발행을 앞두고 있는 ISO 30301 (Management Standard for Records, MSR)

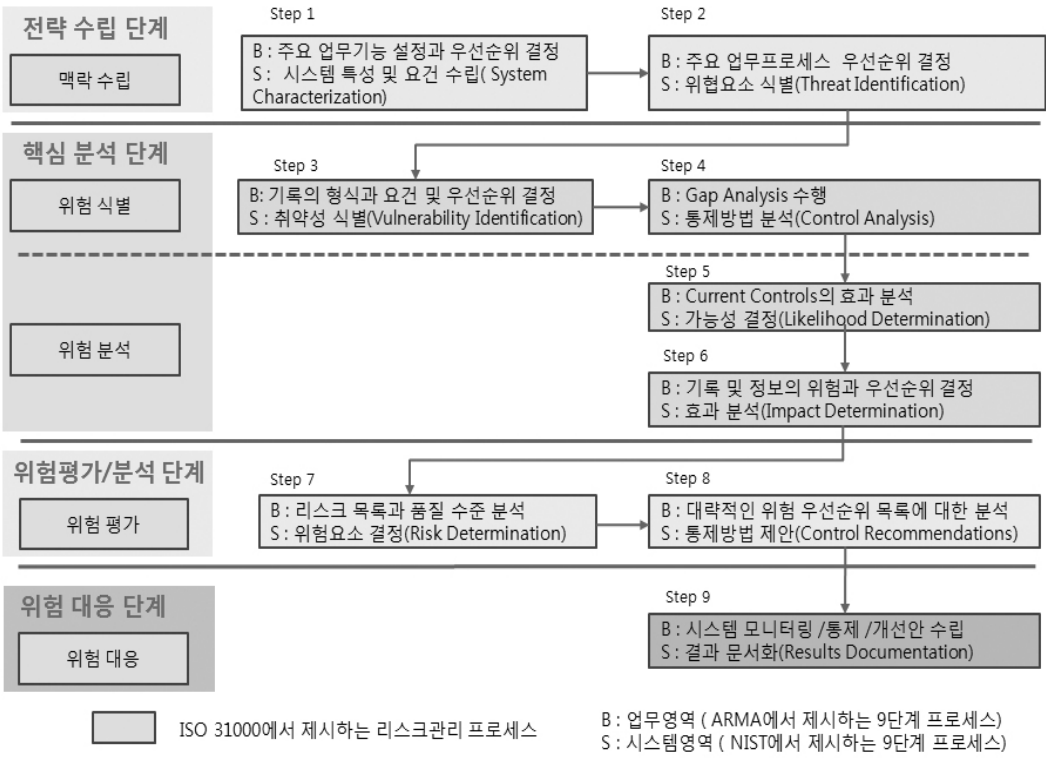
의 체계는 ISO 31000과 유사한 운영 프레임웍을 가지고 있어 기록관리의 위험관리 적용 툴로서 적절하게 활용할 수 있다. ISO 31000과 ISO 30301의 프레임워크가 모두 PDCA 사이클을 기반으로 하고 있기 때문이다. 사실 기록관리 프로세스는 조직의 경영과 전략 기반의 계획을 토대로 수행되어야 하는 원칙은 기존의 기록보존 표준 모델인 ISO 14721의 OAIS 모델에서도 제시되어 있다. 문제는 단편적으로 원칙의 선언만 되어 있을 뿐 구체적인 방법론이 제시되지 못해 실무 현장에 적용하기에는 아쉬움이 있었다. MSR은 아래의 〈그림 7〉과 같이 기록관리표준을 조직의 경영 시스템 차원에서 적용하는데 매우 유용한 틀을 제공한다.

〈그림 7〉에서 MSR은 크게 경영관리 영역과 기록관리 실무 영역으로 구분하고 있다. 경영관리 영역인 왼쪽 프레임의 내용은 기록관리를 위한 경영관리 측면에서의 요건과 감사와 인증체계 및 자체 점검 및 평가 가이드를 제시한다. 반면에 오른쪽 프레임은 기록관리 실무 영역으로서 기존의 기록관리 업무 영역별로 적용되는 표준을 제시하고 있다. 기록관리의 위험관리체계 적용은 주로 업무 프로세스 단계에서 집중되어야 함을 감안하여 본 연구에서는 ISO 31000의 프로세스를 기반으로 각 단계별로 ISO 15489와 ISO TR 26122 및 ISO 16175-3의 내용에서 대응 항목을 추출하였다.

