논문

전자기록 장기보존 위험관리 사례*

임 진 희*

* 이 논문은 2010년 국가기록원이 발주하여 저자가 연구책임자로 수행한 "전자기록물 장기보존 위험관리방안 연구용역" 결과의 일부를 재구성하여 정리한 것임.
** 명지대학교 기록정보과학전문대학원 조교수. 주요 논저 : 「대량기록물 처리를 위한 영구기록물관리시스템의 디지털저장소 배치형상 연구」, 『기록학연구』 제32호, 한국기록학회, 2012. 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 제27호, 한국기록학회, 2011.
▪투고일 : 2013년 12월 16일 ▪최초심사일 : 2013년 12월 28일 ▪게재확정일 : 2014년 01월 24일.

[국문초록]

이 논문에서는 2010년 국가기록원에서 DRAMBORA(Digital Repository Audit Method Based on Risk Assessment) 프레임워크를 응용하여 전자기록 장기보존 업무에 대해 점검했던 사례를 상세히 제시하고 있다. 국가기록원은 2010년 전자기록 장기보존 업무에 관련하여 총 44개의 위험요소를 도출하여 정의하였고, 업무담당자들의 평가를 거쳐 위험도 등급에 따라 분류하였으며, 고위험도를 지닌 2개의 위험요소에 대해서는 상세한 관리방안을 개발하였다. 이 논문에서는 NR04 '기록정보의 무결성 손실' 위험요소에 대한 사전관리방안, 사후관리방안, 비상대책조직, 재난선포 주체와 기준, 개인임무카드 개발 내역을 소개하고 있다. 이 논문 내용을 통해 기록관리자들은 위험관리 기법을 구체적으로 이해할 수 있을 것이며, 기록관리 기관들은 중요 업무관리 방법으로 위험관리 기법을 수용할지 점검하는데 참고할 수 있을 것이다.

주제어 : 전자기록, 장기보존, DRAMBORA, 위험관리, 사례분석

1. 머리말

국가기록원은 2015년부터 본격적으로 대량의 전자기록을 이관받아 장기보존할 예정이다. 진본성(Authenticity)과 이해가능성(Understandability)[1]

1) DRAMBORA에서는 이해가능성(Understandability)을 진본성(Authenticity)과 함께 디지털객체를 장기보존 하는 과정에서 유지해야 할 핵심 품질 요건으로 보고 있으며, 위험요소를 도출할 때 이 두 가지 품질요건이 훼손될 가능성과 영향에 초점을 맞추고 있다. 이해가능성은 조직 내외의 이용자가 기록의 위치를 찾아 검색 및 이용할 수 있으며, 기록의 내용을 해석하고, 이해할 수 있는 조건과 상태를

을 안정적으로 유지하면서 전자기록을 장기간 보존하는 것이 국가기록원의 핵심성과지표(KPI)의 하나일 것이다.

국가기록원은 2009-2011에 걸쳐 전자기록 재난복구체계 구축 사업을 진행하였다. 2009년에는 재난관리에 필요한 인프라를 구축하였고, 2010년에는 재난관리에 필요한 운영환경을 마련하였으며, 2011년 이후에는 재난관리 업무를 확대 운영하고 있다. 2010년에는 기록관리 특성을 고려한 국가기록원 전자기록 위험평가를 시범적으로 실시하였으며, 이를 위해 DRAMBORA(Digital Repository Audit Method Based on Risk Assessment) 프레임워크를 기반으로 하여 국가기록원 전자기록 장기보존 업무에 관련된 위험요소를 확인한 바 있다.[2] 이 결과를 토대로 DRAMBORA를 응용하여 우리나라 정부 공공영역의 기록관리기관이 전자기록 장기보존 업무를 대상으로 위험관리 체계를 만들어 가는 절차와 방법은 이미 제시된 바 있다.[3] 이 논문에서는 전자기록 장기보존이라는 목표를 달성해야 하는 기록관리기관이 위험관리 기법을 적용하여 관련 업무를 점검하고 위험에 대비하는 방법을 사례를 통해 상세히 제시하고자 한다.

대량의 전자기록이 사이버 테러에 의해 순식간에 망실될 수도 있고, 전자기 저장매체가 자석에 노출되는 실수로 대량 데이터 소실이라는 심각한 재난 상황이 발생할 수도 있는 디지털 환경의 특성을 고려했을 때 전자기록 관리 업무를 '디지털 환경에서 발생가능한 위험요소'라는 새로운 관점에서 점검해볼 필요가 있다. 기술 집약적인 분야일수록 위험요소 하나가 전체 체계에 미치는 악영향의 정도가 막대해지고, 고도화된 정보기술이 갖는 강점이 동전의 양면처럼 동시에 최대의 취약점이

갖추는 것으로 ISO 15489의 이용가능성(Usability)와 거의 동일한 의미로 볼 수 있다.

2) 임진희, 『전자기록관리론』, 선인, 2013, 377-378쪽.

3) 임진희, 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 27호, 2011, 119-168쪽.

될 수도 있다는 점을 고려해야 하기 때문이다. 전자기록을 관리하기 위한 디지털 환경과 채택한 정보기술의 특성을 충분히 이해하고 완벽하게 통제할 수 있느냐 여부가 전자기록관리의 성패를 가름할 것이다.[4]

2. 전자기록 장기보존 위험요소의 정의

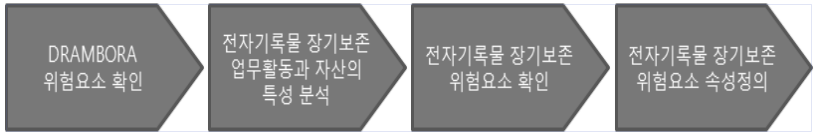
1) DRAMBORA 산출을 활용한 위험요소 정의

국가기록원이 전자기록을 장기보존 과정에서 내포하고 있는 위험요소를 확인하기 위해서는 선행작업으로 국가기록원의 업무활동과 자산에 대한 조사가 필요하다. 업무활동을 조사하고 정의하기 위해서는 전자기록의 장기보존과 관련된 업무활동과 자산이 무엇인지를 파악한 후 각각의 업무활동별, 자산별 전자기록 보존소가 직면한 위험이 무엇인지 확인해야 할 것이다. 업무활동의 측면에서는 전자기록을 보존하는 업무가 지속적이고 안정적으로 수행되는 것을 위협하는 요소가 있는지, 효과적이고 효율적으로 수행되는 것을 방해하는 요소가 있는지를 중심으로 살펴보고 자산의 측면에서는 전자기록을 장기보존하는 과정에서 함께 보존해야 할 핵심 품질특성인 진본성(Authenticity)과 이해가능성(Understandability)을 위협하는 요소가 있는지를 중심으로 살펴보아야 할 것이다. 국가기록원이 수행하는 업무활동을 조사하고 분석하여 구체적으로 정의를 내리기 위해서는 상당한 노력과 비용이 필요하며, 업무활동 정의 내역에 대해 조직 내외에서 동의하고 공유하는 데에도 추가적인 노력과 비용이 소요될 것으로 예상되었다. 2010년 현재 국가기

4) 정기애 · 이정훈 · 남영준, 「위험관리체계의 기록관리표준 적용방안 연구」, 『한국기록관리학회지』 제11권 제2호, 2011, 193-201쪽.

록원은 전자기록 장기보존과 관련된 세부 업무활동을 현행(AS-IS)과 향후계획(TO-BE)으로 나누어 정의한 바가 없었고, 바로 업무분석을 수행할 수 있는 여건도 마련되지 못한 상태였다. 따라서, 현실적 여건을 고려하여 DRAMBORA가 제시하는 산출물을 최대한 활용하는 방식으로 국가기록원 전자기록 장기보존 업무에 관련된 위험요소를 정의하게 되었다. 다음 〈그림 1〉은 작업의 세부 프로세스를 보여주고 있다.[5]

〈그림 1〉 전자기록 장기보존 위험요소 확인 세부 프로세스



첫 번째 작업으로 DRAMBORA가 제시하는 위험요소를 확인하였다. DRAMBORA에서는 디지털객체 보존소의 업무기능(Functional Classes)을 총 8개로 범주화하고 그 하위의 업무활동(Activities)을 총 52개로 제시하고 있다.[6] 또한, 업무의 대상이 되거나 업무수행에 필요한 자산(Assets)을 고려했을 때 관리할 필요가 있는 위험요소를 78개 제시하고 있다.[7] 이 78개의 위험요소는 DRAMBORA의 작업 과정에 참여한 여러 디지털객체 보관소들이 각 기관별로 찾아낸 위험 중 공통적이면서도 위험도가 높은 요소들을 정리한 것이다. 위험도(Risk Severity)는 수치로 표현이 되어있는데 해당 위험요소가 발생할 가능성(Risk Probability)을 6점 척도로 평가하고 위험의 발생 시 조직에 주게 될 충격의 예상치(Risk Potential Impact)을 7점 척도로 평가하여 두 결과값을 곱하기하여 점수

5) 임진희, 『전자기록관리론』, 선인, 2013, 378쪽, 〈그림 5-11〉 재인용.
6) 임진희, 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 제27호, 2011, 163-164쪽.
7) 임진희, 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 제27호, 2011, 165-166쪽.

