논문

DRAMBORA[1]를 응용한 전자기록 장기보존 업무 위험관리체계 연구

임 진 희*

* 사)한국국가기록연구원 학술연구처장

1) Digital Repository Audit Method Based on Risk Assessment http://www.repositoryaudit.eu/download

[국문초록]

국가기록원을 포함한 우리나라 정부 공공영역의 기록관리 기관들이 공통으로 갖고 있는 전자기록의 장기보존이라는 업무 목표를 달성하기 위해 점검체계로서 위험관리기법을 제시한다. 위험관리기법의 역사와 핵심 개념을 살펴보고, 위험평가에 기반한 자가 점검체계로 개발된 DRAMBORA의 구조와 내용을 살펴본 후, 이를 응용하여 우리나라 정부 공공영역의 기록관리기관이 전자기록 장기보존 업무를 대상으로 위험관리 체계를 만들어 가는 절차와 방법을 제안한다.

기록관리 기관의 업무배경을 정의하는 절차와 방법, 업무를 정의하고 위험요소를 도출하는 절차와 방법, 위험을 평가하는 절차와 방법과 고려사항 등을 DRAMBORA를 응용하여 제시하고 있다.

위험관리기법은 모든 업무영역에서 응용이 가능한 업무품질 향상기법이라 할 수 있으며 DRAMBORA는 전자기록관리 업무를 수행하는 기관이 참조할 만한 업무 점검 프레임워크를 제시하고 있다. 전자기록을 관리하는 기관들이 스스로의 업무 영역과 활동을 정의하고, 업무 영역별 전자기록의 품질 목표를 정의할 수 있다면 이를 기반으로 DRAMBORA의 프레임워크를 응용하여 보다 용이하게 위험관리 기법을 적용할 수 있다.

주제어 : 전자기록, 장기보존, DRAMBORA, 위험관리체계

1. 머리말

우리나라 전자정부 수준은 세계 최고 수준이다. 2010년 UN 전자정부 평가 항목 중 전자정부 준비지수, 온라인 참여지수 등에서 우리나라는 여러 선진국들을 제치고 1위를 차지했다[2]. 한편, 우리나라 정부는 '페이퍼리스 코리아'를 목표로 현재 30% 수준의 전자문서 사용비율을 2015년까지 50%로 확대할 계획이다[3]. 이처럼 정부 공공영역을 중심으로 기록정보의 생산과 유통, 관리 및 활용이 가속적으로 디지털화됨에 따라 기록관리 기관들은 전자기록을 진본인 상태로 이관받아 안정적으로 장기보존해야 하는 중요한 핵심과제에 직면하고 있다. 여기서 장기(long-term)이라는 것은 ISO14721[4]에서 정의하듯이 기술의 변화로 인해 영향을 받을 만한 시간의 간격을 말하는 것으로, 새로운 매체와 데이터 포맷의 출현이나 사용자 집단이 변화할 만한 시간의 개념이다. 현행 공공기록물관리법령에 따르면, 정부공공기관에서 생산한 장기보존 대상 전자기록은 1년 내지 2년 내에 기록관으로 이관하고, 기록관에서 7년 내에 영구기록물관리기관으로 이관하여 관리하도록 되어 있다. 따라서, 국가기록원을 포함한 영구기록물관리기관은 전자기록의 장기보존을 핵심 과제로 부여받고 있다. 뿐만아니라 IT의 발전속도와 전자기록의 존재적 취약성을 감안할 때 기록관 역시 전자기록의 장기보존 능력을 갖추는 것이 필수적이라 할 수 있다. 기록관에서 관리 중

2) 디지털타임스 2010년 1월 15일자 기사,
http://www.dt.co.kr/contents.html?article_no=2010011502010351745001
3) 디지털타임스 2010년 12월 5일자 기사,
http://www.dt.co.kr/contents.html?article_no=2010120602010151614002
4) CCSDS 650.0-B-1 1.Introduction 참조

인 전자기록이 품질을 제대로 유지하다가 영구기록물 관리기관으로 이관되는 것이 장기보존을 효과적으로 하는 첫 관문이 되는 만큼 우리나라 정부 공공영역의 기록관리 기관은 모두 전자기록의 장기보존이라는 공통의 목표를 갖고 있다고 볼 수 있다.

전자기록의 장기보존이라는 목표를 달성하기 위해서 기록관리 기관들은 목표 달성을 위해 필수적인 업무기능을 설계하고, 각 기능별로 전문 인력을 배치하며, 정보시스템을 고도화하는 등의 필요 조치를 취하여야 한다. 한편으로는 이러한 조치들이 목표 달성에 효과성을 보이고 있는지를 스스로 점검하는 체계를 갖추어야 한다. 이 논문에서는 전자기록의 장기보존 책무를 지닌 기관들이 관련 업무를 제대로 수행하여 원하는 목표를 잘 달성하고 있는지를 스스로 점검할 수 있는 체계로 위험관리기법을 제시하고자 한다. 정부 공공기관의 업무 평가를 위한 지표는 BSC 도입을 통해 상당한 수준으로 발전해가고 있다. 내부 업무프로세스 관점에서 업무의 효과성과 품질을 향상시키기 위해서는 상세한 업무 점검체계가 필요하다. 위험관리기법은 이러한 업무 점검체계의 방법론으로 유용성을 갖는다. 내부 업무활동의 목표가 달성되지 않을 경우 조직의 임부와 목표가 달성되지 않는다는 점을 반영하여, 목표 달성에 필요한 자원(resource)과 활동(activity)이 불충분하거나 결핍되는 경우를 조직의 위험요소로 도출하고, 각 위험요소 별로 관련 업무활동의 수준을 점검·평가하여 위험도라는 일관된 지표로 정량화하며, 주기적인 위험평가를 통해 업무의 발전과정을 점검할 수 있기 때문이다. 이 논문에서는 먼저 위험관리기법의 역사와 핵심 개념을 살펴보고, 위험평가에 기반한 자가 점검체계로 개발된 DRAMBORA의 구조와 내용을 살펴보고, 이를 응용하여 우리나라 정부 공공영역의 기록관리기관이 전자기록 장기보존 업무를 대상으로 위험

관리 체계를 만들어 가는 절차와 방법을 제안하고자 한다.[5]

2. 위험관리기법의 특징

2.1 위험관리기법의 등장과 확산

김종호[6]에 따르면 초기의 위험관리는 기업이 자금조달 및 투자 등의 업무 수행과정에서 분산투자나 금융상품을 이용하여 재무적 불확실성을 제거하기 위한 목적으로 주로 활용되어 왔다. 이후 기업 경영 환경이 글로벌화, 시스템화, 분권화, 금융화됨에 따라 정치, 경제, 사회, 기술 영역의 불확실성(Uncertainty)이 기업의 경영 활동에 미치는 직간접적인 영향이 커지면서 불확실성을 대상으로 한 위험관리가 주류를 이루게 되었다.

미국의 경우 1970년대 이후 변동금리제도와 변동환율제 도입에 따라 금융시장이 변화하고 금융기관이 부담해야 할 시장위험과 신용위험이 급격히 증가하게 되면서 위험관리가 중요 이슈로 자리 잡게 되었다. 1980년대 이후 저축대출은행(Saving and Loans)의 파산으로 시장위험관리의 중요성 새롭게 인식되었으며, 1978년에서 1982년 사이에는 금리 상승으로 장기대출의 시장가치가 큰 폭으로 하락하면서 시장위험의 효과적인 관리를 위해 새로운 위험관리기법들이 개발되었다.[7] 1987년 10월 19일 블랙

5) 이 논문은 2010년 국가기록원 발주로 수행한 "전자기록물 장기보존 위험관리 방안 연구용역" 과정에서 취득한 발상을 정리한 것이며, 연구용역의 결과는 추후 별도의 연구 논문으로 발표될 예정임

6)「위험관리, 어떻게 할 것인가」, LG경제연구원, 김종호, 2003

7)『위험관리론』, 오세경 외, 경문사, 1999 참조

먼데이[8] 사건은 미국 뿐 아니라 전 세계에 영향을 미치면서 변동 시장의 내재적 위험에 대한 관리의 필요성을 절감하게 되고 같은 해 물리학자이자 시스템 방법론 박사인 Dr. Vernon Grose가 위험평가와 위험관리 분야의 기본 지침서가 된『Managing Risk: Systematic Loss Prevention for Executives』를 발간하였다. 1993년 GE 캐피탈의 James Lam가 위험관리담당자인 "Chief Risk Officer[9]" 개념을 제시하여 위험관리를 위한 정책개발과 전문 인력 및 프레임워크 개발의 중요성을 확인하였다. 2000년 Y2K버그[10]와 2001년 9.11 테러[11] 및 엔론사 파산 사건[12] 등을 통해 위험관리방법론의 필요성에 대한 인식이 확산되었다.[13]

우리나라의 경우는 1990년 5개 시중 은행을 중심으로 자산과 부채의 종합관리를 위해 ALM(Asset Liability Management, 자산부채종합관리) 위원회를 설치・운영하면서 금융산업을 중심으로 위험관리가 본격 도입되었다. 초기의 위험관리는 기업의 재무적 측면이나 인사, 감사 등 개별 활동으로 국한되었으나, 현재는

---

8) 1987년 10월 19일(월요일) 뉴욕증권시장에서 일어났던 주가 대폭락 사건. (네이버 백과사전)

9) 최고 위기 관리자(最高危機管理者, Chief Risk Officer, CRO)는 잠재적인 경영위험을 파악, 측정하고 이에 대한 계획을 세워 관리하는 기업의 임원을 말한다. (위키백과)

10) 밀레니엄 버그. 컴퓨터가 2000년 이후의 연도를 제대로 인식하지 못하는 결함. (네이버 용어사전)

11) 미국대폭발테러사건 [美國大爆發—事件]: 2001년 9월 11일 발생한 미국 뉴욕의 110층 세계무역센터(WTC) 쌍둥이 빌딩과 워싱턴의 국방부 건물에 대한 항공기 동시 다발 자살테러 사건.(네이버 백과사전)

12) 내부 고발자에 의해 회계부정 사실이 드러난 엔론사의 기업범죄 사건으로 2001년 이중장부를 작성하고 4년간 15억 달러(약 1조 4182억 5000만원) 정도를 분식 회계한 사실이 발각되면서 파산했다. 엔론사는 미국의 에너지회사로 2007년 'Enron Creditors Recovery Corporation'으로 사명을 변경했다.

13) http://www.wepapers.com/Papers/50209/A_Short_History_of__Risk_Management-_1900_to_2002 참조

기업의 운영 목적과 목표 및 전략 계획을 위협하는 다양한 위험을 통합적으로 인식하고 효과적으로 대응 및 관리하기 위한 체계로 발전하고 있다. 위험관리는 이제 기업 경영의 필수 요소로 자리 잡아 가고 있다. 과거 위험관리가 단순히 위험을 회피하고 제거하려던 소극적인 활동이었다면, 최근에는 위험이 조직의 업무 활동이나 자산 및 이익 창출과 갖는 상관관계를 파악하는 등 이를 적극적 관리 대상으로 인식하게 된 것이다. 한편으로는 위험관리를 위한 프로세스를 정의하고 이를 지원하는 정보시스템도 함께 발전하고 있다.[14)]

최대수[15)]에 따르면 이러한 위험관리는 기업의 경영 측면뿐 아니라 생명공학, 정보보안과 기술, 보험 등의 다양한 분야에 적용되고 있다. IT 분야에서는 각종 사이버 침해사고와 더불어 예방활동의 중요성이 강조되면서 위험관리를 자동화하는 시스템에 관심이 모아지고 있다. 국내에는 2000년도 초반에 통합보안관리시스템(Enterprise Security Management, ESM)이 보안관제의 위험관리 솔루션으로 도입되었으며, 사이버 침해사고가 발생하기 전 조기에 위협정보를 경보해 주는 위협관리시스템(Threat Management System, TMS)이 발전하였다. 최근에는 정보시스템과 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해 정보시스템의 취약점을 인식하고 이로 인해 예상되는 손실을 분석하는 기능을 포괄하는 위험관리 종합 시스템이 개발되고 있다.