위험관리 프로세스 단계에 대한 기록관리 표준 대응을 보다 효율적으로 구분하기 위해 업무 프로세스에 대한 표준은 ARMA에서 제시한 위험관리 단계를 기반으로 하였고, IT 정보시스템 측면의 적용은 NIST에서 제시하고 있는 각각의 단계를 공통의 분석 기반으로 설정하였다. 위험관리에 대한 ARMA에서 제시한 프로세스와 NIST에서 제시한 프로세스를 활용하여 위험관리 프로세스를 도식화하면 〈그림 8〉과 같다.



〈그림 7〉 ISO 30301의 기록경영시스템 표준 구성체계



〈그림 8〉 기록관리 업무 및 시스템 영역에 대한 위험관리 프로세스

첫째는 전략수립 단계로서 ISO 31000에서는 조직의 맥락을 정의하고 미션을 정의하는 단계이다. 이 단계에서는 업무 측면에서 주요 업무 기능과 우선순위가 설정되어야 하며, 주요 업무 프로세스별로 우선순위가 결정되어야 한다. 또한 NIST에서 제시하는 요건으로 시스템 측면에서는 시스템의 특성과 요건을 수립하고 해당 시스템의 위험요소 식별을 요구한다. 두 번째는 핵심 분석 단계로서 ISO 31000에서는 위험요소 식별과 분석을 요구하는 단계인데, 업무 측면에서는 기록의 형식과 요건에 따른 우선순위를 결정하고 실제 업무와 요건 사이의 차이를 분석하며 현재 시점에서의 적용 실험을 통해 효과를 분석하고 기록에 대한 위험요소별로 우선순위를 결정한다. 시스템 측면에서는 앞에서 식별한 위험요소에 대해 취약성을 식별하고 구체적인 통제방법과 가능성 및 효과를 분석한다. 세 번째는 위험평가/대응 분석 단계이다. 위험 평가는 위험 목록과 품질 수준을 분석하고 위험에 대한 빈도, 영향력의 정도를 목록에 기재한다. 시스템 측면에서도 유사한 과정을 수행하고 결정된 위험요소에 대한 통제방법을 제안한다. 마지막으로 네 번째는 위험대응 단계로서 업무과정과 시스템에 대한 모니터링을 수행하고 결과를 다시 업무에 수정하도록 반영하며, 예상되는 위험요소의 발생 가능성과 피해를 최소화하는 단계이다. 각 단계별 상세한 내용은 다음 장에서 설명한다.

4. 위험관리 프로세스의 기록관리표준 대응 전략

4.1 전략수립 단계

위험관리 프레임웍의 첫 번째 단계는 맥락 수립 단계이다. 업무 영역과 시스템 영역에서 위험요소를 정확하게 식별하고 평가하기 위해서는 조직 전반의 통합(Enterprise) 차원의 맥락 분석이 요구된다. 통합 차원의 맥락 분석은 업무단위별 조직구성과 프로세스, 각 프로세스 단계별 기록 생산물 현황과 위험관리 대상 구분에서 출발한다. 이를 위해 기록관리표준에서는 조직의 업무환경, 지배요건, 실무표준, 윤리강령을 파악하고 문서화하도록 한다.[6)]

또한 위험관리 프로세스에서 맥락은 외부적 맥락과 내부적 맥락으로 구분된다. 외부적 맥락 수립은 해당 기관의 사회, 문화, 정치, 법, 규제요건, 기술, 경제, 경쟁 대상을 설정하는 일이다. 또한 조직의 목표에 영향을 미치는 주요 원인과 외부 이해관계자의 가치관과 해당 조직과의 관계를 측정한다. 반면에 내부적 맥락은 조직이 수행하고자 하는 목표를 위해 장애가 되는 위험인자를 예측해야 한다. 즉 조직의 목표 달성과 가치 실현을 위해 고려되어야 할 특별한 프로젝트나 요건을 규정하고, 특정 업무의 프로세스에 대한 면밀한 분석을 요구하기도 한다. 또한 위험관리 프로세스의 맥락 수립은 목표, 업무활동, 범위, 프로세스, 관리방법론에 대한 정의가 우선 수립되어야 하며 그에 따라 위험관리 기준이 설정된다. 위험관리의 전략수립 단계에 대응할 수 있는 기록관리 표준은 KS X ISO TR 26122의 4.2항과 5항이고, 구체적인 내용은 아래의 〈표 5〉와 같다.