화한 것이다.[8] 즉, 최고의 위험수준은 위험도 42로 표기되며 값이 높을수록 위험도가 높은 것으로 해석할 수 있다. DRAMBORA는 참여 기관들이 제출한 위험요소 중 위험도 점수가 12점 이상인 것을 사례로 제시하고 있다.[9]

두 번째 작업으로는 국가기록원이 수행하는 전자기록의 장기보존 업무활동과 자산의 주요 특성을 분석하였다. 앞서 언급한 바와 같이 국가기록원 업무를 상향식 방식(Bottom-Up Approach)으로 전수조사하여 분석을 할 수 없는 조건이었으므로 먼저 DRAMBORA에서 정의한 디지털객체 보존소의 기능과 업무활동 중에서 국가기록원에서도 수행 중이거나 수행 예정인 업무를 확인하였다. 다음으로 국가기록원이 전자기록 장기보존 업무에서 중요시하는 자산을 확인하였다. 중요 자산으로는 전자기록 자체와 이를 관리하기 위한 정보시스템, 그리고 전자기록을 저장하기 위한 매체가 선정되었다. 이 세 개의 핵심 자산이 갖는 특성 혹은 자산 관리를 위한 필수 요건을 다음과 같이 정리하였다.

- 전자기록은 진본성, 무결성, 신뢰성, 이용가능성이 보장되게 관리되어야한다.
- 전자기록은 내용정보인 전자기록과 구조 및 맥락정보인 메타데이터로 구성된다.
- 전자기록은 시스템을 통해 전자적으로 생산, 보존, 관리되며, 물리적 형태가 없으므로 기록매체에 저장되어 주기적인 상태점검을 통해 오류검사를 시행해야 한다.

8) 영문은 DCC&DPE에서 2007년 발행한 「Digital Repository Audit Method Based on Risk Assessment v1.0」의 88-89쪽 참조. 한글은 임진희, 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 제27호, 2011, 153쪽.

9) 영문은 DCC&DPE에서 2007년 발행한 「Digital Repository Audit Method Based on Risk Assessment v1.0」의 134-212쪽 참조. 한글은 임진희, 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 제27호, 2011, 153쪽.

- 전자기록의 특성을 고려하여 안전하게 장기보존하기 위해 주기적으로 장기보존포맷으로 변환해야 한다.
- 전자기록은 이관 받은 이후부터 전자기록 장기보존을 위한 특별한 관리가 필요하다.

세 번째 작업으로는 전자기록을 장기보존하는 과정에서 관리해야 하는 위험요소를 확인하였다. DRAMBORA가 제시하는 78개 위험요소 목록 중에서 국가기록원에 연관된 요소를 찾기 위해 다음과 같이 작업하였다.

- DRAMBORA가 정의한 보존소 기능 중 전자기록의 장기보존 정책을 결정하고 내용정보가 담긴 디지털컴포넌트의 안전한 저장을 다루는 등 핵심 업무를 다루고 있는 '보존과 저장(Preservation and Storage)'기능에 해당되는 위험요소는 모두를 대상으로 검토하였다.
- 전자기록은 내용정보인 디지털컴포넌트와 메타데이터의 결합물이며 장기보존 과정정보를 기록화하여 메타데이터로 남기게 되므로 메타데이터가 중요하다고 보고 '메타데이터 관리(Metadata Management)'기능에 해당되는 위험요소를 관심있게 검토하였다.
- 전자기록은 정보시스템을 통해 전자적으로 생산·관리되며 장기보존 대상 전자기록의 모든 객체들이 정보시스템에 의해 통제되므로 '기술 인프라 및 보안(Technology Support and Security)' 기능이 중요하다고 보고 관련 위험요소를 검토하였다. 특히, 시스템 일반에 관한 위험요소 보다는 전자기록 객체 관리와 직접적으로 관련이 있는 위험요소를 집중적으로 검토하였다.
- 보존소에 입수될 때부터 제대로 된 품질일 때 해당 기록을 보존하는 것이 의미있을 뿐만 아니라 입수 시점에 향후 장기보

존에 필요한 내용을 확보하는 것이 중요하므로 '획득 및 입수(Acquisition and Ingest)' 기능에 관련된 위험요소를 선택적으로 검토하였다.

네 번째 작업으로는 검토결과 국가기록원이 관리해야 할 것으로 확인된 전자기록 장기보존 업무 위험요소별로 속성 값을 정의하였다. 위험요소의 속성 값들은 이후 위험도를 평가하는 과정에서 그리고 해당 위험요소를 관리하는 과정에서 유용하게 활용될 정보들이다. 각 위험요소별로 정의한 속성 값들은 다음과 같다.

- 위험요소 ID : 위험요소별로 고유한 식별번호를 붙여주었다. DRAMBORA의 경우 R01 - R78의 ID를 붙여 관리하고 있다. 'Risk' 의 줄임 문자로 'R'을 적고 일련번호를 붙인 것으로 파악된다. 국가기록원이 관리할 위험요소에 대한 ID 체계는 'NAK's Risk'의 줄임 문자로 'NR'을 적고 일련번호를 붙이기로 하였다.
- 위험요소명 : 위험요소의 명칭을 적어주었다. DRAMBORA의 위험요소 명칭을 국가기록원의 업무 배경을 고려하고 공공 전자기록이라는 자산의 특성에 맞춰 번역하였다.
- 위험요소설명 : 위험요소의 특징을 간략히 설명해주었다.
- 위험사례 : 위험이 발생하는 상황에 대한 예시를 작성하였다.

2) 국가기록원 위험요소 정의 사례

1)에서 설명한 프로세스에 따라 작업한 결과 국가기록원이 장기보존 대상 전자기록을 안전하게 보존하기 위한 업무를 수행하는 과정에서 발생할 수 있는 위험을 총 44개의 요소로 정의할 수 있었다.[10] 44개의 위험요소는 DRAMBORA에서 제시한 총 78개 위험요소의 부분집합으로

구성된다. 국가기록원은 보존업무에 초점을 맞추었기 때문에 DRAMBORA가 전제로 했던 디지털객체 보존소가 수행하는 8개의 기능 중에서 '보존과 저장'기능을 중심으로 하여 보존에 직접적 영향을 주는 '메타데이터 관리', '기술 인프라 및 보안', '획득 및 입수' 기능 등 관련 기능에서 관련된 위험요소를 찾아 정의할 수 있었다. 44개의 위험요소를 소개하면 다음과 같다.

첫째, 국가기록원이 '보존과 저장' 기능을 수행하는 과정에서 발생할 수 있는 주요한 위험요소는 〈표 1〉과 같이 총 17개가 확인되었다. 예를 들어, NR02, NR03, NR04, NR07의 위험요소는 전자기록이 장기간 보존되는 과정에서 이용가능성, 진본성, 무결성, 신뢰성 등의 핵심 품질이 저하될 위험을 유의해야 한다는 점을 명시화한 것이다. NR01은 보존 과정에서 기록의 기밀성이 지켜지지 않는 것의 위험성을 명시화하였으며, NR08은 장기간 보존되는 과정에서 기록의 보존자가 지속적으로 변경되었을 때 보존자 이력정보와 같은 출처정보를 제대로 관리하지 못했을 때의 위험을 명시화하고 있다. NR10은 장기보존을 위한 조치의 결과로 기록의 진본사본이 복수 개 존재하는데 이들 간에 불일치가 발생하는 경우의 위험을 명시화하였으며, NR09는 장기보존 대상 기록에 문제가 생겼으나 백업본이 제 역할을 하지 못해 복구가 불가능해졌을 때의 위험을 명시화하고 있다. NR14, NR15, NR16은 장기보존을 위해 적절한 계획을 세우고 그에 따라 제대로 실행하지 못했을 때 발생할 위험들을 명시화하고 있다.