이러한 위험관리기법은 2009년 ISO 국제 표준으로 제정되었다. ISO 31000에서는 위험관리를 위한 여러 활동 가운데 위험평

14) 「위험관리, 어떻게 할 것인가」, LG경제연구원, 김종호, 2003

15) 최대수, 「자동화된 IT 위험관리시스템으로 비즈니스 연속성 보장: 수동적 모니터링에서 능동적 예방・대응으로」, 『Network times』, 통권165호, 2007, pp.226-229참조

가(Risk Assessment) 절차를 [그림 1]과 같이 위험 /식별정의(Risk Identification), 위험 분석(Risk Analysis), 위험 평가(Risk Evaluation)의 3가지 단계로 제시하고 있다.[16]

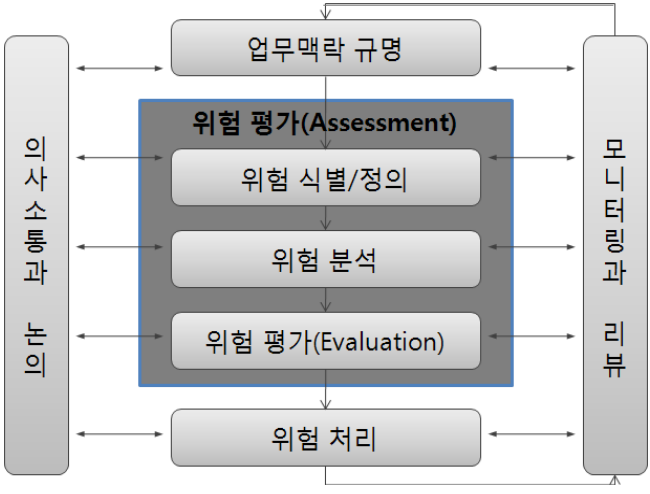


그림 1. ISO 31000:2009의 위험평가 절차

위험관리와 연관된 개념으로 업무연속성계획(Business Continuity Plan, BCP)이 있다. 강희조[17]는BCP는 위험관리 영역의 일부이며, 각종 재해・재난으로 인한 비상사태 발생 시 조직의 핵심 업무를 지속하고 적정시간 안에 업무의 한 주기를 회복하기 위해 실행되는 것이 BCP라고 하였다. 기존의 BCP가 재해발생시 전통적인 전산 복구업무와 기술 중심의 IT관점에서 접근했던 것에 비

16) 「ISO 31000:2009, Risk management - Principles and guidelines」, 2009, pp14 참조
17) 강희조, 「업무연속성계획(BCP)관점에서 위기관리통합체계 구축 시리즈」, 2010년 10월 8일자 etNews 신문기사, http://www.etnews.co.kr/news/detail.html?id=201010070198

해, 급격한 기술변화로 잠재적인 위험이 증가하고 테러 및 국제 분쟁, 불규칙한 일기변화와 이상기후 등 환경 위험의 노출로 인해 업무환경의 취약성이 날로 증가하는 추세에 따라 전사적 관점의 접근으로 바뀌어 가고 있다. BCP 솔루션은 전문 컨설팅 업체를 통해 도입되는 것이 일반적이다.[18]

2.2 디지털자원 및 전자기록에 대한 위험관리 사례

디지털 자원과 전자기록 관리 분야에서도 점차 위험관리기법의 필요성이 대두되고 있으며 위험관리 기법을 적용한 몇 가지 사례를 살펴보면 다음과 같다.

코넬대학은 위험관리기법을 적용한 프리즘 프로젝트를 진행하였다. 웹 자원을 보존하는 과정에서 발생 가능한 위험의 성격을 파악하고 자동화된 점검 기능을 설계하는 한편 위험 정도를 평가하는 프로그램을 개발하였다. 일반적인 위험관리 단계가 위험의 식별, 유형화, 평가, 분석, 관리로 구성된다면 프리즘은 데이터 수집과 정의, 위험에 대한 정의와 진단, 상호 관련된 위험의 정의와 진단 및 자동화된 보존 정책의 실행이라는 4단계로 구성된 위험관리 기법을 적용한 점이 특징적이다.[19]

콜롬비아 대학의 국제 지구 과학 정보 네트워크 센터(Center for International Earth Science Information Network, CIESIN)는 수십 년간

18) LIG엔설팅의 'PRISM', (주)엘림티엔씨의 'eBCMS' 등이 있다. 'eBCMS'는 2009년부터 정부통합전산센터에서 재난대비 및 재해복구를 위한 운영체계 구축 및 상황운용과 유지보수에 도입되어 사용되고 있으며, 'PRISM'은 2010년 국가기록원의 재난 및 재해복구와 위험관리를 위해 도입되어 사용중이다.

19) Anne R. Kenney,「Preservation Risk Management for Web Resources _ Virtual Remote Control in Cornell's Project Prism」,『D-Lib magazine』,Volume 8 Number 1, 2002

의 누적된 전자적 공간정보 데이터와 관련 기술정보를 관리하고 있다. 이 정보는 정부의 세금 징수, 자원관리, 공중안전, 공중위생 등과 관련된 업무의 수행에 있어 중요한 정보일 뿐 아니라 역사적, 잠재적 가치도 지니고 있는 것으로 평가되고 있다. 센터는 위험관리기법을 활용하여 이러한 정보가 제대로 관리되지 않아 접근과 활용이 어려워지는 위험이 발생하는 것을 방지하고 있다.[20]

미국립인문재단(National endowment for the humanities)과 미의회도서관(National Congress, LC)은 2006년 National Digital Newspaper Program(이하 NDNP) 팀을 구성하여 캘리포니아, 플로리다, 켄터키, 뉴욕, 유타, 버지니아, 콜롬비아에서 1900년에서 1910년 사이에 발행된 역사적으로 중요한 가치를 지니는 공공신문을 디지털화하고 공동 이용할 수 있도록 하는 한편 장기보존하기 위해 'Chronicling America'[21]라는 웹 사이트를 개발하였다. NDNP팀은 위험관리 기법을 적용하여 'Chronicling America' 웹 페이지 개발 및 베타버전 운영과정에서 경험한 위험을 유형화 및 분석하고 관리 방안을 마련하여 디지털화한 신문의 접근성과 영구 보존 환경을 구축하였다. NDNP팀이 분석해낸 위험 유형으로는 매체 실패, 하드웨어 실패, 소프트웨어 실패 및 운영 실패가 있다. 이는 Rosenthal[22]이 제시한 디지털 자원의 보존과정에서 발생 가능한 4가지 위험 유형과 동일한 것으로 전송 전후의 파일 비교 및 백업, 다중 하드드라이브 배치 및 RAID 데이터 손실 방지를 위한 핫 스페어(Hot Spare) 설정 등의 방법을 통해 위험을 감소시키거

20) 「Guide to managing geospatial electronic records」, CIESIN, 2005

21) http://chroniclingamerica.loc.gov/

22) Rosenthal, David S. H., Thomas Robertson, Tom Lipkis, Vicky Reich, Seth Morabito. Requirements for Digital Preservation Systems: A Bottom-Up Approach. D-Lib Magazine. <doi:10.1045/november2005-rosenthal>.

나 예방할 수 있었다.[23]

서은경[24]은 대학도서관 디지털 정보자원의 안정성과 기능성을 최대한 확보, 유지하는 차원에서 보존 전략을 강구하기 위해 위험분석을 실시하였다. 대학도서관 별로 대표적인 디지털 정보자원 보존기술인 매체 재생, 매체 변환, 포맷 변환, 정보 전환, 에뮬레이션 등이 사용되는 정도를 조사하고, 대학도서관 디지털 정보관리 담당자들이 각각의 보존 기술에 대해 인지하고 있는 위험가능성과 위험영향력을 조사하였다.

이미화[25]는 디지털 아카이빙 실행을 위한 위험관리의 필요성을 인식하여 국내에서 위험관리의 실행을 위한 방안을 제안하였다. 먼저 위험을 줄이기 위한 방안을 모색하기 위해 OCLC와 코넬대학 도서관의 사례를 조사하고, 이를 바탕으로 위험관리 요소 규명, 파일 포맷과 마이그레이션 프로그램 등의 실험 테스트, 위험관리 수행 전담기구 설립을 제안하였다.

이 밖에도 디지털자원 혹은 전자기록 관리에 위험관리기법의 필요성과 유용성을 제기한 사례는 다수 발견할 수 있는데 이 중 한 두가지를 살펴보면 다음과 같다.

유네스코는 '디지털 유산의 보존을 위한 헌장(Charter on the preservation of the digital heritage)'을 통해 인류 문화적 가치를 갖는 지적 표현물로써 다양한 영역에서 생산된 디지털 자원(텍스트 파일, 데이터베이스, 고정 및 동적 이미지, 오디오, 그래픽, 소프트웨어, 웹 페이지, 포맷 등)의 영속성을 유지・보존할 것을 선

23) Littman, Justin, 「Actualized Preservation Threats : Practical Lessons from Chronicling America」, 『D-Lib Magazine』, Volme13 Number7/8, 2007

24) 서은경, 「디지털 정보자원 보존의 위험관리 분석: 대학도서관 전자정보실 중심으로」, 『정보관리학회지』 Vol.20, No.1 ,2003, pp5-29 참조

25) 이미화, 「디지털 자원의 위험관리 사례연구」, 『정보관리연구』 제37권 제1호, ,2006, pp131-148 참조

언하였다. 이를 위해 디지털 정보를 라이프 사이클 내에서 진본성을 유지시킬 수 있는 법적, 기술적 프레임 워크를 사용하여 의도적 변경을 방지하기 위한 위험관리가 필요함을 역설하였다.[26]

영국의 박물관과 도서관, 아카이브즈를 위한 국립개발 에이전시인 MLA(Museums, Libraries and Archives Council)는 디지털 자원의 장기보존을 위한 박물관과 도서관 및 아카이비즈의 공동의 인식 제고와 해결 방안 모색을 위해 2004년 12월부터 2005년 3월까지 설문조사를 실시하였다. 조사 결과 디지털 자원의 장기보존을 위해서는 명확한 보존 프로세스와 전략적 사고 및 계획이 수반되어야 하며, 저장된 디지털 자원의 광범위한 손실 위험에 대비하기 위한 위험관리가 필요함을 확인하였다.[27]

2.3 시사점

디지털 정보의 관리 분야에서 위험관리는 도서관 및 박물관을 중심으로 다양한 영역에서 방법론이 구축・활용되어왔으며 기록관리 분야의 전자기록의 장기보존을 측면에서의 위험관리 기법의 적용은 아직 초기단계이다[28]. 전자기록의 생산과 활용이 일반화되고 있는 현 시점에서 전자기록의 진본성과 이해가능성을 보장하기 위해 전자기록의 장기보존을 임무로 갖고 있는 조

26) 「Charter on the Preservation of Digital Heritage」, UNESCO, 2003

27) 「Digital preservation in the regions」, MLA, 2005

28) 국가기록원은 BCP/DR(Business Continuity Planning/Disaster Recovery, 업무연속성 계획/재난복구)차원에서 2008년 "전자기록관리 재난복구체계 표준모델 연구"를 수행하였으며, 전자기록 관리에 관련하여 자연적 재해 3가지, 기술적 재해 5가지, 인적 재해 4가지 등 총 12가지의 위협요소를 정의하였다. 또한, 2010년에는 DRAMBORA기반의 위험관리기법을 적용하여 전자기록물 장기보존 업무와 관련된 위험요소 44개를 도출하여 자체 평가, 분석하였다.

직이 업무 전체 차원의 표면적·내재적 위험요소를 확인하고 평가, 분석하여 예방·통제·관리 업무를 수행하는 것은 필수적이라 할 수 있다.