기록관리의 위험관리는 조직의 핵심 업무와 핵심 기록을 파악하는 것에서부터 시작해야 한다. 기록관리 측면에서 조직의 맥락 수립이 중요한 이유는 핵심 업무와 그에 대한 핵심 기록

〈표 5〉 위험관리 대응 기록관리 표준: 맥락 수립 단계

표준 항목	내용 요약	주요목적
KS X ISO TR 26122 (4.2항)	- 기록의 생산, 획득, 통제 과정의 분석 - 기능 문서화를 위한 기록 요건 식별 및 분류체계 개발 - 기록과 기록 생산 맥락간의 연계 유지 - 기록 소유권의 식별 - 적절한 기록 보유기간 결정 - 기록 시스템 맥락에서의 위기관리 분석과 보안수준 결정 개발	정당성 확보
KS X ISO TR 26122 (5항)	- 업무과정 및 기능을 통할하는 특정 법률/사명 선언문, 표준, 강령, 정책지침, 절차 등 - 해당 조직의 환경을 결정하는 법규, 판례법 - 의무적으로 적용해야 하는 표준, 기준, 강령 등 - 식별 가능한 공동체의 기대치 - 조직의 정책 및 지침 - 조직의 규칙 및 절차	정당성 확보

6) KS X ISO 15489-1, 5항.

의 정의가 맥락 파악에서 시작되기 때문이다. 이를 위해 기록관리 표준에서는 앞의 표와 같이 업무프로세스 분석 절차를 제시하고 있다. 조직의 입장에서 가장 큰 위험요소는 해당 조직의 메인 기능에서 발생할 가능성이 크며, 따라서 해당 업무에서 발생한 기록의 위험요소는 가중치를 부여하여 통제해야 한다. 핵심 기록의 파악은 기록의 보존기간과 보안 레벨에 영향을 주는 중요한 척도가 되고, 결국 기록의 보존과 보안기능에까지 영향을 미치게 된다. 또한 정당성 확보 측면에서 증거력 확보가 관건이며 이를 위해 기록을 생산하는 조직의 외부기관 즉 이해관계자에 대한 구분과 이해관계의 정도와 범위를 파악하고 이를 시스템에 반영해야 한다.

4.2 위험 식별 및 분석 단계

위험 식별은 위험의 원인과 파급효과 및 환경의 변화 등 주요 이벤트와 인과관계를 분석하는 단계로서 목표 달성에 영향을 미치는 전체 위험 리스트를 작성하는 단계이다. 또한 위험의 원인에 대한 통제 가능 정도와 이벤트의 파급효과와 누적효과가 검토되어야 하며 위험의 원인과 그에 따른 영향을 시나리오로 검토하여야 한다. 업무 영역 측면에서 우선 기록의 형식과 요건 및 우선순위를 결정하고 어느 부분이 취약한지를 구분해야 한다. 그리고 이 결과를 토대로 해당 조직의 표준이나 규정의 요건과 비교하여 범위 밖에 벗어나 있는 부분은 없는지, 벗어나 있다면 어느 정도 벗어나 있는지를 파악해야 한다. 요건에서 벗어난 정도에 따라 위험의 크기가 결정된다. 이 부분은 시스템 영역의 취약성 식별과 밀접한 연관성 있다. 즉 업무의 위험요소는 시스템의 취약성이 될 수 있으며 그에 따라 통제 방법이 달라진다. 또한 위험요소는 해당 조직의 내부와 외부의 이해관계자 영역과 기술적 영역, 법적 영역으로 구분하여 검토해야 한다. 다음의 〈표 6〉은 위험의 식별과 분석에 대한 기록관리 표준 대응 항목표이다.