10) 업무 정의 및 위험요소 도출 절차와 방법은 임진희, 「DRAMBORA를 응용한 전자기록 장기보존 업무 위험관리체계 연구」, 『기록학연구』 제27호, 2011, 144-151쪽.

〈표 1〉 '보존과 저장' 기능 수행 시 발생할 수 있는 위험요소

ID	위험요소명	위험요소설명
NR01	기록정보의 기밀성 손실	허가받은 특정 집단이나 사람에게만 공개하도록 되어 있는 기록정보가 외부에 유출된다.
NR02	기록정보와 서비스의 이용가능성 상실	허가받은 특정 집단이나 사람이 기록정보와 서비스를 제공받지 못한다.
NR03	기록정보의 진본성 손실	기록정보가 위조 또는 변조 되지 않은 원래 그대로의 것이며, 훼손된 바 없는 상태임을 입증할 수 없다.
NR04	기록정보의 무결성 손실	기록정보가 망실·훼손·손상·변조 등에 의하여 변경되지 않고 완전한 상태를 유지하고 있음을 입증할 수 없다.
NR05	기록정보의 변경 미식별	기록정보 중 하나 이상의 변경이 발생했음에도 불구하고 어디에서 변경이 발생하였는지를 추적하거나 모니터링할 수 없다.
NR06	부인방지 약속의 불이행	기록정보의 이관 시 인계자와 인수자 간의 부인방지 약속이 지켜지지 않는다.
NR07	기록정보의 신뢰성 손실	기록정보가 업무 활동의 완전하고 정확한 표현물로서 믿을 만 하다는 것을 입증할 수 없다.
NR08	기록정보의 출처 손실	기록정보에 대한 이관에서부터의 출처를 입증할 수 없다.
NR09	백업의 비적합성 혹은 손실	백업 절차에 따라 백업을 수행하였으나 데이터나 시스템을 복구할 수 없다.

NR10	진본 사본(복본)들 간의 불일치	진본 사본(복본)들 간에 저장된 전자기록이 일치하지 않는다.
NR11	보존할 개별 전자기록 범위 불분명	지속적으로 보존되어야 하는 전자기록의 대상, 범위(규격), 보존기간 등을 명확하게 지정하지 못한다.
NR12	입수 과정의 유효성 검증 불가능	이관 대상 전자기록에 대한 이관 과정 중 무결성과 진본성이 유지되고 있는지를 단정하지 못한다.
NR13	참조식별자의 무결성 불확실	부여된 참조식별자(Reference ID)를 통해 기록정보를 찾아 낼 수 없다.
NR14	보존계획의 실행 불가능	착수한 보존계획을 실제로 실행할 수 없다.
NR15	보존전략 실행 결과 정보손실 초래	보존계획 수행을 위해 전자기록을 보존처리하는 과정에서 전자기록의 고유한 특성을 하나 또는 그 이상 손상 또는 손실시킨다.
NR16	보존전략 및 보존활동의 유효성 검증 불가능	업무 목표는 설정하였으나 성공적으로 수행되고 있는 실제 보존전략과 보존활동의 범위를 효과적으로 측정하지 못한다.
NR17	입수·보존·배부기록패키지(SIP·AIP·DIP)의 추적 불가능	업무담당자가 기록정보 라이프사이클(information lifecycle)의 특정시점에 해당되는 입수·보존·배부기록패키지를 추적할 수 없다.

둘째, 국가기록원이 '메타데이터 관리' 기능을 수행하는 과정에서 전자기록 장기보존과 관련하여 관리해야할 주요한 위험요소는 〈표 2〉

와 같이 총 5개가 확인되었다. 메타데이터는 데이터베이스로 관리되는 것이 일반적이며, 만약 메타데이터가 관계형 데이터베이스로 구축되어 관리된다면 데이터 간에 참조무결성이 유지되는 것이 가장 기본적인 품질 요건이 되며 NR18이 이 내용을 위험요소로 명시화하고 있다. NR19는 장기보존 과정에서 메타데이터가 변경되었을 때 변경 전의 값과 새로운 값의 이력이 잘 남겨져 있지 않았을 때의 위험을, NR20은 메타데이터가 불충분하여 기록을 검색해 보는 것이 불가능해졌을 때의 위험을, NR21과 NR22는 이용자들이 메타데이터를 통해 기록의 배경이나 내용 자체를 충분히 이해할 수 없을 때의 위험을 명시화하고 있다.

〈표 2〉 '메타데이터 관리' 기능 수행 시 발생할 수 있는 위험요소

ID	위험요소명	위험요소설명
NR18	참조정보 메타데이터의 파손	보존기록패키지와 메타데이터사이의 연관성이 손상되어 더 이상 연결되지 않는다.
NR19	메타데이터 변경이력 문서화 불완전 혹은 실패	보존기록패키지에 실행된 보존전략, 보존절차 및 메타데이터 기록 과정이 일부 혹은 전체가 문서화되지 않았거나 부정확하다.
NR20	기록정보의 검색 불가능	기록정보의 검색을 지원하는 메타데이터가 불충분하다.
NR21	이해가능성 정의의 애매모호함	이용자들이 필요로 하는 또는 기대하는 이해가능성에 대한 의미를 제대로 기술할 수 없다.
NR22	기록의 완전한 재현을 위한 제반 정보의 부족	기록정보를 완전하게 재현할 수 있는 제반 정보(기록물 계층구조, BRM 분류체계 등)를 유지하지 못한다.

셋째, 국가기록원이 '기술 인프라 및 보안' 기능을 수행하는 과정에서 전자기록 장기보존과 관련하여 치명적일 수 있는 주요한 위험요소는 〈표 3〉과 같이 총 18개가 확인되었다. 예를 들어, NR23, NR24, NR19, NR30은 기록관리에 사용되는 시스템의 하드웨어나 소프트웨어에서 문제가 발생할 가능성에 대해, NR24는 기록이 저장되어 있는 매체가 기술적 측면에서 노후화되는 상황에 대해 위험요소로 명시화하고 있다. NR31, NR, 32, NR33, NR34, NR36은 시스템에 대한 해킹, 서버실에 침입 등 다양한 방식과 수준의 시스템 보안사고가 발생할 경우를 위험요소로 다루고 있다. NR35, NR37, NR38은 시스템의 가용성이 지속되지 못했을 때의 위험을 명시화하고 있으며, NR27은 기록관리기관이 외부 기관의 서비스를 이용하여 시스템을 관리하고 있을 때 해당 서비스가 중지되어 발생하는 업무 위험을 명시화하고 있다.

〈표 3〉 '기술 인프라 및 보안' 기능 수행 시 발생할 수 있는 위험요소

ID	위험요소명	위험요소설명
NR23	하드웨어 혹은 소프트웨어가 조직의 새로운 목표 지원 불가능	하드웨어, 소프트웨어 등 기술 인프라가 기관의 업무 변화를 지원할 수 없다.
NR24	하드웨어나 소프트웨어의 불용화	현재 사용하고 있는 하드웨어나 소프트웨어가 일반적으로 사용하는 기술과 부합하지 않는다.
NR25	매체 불용화나 구형화	기록매체의 불용화나 구형화로, 읽거나 쓰는데 제한이 발생한다.
NR26	보안 취약성 및 부당 이용의 미식별	보안상의 취약점이나 부당한 이용이 업무 담당자와 시스템에 의해 식별 및 모니터링되지 못한다.
NR27	제3자 서비스 손실	제3자 서비스가 마비되어 아웃소싱 업무 등 일부 업무가 마비되었다.

NR28	중요 문서의 파손	운영관련 업무 수행 중 발생하거나 참고가 되는 중요 문서가 부분적 또는 완전하게 파손되었다.
NR29	하드웨어 장애	시스템 하드웨어 장애 또는 고장으로 현재 업무가 원활하게 진행되지 못한다.
NR30	소프트웨어 장애	시스템 소프트웨어 장애로 현재 업무가 원활하게 진행되지 못한다.
NR31	시스템 보안 취약성 심화	보안대책에서 결함이 발견되고 미인가된 접근이 이루어진다.
NR32	시스템 공간의 물리적 침입	기술적 하드웨어가 물리적으로 위치한 구역(서버실 등)에 침입자가 접근한다.
NR33	원격 혹은 로컬지역의 소프트웨어 침입	네트워크 보안 대책을 우회하여 구내 또는 외부에서 소프트웨어에 침입한다.
NR34	지역 내 파손이나 침입 현상	시설이 위치하고 있는 지역에 영향을 미치는 외부적인 현상(지진, 태풍 등)에 의해 업무활동이 영향을 받는다.
NR35	불시 시스템 혼선	고의적이지 않은 활동 또는 좋지 않은 결과를 초래할 목적이 없는 활동에 의해 업무활동이 나쁜 영향을 받는다.
NR36	고의적인 시스템 방해	나쁜 결과를 목적으로 시스템에 대한 고의적으로 활동으로 인해 시스템이 중단되거나 피해를 입는다.
NR37	영구기록물관리기관내 파손 및 이용 불가능	기관 내 시설이 파괴되거나 영구적으로 또는 일시적으로 사용이 불가능하다.
NR38	핵심 유틸리티의 이용 불가	외부에서 공급되는 주요 제3자 서비스가 일시적으로 중단되고, 이 서비스의 이용이 불가능하다.
NR39	제3자 서비스 내에서의 조건 변경	공급되는 제3자 서비스의 상태가 대폭 변경된다.
NR40	기술적 인프라 및 보안 효율성에 대한 측정 불가능	기술 인프라와 보안 대책이 업무활동 수행에 어느 정도 부합하고 있는지를 측정할 수 없다.