앞에서 살펴본 디지털자원 및 전자기록 관련 위험관리 대상의 유형을 종합해 보면 표3과 같다.

연구자	관리 대상 위험의 유형
서은경	콘텐츠에 직접적 손실을 입히는 위험 요인, 시스템 환경변경으로 발생되는 위험 요인, 행정적 지원 부족으로 발생되는 위험 요인
Gregory W. Lawrence	파일 포맷의 조사를 통해 콘텐츠 불변, 보안, 맥락과 무결성, 참조, 비용, 직원, 업무 기능 및 법률(저작권 등)
Johe C. Bennett	디지털 자원, 포맷, 매체
Gerard Clifton	디지털 자원, 데이터, 파일, 포맷, 프로세스, 내외부요인
Arms, Caroline R.[29]	기반 시설 위험, 파일 포맷 위험, 변환 프로세스 위험

표 1. 디지털 자원과 관련된 위험의 유형

서은경[30]은 대학도서관에서 수행하고 있는 디지털 보전방법에 대한 위험평가를 실시하기 위해 각 방법이 지닌 위험요인과 가능성 분야를 문헌조사를 통해 수집하였다. 그 결과 위험의 유형을 콘텐츠에 직접적 손실을 입히는 요인, 시스템 환경변경으로 발생되는 위험요인, 행정적 지원 부족으로 발생되는 위험요인으로 범주화 하였다. Gregory W. Lawrence[31]는 파일 포맷의 조사

29) 「Risk Management of Digital Information: A File Foramt 」, 『RLG DigiNews』, Arms, Caroline R.. 2000

30) 서은경, 「디지털 정보자원 보존의 위험관리 분석: 대학도서관 전자정보실 중심으로」, 『정보관리학회지』 Vol.20, No.1 p14, 2003

31) 「Risk Management of Digital Information: A File Format Investigation」, Gregory W. Lawrence, William R, Kehoe 외 공저, 2000

를 통해 디지털 정보의 관리과정에서 확인할 수 있는 위험의 유형을 콘텐츠 불변, 보안, 맥락과 무결성, 참조, 비용, 직원, 업무 기능 및 법률(저작권 등)의 8가지 분야로 범주화 하였다.

Johe C Bennett[32]은 디지털 자원의 장기보존 관점에서 위험 유형을 디지털 자원, 포맷, 매체로 범주화 하였다. Gerard Clifton[33]는 디지털 자원의 보존과 관련된 위험이 디지털 자원 그 자체와 프로세스, 조직 내·외부 요인 및 프로세스 상에서 발생하며, 좀 더 넓은 의미에서 매체, 데이터와 파일, 포맷, 조직 내·외부 요인 및 컬렉션 단위의 디지털 자원과 관련된 요인으로 위험의 유형을 범주화 할 수 있다고 하였다.

이상에서 살펴본 바와 같이 선행연구는 대부분 발생 원인이 조직의 내부에 있는지 외부에 있는지를 중심으로 위험요소를 제시하거나, 중요 자산을 중심으로 위협이 되는 요소를 제시하고 있다. 이 과정에서 위험요소의 도출하는 과정을 세밀하게 설계하기 보다는 연구자나 실무자가 중점적으로 들여다보고 싶은 대상을 위험요소로 결정한 후 해당 위험의 발생가능성과 영향도를 평가하는 방식을 취하고 있다. 이 논문에서는 위험관리기법을 채택하여 업무를 점검하는 체계를 제시하고자 하며, 특히 위험요소를 도출하고 확인하는 과정, 평가하는 과정 등을 보다 정밀하게 설계하여 제시하는 것에 목적을 두고 있다. 이를 통해 신뢰성있는 점검 수행이 가능해 지며, 반복적인 점검과정에서 업무의 개선이 보장될 수 있을 것이다.

---

32) 「A FRAMEWORK OF DATA TYPES AND FORMATS, AND ISSUES AFFECTING THE LONG TERM PRESERVATION OF DIGITAL MATERIAL」, Johe C. Bennett, 1997

33) 「Risk and the Preservation Management of Digital Collections」, 『International Preservation New』, No. 36, 2005, p21-23

3. DRAMBORA프레임워크의 구조와 내용

이 장에서는 전자기록 관리기관이 장기보존이라는 목표 달성을 위해 업무를 점검하는 체계에 참조할 목적으로 DRAMBORA의 구조를 살펴보자 한다[34].

3.1 DRAMBORA의 구조

DRAMBORA는 DCC(Digital Curation Center)[35]와 DPE(Digital Preservation Europe)[36]가 '위험평가에 기초한 디지털 저장소 감사 방법'으로 공동 작성한 것이다. 기관이 디지털객체의 장기보존에 적합한 기관인지 여부를 스스로 감사하고 인증하는 도구로 개발된 것이다. 이 도구를 이용하여 디지털 저장소는 자체 감사를 위해 기관의 기능과 의무, 업무활동과 중요 자산을 정의하고, 이와 관련된 위험요소들을 찾아내어 평가·측정함으로써 현재의 업무 수준을 평가한다. 위험도가 높은 위험요소를 적절히 관리함으로써 기관의 업무 수준을 향상시킬 수 있다.

DRAMBORA는 현재 우리나라 국가기록원 뿐만 아니라 영국의 British Library, 스코틀랜드 국립보존소, 체코 국립보존소, 이탈리아 플로란스 국립 도서관 등 여러 다양한 기관에서 참조 활용되고 있다[37].

DRAMBORA는 [표 4][38]과 같이 총 3개의 장과 4개의 부록으로

34) 이 논문에서는 2007년 2월 28일 출시된 버전 1.0을 참조하고 있음
35) DCC(Digital Curation Centre), http://www.dcc.ac.uk/
36) DPE(Digital Preservation Europe), http://www.digitalpreservationeurope.eu/
37) http://www.repositoryaudit.eu/users/
38) 정준용, 디지털 저장소의 신뢰가치 제고에 관한 연구, 명지대학교 석사학위논

구성되어 있다.

구분	내용
PART Ⅰ 감사방법에 대한 배경지식	저장소라는 개념, 위험관리 기반의 감사 접근에 대한 발상, DRAMBORA 도구 제작을 위한 사전 연구에 대해 소개한다.
PART Ⅱ DCC/DPE의 감사도구	감사 프로세스를 구체화하고 감사의 6단계를 설명한다.
PART Ⅲ 결론 및 향후과정	더 정련된 감사도구 개발을 위한 설명과 그러한 도구 개발 프로세스 참여에 대한 공동체의 요구에 대해 설명한다.
부록 1 감사의 글	DRAMBORA 도구 개발을 위해 다양한 유형의 저장소가 서로 다른 환경에서의 성공적으로 감사 프로세스를 수행하는 방법에 대한 공동체의 공헌에 대해 설명한다.
부록 2 자체감사도구 템플릿	자체감사 수행 프로세스를 지원하는 템플릿을 통합하여 보여준다.
부록 3 저장소의 위험요소에 대한 설명예시	저장소에 존재할 수 있는 위험의 위험등록부 예시를 제공한다.
부록 4 감사보고서의 구조	유용하게 쓰일 수 있는 감사 보고서의 예시를 제공한다.

표 2. DRAMBORA 구성 내용

본문인 PART I에서는 DRAMBORA가 개발된 배경이나 감사방법을 이해하기 위한 배경 설명이 제시되고 있으며, PART II에서는 자체감사 및 인증 도구의 핵심이 되는 절차와 방법이 제시되어 있고, PART III에서는 도구의 유용성과 향후 발전 방향이 제시되어 있다. 부록은 감사의 글, 자체감사도구 템플릿, 저장소의 위험요소에 대한 설명예시 및 감사보고서의 구조로 구성되어 있는데, 실제 적용을 위한 템플릿과 예상되는 일반적인 위험요소 78개에 대한 목록이 포함되어 있다.[39]

문, 2008 p81 인용

DCC와 DPE는 본문과 부록 이외에 DRAMBORA 활용의 이점을 설명하고 DRAMBORA가 제공하는 Toolkit의 설계, 개발, 평가 및 정련 측면에서의 적절한 활용을 지원하기 위해 별도의 설명 자료도 제작하였으며 런던, 버지니아, 헤이그에서 교육을 갖기도 하였다.

3.2 DRAMBORA의 위험관리 프레임워크[40]

DRAMBORA는 위험관리기법을 기반으로 하여 [그림 2]와 같이 6단계로 구성된 위험관리 프로세스와 각 단계 별로 수행해야 할 10개의 세부 태스크를 제시하고 있다.

첫 번째 '업무 배경 확인' 단계에서는 디지털 저장소의 의무와 조직의 목표와 목적을 확인함으로써 위험분석의 범위를 설정한다. 그리고, 기관의 사명이나 비전, 법적 의무를 상술하고 목표와 목적을 목록화한다.

두 번째 '정책과 규정 프레임워크의 문서화' 단계에서는 먼저 감사자가 계약 및 법률 담당자를 통해 증빙자료 및 참조자료 등 주요 문서를 획득한다. 이를 토대로 목표 수행을 위한 전략 계획을 문서화하고, 기관이 준수해야 하는 법령이나 계약서, 동의서 등을 목록화하며, 기관이 자발적으로 동의하여 활용하거나 참조하는 규정들을 목록화한다.

---

39) 「(국제모범기준과의 격차분석에 기반한)대통령기록관의 디지털 아카이브 발전전략 연구」, 국가기록원 대통령기록관, 2008, p65

40) DRAMBORA의 원문과 「(국제모범기준과의 격차분석에 기반한)대통령기록관의 디지털 아카이브 발전전략 연구」, 국가기록원 대통령기록관, 2008, p69-75을 참조하여 요약함

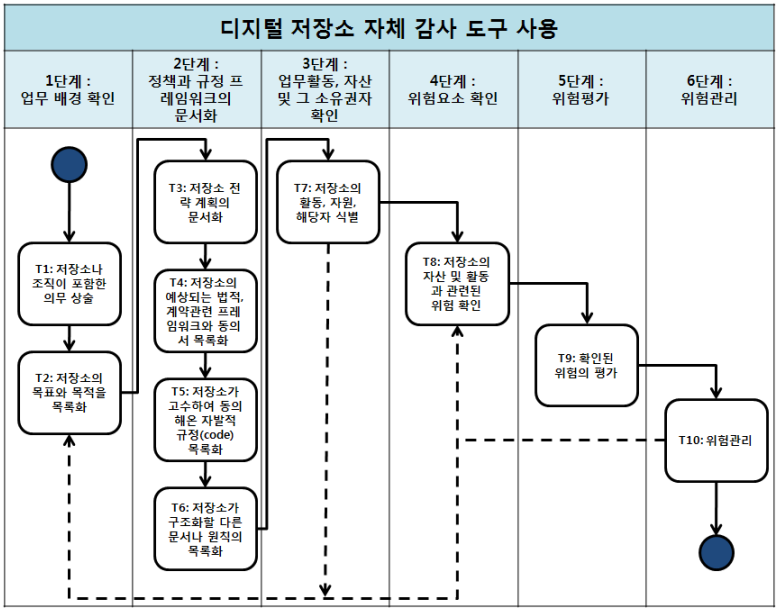


그림 2. DRAMBORA 위험관리 프로세스

세 번째 '업무활동, 자산 및 그 소유권자 확인' 단계는 감사 수행자가 조직에 대한 전반적인 지식을 갖추고 위험을 식별하기 위한 기초 자료를 확보하는 단계이다. 기관의 주요 자산인 직원, 핵심기술, 핵심자산, 업무프로세스와 활동을 조사한다. DRAMBORA는 디지털 저장소가 수행하는 업무기능을 [표 5]와 같이 크게 지원기능과 운영기능으로 구분하여 총 8개의 기능(Functional Class)을 정의하고 있다. 기능 하위에는 52개의 업무활동(Activities)을 정의하고 있다[부록1 참조]. 기능별로 업무활동과 관련된 자산을 확인함으로써 업무 활동의 영속성을 위협하고 자산 손실을 초래할 수 있는 모든 위험요소를 확인할 수 있도록 준비한다.