〈표 6〉 위험관리 대응 기록관리 표준: 위험 식별 및 분석 단계

표준 항목	내용 요약	주요목적
KS X ISO 16175-3 (4.3.4항/ 4.3.6항/ 4.4.2항)	- 기록의 생산 맥락정보 확보를 위한 시스템 정보 확보 - 시스템 연계성 및 의존성 확인(시스템 장애, 시스템 규모, 업무규칙, 파일포맷, 개인정보관리, 데이터구조, 데이터 및 클래스 모형, 작업흐름에 대한 일상 규칙, 감사 증적 등) - 기록관리 측면에서의 위험요소 및 옵션 평가 - 핵심 기록 추출작업 수행 및 기준 반영(맥락정보를 가진 기록의 생산단계 파악, 관련 시스템간 상호운용성 지원, 기록 보유 및 처분 정보)	정당성/ 지식자원 확보
KS X ISO 26122 (4.4-4.5항)	- 기록의 생산, 유통, 보존, 활용 단계별로 참여자의 역할과 타당성을 확인 - 기록 관리에 대한 책임 설정과 문서화를 수행	정당성 확보
KS X ISO 16175-3 (4.3.1-4.3.2항)	- 업무흐름 및 표준화 확인 단계로서 업무시스템에 의해 통제되어야 할 데이터의 형식을 정의 - 업무활동 다이어그램, 프로세스 분해, 업무 흐름도를 분석 - 업무과정의 증거력 확보여부를 파악하는 단계로서 광의의 업무기능 및 상세 활동의 범위를 결정하고 각각의 활동 및 처리행위에 대한 업무과정 단계에서의 증거확보 능력을 검토(증거요건, 증거구성내용, 데이터 확인 등)	정당성/ 지식자원 확보

앞의 〈표 6〉과 같이 기록관리 영역에서의 위험 식별단계는 기록의 생산 맥락과 그에 대한 시스템 정보를 확보하고 시스템의 문제점, 장애, 업무규칙과 파일포맷, 개인 정보관리 상태, 데이터 구조 등에 대하여 관련 요건에 근거하여 차이점과 그 정도를 점검하는 단계이다. 또한 위험 분석단계는 위험을 평가하기 위한 기초정보를 수집하는 단계로서 통제가능 여부를 점검하고 위험대응 전략과 방법에 대한 결정을 하기 전 준비단계이기도 하다. 위험의 원인과 영향 및 그 발생 가능성을 고려하여 위험유형을 분류하고 위험의 수준과 민감도 분석을 통해 위험 발생 가능성의 모델화 및 정량화를 수행한다. 기록관리 영역에서의 위험 분석을 위해서는 우선 기록의 생산, 획득, 통제 과정의 참여자에 대한 역할 분석이 이루어져야 한다. 또한 업무과정에서 발생하는 기록물별로 책임사항의 명확한 구분과 업무 시스템에 의해 통제되는 데이터 형식의 정의와 업무 활동 다이아그램 및 프로세스가 분석되어야 한다. 특히 업무과정의 증거력 확보를 위해 광의의 업무기능 및 구체적인 활동과 처리행위에 대한 결정 즉 시스템 투입 및 산출 정보 및 업무과정에 대한 조직의 증거 확보 능력이 점검되어야 한다.

특히 기록관리의 위험 식별과 위험 분석은 업무과정에 대한 명확한 분석에 기반을 두어야 한다. 따라서 업무 기능의 중요도에 따른 순위 결정과 각 업무 기능에서 산출되는 결과물 즉 기록의 정의 및 파일 포맷과 보존 연한에 대한 설정과 타당성이 검토되어야 한다. 또한 기록과 기록의 상호 연관성이 맥락정보로 유지될 수 있도록 메타정보에 대한 검토가 필요하다. 이를 위해서는 기록의 생산, 유통 단계에서 보존, 활용 단계까지 기록의 라이프사이클 측면에서의 관리 요건이 요구되며 이러한 요건이 업무 시스템과 기록 시스템간의 상호연관성을 가지고 운영되는지 점검해 보아야 한다. 또한 기록의 보존연한의 설정과 보존연한에 맞게 매체와 표준 포맷 및 적절한 마이그레이션 전략이 수립되어 있는지 점검해 보아야 한다.