넷째, 국가기록원이 '획득 및 입수' 기능을 수행하는 과정에서 전자기록 장기보존에 치명적인 영향을 줄 수 있는 주요 위험요소는 〈표 4〉와 같이 총 4개가 확인되었다. NR41, NR42는 입수기록패키지가 보존에 적합하지 않거나 보존에 필수적인 정보를 포함하고 있지 않았을 때의 위험을 명시화하였으며, NR43과 NR44는 입수되는 과정에서 외부의 요인에 의해 기록이 변경되는 일이 발생하거나, 입수기록패키지에서 부터 현재의 보존기록패키지까지 변화되는 전 과정을 추적할 수 없게 될 때의 문제점을 명시화하였다.

〈표 4〉 '획득 및 입수' 기능 수행 시 발생할 수 있는 위험요소

ID	위험요소명	위험요소설명
NR41	입수기록패키지의 구조적 비유효성과 기형	입수된 입수기록패키지가 보존에 적합한 형태가 아니다.
NR42	입수기록패키지의 불완전성	입수된 입수기록패키지가 보존을 위해 필요한 정보를 포함하지 않고 있다.
NR43	입수 과정에서의 입수기록패키지 변경	입수기록패키지가 생산되거나 입수되는 중에 외부요인의 의해 변경 된다(입수과정은 생산시스템에서 추출된 직후부터 CAMS의 입수모듈에 의해 등록될 때까지의 모든 프로세스).
NR44	입수기록패키지에서 보존기록 추적 불가능	보존기록패키지를 그에 상응하는 입수기록패키지로부터 추적할 수 없다.

44개의 위험요소는 각기 속성 정의표를 만들어 상세한 기술을 하였다. 〈표 5〉는 예를 들어, NR10 '진본 사본(복본)들 간의 불일치' 위험요소의 속성을 국가기록원의 전자기록 관리업무 관점에서 정의한 사례이다.

〈표 5〉 NR10 '진본 사본(복본)들 간의 불일치' 속성 정의

위험요소ID	NR10
위험요소명	진본 사본(복본)들 간의 불일치
위험요소설명	보존소가 보존정보(archived information)의 복본을 유지하는 곳에 하나 또는 그 이상으로 다른 복본과 다른 것이 존재한다.
위험사례	진본 사본에 대한 복본 불일치 검사 결과가 불일치 할 경우 이중분산보존을 위해 생산된 진본 사본 간의 필수 메타데이터 값이 일치하지 않는 경우 진본 사본 중 일부가 렌더링(rendering)[11]의 차이를 보이는 경우 진본 사본 간의 불일치를 발견하였으나 이를 처리할 절차서 및 규정이 마련되어있지 않은 경우

3. 위험평가 절차와 방법

1) 위험도 평가서식 개발

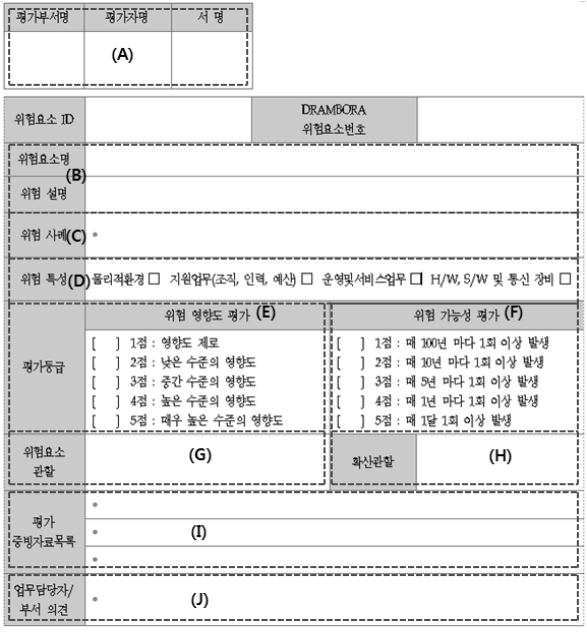
위험요소별로 위험도를 평가하기 위해서는 먼저 평가서식을 개발해야 한다. 평가서식은 다음과 같이 이용될 것을 고려하여 설계하였다. 첫째, 이 서식은 국가기록원의 전자기록 장기보존과 관련된 업무활동을 수행하거나 자산(특히 전자기록)을 관리하는 업무담당자가 평가수행자가 되어 위험평가를 할 때 사용할 것이다. 둘째, 평가에 참여하는 업무담당자는 본인의 업무와 관련된 위험요소는 필수적으로 평가하고 유관 위험요소는 선택적으로 평가할 수 있도록 한다. 셋째, 하나의 위험요소

11) 렌더링(rendering)이란 사전적 의미로는 컴퓨터 프로그램을 사용하여 모델로부터 영상을 만들어내는 과정을 의미한다. 전자문서의 경우, 뷰어를 이용하여 전자문서를 열어 화면에 디스플레이하는 것, 프린터로 인쇄하여 출력하는 것 등이 전형적인 렌더링의 방식이다.

에 복수 개의 위험요소 사례가 제시되어고 사례마다 경중이 있을 경우 각 사례별로 위험평가를 하도록 하고 그 중 높은 점수를 채택하도록 한다. 넷째, 위험평가 시 해당 위험요소와 관련된 업무 프로세스를 사전에 충분히 검토하도록 한다.

국가기록원 전자기록 장기보존 업무의 위험요소 44개를 평가하기 위해 개발한 서식은 〈그림 2〉와 같다.

〈그림 2〉 위험평가서 서식



〈그림 2〉서식에서 (A)는 평가수행자 정보를 입력하는 곳이다. (B)와 (C)는 앞 단계에서 정의한 위험요소에 대한 정보를 입력하는 곳이다. (D) - (J)가 평가수행자가 입력해야 하는 곳으로 평가의 핵심에 해당하는 영역이다.

평가수행자는 (D)영역에 해당 위험요소가 어떤 특성을 가진 요소인지 판단하여 체크하도록 한다. 위험요소는 발생 원인이 무엇이냐에 따라 물리적환경에서 초래하는 것, 지원업무에서 초래하는 것, 운영 및 서비스 업무에서 초래하는 것, H/W, S/W, 통신장비에서 초래하는 것 등 네 가지의 특성으로 구분될 수 있다. 특정 위험요소의 경우 복수 개의 원인을 가질 수도 있으며, 일반적으로 원인에 따라 문제의 해결방법이 달라지므로 특성을 파악하는 것은 중요한 작업이 된다.

평가수행자는 (E)영역에 위험영향도(Risk Impact Score)를 추정하여 입력하도록 한다. 위험요소가 발생했을 때 핵심 자산에 미치는 악영향이 얼마나 클 것이냐를 판단하는 것으로 현행 업무의 통제가능 정도(가능성 감소, 영향도 감소를 위한 조치, 관리 등)를 고려하여 추정하도록 하였다. 만약, 해당 위험요소가 '진본성' 또는 '이해가능성'의 손상 또는 손실 등 자산과 관련성이 매우 약한 것으로 판단되는 경우에도 국가기록원의 이미지나 평판의 손상, 외부평가에 미치는 악영향의 정도 등을 추가로 고려하여 추정하도록 하였다. 위험영향도는 〈표 6〉과 같이 5점 척도로 평가하도록 하였다.