지원 기능 (Supporting Functional Class)	운영 기능 (Operational Functional Class)
조직 관리 (Organization Management)	획득 및 입수 (Acquisition & Ingest)
직원 (Staffing)	보존 및 저장 (Preservation & Storage)
재정 관리 (Financial Management)	메타데이터 관리 (Metadata Management)
기술 인프라 및 보안 (Technology Infrastructure & Security)	접근 및 배부 (Access & Dissemination)

표 3. DRAMBORA가 정의한 기능

네 번째 '위험요소 확인' 단계에서는 디지털 저장소가 당면한 위험을 찾아내어 업무활동과 자산으로 범주화하여 목록화한다. 위험요소별로 정의, 유형, 책임자, 다른 위험과의 관계 등에 대해 기술해 준다. DRAMBORA는 8개의 기능별로 총 78개의 위험요소 목록을 제시하고 있다(부록2 참조).

다섯 번째 '위험평가' 단계에서는 앞 단계에서 확인한 위험이 어떤 속성을 갖고 있는지 파악하고 위험별 중요도, 위험의 발생가능성, 위험정도 등을 수치로 평가한다. 이 때, 위험의 방지와 처리를 위한 법적, 시스템적 도구나 위험에 대한 정보를 담고 있는 조직 내외부의 다양한 문건을 증빙으로 확보하여 객관적이고 정확한 평가가 이루어 질 수 있도록 해야 한다. DRAMBORA에서는 위험의 발생가능성과 발생 시의 영향도를 측정한 후 두 측정치를 곱하여 위험도를 산출하는 방식으로 평가한다.

여섯 번째 마지막 '위험관리' 단계로 확인된 위험을 적절하게 관리하는 단계이다. 위험관리와 관련된 모든 내용을 포함하여

위험등록부를 작성하고, 조직이 수용할 수 있는 위험관리계획을 수립한다. 위험 예방조치와 위험발생 후 조치 등 상황별 관리방법을 설계한다.

3.3 시사점

위험관리기법을 채택했을 때 핵심성공요인은 위험요소를 실천적으로 의미있게 도출하는 것이라 볼 수 있다. 왜냐하면,. 위험요소가 해당 조직과 업무의 목적에 맞춰 제대로 도출되었을 때 이후의 평가가 의미를 가지게 되며 평가 결과에 따른 정책적 대안도 실효를 거둘 수 있기 때문이다. 따라서, 정해진 업무 영역 내에 존재하는 위험요소를 도출하는 과정을 정밀하게 설계하여 집행하는 것이 필요하다. 위험요소를 제대로 도출하기 위해서는 먼저 위험관리기법을 적용하고자 하는 업무 영역에 대해 현재의 업무(AS-IS Business)와 향후 지향하는 업무(TO-BE Business)를 분석하여야 한다. 이 과정에서 단위업무에 대한 정의와 핵심성과지표가 조직적 차원에서 정의되고 공유되어야 한다. 그런데, 일반적으로 업무에 대한 분석 작업은 많은 비용과 노력을 수반한다.

이 논문에서는 DRAMBORA에 기반하여 용이하고 신속하게 전자기록의 장기보존 업무 영역에 존재하는 위험요소를 도출하는 과정을 보여줌으로써 비용과 노력을 절감할 수 있는 방법을 제시하고자 한다. 앞에서 살펴본 바와 같이 DRAMBORA는 디지털 객체를 장기보존하는 디지털 저장소의 업무기능을 정의하고 그에 관련한 위험요소를 도출하는 절차와 방법을 제시하고 있다는 점에서 향후 위험관리 기법을 도입하고자 하는 전자기록 관리기관이 위험관리 프레임워크를 설계하는데 유용한 시사점을

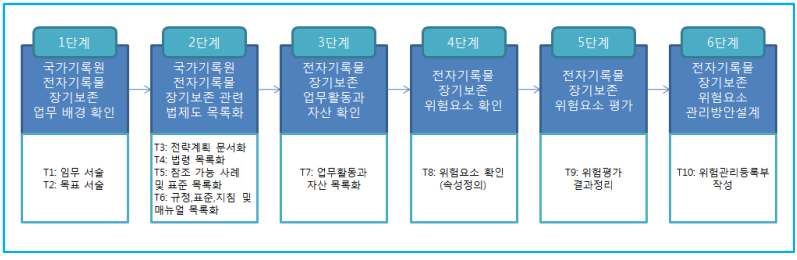
제공한다. 또한, 여러 기관의 위험관리 사례를 기반으로 디지털 객체 장기보존 과정의 위험요소 78개 목록을 제공하고 있어 전자기록 관리기관이 위험요소 도출에 유용하게 참조할 수 있다.

4. 전자기록 장기보존 업무 위험관리 절차와 방법

이 장에서는 DRAMBORA의 프레임워크를 응용하여 전자기록의 장기보존 업무를 수행하는 기록관리 기관이 위험관리기반의 업무 점검체계를 만들어가는 절차와 방법을 제시하고자 한다. 예를 들어, 앞에서 살펴본 DRAMBORA의 6단계 위험관리 프레임워크를 국가기록원의 전자기록 장기보존 업무에 맞춰 맞춤화를 하면 [그림 3]과 같다. DRAMBORA는 다양한 분야의 디지털객체 장기보존소에 적용하여 활용할 수 있는 자체감사도구로 개발되었으며, 주로 계약을 통해 디지털 자원을 수탁 받아 관리하는 기관을 위한 위험관리 프레임워크를 제시하고 있다. 이러한 디지털객체 관리기관이 다루는 관리 대상은 문서기록을 포함하여 웹자원, 데이터세트, 문화유산자원, 예술자료 등 다양한 종류의 디지털 정보를 포괄하고 있다. 그런데, 본 논문에서 대상으로 삼고 있는 정부 공공영역의 기록관리 기관은 계약에 기반한 관계가 아니라 법적 구속력에 따라 기록물을 이관받아 관리하는 기관이라는 기본 특징을 지니고 있다. 관리대상 전자기록물로는 표준전자문서와 비표준전자문서, 데이터세트, 웹기록, 시청각물 등을 관리하고 있으며 향후 공적 내용이 담긴 이메일, 모바일콘텐츠 등도 관리대상으로 포괄해 나갈 예정이다. 기록관리 기관은 다양한 종류의 기록을 이관받아서 단일한 기록분류

체계와 파일링 구조, 처분지침에 따라 일관되게 조직화하여 관리한다. 정부 공공영역의 기록관리 기관이 갖는 이러한 특징을 고려하여 2단계의 태스크를 조정하였다.

각 절에서는 1-5단계의 과정에서 DRAMBORA의 내용을 전자기록의 특성이나 전자기록 관리기관의 특수성을 고려하여 맞춤화하는 방법을 제시하고자 한다.



<그림 3> 전자기록물 장기보존 업무의 위험관리 프레임워크

4.1 기관의 업무 배경 정의 절차와 방법(1-2단계)

전자기록의 장기보존을 위협하는 위험을 제대로 도출하고 평가하여 관리방안을 설계하기 위해서는 DRAMBORA의 1-2단계 과정인 '업무 배경 확인', '정책과 규정 프레임워크의 문서화' 과정이 충실히 선행되어야 한다. 이 과정에서 기관이 무엇을 대상으로 왜, 어떻게 수행해야 하는지에 대한 임무 및 목표가 확인되며, 위험관리 대상 업무의 범위를 설정하게 되고, 대상 업무를 수행할 때 준수해야 하는 법규, 표준, 지침 등 기본 방향과 원칙을 확인할 수 있다. 예를 들어, 국가기록원에 맞춰 변형한 1-2단계는 '전자기록물 장기보존 업무 배경 확인', '전자기록물 장기

보존 관련 법제도 목록화' 이다.

1단계인 '전자기록물 장기보존 업무 배경 확인' 과정에서는 정부 공공영역의 기록관리 기관이 전자기록 관리와 관련하여 어떤 임무와 목표를 갖고 있는지를 문서화한다. 기관의 사명과 비전을 문서화하는 일이 이 단계에 포함되는 작업이다. 예를 들어 국가기록원이라면 홈페이지에 명시된 바와 같이 '세계 일류 기록국가 실현'이 현재 기관의 비전이라 할 수 있을 것이다. 이는 전자기록의 장기보존이라는 업무적 관점에서 볼 때 전자기록의 진본성을 유지하는 기록관리로 신뢰받는 정부를 구현하고 이해가능성을 보장하는 전자기록 관리체계를 위한 선진 인프라를 확충하겠다는 목표로 재해석이 가능할 것이다. 이처럼 기관별로 전자기록 장기보존 업무의 목표를 명확하게 정의하여 문서화하고 공표할 뿐 아니라 목표를 상술하려는 노력이 필요하다.

현재 정부공공기관의 전자기록 장기보존을 위한 업무에서 핵심적인 목표로 삼을 수 있는 것으로 ISO15489를 준용하여 법령에 명시된 전자기록의 진본성, 무결성, 신뢰성, 사용가능성 확보를 들 수 있다. 그런데, 이 네 가지 속성 혹은 기준은 상호배제와 전체포괄(MECE, Mutually Exclusive and Collectively Exhaustive)이 지켜지지 않는데다 각 속성 혹은 기준이 어떤 업무적 필요충분조건을 만족해야 충족되는 것인지에 관해 구체화되고 심화된 연구가 부족하다는 점에서 이를 기록관리 기관의 목표로 잡는데 한계가 있다.

DRAMBORA는 디지털객체의 '진본성(Authenticity)'과 '이해가능성(Understandability)' 확보를 디지털객체 장기보존소의 목표로 제시하고 있다. DRAMBORA가 정의하는 이해가능성은 사용가능성보다 넓은 의미로 기술적인 측면, 맥락의 측면, 문법적 측면, 의미

적 측면 모두를 포괄한다. 즉, 먼 미래에도 해당 디지털객체를 맥락적으로, 문법적으로, 의미적으로 이해할 수 있도록 기술적인 지원이 가능해야 함을 의미한다. 진본성과 이해가능성이라는 두 가지 목표는 ISO15489의 네 가지 기준보다는 MECE한 것으로 이해된다. 전자기록은 디지털 객체의 일종이므로 DRAMBORA의 진본성과 이해가능성이라는 목표를 그대로 수용하는 것도 가능하다고 본다. 다만, 기록은 별도의 구조화 및 관리 원칙을 준수해야 하므로 진본성과 이해가능성을 보장하는 방법이 달라지며, 그 결과 업무과정에 잠재한 위험요소의 성격도 달라짐에 유의해야 할 것이다.

2단계인 '전자기록물 장기보존 관련 법제도 목록화' 과정에서는 1단계에서 명시한 임무와 목표를 달성하기 위해 업무를 수행하는 전략과 방법을 문서화한다. 방법에는 법규, 표준, 지침, 매뉴얼 등 업무의 방향과 방식을 제시하는 다양한 수준의 도구가 포함된다. 이러한 목록화를 통해 업무 구조가 어느 수준에서 어느 정도까지 공식화, 표준화되었는지를 알 수 있다.