4.3 위험 평가 단계

위험 평가 단계에서는 위험식별 결과에 따라 위험의 수준을 비교하고 평가하며, 위험 수준에 따라 대응 혹은 추가 분석의 필요성을 판단해야 한다. 위험 평가를 위해서는 앞 단계에서 작성된 위험 목록을 토대로 해당 업무 영역에서 요구하는 품질 수준을 확인하고 현황 대비 분석을 실시한다. 이 분석 결과를 토대로 위험요소를 확정하고 그에 대한 통제방법을 강구해야 한다. 기록관리 영역에서 위험 평가 작업은 앞 단계에서 이루어진 조직의 맥락을 토대로 수립된 업무환경의 지배요건, 핵심 업무 및 기능 분석 결과에 의거한 핵심 기록 목록, 기록의 라이프사이클 단계별 책임사항, 기록관리 프로그램 원칙 등을 토대로 수행되어야 한다. 기록관리표준에서는 이 부분에 대해 주로 업무과정에 대한 요건으로 〈표 7〉과 같이 제시하고 있다.

다음의 〈표 7〉에서 제시된 기록관리 표준에서의 위험 평가는 주로 업무기능 분석결과를 토대로 이루어진다. 따라서 업무 기능의 중요성과 해당 업무 과정의 분석은 결국 해당 업무 결과물인 기록의 품질 손실과 연계하여 검토되어야 한다. 즉 기록의 품질요소적 측면에서 기록관리의 실패로 인한 영향 및 위험 발생 가능성 측

〈표 7〉 위험관리 대응 기록관리 표준: 위험 평가 단계

표준 항목	내용 요약	주요목적
KS X ISO 16175-3 (4.3.1항)	- 업무영역에 대한 요구사항의 반영 여부를 확인. 즉 특정 업무기능에 대한 위험수준을 포함한 업무적 요구사항과 위험도가 높은 업무 기능을 구분하고 문서화	정당성/ 지식자원 확보
KS X ISO 26122 (6항-7항)	- 업무 기능에 대해 아래와 같은 상세한 분석이 요구되며 그 결과로서 해당 기능의 기록물 설정과 관리요건을 비교 ▪ 조직의 목표와 전략 식별과 목표 달성 기능 설정 ▪ 기능을 구성하는 조직의 업무과정 식별 ▪ 조직의 운영기능 및 행정기능의 정의 ▪ 관계되는 타 조직 수행 기능의 정의 - 업무과정에 대한 순차 분석 및 결과 확인 ▪ 업무과정의 일상적 수행과 변화를 확인 ▪ 업무과정을 구성하는 처리행위와 순차를 식별 ▪ 업무과정의 변화를 식별하고 분석 ▪ 구성요소가 다른 처리행위의 식별과 관련 규칙을 확인 ▪ 다른 과정 및 시스템간의 연계관계를 식별	정당성/ 지식자원 확보

면에서 위험 평가가 이루어져야 한다. 기록의 품질요소는 이용가능성, 완전성, 정확성, 진본성, 접근성 등이다. ARMA에서는 기록관리의 위험 평가를 할 때 개념적으로 다음과 같은 전제요건을 제시한다.

첫째, 업무 기능과 업무 프로세스의 중요성은 해당 기능의 기록의 중요성에 비례한다.

둘째, 기록의 중요성은 기록의 유형과 관련성이 크다.

셋째, 기록 품질의 중요성은 위험과 관련성이 크다.

넷째, 현재의 기록 품질에 대한 만족 수준은 일반적으로 관련 요건에 비해 낮다.

다섯째, 현 기록관리시스템의 영향력은 크지 않다.

여섯째, 기록관리 실패로 인한 조직 위험의 영향력과 가능성은 모두 크다.

시스템 측면에서의 평가 단계는 업무 영역에서 분석된 위험 영역과 IT 측면에서의 위험요소에 대해 종합 분석과 더불어 구체적인 통제방법을 제안하는 단계이다. 위험 통제는 위험의 발생가능성과 크기 및 그로 인한 파급효과에 따라 다른 전략이 수립될 수 있다.