〈표 6〉 위험영향도 평가 점수표

점수	상세설명	비고
1	영향도 미미(Negligible impact), 해당 위험요소 발생 시 전자기록의 진본성(authenticity) 또는 이해가능성(understandability)의 손실이 거의 없음	-
2	낮은 수준의 영향도(Low impact), 해당 위험요소 발생 시 일부 전자기록의 진본성 또는 이해가능성의 손상이 제한적이며, 손상된 진본성 또는 이해가능성을 완전히 회복시키는데 특별한 시간과 노력이 필요 없음	진본성 및 이해가능성 회복 가능 복구를 위한 시간, 노력(비용)이 거의 소요되지 않음

3	중간 수준의 영향도(Medium impact), 해당 위험요소 발생 시 일부 전자기록의 진본성 또는 이해가능성의 손상이 어느 정도 발생하지만, 손상을 완전히 회복시키는데 어느 정도 시간과 노력이 필요함	진본성 및 이해가능성 회복 가능 복구를 위한 시간, 노력(비용)이 소요됨
4	높은 수준의 영향도(High impact), 해당 위험요소 발생 시 상당 부분의 전자기록의 진본성과 이해가능성의 손상이 발생하며, 손상된 진본성 또는 이해가능성을 회복시키는 것이 가능하기는 하나 상당한 시간과 노력이 필요함	일부 전자기록의 진본성 및 이해가능성 회복 불가능 복구를 위한 시간, 노력(비용)이 천문학적으로 소요됨
5	매우 높은 수준의 영향도(Low impact), 해당 위험요소 발생 시 저장중인 대부분이 전자기록의 진본성과 이해가능성의 손상이 발생하며, 손상된 진본성 또는 이해가능성을 회복시키는 것이 완전히 불가능함	모든 전자기록의 진본성 및 이해가능성 회복불가능

평가수행자는 (F)영역에 위험의 발생가능성(Risk Probability Score)을 추정하여 입력하도록 한다. (D)에 체크한 특성과 현 업무 상황을 염두에 두고 평가 점수를 부여하도록 한다. 업무의 수행과정에서 위험이 발생할 수 있기 때문에 특정 업무의 수행주기를 살펴볼 필요가 있다. 예를 들면, 다음과 같은 업무의 수행주기를 살펴 위험발생가능성을 추정할 필요가 있다.

- 기록물 이관 주기
- 기록물 재배치 주기
- 공개·비공개 재분류 주기
- 매체 교체 주기
- 보존전략 실행 주기
- 상태점검 및 정수점검 주기
- 시스템 업데이트 주기

– 업무 담당자 교체 주기
– 조직 목표 혹은 업무 전략 변경 주기

또한, 실제 업무 수행 중의 경험(통계 데이터 포함)이나 민원 발생 통계, 유사 기관의 경험 또는 통계 등을 참고하여 위험의 발생가능성을 추정하도록 한다. 위험발생 가능성은 다음 〈표 7〉과 같이 5점 척도로 평가하도록 하였다.

〈표 7〉 위험 발생가능성 평가 점수표

점수	상세설명
1	최소 발생 가능성(Minimal probability), 매 100년 이상에 한 번 발생
2	낮은 발생 가능성(Low probability), 매 10년 마다 한 번 정도 발생
3	중간 발생 가능성(Medium probability), 매 5년마다 한 번 정도 발생
4	높은 발생 가능성(High probability), 매 년 한 번 정도 발생
5	매우 높은 발생 가능성(Very high probability), 매 월 한 번 이상 발생(매일 포함)

평가수행자는 (G)영역에 해당 위험요소에 대해 책임지고 통제할 수 있는 책임권한을 지닌 관할 조직명을 입력하도록 한다. 2010년 현재 국가기록원 내에 전자기록 장기보존과 관련하여 6개의 처리과가 책임을 나누어 가지고 있었으며 평가수행자가 가이드를 참조하여 각 위험요소별로 주무 관할이라 생각되는 처리과명을 평가서에 기입하도록 하였다.

평가수행자는 (H)영역에 해당 위험이 발생하여 관할 단위조직에서 통제가 불가능해졌을 경우 통제권을 넘겨줄 확산관할 조직명을 입력하도록 한다. 2010년 현재 국가기록원 내에 전자기록 장기보존과 관련하여 확산관할권을 지닌 부서로 3개의 부가 있었으며 평가수행자는 가이

드를 참조하여 각 위험요소별로 확산관할이라 생각되는 부의 명칭을 평가서에 기입하도록 하였다.

평가수행자는 (I)영역에 위험 영향도와 발생가능성 평가 결과를 증빙할 수 있는 자료 목록을 기입하도록 한다. 관련 문서명을 기입하거나 시스템에 구현되어 있는 관련 기능을 기술하도록 한다.

평가수행자는 (J)영역에 위험요소에 관한 다양한 의견들을 기술하도록 한다. 예를 들어, 발생가능성이나 위험영향도를 현 상태보다 경감시킬 수 있는 규정, 업무절차 등이 개발 중이라거나, 발생가능성이나 위험영향도를 감소시키는데 필요한 대책(관리, 시설, 절차 등)을 대략적으로 기술하도록 한다.

2) 위험평가 실행 절차

국가기록원에서는 다음과 같은 절차에 따라 위험요소 44개에 대한 평가를 수행하였다. 평가 전에 먼저 전자기록 장기보존의 주무 처리과 업무담당자들 전체를 대상으로 사전설명회를 개최하였다. 평가작업에 대해 충분히 이해할 수 있도록 DRAMBORA 프레임워크를 교육하고 평가 절차에 대해 공유하였다. 다음으로는 총 6명의 평가수행자들을 선정하여 이들을 대상으로 별도 교육을 실시하고 위험평가를 실행하였다.

위험평가는 1차, 2로 나누어 반복적으로 실행하였다. 먼저 1차 위험평가 후 결과를 검토하고 평가수행자에게 피드백한 후 2차 위험평가를 실행하였다. 1차 위험평가를 실행해 보니 동일 위험요소에 대하여 평가수행자별로 평가 결과값의 편차가 크게 나오기도 하였다. 이는 평가수행자 별로 담당업무가 달라 위험요소를 바라보는 관점이나 경험, 인식이 서로 다르기 때문인 것으로 분석되었다. 또한, 개인별로 상황을 긴박하게 보는 성향과 그렇지 않은 성향이 반영되어 평가 결과값의 분포에 차이를 보이기도 하였다. 평가 신뢰도를 높이기 위해서는 개인별로

평가한 점수에 대해 통계적 처리과정이 필요하다는 것을 알 수 있었다. 1차 평가를 통해 의외의 성과도 얻었는데, 이는 평가수행자가 44개의 위험요소 중 자신의 업무와 관련이 있는 것을 찾아 평가하는 과정에서 자신의 업무와 관련이 있는 위험요소를 새로이 인식하게 되는 효과를 얻었다는 점이다. 한편, 1차 평가 시 평가수행자들은 몇몇 위험요소에 대해서는 내용을 이해하는 데 어려움을 느끼기도 하였는데 이는 본인들이 직접 위험요소를 도출하지 않았다는 점과 일부 위험요소는 현재 국가기록원이 미처 활발하게 수행하고 있지 않은 미래의 업무에 연관되어 있기 때문인 것으로 분석되었다. 당연히 위험요소에 대한 이해도가 낮은 평가수행자는 발생가능성과 영향도의 추정과정에서 어려움을 표시했다. 그러나, 2차 평가 시에는 평가의 초점을 전자기록의 "진본성"과 "이해가능성"으로 명확히 함으로써 발생가능성과 영향도의 등급 점수를 매기는 기준에 대한 모호함을 줄일 수 있었고 평가수행자들의 위험요소에 대한 인식 수준도 동질화할 수 있었다.

3) 국가기록원 위험평가 결과 사례

44개 위험요소를 평가한 결과를 취합해 보니 평가서는 모두 236장이었다. NR01-NR28까지는 6명, NR29-NR40까지는 4명, NR41-NR44까지는 5명이 평가서를 작성해주었기 때문이다. 다수의 평가수행자가 참여했으므로 평가결과에 대한 신뢰도는 높아졌다고 볼 수 있는 반면 평가수행자 각각의 관점이 달라 위험요소의 특성, 관할/확산관할 등에 대한 값에는 편차가 크게 나타났다. 따라서, 하나의 위험요소에 대해 복수자가 평가한 결과 값을 취합하기 위해 몇 가지 원칙이 필요했다. 예를 들어, 평가수행자마다 위험요소의 특성을 다르게 체크한 경우가 다수 있었는데 이 경우 평가수행자들의 의견을 존중하여 합집합으로 정리하기로 하였다. 특성별로 관할 조직도 달라질 수 있어 관할 조직 정보도 합집

합으로 정리하기로 하였다. 한편, 평가 결과 값 중에 일관성이 없는 데이터를 발견하였는데, 이는 특정 평가수행자의 데이터로 논의 끝에 무성의한 평가값이 전체 결과를 오도할 가능성이 있으므로 취합에서 제외하기로 결정하였다.