첫째, 1단계에서 정의한 목표 수행을 위한 전략 계획을 문서화한다. 예를 들어, 국가기록원의 경우 국가기록관리 선진화전략[41]이 문서화대상이 된다. 국가선진화전략 4대 과제의 세부과제로 '행정정보 데이터세트 및 웹기록의 체계적인 관리'에서 다양한 전자기록물의 획득 및 유지를 위한 인프라 구축 전략을 제시하고 있으며, '전자기록 보존전략 및 재해복구 체계 마련'에서 전자기록물 보존 프로세스와 방법에 대한 세부적인 전략과 3개 서고에 광역분산 및 다중매체 보존체계를 확립하는 전략 등이 제시되고 있다. 둘째, 전자기록물 장기보존 관련 업무환경

41) 「국가기록관리 선진화 전략」(2009), 국가기록원

과 업무활동을 규제하는 다양한 법제도를 목록화한다. 앞서 살펴본 바와 같이 디지털객체 관리기관은 디지털객체의 예치 혹은 위탁자와의 계약관계에 의해 관리업무를 수행하게 되므로 계약서나 업계의 표준 및 규제 등이 주요 대상이 되겠으나, 금전적 계약관계를 기반으로 하지 않는 정부공공영역의 기록관리 기관은 의무와 목표의 직접적 근거가 되는 법규와 국가 및 기관 표준 등이 대상이 될 것이다. 정부 공공영역의 기록관리 기관들을 공통적으로 공공기록물관리법령, 정보공개법령, 개인정보보호법령, 전자정부법령 등의 법규를 기본적으로 목록에 포함해야 한다. 여기에 기관별 업무 특성에 따라 추가적인 법규를 식별하여 목록에 추가한다. 셋째, 전자기록물 장기보존과 관련하여 참조 가능한 국내외 선진 사례와 표준을 목록화한다. 국가기록원이라면 업무 수행과정에서 참조할 사례로서 TRAC[42], 공인전자문서보관소 등을 목록에 포함하고, 기록관리 관련 국제 표준으로서 KSX ISO15489, KSX ISO23081, ISO19005-1:2005 등을 포함할 수 있다. 넷째, 전자기록물 장기보존 관련 지침 및 매뉴얼을 목록화한다. 큰 틀에서 법규와 국가표준을 준수하면서 선진실무 사례를 참조하여 만들어진 상세 업무지침과 규범화된 매뉴얼이 대상이다. 국가기록원이 작성하여 배포하는 각종 기술규격과 SOP(Standard Operating Procedures), 시스템 기능요건 표준들이 여기에 속한다.

42) TRAC(Trustworthy Repositories Audit & Certification: Criteria and Checklist): 미국국립기록청(NARA)과 연구도서관그룹(RLG)이 합동T/F를 구성하여 실행한 사업결과로, 신뢰할 수 있는 디지털아카이브' 인증을 위한 체크리스트. 장기보존을 위하여 디지털아카이브를 설계할 때 사용될 수 있는 도구일 뿐만 아니라, 현재 운영 중인 디지털아카이브가 국제모범기준에 부합하는지 여부를 자가 진단할 수 있는 도구

4.2 업무 정의 및 위험요소 도출 절차와 방법

3단계인 '전자기록물 장기보존 업무활동과 자산 확인' 과정에서는 앞 단계에서 목록화한 자료를 바탕으로 전자기록의 장기보존을 지원하는 업무활동을 세분화하여 정의하고, 각 업무활동에 관련된 중요 자산을 목록화한다. 정상적인 업무활동의 수행이 불가능해지거나 중요 자산이 훼손되는 위험이 발생하는 경우가 발생할 가능성과 그로 인해 조직의 임무와 목표 달성이 어려워지는 정도를 평가하고자 하는 것이 위험관리 방법적인 업무 점검체계이므로 이 단계의 산출은 위험요소 도출을 위한 직접적인 기반이 된다.

조직의 업무활동과 자산을 확인하기 위해서는 현행의 업무활동에 대한 정확한 조사와 분석이 이루어져야 된다. DIRKS 매뉴얼[43]의 A, B, C 단계를 수행하거나 ISO/TR26122:2008[44]를 이용한 기능분석 및 순차분석 기법을 적용할 수 있을 것이다. 그런데, 조직의 업무기능 및 활동을 조사 분석하는 데는 노력과 비용, 그리고 시간이 소요되므로 위험관리방법론을 적용하고자 할 때 최대의 난점으로 부상될 수 있다. 본격적으로 업무분석을 수행할 여건이 조성되지 않을 때 DRAMBORA의 프레임워크를 응용하여 위험요소를 도출할 수 있는 수준에서 업무활동과 자산을 목록화할 수 있다. 방법은 다음과 같다. 먼저, 현재 위험관리기법을 적용하고자 하는 업무 범위에서 업무 기능 및 활동에 관해 정의된 모든 문서를 수집한다. 국가기록원의 경우라면 첫째, 정

43) NAA, 「Designing and Implementing Recordkeeping System: A Manual for Commonwealth Agencies」, 2000. 호주국가기록원에서만든전자적기록관리시스템구축방법론

44) 표준의 제목은 "Information and documentation -- Work process analysis for records" 임.

부업무관리시스템을 사용하므로 BRM시스템에 정의된 업무기능과 단위과제를 수집할 수 있다. 둘째, 정부기관이므로 직제규정에 따른 업무분장 정보를 수집할 수 있다. 셋째, EA(Enterprise Architecture) 프로젝트와 BSC(Balanced Score Card) 프로젝트 과정에서 정의한 업무 정보를 수집할 수 있다. 이처럼 여러 출처에서 수집한 업무 정보를 내용적 유사성을 중심으로 유형화하여 정리한다. 다음으로는 정리된 업무 기능 및 활동을 DRAMBORA가 제시한 8개의 기능, 52개의 업무활동 중 동일한 업무로 매핑을 한다. [표 5]는 우리나라의 대표적 전자기록 관리기관인 국가기록원과 대통령기록관의 직제규정을 보고 전자기록 장기보존 업무영역을 선별한 후 DRAMBORA의 기능과 매핑을 시도한 사례이다.

DRAMBORA 기능	국가기록원 업무기능	대통령기록관 전자기록 관리업무
조직관리	행정지원, 정책기획, 표준협력	운영관리, 분류체계 및 기준정보 관리
직원	행정지원, 기록관리교육	
재정관리	행정지원	운영관리
기술인프라 및 보안	기록정보화	시스템 관리, 접근통제 및 보안, 모니터링・감사증적・통계
획득 및 입수	기록관리(수집, 평가 등)	입수, 등록・기술
보존 및 저장	보존관리, 보존복원	저장, 보존
메타데이터 관리	기록관리, 보존관리	분류체계 및 기준정보 관리
접근 및 배부	기록편찬, 공개서비스	서비스, 검색도구 제공

표 4. DRAMBORA의 기능과 전자기록 관리기관의 업무기능 매핑

기록관리 기관의 핵심 자산은 관리대상 객체들이며 그 중에

서도 기록물 자체이다. 우리나라 공공기관 전자기록 관리기관의 경우 표준 및 비표준 전자문서, 간행물, 시청각기록물, 데이터세트기록, 웹기록, 이메일 및 모바일 콘텐츠 등의 관리 대상 기록물들이 모두 기본 자산으로 목록화되어야 한다. 전자기록을 목록화 과정에서 데이터세트의 DBMS 종속성, 웹기록의 딥링크 특성, 이메일의 메시지 간 연관 특성, 시청각기록의 대용량 특성 등 유형별 특성에 대해 상세히 기술하여 다음 단계에서 잠재적 위험요소를 용이하게 도출할 수 있도록 해야 한다. 또한 여러 유형의 전자기록들을 동일 분류체계와 처분지침 하에 관리할 것인지, 동일한 철과 건의 구조로 구조화시켜 관리할 것인지 여부를 명시함으로써 그에 따른 잠재적 위험요소를 고려할 수 있도록 해아 한다. 관리 대상 객체에는 기록물 자체 외에도 기록관리 과정을 기록화한 각종 문서와 감사증적 데이터, 요약정보, 백업정보, 임시 사본파일, DIP(Dissemination Information Packages) 등 기록관리 과정에 필수적인 다양한 객체가 포함될 수 있다. 특히, 전자기록의 진본성과 이해가능성을 보장하기 위해 필수적인 정보 대상이 빠짐없이 관리 대상으로 목록화되는 것이 중요하다.

기록관리 기관의 또 다른 중요한 자산으로는 전자기록을 관리하는 시스템과 보존매체, 업무담당자 등이 있다. 전자기록은 시스템에 의해 저장, 관리, 활용될 수 있다는 특성에 의해 시스템에 의존적이다. 시스템의 취약성이 전자기록의 장기보존에 위협이 된다는 점에서 시스템은 중요한 자산으로 목록화되어야 한다. 시스템에 대한 프로파일, 설치 및 관리 이력, 매뉴얼, 프로그램 파일 등이 파악될 수 있어야 한다. 국가기록원의 경우 CAMS(Central Archives Management Systems)로 통칭되는 여러 기록관리 정보시스템을 운영하고 있다. 대통령기록관의 경우는

PAMS(Presidential Archives Management Systems)를, 기록관에서는 RMS(Records Management Systems)를 운영하고 있다. 기록관의 경우에는 RMS 외에도 업무관리시스템, 전자문서시스템, 행정정보시스템 등 기록의 생산시스템들이 모두 중요 자산에 포함될 수 있다. 또한, 전자기록은 비트스트림 자체로는 존재할 수 없으며 하드디스크, USB, DVD, WORM 스토리지 등 다양한 매체에 저장되어 존재한다. 전자기록이 저장된 매체가 훼손되면 그 안에 담겨진 전자기록도 위협받게 된다. 따라서 매체 자체도 중요한 자산으로 목록화되어야 한다. 이러한 시스템과 매체를 이용하여 전자기록을 관리하기 위해서는 IT에 관한 지식과 기록관리에 관한 지식이 겸비된 전문적 업무담당자가 필요하다. 전자기록 관리기관에서 업무담당자의 전자기록 장기보존에 관련한 전문성이 부족하거나 인력자체가 부족하다면 그 자체가 전자기록 관리에 위협이 된다. 따라서 업무담당자 인력들도 중요한 자산으로 목록화되어야 한다.

4단계인 '전자기록물 장기보존 위험요소 확인' 과정에서는 앞의 세 단계에서 목록화한 조직의 임무와 목표, 법제도와 업무활동, 자산 등을 참조하여 전자기록 장기보존 업무 과정에서 발생 가능한 표면적・내재적 위험요소를 도출한다. 위험요소를 제대로 도출하기 위해서는 먼저 앞 단계의 과정 산출물을 정확히 이해하는 것이 필요하다. 위험관리 기법을 처음 도입하는 기관에서는 위험요소를 확인하는 일 자체가 모험적인 도전이 될 수 있다. 위험요소를 도출하는 과정에서 내부적인 업무 미숙이 위험요소로 드러나는 것을 우려하여 업무담당자들의 조직적 저항에 직면할 수도 있다.

위험요소 도출의 효과적인 방법 중 하나는 해당 기관의 업무

와 기록을 잘 이해하고 있는 외부전문가와 내부 업무담당자들로 포커스그룹을 구성하여 브레인스토밍을 하는 것이다. 그 과정에서 앞 단계의 과정 산출물이 보완될 수 있으며, 포커스그룹에 참여한 내부 업무담당자들은 도출한 위험요소의 내용과 속성을 정확히 이해할 수 있고 이후 단계인 위험평가에 필요한 사전 지식을 충분히 얻을 수 있다.

기록관리 기관들은 DRAMBORA를 응용하여 위험요소를 신속하게 확인할 수 있다. DRAMBORA가 여러 유형의 디지털객체 관리기관의 의견을 토대로 정리하여 제시하고 있는 78개(부록2 참조)의 기본적인 위험요소를 점검하여 참조하는 방식이다. 78개의 위험요소들은 기능과 매핑되어 있고, 세 번째 단계에서 기록관리 기관의 업무 기능 및 활동을 DRAMBORA의 기능과 매핑하였으므로, 기관의 기능 및 활동 영역에 잠재한 위험요소 후보군을 바로 식별할 수 있다. 앞 단계에서 파악한 기관의 업무적 특성을 염두에 두고 후보군의 위험요소를 자기 기관에 고유한 위험요소로 변형하여 정의하고 확인하도록 한다. 이 절차를 정리하면 다음과 같다.