4.4 위험 대응 단계

위험 대응은 크게 위험 평가 결과에 따른 대응전략 수립 단계와 주기적이고 지속적인 위험에 대한 모니터링 및 검토 단계로 구분된다. 위험 대응은 결국 선택적 사항으로서 업무영역과 시스템 영역이 모두 공통적으로 모니터링과 결과에 대한 문서화를 요구한다. 위험 대응은 조직이 가지고 있는 인적, 물적 자원과 내부와 외부 소통 기반을 토대로 회피, 흡수, 조정, 전가 등의 방식 중에서 가장 적절한 방법을 선택하여야 한다. 일반적으로 기록관리 영역의 위험은 회피 혹은 조정의 방식으로 대응하게 된다. 즉 기록관리의 위험은 가능한 한 사전에 발생가능성을 예측하고 미리 대비하여야 하며, 실패할 경우 회복이 어렵고 보험 적용이 안 되는

분야이기 때문이다.

위험 대응의 대안 선택은 먼저 외부 규제와 위험 수준에 따른 위험 대응의 필요성 판단과 비용 및 효과 분석을 통해 이루어지며, 이러한 분석 결과를 토대로 위험 대응의 우선순위를 결정한다. 또한 위험 대응 계획은 수립만큼이나 문서화가 중요하다. 특히 위험 대응의 대안 선택이유와 기대효과, 위험대응의 승인 및 실행 책임자, 실행 계획 및 상황에 따른 자원 배정 요구, 성공기준 및 제약 요인, 보고 및 모니터링 방법 등에 대해 문서화 작업이 필수적이다. 기록관리 표준에서 위험의 대응 전략의 수립은 다음의 표에서와 같이 우선 핵심 고려사항을 토대로 제시하고 있다(〈표 8〉 참조).

〈표 8〉에서 제시된바와 같이 디지털 기록관리 영역의 위험관리는 기록으로 이관된 이후보다는 기록의 생성, 유통 단계에서 고려되어야 할 사항이 누락될 경우에 주로 문제가 발생한다. 업무 영역에서 기록화 되어야 할 기록이 당초부터 생산되지 않거나 보존해야 할 기간보다 일찍 삭제 혹은 폐기 되는 경우가 있을 수 있다. 이는 당초 기록보존의 범위 설정에서 누락되었거나 보존기한이 잘못 설정되는 경우이다. 또한 기록의 품질 요건 측면에서 기록의 생산, 유통과정에서 메타데이터나 기록의 파일 포맷의 표준이나 관리 요건이 미리 제시되지 못한 경우에는 기록의 접근성, 가독성의 문제가 발생하거나 증거력 확보가 미흡할 수 있다. 또한 핵심 업무 영역에서 생산되는 중요 기록에 대한 등급 설정이 잘못되었을 경우 보안상의 문제가 발생한다. 이러한 기록관리 영역의 위험 발생은 기록의 생산, 유통체계의 분석과 해당 업무 영역의 외부조직과의 연관성 분석을 기반으로 설정되어야 한다.

다음은 위험 대응 단계에서 마지막으로 고려할 단계는 위험 모니터링과 피드백이다. 위험요소는 해당 조직의 내부와 외부 환경 변화에 민감하다. 따라서 프로세스에 대한 정기적인 점검과 감시 감독 기능을 운영해야 하며 변경요소를 위험관리 프로세스에 반영하고 위험 통제 전략의 유효성을 검토하여 새로운 프로세스 개선에 반영해야 한다. 이를 위해 기록관리 표준에서는 다음의 〈표 9〉의 항목을 제시하고 있다.

기록관리의 위험 대응 단계로서 모니터링 및 피드백 단계는 업무과정에 기록보존요건이 적용되었는지를 점검하는 과정이다. 또한 처리행위에 대한 문서화와 처리행위간의 순차의 정확성을 파악해야 하며 각 업무과정 간의 연계관

〈표 8〉 위험관리 대응 기록관리 표준: 위험 대응전략 수립 단계

표준 항목	내용 요약	주요목적
KS X ISO 16175-3 (4.3.6항)	- 기록을 작성하지 않는 경우 - 기록이 너무 일찍 처분된 경우 - 지속적인 접근성, 가독성을 확보하지 못한 경우 - 필요한 증거력 확보 수준을 정하고 기록관리의 통제 수준 결정 - 증거력 확보 분야별 요건의 우순순위 결정 - 기록물에 대한 위험요소 등급 정의 - 기록의 생산, 유통체계 분석을 통한 외부조직 관여 정도의 분석과 통제 - 외부 기관과의 공유시스템 정의와 통제요건 및 협약 요건 제시	정당성/ 지식자원 확보