위험요소별 영향도와 발생가능성을 입력으로 하여 위험도를 계산했는데, 하나의 위험요소에 대해 복수의 평가 결과가 존재하므로 계산수식은 "위험도 = Average(발생가능성) x Average(위험영향도)"로 구성하게 되었다. 즉, 발생가능성의 평균값과 영향도의 평균값을 구하여 곱하여 위험도를 계산하는 것이다. 따라서 위험도는 최고 25점부터 최하 0점 사이의 값을 가지게 된다. 만약, 평가자가 7인 이상일 경우에는 최상위 값과 최하위 값을 먼저 제외한 후 나머지 값들로 평균을 구하는 방식을 채택하는 것이 통계적 유의성을 확보할 수 있는 방법임을 확인하였으며, 모든 수치는 소수 둘째자리에서 반올림하여 계산하기로 하였다.

위험도 점수에 따라 1등급(20점 초과 - 25점), 2등급(15점 초과 - 20점), 3등급(10점 초과 - 15점), 4등급(5점초과 - 10점), 5등급(0점 - 5점)으로 나누어 분류를 해보면, 2010년 위험평가 결과 1등급 위험요소는 없었고, 2등급에 해당하는 위험요소는 NR03 '기록정보의 진본성 손실', NR05 '기록정보의 변경 미식별', NR20 '메타데이터 변경이력 문서화 불완전 혹은 실패' 등 3개가 존재하는 것으로 밝혀졌다. 전체 44개 위험요소의 최종 위험도, 등급, 위험도 순위는 〈표 8〉과 같다.

〈표 8〉 위험도 평가 결과

ID	위험도	등급	순위	ID	위험도	등급	순위
NR01	6.4	4	35	NR23	9.6	4	18
NR02	7.6	4	30	NR24	6.8	4	32
NR03	16.6	2	1	NR25	8.8	4	25
NR04	13.4	3	7	NR26	10.6	3	15
NR05	15.2	2	3	NR27	11.0	3	13

NR06	8.3	4	26
NR07	9.6	4	19
NR08	9.6	4	19
NR09	9.4	4	21
NR10	10.9	3	14
NR11	12.2	3	11
NR12	13.7	3	6
NR13	8.2	4	27
NR14	8.9	4	22
NR15	10.1	3	17
NR16	10.6	3	15
NR17	12.2	3	9
NR18	8.8	4	24
NR19	16.0	2	2
NR20	6.6	4	34
NR21	6.8	4	31
NR22	7.8	4	29

NR28	6.7	4	33
NR29	8.9	4	23
NR30	6.2	4	36
NR31	8.0	4	28
NR32	6.0	4	38
NR33	12.2	3	10
NR34	4.7	5	40
NR35	3.3	5	44
NR36	4.0	5	43
NR37	4.7	5	40
NR38	5.0	4	39
NR39	4.7	5	40
NR40	6.2	4	36
NR41	13.1	3	8
NR42	14.0	3	4
NR43	13.8	3	5
NR44	11.3	3	12

4. 위험관리 방안의 설계

1) 위험관리 방안 설계 요소

위험도가 높은 위험요소에 대해서는 발생을 예방하기 위한 조치를 실행하고, 발생 시에는 악영향을 최소화하기 위한 대응 조치 계획을 세워 두고 이에 대비한 훈련을 실시해야 한다. 전자기록 장기보존 업무가 잘못되어 어느 순간 대량의 전자기록이 진본성이 훼손되고 이해가능성이 상실되어 버린다면 기록관리기관의 입장에서는 상황에 따라 재난으로 취급하고 대응할 필요가 있을 수 있다. 따라서, 고위험도의 위험요소에 대해서는 발생의 사전·사후 관리방안과 비상대책조직, 위험 상황

발생 시 피해를 평가하는 방법, 재난기준 및 재난선포방법, 개인임무카드 등의 개발이 필요하다. 조직에서는 이러한 내용이 담긴 위험관리등록부를 따로 관리해야 한다.

먼저, 위험관리등록부를 작성한다. 조직 내 체계적 관리가 용이하도록 위험관리등록부에 각 부서별 위험관리 정보를 일괄 등록하도록 한다. 위험관리등록부에는 위험요소별로 위험기본정보(〈표 9〉)와 위험평가정보(〈표 10〉), 그리고 위험관리정보(〈표 11〉)를 각각 입력하고 갱신하도록 한다. 먼저, 위험기본정보는 위험요소의 고유식별자인 위험요소 ID와 위험요소명, 그에 대한 설명과 사례, 위험 특성, 기본정보변경일시, 변경사항으로 구성된다. 위험평가정보는 점검주기, 위험식별일시, 평가일시, 평가자명, 위험요소관할, 위험요소 확산관할, 위험가능성, 위험영향도, 위험도, 위험등급, 평가증빙자료목록, 평가정보 변경일시, 변경사항으로 구성된다. 위험관리정보는 사전관리방안, 사후관리방안, 관리정보 변경일시, 변경사항으로 구성된다.

〈표 9〉 위험등록부의 위험기본정보 구성

위험기본정보	**위험요소 ID**	고유식별자 기술	**위험요소명**	위험요소이름 기술
	위험 설명	위험요소에 대해 문장으로 정의해서 기술		
	위험 사례	• 위험이 발생한 사례 기술		
	위험 특성	1)물리적환경, 2)지원업무(조직, 인력, 예산), 3)운영및서비스업무, 4)H/W, S/W 및 통신 장비 중 이전 평가 결과 도출된 특성을 기술		
	기본정보 변경일시	기본정보가 변경된 날짜, 시간, 장소 등을 기술	**변경사항**	변경이력 기술

〈표 10〉 위험등록부의 위험평가정보 구성

위험평가정보	**점검주기**	위험평가를 실행하는 주기 기술	**위험식별일시**	위험을 식별한 일시 기술
	평가일시	평가를 실행 한 일시 기술	**평가자명**	평가를 수행한 평가자의 소속과 이름을 기술
	위험요소 관할	위험요소 관할 과단위 기술	**위험요소 확산관할**	위험요소 확산관할 부단위 기술
	위험가능성	위험가능성 평균 점수 기술	**위험도**	위험도 기술
	위험영향도	위험영향도 평균 점수 기술	**위험등급**	위험등급 기술
	평가증빙자료 목록	• 증빙자료 기술 • 중복기술 가능 • 되도록 문서화된 자료를 첨부하고, 참조를 하이퍼링크		
	평가정보 변경일시	평가정보가 변경된 날짜, 시간, 장소 등을 기술	**변경사항**	변경이력 기술

〈표 11〉 위험등록부의 위험관리정보 구성

위험관리정보	**사전관리 방안**	사전관리방안 기술 정책 요구/시스템 구성/관리방안 실행 방법 등		
	사후관리 방안	위험발생 이후 위험을 수습하기 위한 방법과 절차 등을 기술		
	관리정보 변경일시	관리정보가 변경된 날짜, 시간, 장소 등을 기술	**변경사항**	• 변경이력 기술

다음으로는 위험이 발생되었을 때 필요한 비상대책조직을 구성해 두어야 한다. 비상대책조직 체계는 해당 업무활동의 연속성을 유지 · 관리

하고 비상상황 발생 시 피해를 최소화 하기위한 신속한 대응 및 복구의 지원을 목적으로 한다. 비상시의 위계를 명시한 조직 구성도를 제시하고, 각 조직의 역할과 책임을 명시하여야 한다. 이 체계를 이용하여 평소 모의훈련을 실시함으로써 위기 발생 시 일사불란한 지휘통제 하에 신속한 대응이 가능하도록 한다.

다음으로는 피해평가 및 재난기준과 재난선포 방법을 정해둔다. 위험요소의 발생 시 누가 어떻게 피해규모와 원인을 평가해야 하는지 정하고, 피해평가의 결과 재난으로 판단할 수 있는 기준값을 제시하여 일정 수준이상의 피해가 발생했을 경우 재난을 선포하거나 관할권을 상부조직 체계로 이관하는 등의 조치를 취하도록 한다. 예를 들어, 전자기록의 무결성과 진본 사본(복본) 간의 불일치가 발생했을 때의 피해를 평가하는 기준으로는 훼손이나 불일치가 발생한 기록 건 수량, 피해 기록의 복구에 걸리는 시간과 비용을 적용할 수 있다.