(1) 기관의 업무 기능 및 활동과 DRAMBORA 업무 기능 및 활동을 매핑하고 위험관리 대상 업무의 범위 정하기
(2) 관리 대상 범위에 속하는 DRAMBORA의 위험요소를 선별하기
(3) 선별한 DRAMBORA의 각 위험요소별 정의 내역을 기관의 업무 및 자산 특성에 맞춰 변경하기
(4) 내부 워크숍을 통해 위험요소의 내용 수정보완 및 확정하기

예를 들어, 국가기록원이 전자기록의 장기보존 업무를 대상

으로 위험관리를 하겠다고 한다면 DRAMBORA의 기능 중 “보존 및 저장”은 대상 업무에 포함될 것이며 총 17개(R52 ~ R68)의 위험요소가 후보군이 된다. 후보군의 위험요소들은 MECE하지는 않으므로 혹시 빠진 위험요소가 있는지 확인하며 검토하는 것이 중요하다. 그리고, 위험요소의 정의가 일반적인 ‘정보(information)'에 대한 것으로 기술되어 있는 것을 ’기록정보(records information)' 로 수정하는 등 기록관리 기관의 특성에 맞춰 내용을 수정 보완하는 것이 필요하다. DRAMBORA는 78개의 위험요소별로 [표7]과 같이 위험요소ID, 위험요소명, 위험 설명 및 위험의 연관성, 위험 발생 사례, 위험의 특성, 이해관계자 등의 속성을 제시하고 있다.[45] 위험요소 ID는 해당 위험의 고유식별자이며, 위험요소명은 위험의 명칭이다. 위험 설명은 위험에 대해 문장으로 기술한 것이며, 위험과 연관된 다른 활동이나 적절한 대응활동이 이루어지고 있는지 여부는 위험의 연관성을 통해 확인할 수 있다. 위험사례는 위험이 발생하는 상황에 대한 예시이며 위험의 특성은 해당위험이 ‘물리적환경’, ‘인사과, 경영과 행정절차’, ‘운용 및 서비스 전달’, ‘하드웨어・소프트웨어 또는 통신장비 및 기능’ 중 어떤 영역의 특성을 갖는지 보여준다. 관할은 업무활동과 자산에 위험이 되는 요소를 식별・평가하여 관리방안을 마련하고, 위험 발생 시 이를 통제할 수 있는 책임권과 결정권을 가진 개인 혹은 조직이며, 확산관할은 위험이 관할의 통제범위를 벗어났을 때 책임권과 결정권을 갖는 개인 혹은 조직이다. 관할은 효율적 위험 관리와 통제 및 책임권의 명확화 및 집중을 위해 부서로 제시하는 것이 바람직하다. 관할 및 확산관할과 관련하여 업무기능이 정교하게 정의되어 있는 전자기록 관리기관은 위험 평가 과정 중 위험의 속성을 정이하

45) DCC,「DRAMBORA」,2007, pp 152

는 과정에서 위험이 발생 했을 때 이를 관리하고 책임을 질 권한을 갖는 관할 부서나 담당자를 정의내릴 수 있다. 하지만 업무기능이 존재하지 않거나 정교하게 정의되어 있지 않은 전자기록 관리기관에서는 평가 실행 과정에서 평가자를 대상으로 위험의 특성과 권한 부서 및 담당자가 무엇이 되어야 할지에 대한 평가를 수행하여 브레인스토밍 방식을 통해 이후의 업무기능 설계 및 정의에 활용할 수 있다.

위험요소 ID	R54	
위험요소명	정보의 진본성 손실	
위험 설명	저장소가 정보 객체의 진본성을 논증할 수 없다.	
위험의 연관성	· 보존소는 정보의 진본성을 보존/보호하기 위한 충분한 노력을 기울였는가?	
위험 사례	· 보존소가 정부 부처의 경비사용을 기술하기 위해 보존중인 기록의 진본성을 입증할 수 없음	
위험의 특성	물리적 환경	
	인사과, 경영과 행정 절차	
	운용과 서비스 전달	X
	하드웨어, 소프트웨어 또는 통신장비 및 기능	
관할	보존담당자	
확산 관할	보존담당자	
이해관계자	관리자; 재정관리자; 직원들; 저장소; 이용자; 생산자	

표 5. DRAMBORA의 위험요소 정의 사례

이처럼 DRAMBORA에서 정의한 위험요소의 주요 속성값을 우리나라 정부 공공영역의 전자기록 장기보존 업무의 관점에서 재정의한 사례를 R52 ‘정보의 기밀성 손실’ 위험요소로 제시하면 [표8]과 같다.

속성	DRAMBORA의 정의	전자기록 관리기관에 맞춘 정의
위험요소명	정보의 기밀성 손실	기록정보의 기밀성 손실
위험 설명	기밀성 협약에 따라 보호되어야 하는 정보가 협약을 위반하여 커뮤니티에 제공됨	기록관리기준표에 따라 비공개나 부분공개로 지정된 기록정보가 접근권한을 가진 사용자 범위를 벗어나 제공됨
위험의 연관성	저장소가 정보 기밀성을 유지하기로 하는 의무를 지니고 있는가?	기관이 기록정보의 기밀성을 유지할 법적, 업무적 의무를 지니고 있는가?
위험 사례	저장소의 권한관리시스템이 제대로 작동하지 않아 상업적으로 민감한 정보가 수탁협약에 따라 적법하게 접근할 수 있는 커뮤니티의 범위를 넘어서 공개됨	기록관리기준표가 마련되지 않았거나, 기록관리기준표에 맞춰 기록정보의 통제가 실행되지 않아 비공개나 부분공개로 지정된 기록물이 접근권한이 없는 사용자에게 제공됨

표 6. 위험요소의 재해석 사례

4.3 위험평가의 절차와 방법(5단계)

위험의 평가는 범주화된 위험 발생 영역 및 업무활동이나 관련 자산 등으로부터 구체적인 위험을 확인하여 목록화하고 그에 대한 속성을 정의내리는 것에서부터 시작된다. 정의한 속성을 바탕으로 위험의 발생가능성과 영향도 등의 지표를 활용하여 위험도를 평가하게 된다. DRAMBORA에서는 지표를 제시할 뿐 두 지표의 값을 측정하는 상세한 절차와 방법을 제시하지는 않는다. 정부 공공영역 기록관리 기관에 맞춰 위험평가 절차를 제시해 보면 다음과 같다.

(1) 위험의 속성 검토 - 위험요소명과 설명, 위험이 발생한 사례, 특성, 이해관계자 등의 속성값의 내용을 검토한다.

(2) 평가 실행 - 발생가능성과 위험영향도 지표별로 점수를 부여하여 위험도를 산출한다. 이 때, 해당 점수를 증빙하는

자료를 첨부하도록 한다.

(3) 피드백 - 내외부 전문가와 업무담당자의 검토 의견을 받아 평가값을 조정한다.

(4) 평가결과 분석 - 최종적인 평가 결과를 토대로 관리의 우선순위 등을 정렬한다.

위의 두 번째 단계인 평가 실행의 과정을 다시 세분화하면 다음과 같은 절차로 나눠볼 수 있다.

(1) 평가 대상 지표 확정

(2) 지표 측정 스케일 확정

(3) 업무담당자 평가 실행

(4) 증빙자료 첨부

평가 대상 지표는 일반적으로 발생가능성과 영향도 등을 기본요소로 하며 추가적으로 전자기록이나 업무의 중요도 등을 보조 지표로 활용할 수 있다. 어떤 지표를 활용하느냐에 따라 다양한 위험 평가가 가능하지만 위험관리에 있어 일반적으로 널리 활용되는 위험도 평가 지표는 위험의 발생가능성과 영향도이다. DRAMBORA는 위험이 발생할 가능성(Probability)와 영향도(Impact)를 측정하여 두 값을 곱한 위험도를 산출한다. 지표의 측정 스케일도 다양한데 DRAMBORA는 위험의 발생가능성과 영향도를 측정하는 스케일로 [표 9], [표 10]과 같이 각각 6분 척도와 7분 척도를 제시하고 있다. 따라서, 위험도는 최고 42점에서 최저 1점까지 값의 분포를 갖게 된다.

점수	위험 발생가능성 설정 기준
1	최소의 발생가능성, 백년 혹은 그 이상의 기간 중 한번 정도 발생
2	매우 낮은 발생가능성, 10년에 한번 정도 발생
3	낮은 발생가능성, 5년에 한번 정도 발생
4	중간 발생가능성, 1년에 한번 정도 발생
5	높은 발생가능성, 1달에 한번 정도 발생
6	매우 높은 발생가능성, 1달에 2번 이상 발생

표 7. DRAMBORA의 위험 발생가능성 지표

점수	위험 영향도 설정 기준
1	영향도 없음, 디지털 자원의 진본성과 이해가능성[46] 손상 없음
2	무시해도 될 영향도, 국소한 부분에 영향을 미치지만 디지털 자원의 진본성과 이해가능성 손상을 완전히 복구시킬 수 있음
3	가벼운 영향도, 비교적 넓은 부분에 영향을 미치지만 디지털 자원의 진본성과 이해가능성 손상을 완전히 복구시킬 수 있음
4	중간 영향도, 전체적으로 영향을 미치지만 디지털 자원의 진본성과 이해가능성 손상을 완전히 복구시킬 수 있음
5	높은 영향도, 국소한 부분에 영향을 미치며 디지털 자원의 진본성과 이해가능성 손상을 일부 복구시키지 못함
6	상당히 높은 영향도, 비교적 넓은 부분에 영향을 미치며 디지털 자원의 진본성과 이해가능성 손상을 자체적으로 복구 시키지 못하며 제3자에 의해 복구시킬 수 있음
7	대재앙 수준의 영향도, 전체 디지털 자원의 진본성과 이해가능성을 복구시킬 수 없음

표 8. DRAMBORA의 위험 영향도 지표

한편, DIRKS 매뉴얼의 위험평가기법에서는[47] 위험 발생가능

46) 이해가능성(understandability): 조직 내외의 이용자가 기록의 위치를 찾아 검색 및 이용할 수 있으며, 기록의 내용을 해석하고, 이해할 수 있는 상태 (DRAMBORA)

성(Likelihood)과 영향력(Severity)를 측정한 후 위험 충격 매트릭스(Risk Impact Matrix)에 따라 위험수준을 구하도록 제시하고 있다.

가능성	영향력				
	심각	높음	중간	낮음	무시
발생 확실	심각한 위험	심각한 위험	상위 위험	주요한 위험	현저한 위험
발생 의심	심각한 위험	상위 위험	주요한 위험	현저한 위험	보통의 위험
보통	상위 위험	주요한 위험	현저한 위험	보통의 위험	낮은 위험
미발생 유력	주요한 위험	현저한 위험	보통의 위험	낮은 위험	사소한 위험
미발생 수준	현저한 위험	보통의 위험	낮은 위험	사소한 위험	사소한 위험

표 9. DIRKS 매뉴얼의 위험 충격 매트릭스

위험도와 위험수준에 따라 위험요소별 관리의 우선순위가 달라지게 되는데, DIRKS 매뉴얼은 각 위험 수준 별로 위험관리가 어떻게 이루어져야 하는지를 [표 12]와 같이 간략히 제시하고 있다.