〈표 9〉 위험관리 대응 기록관리 표준: 모니터링 및 피드백 단계

표준 항목	내용 요약	주요목적
KS X ISO TR 26122 (8항)	- 업무과정에 모든 필요한 처리행위 포함 여부 - 처리행위에 대한 문서화 사유와 정확성 검토 - 처리행위의 순차와 각 행위간의 관계의 정확성 - 기능을 구성하는 모든 과정의 식별과 문서화 여부 - 과정 간의 연계관계의 문서화 여부 - 조직의 업무과정상의 맥락기술의 정확성/문서화	정당성/ 지식자원 확보
KS X ISO 16175-3 (3항)	- 기능요건 평가(기록의 관리 범위 및 기능요건의 적절성 평가) - 기능요건의 적절성 점검 - 의무항목의 적절성 점검 - 기능요건 내의 결핍 부분 확인 - 업무시스템의 점검, 평가, 감사 절차와 이행 여부	정당성/ 지식자원 확보

계에 대한 문서화와 조직의 업무과정상의 맥락기술이 정확한지 보아야 한다. 또한 각 기록관리 요건에 대한 적절성을 평가하고 그 결과를 해당 업무 프로세스나 기능 개선 요건으로 제시되어야 한다. 이러한 모니터링과 피드백 절차는 내부적으로 규정으로 명시하여 주기적으로 시행하는 것이 중요하다.

5. 결론 및 제언

기록관리 영역의 위험관리는 업무과정에 대한 요건 반영과 적절한 통제를 통해 향후 기록의 증거력에 기반한 정당성 확보와 지식자원의 축적을 보다 효과적으로 수행하기 위함이다. 정당성 확보는 조직의 업무결과에 대한 책임 유무를 가름하고 지식자원의 축적은 선행 경험의 공유를 통해 후속 업무의 시행착오를 최소화한다. 하지만 오늘날 대부분의 조직에서 위험관리체계는 정보시스템의 IT기술에 의한 단편적 방법론에 치중하고 있다. 조직이 수행한 업무 과정에서 필수적으로 생산되어야 할 기록의 정의와 범위는 설정되어 있는지, 기록의 생산과 유통 단계에서 표준 요건에 따라 작성되고 정상적인 인증 처리가 이루어져 향후 증거력 확보 차원에서 문제는 없는지, 또한 해당 기록의 내용적 가치에 따라 적절한 보안 등급과 보존 기준이 적용되고 있는지에 대해서는 그다지 관심을 두고 있지 않은 것이 현실이다.

따라서 통합 위험관리 체계의 기록관리 요건의 적용에 대한 구체적인 방법론이 필요하며 이를 위해 기록관리표준이 매우 적절한 툴이 될 수 있다. 왜냐 하면 기록관리 표준은 애초부터 기록관리의 위험과 실패를 최소화하고, 궁극적으로 조직의 성과에 기여하는데 목적이 있기 때문이다. 기록관리 표준의 적용은 위험관리표준(ISO 31000)에서 제시하는 프레임워크와 프로세스에 의거하여 각 단계별로 기록관리표준의 항목을 대응함으로써 보다 구체적인 업무 과정에 대한 기록관리 영역의 위험관리 요소를 추출할 수 있고, 위험관리를 보다 체계적으로 수행할 수 있는 틀을 제공해 줄 수 있다.

하지만 현실적으로 기록관리가 부수적 기능이나 요식 행위로 시행되는 한 위험관리체계의

기록관리 요건 적용은 어려울 것이다. 따라서 기록관리에 대한 인식 전환과 제도적 보완이 우선되어야 한다. 따라서 현재 ISO에서 최종 발행을 확정한 기록경영시스템 표준의 시행과 인증제도의 도입 등 다양한 국제 환경의 변화와 그 흐름을 주시하면서 대응해 나가야 한다. 기록관리의 위험관리 프로세스는 궁극적으로 조직의 경영정책과 시스템 구축 전략에 기록관리 요건의 반영이 전제되어야 하기 때문이다. 향후 이에 대한 보다 적극적인 논의와 연구가 진행되기를 기대한다.