다음으로는 개인임무카드를 작성한다. 전자기록 장기보존 업무담당자들이 위험요소와 관련하여 숙지하고 있어야 하는 임무내용을 담은 카드로 위험발생 시에는 일관된 조치를 취할 수 있도록 절차별 행동요령을 담아 업무담당자들에게 배포한다. 국가기록원 전자기록 장기보존 위험관리를 위한 개인임무카드는 총 8면의 카드로 설계하였으며 구성은 다음과 같다.

- 1면 : 임무카드의 목적과 범위를 명시하고, 해당 임무카드를 소지해야하는 업무담당자 목록을 적는다.
- 2면 : 평소에 전자기록의 무결성 검증과 사본(복본)들 간의 일치성 검증을 위해 수행하는 업무내용과 위험의 발생여부를 모니터링 하는 업무내용을 담는다.
- 3면 : 위험이 발생하여 고지를 받았을 때의 즉각적인 행동요령을 담는다.

- 4면 : 비상대책반의 구성 체계를 담는다.
- 5면 : 피해평가와 재난선포의 기준 및 행동요령을 담는다.
- 6면 : 재난 선포 요령을 담는다.
- 7면 : 복구를 위한 활동과 복구 이후 위험처리 이후 평시업무로 돌아가는 과정을 담는다.
- 8면 : 업무담당자들의 위험관리 절차와 행동요령을 프로세스 맵으로 도식화한다.

위험관리 방안을 설계하는 것은 시간과 비용이 소요되는 작업이므로 2010년 국가기록원에서는 2개의 고위험도 위험요소에 대해 관리방안을 개발한 바 있다. 평가결과 시급한 조치가 필요한 고위험도의 위험요소 중 영향도가 크고 시스템화를 통해 관리할 수 있는 요소를 선별한 후 업무 상 우선순위가 높은 것으로 최종 다음 2개의 위험요소를 선정하였고 관리방안을 개발하였다.

- NR04 '기록정보의 무결성 손실'
- NR10 '진본 사본(복본)들 간의 불일치'

〈표 12〉 NR04 위험요소의 기본정보

위험요소 ID	NR04	**위험요소명**	기록정보의 무결성 손실
위험 설명	망실·훼손·손상·변조 등에 의하여 기록이 변경되지 않고 완전한 상태를 유지하고 있음을 입증할 수 없다.		
위험 사례	마이그레이션 등 관리상의 변경이 있었으나, 감사증적 이력과 일치하지 않아 이를 입증할 수 없는 경우 공공기록물관리법 시행령 제50조에 규정된 전자기록 상태검사를 수행하지 않아 무결성 손실을 모니터링하지 못하는 경우		

〈표 13〉 NR10 위험요소의 기본정보

위험요소 ID	NR10	위험요소명	진본 사본(복본)들 간의 불일치
위험 설명	진본 사본(복본)들 간의 일치 여부를 증명할 수 없다.		
위험 사례	보존안정성 강화를 위해 생성된 진본 사본(복본)들 간의 일치 검사 결과가 동일하지 않은 경우 진본 사본(복본)들 중 일부가 렌더링(rendering)의 차이를 보이는 경우		

2) '기록정보의 무결성 손실' 위험관리 방안 사례

NR04 위험요소에 대한 사전관리방안과 사후관리방안은 기본 정보와 함께 위험관리등록부에 기재하였다. NR04의 위험관리 방안은 전자기록관리시스템이 다음의 기능을 제공한다는 것을 전제로 하고 작성되었다.

- 전자기록의 무결성을 검증하기 위한 체크섬 정보가 생성되어 유지되고 있다.
- 전자기록의 무결성이 훼손되었을 때 복구하기 위한 백업본이 존재한다.
- 전자기록에 대한 무결성을 주기적으로 체크한다.
- 무결성이 훼손되었음을 감지하여 업무담당자에게 고지해 준다.
- 무결성 훼손의 범위와 내용을 보고서로 생성해 준다.
- 업무담당자가 가장 적합한 백업본을 선택하여 복구에 사용할 수 있도록 기능을 제공한다.

NR04의 위험관리등록부는 〈표 14〉와 같이 작성 완료되었다.

〈표 14〉 NR04 위험관리등록부 사례

위험관리등록부					
위험기본정보	위험요소 ID	NR04	위험요소명	기록정보의 무결성 손실	
	위험 설명	망실·훼손·손상·변조 등에 의하여 기록이 변경되지 않고 완전한 상태를 유지하고 있음을 입증할 수 없다.			
	위험 사례	• 마이그레이션 등 관리상의 변경이 있었으나, 감사증적 이력과 일치하지 않아 이를 입증할 수 없는 경우 • 공공기록물관리법 시행령 제50조에 규정된 전자기록 상태검사를 수행하지 않아 무결성 손실을 모니터링하지 못하는 경우			
	기본정보 변경일시	2010.08.13	변경사항	사례추가, 위험특성 수정	
위험평가정보	점검주기	1년	위험식별 일시	2010.07.03	
	평가일시	2010.08.19	평가자명	김00	
	위험 특성	운영 및 서비스 업무 H/W, S/W 및 통신장비			
	위험요소 관할	사회·경제·특수기록관리과 보존관리과 보존복원연구과 기록정보화과	위험요소 확산관할	기록관리부 기록정보서비스부	
	위험가능성	4.2	위험도	13.4	
	위험영향도	3.2	위험등급	3	
	평가 증빙자료목록	•			
	관리정보 변경일시	2010.08.19	변경사항	• 평가	

위험관리정보	사전관리방안	• 기록물관리 법령에 근거하여 전자기록의 무결성에 관한 개념을 실무적, 구체적으로 정의 • 국가기록원이 장기 보존하는 전자기록을 어느 수준으로 무결성 보장할 것인지 정책과 목표를 설정 • 전자기록의 관리과정을 상세 분석하여 무결성 취약지점을 선별하고 대응책을 마련하는 업무절차 유지 • 소프트웨어, 하드웨어, 네트워크 등 보존관리에 사용되는 시스템적 요소들이 전자기록의 무결성 보장 목표에 적합하도록 상태 유지 • 무결성 유지를 위한 법령, 정책, 목표, 업무절차, 시스템을 포함한 프레임워크를 문서화		
	사후관리방안	• 이전 백업 자료로부터 기록물과 메타데이터 등 훼손된 정보를 복원		
	관리정보 변경일시	2010.08.23	변경사항	• 사전관리방안 추가

NR04에 대한 구체적인 위험관리 방안을 만들기 위해 내부 업무담당자와 연구팀, 외부 전문가그룹의 참여하에 심도깊은 워크숍을 진행하였다. 그 결과 전자기록 무결성 유지를 위해서는 〈표 15〉와 같은 세부적인 대응책이 제시되었다.

〈표 15〉 전자기록 무결성 손실 방지 및 대응책

논의 항목	제안내용
기록정보의 무결성 개념 정의와 체크의 기본 단위	무결성 훼손의 개념을 “인가되지 않은 조작에 의해 관리대상 전자기록 객체의 비트스트림과 내용이 동시에 변경되는 경우”로 정의하는 것이 위험요소의 핵심에 접근하는 것이라고 판단함 이는 전자기록의 유통 시 무결성 훼손 문제보다는 보관 중인 전자기록의 무결성 훼손을 주요 사안으로 다루고자 하는 것임 무결성 유지의 의미있는 최소 단위를 기록 건으로 정하며, 철단위, 매체단위로 중첩하여 무결성 확인 및 복구를 적용하도록 함.
기록정보의 무결성 확인 방법과 주기	보존과정에서의 무결성 확인을 위해 별도의 체크섬 정보를 생성, 유지, 활용하도록 함. 복구기능까지는 필요없이 빠르게 단위별 무결성 확인이 가능한 알고리즘으로 충분하다고 판단함. 무결성 체크 대상의 상위레벨에서 먼저 체크섬들의 체크섬 정보를 생성하여 메타데이터에 보관하고 있는 체크섬 정보와 비교해 봄. 값이 서로 다를 경우 하위레벨에서 다시 한 번 무결성 체크를 해줘야 함 기록 건의 체크섬 정보를 생성하여 메타데이터에 보관된 이전의 체크섬 정보와 상호 비교하여 동일하지 않은 경우 무결성이 훼손된 것으로 추정함. 보존되면서 관리되는 모든 전자기록은 최소한 일 년에 한 번 이상 무결성 검증을 받아야 함
기록정보의 무결성이 훼손된 원인 추적 방법	비트스트림과 내용이 변경되는 과정을 살펴볼 수 있는 감사증적과 시스템 로그를 활용하는 등 일차적으로는 기술적인 추적 기반이 필요함
기록정보의 무결성 손실이 재난으로 인식되는 수준	무결성이 훼손된 기록물의 가치에 따라 손실의 정도가 달라질 수 있으나 현재로서는 모든 기록물에 대해 손실의 위험을 평가하지 않고 있으므로 양적인 기준을 세우는 것이 현실적임 기록물의 이동과정에 따른 무결성 확보가 전제된 상황에서의 무결성 훼손이라면 기록 건 하나라도 무결성 검증이 안될 때는 주의를 요하는 상황이 됨 또한, 복구를 위한 준비가 얼마나 마련되어 있느냐가 손실의 정도에 영향을 줌. 국가기록원의 1년 예산 전체를 기준으로 하여 무결성 훼손으로 인한 피해를 복구하는데 드는 비용이 1년 예산의 30%를 넘게 된다면 재난의 수준으로 인식할 수 있을 것임
무결성이 훼손된 기록정보를 복구하는 방법과 절차	백업, 미러링 등의 방법을 통해 만들어진 복제본을 이용하여 무결성이 훼손되었다고 판단된 기록을을 대체함