위험 수준	관리 방안
심각한 위험 (Severe risk)	구체적 계획을 가지고 상급 관리진에 의해 관리되어야 함
상위 위험 (High risk)	상급 수준에서 자세한 연구와 관리 계획이 요구됨
주요 위험 (Major risk)	상급 관리진의 주의가 요구됨

47) DIRKS 매뉴얼 부록11에서 위험관리방법론을 제시하고 있음

현저한 위험 (Significant risk)	관리진의 책임이 명기되어야 함
보통의 위험 (Moderate risk)	특수한 모니터링이나 응답 절차에 의해 관리되어야 함
낮은 위험 (Low risk)	일상적 절차에 의해 관리되어야 함
사소한 위험 (Trivial risk)	특별한 자원 이용이 필요하지 않음

표 10. DIRKS매뉴얼의 위험 수준

위험의 가능성과 영향도 지표의 스케일은 [표 13]과 같이 매체수명이나 정보시스템의 수명, 기록관리 업무 프로세스의 실행 주기 등을 기준으로 제시할 수도 있다. 시스템과 저장매체가 평균 3년, 7년마다 기술적 수명이 다한다면 그 주기로 교체 및 업그레이드가 실행되어야 하는데 일반적으로 매체변환과 시스템업그레이드 과정에서 전자기록의 진본성과 이해가능성이 훼손될 가능성이 높아진다. 전자기록 관리기관에서 전자기록의 이관 및 재평가는 일반적으로 1년 단위로 이루어지며 그 과정에서 진본성과 이해가능성의 위험이 발생할 가능성이 높다. 그 밖에 서은경[48]은 대학도서관의 디지털 정보자원을 보존하는 기법에 대한 위험요인을 위험 발생가능성 수준(risk probability scale)과 위험영향력 수준(risk impact scale)을 각 5분 척도로 평가하였다.

48) 서은경, 「디지털 정보자원 보존의 위험관리 분석: 대학도서관 전자정보실 중심으로」, 『정보관리학회지』 Vol.20, No.1 ,2003, p14-15

점수	위험 발생가능성 설정 기준
1	최소 발생가능성(Minimal probability), 매 100년 마다 한 번 이상 발생
2	낮은 발생가능성(Low probability), 매 7년 마다 한 번 이상 발생(매체수명)
3	중간 발생가능성(Medium probability), 매 3년마다 한 번 이상 발생(시스템 업그레이드)
4	높은 발생가능성(High probability), 매년 한 번 이상 발생(이관과 재평가 시기)
5	매우 높은 발생가능성(Very high probability), 매달 한 번 이상 발생(매일 표함)

표 11. 매체수명 및 시스템 수명 기준의 위험가능성 스케일 예시

위험의 발생가능성과 영향도 지표의 측정 스케일을 확정한 이후에는 위험평가자를 대상으로 평가를 실시한다. 위험평가 작업에 처음 참여하는 업무담당자를 위해 평가 절차와 방법에 관한 교육을 실시하고, 가이드를 배포하며, 샘플 평가서 작성을 해보도록 하는 등 원활한 평가가 되도록 필요한 조치를 취한다. DRAMBORA는 평가 점수의 객관성과 정당성을 확보하기 위해 평가의 증거가 되는 각종 증빙자료를 첨부할 것을 강조하고 있다. 증거자료는 법조문, 전략계획서, 계약서, 시스템 기능 정의서, 업무 프로세스 정의서 등 다양한 문서와 정보가 제출될 수 있는데 되도록 가시적으로 확인이 가능한 문서화된 증거자료를 평가결과와 함께 제출할 것을 권장하고 있다. 대통령 기록관 디지털 아카이브 발전전략 연구 과정의 경우처럼 증빙자료 제출에 과도한 시간이 소요되는 것을 방지하기 위해 증빙자료 제출에 관한 상세 지침을 [표 14]와 같이 마련할 수도 있다.[49]

49) 「(국제모범기준과의 격차분석에 기반한)대통령기록관의 디지털 아카이브 발전전략 연구」, 국가기록원 대통령기록관, 2008, pp141-142 참조

번호	내용	내용 관련 설명	작성 관련 설명
1	증빙자료를 반드시 제시하고 업무담당자/부서 스스로 평점 부여	증빙자료를 반드시 제시해야 하는 경우	-
2	증빙자료 제시가 원칙이지만, 업무담당자/부서 의견 서술 후 평점 부여 가능	증빙자료를 제시하는데 과다한 시간이 소요되는 경우	진단시, 업무담당자가 '업무담당자/부서 의견' 란에 어떠한 증빙자료를 제출할 수 있으나 과다한 시간이 소요되는 이유와 평점 부여의 근거를 서술
3	증빙자료 제시 없이, 업무담당자/부서 의견 서술 후 평점 부여	현실적으로 증빙자료 제시가 곤란한 경우	진단시, 업무담당자가 '업무담당자/부서 의견' 란에 평점 부여의 근거를 서술

표 12. 대통령기록관의 평가방법 구분

평가 수행 후에는 피드백을 통해 부족한 증거 자료를 확보 하거나 미 수행된 평가 항목에 대한 설명 등을 통해 이해력을 증진시킴으로써 평가의 완전성을 확보할 수 있게 된다. 필요에 따라 피드백을 거친 후에는 위험평가 결과에 대한 분석을 통해 관리 대상 위험요소를 선정하고 관리 방안을 도출하게 된다.

4.4 위험도 계산 시 고려 사항

위험요소에 대한 평가 결과는 정책결정과 예산 배정의 근거 자료 등 다양한 방법으로 활용될 수 있다. 순위를 매기거나 등급화하여 상위 위험요소 혹은 고위험군에 속하는 위험에 대해 우선적으로 관리방안을 설계하는데 활용될 수 있다. 또는, 상위 위험군에 속하면서 위험요소 간의 연관성이 많아 다른 추가 위험을 발생시킬 가능성이 높은 위험을 중심으로 인력 투입 및 관

리방안을 설계할 수 있다. 위험평가 결과는 위험을 실체를 조직 내외부에 공유하고 이를 예방하거나 조치하기 위한 예산을 확보하기 위한 근거자료로 활용될 수도 있다. 이러한 이유로 위험평가의 결과는 하나의 계량화된 지표로 계산될 필요가 있으며 DRAMBORA는 전체 위험요소를 위험도로 정렬함으로써 시급히 관리해야 할 위험요소를 선정하여 기관의 자원을 우선적으로 투여하도록 권고하고 있다. 관리상 유용한 위험도를 계산해 내기 위해서는 평가 결과의 신뢰성을 확보해야 하며 기관의 상황에 맞춰 조정될 수 있어야 한다. 위험도 계산 시 고려사항을 살펴보면 다음과 같다.

첫째, 유효한 평가값을 선별해내기 위해 통계처리를 고려할 수 있다. 하나의 위험요소에 대해 발생가능성과 영향도의 점수를 부여하는 업무담당자가 복수이고, 업무담당자 한 사람이 여러 개의 위험요소에 점수를 부여한 경우 위험에 대한 개인별 인식의 특성과 편차를 고려함으로써 위험도의 신뢰도를 높일 필요가 있다. 하나의 위험요소를 복수의 평가자가 평가한 경우 위험도를 계산하는 가장 단순한 방법은 발생가능성 값의 평균과 영향도의 평균을 구해 곱하는 것이다. 혹은 평가자별로 발생가능성 값과 영향도 값을 곱한 후 곱셈 결과의 평균을 구하는 것이다. 그런데, 각 업무담당자별로 평가에 임하는 태도와 시각이 달라 의미없는 평가값을 제시하는 경우가 발생하거나 비관적인 혹은 낙관적인 수치로 쏠림 현상이 발생할 수 있다. 이를 통계적으로 보정할 수 있다면 좀 더 유효한 평가 결과를 얻을 수 있다. 예를 들면, 개인별 편차를 보정하기 위해 원점수를 그대로 사용하지 않고 Z분포[50]의 점수를 사용할 수 있다. Z점수를 활용

50) Z분포는 평균이 0, 표준편차가 1이 나오도록 조정한 것으로 평균이 m이고 표준편차가 σ일 때 평가결과가 Z점인 경우의 Z점수는 'Z = (X-m) / σ'로 표현

함으로써 전자기록 관리기능별로 업무담당자 개인 취향이나 특성에 따라 편향된 점수를 부여한 것이 조정됨으로써 유의미한 분석이 가능해진다. 이 때, 전체 평가 결과값을 왜곡시키는 불성실한 평가값은 사전에 제거함으로써 신뢰성과 유효성을 확보할 수 있다.

둘째, 위험도를 산출할 때 위험의 발생가능성과 영향도를 단순 곱셈할 수도 있으나 조직의 내외부 환경을 고려하여 계산방식을 달리 하거나 가중치를 부여하는 등의 방법을 검토한다. Johe C Bennett[51]은 [표 15]와 같이 위험이 가지고 있는 기본 점수(base score)에 복잡성 요인(complexity factors)을 가중치로 적용하여 더하는 방식으로 위험도를 평가하였다. 가중치는 해당 위험과 관련이 있는 업무활동 및 자산 즉, 디지털 정보나 전자기록, 시스템, 데이터베이스, 직원이 지닌 가치나 위험의 파급효과 등을 고려하여 적용할 수 있다. 또한, 발생가능성과 영향도 이외의 새로운 지표의 도입을 고려할 수도 있으나 지표의 단순법칙(law of parsimony)에 벗어나므로 새로운 지표의 도입보다는 가중치 부여의 방식으로 조직의 특성을 반영하는 것이 옳을 것이다.

할 수 있다. Z점수는 표준점수라고도 하는데 통계적 절차를 통해 원점수를 해당 집단의 평균을 중심으로 표준편차 단위로 환산함으로써 점수 간 비교가 가능하게 하며 상대적 위치를 비교할 수 있도록 해줄 뿐 아니라 여러 가지 다른 점수에서 나온 결과들을 서로 의미 있게 비교하는 상대평가가 가능하도록 해준다.

51) Johe C. Bennett,「A FRAMEWORK OF DATA TYPES AND FORMATS, AND ISSUES AFFECTING THE LONG TERM PRESERVATION OF DIGITAL MATERIAL」, 1997, pp.14 인용

전자기록 유형	기본 점수 (Base Score)	가중치(Complexity Factors) (기본 점수에 더함)	위험
텍스트/ 도큐먼트 (인캡슐레이티드)	1	기능(+1), 매크로(+1), 템플릿(+1)	포맷 손실
	1	링크(표준)	링크 손실
	2	링크(+1), HTML(+1)	외부 데이터 손실

표 13 Johe C. Bennett의 위험도 평가 사례(기본 점수 + 가중치)

조정된 평가 결과는 DRAMBORA가 제공하는 Toolkit을 활용하여 위험관리등록부로 작성할 수 있다. 기관의 업무담당자들은 위험관리등록부를 통해 전자기록 장기보존을 위협하는 위험에 대한 기본 속성 정보와 평가 및 분석정보는 물론 해당 위험을 관리하고 통제하기 위한 다양한 활동을 확인할 수 있다.

5. 맺음말

위험관리기법은 모든 업무영역에서 응용이 가능한 업무품질 향상기법이라 할 수 있다. DRAMBORA는 전자기록관리 업무를 수행하는 기관이 참조할 만한 업무 점검 프레임워크를 제시하고 있다[52]. 이 논문에서 살펴본 바와 같이 전자기록을 관리하는

52) DRAMBORA는 기관의 자체평가를 위한 도구이지만 외부 기관이 특정 기관을 감사하고 인증하기 위한 용도로도 사용될 수 있다. 6개의 단계 중 앞 3개의 단계는 기관을 평가하기 위한 사전 준비 과정이 될 것이다.

기관들이 스스로의 업무 영역과 활동을 정의하고, 업무 영역별 전자기록의 품질 목표를 정의할 수 있다면 이를 기반으로 DRAMBORA의 프레임워크를 응용하여 보다 용이하게 위험관리 기법을 적용할 수 있다.

위험관리의 절차 중 위험을 평가하는 과정은 현재의 수행 중인 업무활동의 효과성에 대한 측정 과정이라 볼 수 있다. "측정하지 않으면 관리할 수 없고, 관리하지 않으면 개선할 수 없다"[53]는 말이 있다. 따라서 측정의 신뢰성과 일관성에 관한 의문이나 위험 정도의 정량화 한계에 관해 일부 논란이 있을 수 있으나 이는 향후 측정 기법의 객관화를 도모하는 계기로 여길 필요가 있겠다. 또한, 위험관리 방법을 통해 기관 내부의 업무를 평가하는 과정에서 목표와 현실 업무 사이의 격차로 인해 업무담당자들의 반발이 있을 수 있다. 이는 평가의 목적에 맞춰 업무담당자들에 대한 변화관리를 통해 해소해 가야 할 것이다.