참 고 문 헌

국가기록원. 2006.『기록관리 국가 표준 KS X ISO 15489 해설』. 대전: 국가기록원.

김선규. 2010.『건설위험관리』. 서울: 기문당.

김정덕, 이성일. 2001. 정보기술 위험관리 과정과 기법.『정보보호학회지』, 11(3): 16-23.

김형진, 박찬석. 2009. 정보기술아키텍처 도입기관의 IT Governance 유형에 관한 연구.『정보화정책』, 16(1): 22-44.

삼성경제연구소. 2011. CEO가 주목해야 할 4대 리스크.『CEO Information』, 제800호.

성지은, 정병걸, 송위진. 2007. 탈 추격형 기술혁신의 기술위험 관리.『정책연구』, 7(2): 1-21.

양재훈, 정석모 외. 2011. 글로벌 공급사슬의 위험관리요인과 대응방안 연구.『관세학회지』, 12(1): 459-486.

이해영, 김익한 외. 2010. 신뢰성 있는 전자기록리기관 감사인증도구 개발에 관한 연구.『기록학연구』, 25: 3-46.

임진희. 2011. DRAMBORA를 이용한 전자기록 장기보존 업무 위험관리체계 연구.『기록학연구』, 27: 119-168.

정기애, 남영준. 2008. KM기반의 기록관리 및 일반 자료관리 통합화 연구: 공기업을 중심으로,『비블리아학회지』, 19(2): 23-43.

정기애, 김유승. 2009. 공공기록물 관리에 관한 법률 개선 방향에 관한 연구: KS X ISO 15489표준에 입각하여.『정보관리학회지』, 26(1): 231-257.

정기애, 김유승. 2009. 공공기관의 기록관리와 경영품질의 상관성에 관한 연구.『한국문헌정보학회지』, 43(3): 31-58.

정기애. 2010. 기록경영시스템(MSR) 표준 제정에 대비한 기록관리 발전과제에 관한 연구.『한국기록관리학회지』, 10(2): 171-192.

정기애. 2006. 프로젝트 경험기록의 지식자원화 전략 연구,『프로젝트관리기술』, 52: 26-39.

한국정보보호진흥원.『정보보호 위험관리 가이드』. 2004.11. 82p.

Lemieux, V. L. 2004. *Managing Risks for Records and Information*, ARMA International.

Upward, Frank. 1997. *Based on a Diagrammatic Representation of the Records Continuum Developed*. Manash Uni-

versity, 278-281.

Reed, Babra. 2009.『호주의 EDRMS 표준화 현황』. 2009년 기록관리 표준포럼. 대전: 국가기록원.

Shepherd, Elizageth, Yeo, Geoffery. 2003. *Managing Records: A Handbook of Principles and Practice*. London: Facet Punlishing.

Tupenaite, L., and L. Kanapeckiene. 2008. Knowledge Management for Construction Projects, the 8th International Conf. Reliability and Statistics in Transportation and Communication 2008, pp.313-320.

Valerdi, Ricardo, and Ron J. Kohl. 2004. *An Approach to Technology Risk Management*. Engineering Systems Division Symposium. March 29-31, 2004.

Wilson, D. and D. Collier. 2000. "An empirical investigation of the Malcolm Baldrige national quality award causal model." *Decision Sciences*, 31(2): 361-390.

Wimmer, M. A. 2004. Knowledge Management in Electronic Government, 5th IFIP International Working Conference, KMGoV 2004, Krems, Austria, May 2004 Proceedings, p.342.

KS X ISO TR 26122 : 문헌정보-기록을 위한 업무과정 분석. 2008

KS X ISO 16175-3 : 문헌정보-전자사무환경에서 기록에 대한 원리 및 기능요건-제 3부: 업무시스템의 기록관리지침 및 기능 요건. 2010.

KS X ISO 15489-1 제1부: 일반사항. 2007.

KS X ISO 15489-2 제2부: 지침. 2007.

ISO 31000: Risk Management - Principles and Guidelines. 2009.

ISO 30301: Information and Documentation - Management System for Records - Requirements. 2011.