위험관리기법을 사용하여 성공적으로 업무를 점검하기 위해서는 조직이 다음과 같은 능력을 보유하고 있어야 한다. 첫째, 조직의 사명과 비전, 목표, 업무활동, 자산 등에 관해 포괄적으로 인식하고 이를 명문화하여 공식화할 수 있어야 한다. 둘째, 지속적인 위험요소를 도출하여 확인하고 위험요소별 유형과 서로 간의 관계, 관할권, 발생가능성, 잠재적 영향력 등에 관해 평가할 수 있어야 한다. 셋째, 조직의 성과와 미흡한 점에 관해 내부적인 공유가 이루어지고, 이를 바탕으로 시급한 위험요소의 관리를 위해 효과적으로 자원을 할당하거나 재분배하는 것이 가능해야 한다.

전자기록 관리기관이 주기적으로 위험관리기법을 사용하여

53) 세계적인 경영학자 피터 드러커의 명언 중 하나로, 업무 개선을 위해 관리가 필요하며 관리를 위해서는 성과 측정이 필요함을 역설하고 있다.

업무를 점검하게 되면 특정 위험요소에 대한 위험도의 변화추이를 살펴볼 수 있다. 위험도가 감소하게 된 이유는 외부 위협요인의 완화와 내부 업무 품질의 향상으로 나누어 볼 수 있을 것이다. 위험요소별의 관할부서 성과평가에 내부 업무 품질 향상으로 인한 위험도 감소 정도를 반영할 수 있을 것이다. 우리나라의 전자기록 관리기관, 나아가 디지털자원과 객체를 장기보존하는 임수를 수행하는 여러 기관에서 DRAMBORA에 기반한 위험관리 방법론을 적극 수용하여 업무활동의 개선점에 대한 새로운 시사점을 얻기 바란다.

부록1 : DRAMBORA가 정의한 업무활동 52개 목록

기능명	업무활동
S1.조직관리	S1A1. 조직 목표와 사명을 정의
	S1A2. 보존소의 전 생애에 걸친 지속적 보존을 위한 계획
	S1A3. 식별된 커뮤니티에 대한 규정을 문서화하고 검토
	S1A4. 식별된 커뮤니티의 이해가능성 요구를 충족시키기 위한 규정 마련하며 문서화하고 검토
	S1A5. 식별된 커뮤니티로부터 피드백을 요청하기 위한 메커니즘의 설치와 이용
	S1A6. 정보 보존을 위한 디지털 콘텐츠의 특성 정의
	S1A7. 각 업무 활동을 관장할 정책과 절차를 규정하고 문서화하며 검토
	S1A8. 기록의 생산자와 예치자, 이용자와의 협상 및 합법적 동의
	S1A9. 법규 및 규제와 관련된 책임의 이행
	S1A10. 내외부감사와 위험분석을 포함하는 조직 평가 기법 활용
S2.직원	S2A1. 충분한 자격이 있는 충분한 직원의 임명
	S2A2. 직원의 역할과 책임 및 관계를 규정
	S2A3. 직원 교육 요건을 확인하고 충족시키기 위한 메커니즘을 정의하고 개발
	S2A4: 내외부 감사 및 위험분석을 포함하는 직원 평가 기법 활용
S3.재정관리	S3A1. 장단기 사업계획을 정의내리고 시행하며 검토
	S3A2. 재정적자 상황을 모니터하고 재정적자를 벗어날 수 있는 방안 모색
	S3A3. 사법권의 금융법을 준수
	S3A4. 내외부 감사와 위험분석을 포함하는 재정 평가 기법 활용
S4.기술 인프라 및 보안	S4A0. 전략적 IT 계획의 규정
	S4A0.1. IA 규정
	S4A1. 하드웨어와 소프트웨어의 지속적 적절성과 적합성 보장을 위한 모니터링
	S4A2. 하드웨어와 미디어 refreshment를 이행하기위한 방법론의 실행
	S4A3. 적절한 시기에 보안패치를 설치하고 소프트웨어를 업데이트 할 시스템을 유지시킴
	S4A4. 중요 시스템 변화의 효과 테스트
	S4A5. IT와 물리적 인프라 내에서 보안 기법 시행
	S4A6. 여분의 데이터와 스토리지 및 분산 보관하는 백업 자료를 유지
	S4A7. 재해복구와 업무지속성 계획을 착안하고 테스트

기능명	업무활동
	S4A8. 내외부 감사와 위험분석을 포함하는 기술(technical)과 보안 분야 평가를 위한 기법 활용
C1.획득 및 입수	C1A1. 수용 가능한 제출(입수) 포맷을 규정
	C1A2. 이관 받은 콘텐츠의 무결성을 모니터하고 기록
	C1A3. 입수된 콘텐츠의 완전성과 완벽성 증명
	C1A4. 이관 받은 콘텐츠의 물리적 기술적(technical) 통제 방안 설치
	C1A5. 콘텐츠 생산자와 예치자에게 보존 책임의 수락 또는 거절을 통보하기위한 메커니즘을 도입
	C1A6. 제출된 콘텐츠를 보존포맷으로 변환시킴
	C1A7. 보존포맷으로 전환되지 않는 제출(입수)된 콘텐츠의 처분
	C1A8. 내외부 감사, 위험 분석을 포함하는 기능 평가를 위한 기법 활용
C2.보존 및 저장	C2A1. 보존된 콘텐츠에 유일하고 지속적인 식별자 부여
	C2A2. 보존 콘텐츠의 모든 변화를 문서화
	C2A3. 보존 콘텐츠와 컬렉션 레벨의 무결성을 모니터하고 입증
	C2A4. 물리적 보존 스토리지와 마이그레이션 전략을 실행하고 검토
	C2A5. 보존 전략을 규정하고 검토하며 실행
	C2A6. 내외부 감사 위험분석을 포함하는 기능 평가를 위한 기법 활용
C3.메타데이터 관리	C3A1. 보존 콘텐츠를 위한 보존 메타데이터 획득
	C3A2. 보존 객체의 이용가능성을 확증하기 위해 필요한 의미론적 배경(semantic context)과 기술적 배경(technical context)을 정립하고, 문서화하며 모니터함
	C3A3. 발견을 용이하게 하는 적절한 기술 메타데이터(descriptive metadata)를 획득하거나 생성
	C3A4. 메타데이터와 보존 콘텐츠 간의 참조 무결성(referential integrity)을 유지
	C3A5. 내외부 감사, 위험 분석을 포함하는 기능 평가 기법 활용
C4.접근 및 배부	C4A1. 콘텐츠를 발견·선택·접근하기 위한 메커니즘 제공
	C4A2. 인증과 승인된 접근권한과 제한을 반영한 허가된 서브시스템을 시행
	C4A3. 배포를 위해 보존 콘텐츠의 전환 시행
	C4A4. 제출 당시의 상태처럼 완벽하고 진본성을 갖춘 객체의 배포
	C4A5. 내외부 감사, 위험 분석을 포함하는 기능 평가 기법 활용

부록2 : DRAMBORA의 기능분류별 위험요소 78개 목록

번호	위험요소명	번호	위험요소명
조직 관리			
R01	관리 실패	R11	정보의 필수속성에 대한 보존 실패
R02	신뢰 혹은 명망 상실	R12	업무정책 및 절차 미숙지
R03	활동을 소홀히 하거나, 부족한 자원 할당	R13	업무정책 및 절차 비효율
R04	업무 목표 미달성	R14	업무 정책 및 절차 모순 및 통일성 없음
R05	필수사항 누락	R15	지적 소유권 위반
R06	커뮤니티 요건 변경	R16	계약상 책임에 대한 부분 법적 위반
R07	커뮤니티 요건 오해 및 소통문제	R17	법규 요건에 대한 부분 법적 위반
R08	저장소의 가동 중단	R18	법규 미준수에 대한 책임
R09	커뮤니티 피드백에 대한 미점수	R19	저장소의 성공 측정 불가능
R10	커뮤니티 피드백에 대한 미실행	R20	저장소의 성공 정도의 인식 오류
직원			
R21	핵심인력의 손실	R23	직원의 작업능력 퇴화
R22	직원의 보유 기술 퇴화	R24	직원 효율성이나 적합성 측정 불가능
재정 관리			
R25	저장소 기준 충족에 부족한 재정	R28	수입 제한에 따른 재정 고갈
R26	재정 할당 오류	R29	예산 감소
R27	재정 법률이나 법규에 근거하지 않는 경향		
기술 인프라 및 보안			
R30	하드웨어 오류 혹은 충돌	R39	지역(Local) 내 파손이나 침입 현상
R31	소프트웨어 오류 혹은 충돌	R40	불시 시스템 혼선
R32	저장소 목표의 통합에 대한 하드웨어 혹은 소프트웨어 지원 불가능	R41	고의적인 시스템 방해
R33	하드웨어나 소프트웨어의 불용화	R42	저장소 내 파손 및 이용 불가능
R34	매체 불용화나 구형화	R43	핵심 유틸리티의 이용 불가
R35	보안 취약성 포착	R44	제3자 서비스 손실
R36	미식별된 보안 모호, 취약성 혹은 정보 보안등급 하락	R45	제3자 서비스 내에서의 용어 변경
R37	하드웨어 저장 공간에 물리적 침입	R46	주요 도큐멘테이션 파손

R38	원격 혹은 지역 내 소프트웨어 침입	R47	기술적 인프라 및 보안 효율성에 대한 측정 불가능
획득 및 입수			
R48	구조적 모순이나 입수된 패키지의 유형적 오류	R50	입수 중 정보에 대한 외부 변화나 유지
R49	제출된 패키지의 불완전함	R51	기록 정보가 입수패키지에 흔적이 남지 않음
보존 및 저장			
R52	정보의 비밀성 손실	R61	사본들 간의 불일치
R53	정보와 서비스의 이용가능성 손실	R62	보존할 정보객체의 범위가 불분명함
R54	정보의 진본성 손실	R63	입수과정에 대한 효율성 검증 불가능
R55	정보의 무결성 손실	R64	정보참조 식별자의 무결성 불확실함
R56	정보 변경 미식별	R65	보존계획을 실행할 수 없음
R57	부인봉쇄 약속의 파기	R66	보존전략의 결과로 정보손실 초래
R58	정보의 신뢰성 손실	R67	보존효율성에 대한 검증 불가능
R59	정보의 출처 손실	R68	수취 및 저장, 혹은 배부패키지의 추적 불가능
R60	백업의 비적합성 혹은 손실		
메타데이터 관리			
R69	메타데이터에 대한 정보무결성 불확실	R72	이해 불가능한 모호한 정의
R70	문서화된 변경이력이 불완전하거나 불확실함	R73	정보의 기술 및 의미적인 이해 부족
R71	정보객체의 검색 불가능함		
접근 및 배부			
R74	정보제공 서비스의 비가용성	R77	배부 메커니즘의 효율성 검수 실패
R75	서브시스템에 대한 인증실패	R78	서비스 레벨이나 성능에 대한 손실
R76	서브시스템에 대한 승인 실패		

ABSTRACT

A Study on the Risk Management Framework for the Long-term Preservation Business of Electronic Records

Yim, Jin-Hee

This paper proposed risk management approach as a self-audit framework to achieve the goals which might be common among the records management organizations in Korea governmental and public area. After introducing the history and the concept and process of risk management approach and examining DRAMBORA's framework, the processes and the methods of risk management for the electronic records which are customized from DRAMBORA are explained in details: How to define the business context of organizations, how to determine the business functions and activities and related risks, how to assess the level or severity of each risks and some considerations related to risk assessment. As a result, this paper shows that application of DRAMBORA's framework to the electronic records management organizatioins is not only possible but also useful and effective. The critical point for the success of application for DRAMBORA's framwork or the risk management approach itself each organizations which wants to accept that framework should define its own business functions and activities and the goals in respect areas.

Key words: Electronic Records, Long-term Preservation, DRAMBORA, Risk Management Framework