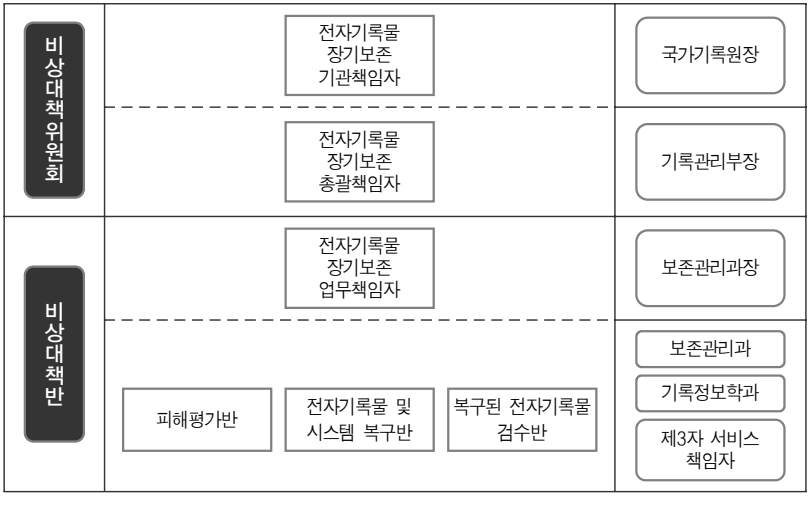
전자기록 장기보존 관련 위험이 발생했을 때 필요한 비상대책조직도는 〈그림 3〉과 같으며, 각 조직의 역할과 책임은 다음과 같이 정하였다.

- 전자기록 장기보존 기관책임자 : 전자기록 장기보존 과정에서 발생하는 재난 수준의 위험(기록정보의 무결성 손실, 진본 사본(복본)들 간의 불일치 등)의 예방 및 대응 전반에 대한 총괄 및 책임을 가지며, 전자기록과 시스템 및 업무의 복구를 위한 협조 사항을 검토하고 승인하고, 위험 발생 결과가 재난 기준을 넘어서면 재난을 선포한다.
- 전자기록 장기보존 총괄책임자 : 전자기록 장기보존 과정에서 발생하는 재난 수준의 위험을 예방하고 대응하는 활동 전반에 대한 실무를 담당하며, 비상 시 '전자기록 장기보존 업무책임자'로부터 보고를 받고, 심각도를 파악하여 이를 '전자기록 장기보존 기관책임자'에게 보고한다.
- 전자기록 장기보존 업무책임자 : 전자기록 장기보존 과정에서 발생하는 재난 수준의 위험을 예방하고 대응하는 활동 전반에 대한 실무를 담당하며, 전자기록과 시스템 및 업무의 신속하고 효과적인 복구를 위해 비상대책반이 상호 협력하여 대응할 수 있도록 관리하고, 운영을 총괄함. 또한 '피해평가반'의 피해평가 결과를 바탕으로 재난기준을 넘어선 위험 발생 시 이를 '전자기록 장기보존 총괄책임자'에게 보고한다.
- 피해평가반 : 발생한 위험의 피해정도를 평가하여 그 결과를 '전자기록 장기보존 업무책임자'에게 보고하고 피해평가 결과를 관리하며, 위험 발생 원인을 규명한다.
- 전자기록 및 시스템 복구반 : 피해를 입은 전자기록과 시스템을 복구하며, 복구 이력을 관리한다. 또한 동일 위험 및 재난이나 유사한 위험 및 재난의 재발을 대비하기 위해 '제3자 서비스 책임자'와의 협조 하에 H/W, S/W 및 보안과 관련하여 필요한 기능을 개발하고 구현한다.

– 업무 복구 및 복구된 전자기록 검수반 : 전자기록 장기보존 업무의 신속하고 원활한 운영을 위해 업무를 복구하며, '전자기록 및 시스템 복구반'에 의해 복구된 전자기록의 상태를 점검하고, 업무의 복구 및 복구된 전자기록의 이력을 관리함. 또한 '피해평가반'이 규명한 위험과 재난의 원인과 유사한 현상의 발생을 예방하기 위한 대책을 마련한다.
– 제3자 서비스 책임자 : '피해평가반'에 의해 규명된 위험 및 재난 발생 원인에 따라 '업무 복구 및 복구된 전자기록 검수반'의 지휘 하에 H/W, S/W 및 보안관련 기능을 복구하며 필요한 기능을 개발하고 구현한다.

전자기록 장기보존 비상대책조직의 역할과 책임은 주기적인 교육 및 모의 훈련을 통해 숙지되어야 하며, 위험이나 재난상황 발생 시 혼란 없이 효과적으로 전자기록과 업무 및 시스템을 복구할 수 있도록 해야 한다.

〈그림 3〉 전자기록 장기보존 비상대책조직도 사례



NR04 '기록정보의 무결성 손실' 위험의 피해평가는 전자기록 장기보존 비상대책조직의 비상대책반에 소속된 '피해평가반'에서 수행하게 되는데, 무결성이 손실된 전자기록의 건과 철, 매체 단위로 이를 복구하기 위해 발생하는 비용(새로운 매체 제작비용, 인력 투입 비용 등)과 업무중단 및 서비스 손실에 따르는 기회비용을 계산하여 전자기록 장기보존을 위해 책정된 국가기록원의 1년 예산과 비교하여 피해 규모를 평가하도록 설계하였다.

3) '기록정보의 무결성 손실' 재난관리 방안 사례

위험이 발생했을 때 이를 재난 수준의 위험으로 판단하여 '비상대책조직'을 공식적으로 가동하기 위한 절차를 '재난선포'라고 하는데, NR 04 '기록정보의 무결성 손실'에 대한 재난을 선포하는 주체와 기준 및 절차는 다음과 같이 설계하였다.

- 관심(Warning, 1단계): 매체와 상관없이 1건의 전자기록의 무결성이 손실되고 1일 이내에 이를 복구 할 수 있는 경우로 비상대책조직을 구성하지 않고 전자기록 장기보존 업무책임자의 관리 하에 위험을 통제한다.
- 주의(Minor, 2단계): 2개 이상의 매체에서 각각 1건의 전자기록의 무결성이 손실되거나 1개의 매체에서 2건 이상의 전자기록 무결성 손실되며 3일 이내에 이를 복구 할 수 있는 경우로 비상대책조직을 구성하지 않고 전자기록 장기보존 업무책임자의 관리 하에 위험을 통제한다.
- 경계(Critical, 3단계): 다수의 매체에서 다수건의 전자기록 무결성 손실이 발생하며 이를 1주일 이내에 복구 할 수 있는 경우

로 필요에 따라 비상대책조직을 소집할 수 있으며 전자기록 장기보존 업무책임자나 전자기록 장기보존 총괄책임자의 관리 하에 위험을 통제함. 필요에 의해 비상대책조직이 구성된 경우에는 전자기록 장기보존 기관책임자가 재난을 선포한다.

- 심각(Fatal, 4단계): 다수의 매체에서 다수건의 전자기록 무결성 손실이 발생하며 이를 1달 이내에 복구 할 수 있는 경우로 전자기록 장기보존 비상대책조직이 소집되며 전자기록 장기보존 기관책임자의 재난 선포 하에 전자기록 장기보존 총괄책임자와 업무책임자가 위험을 통제한다.

관심(1단계)과 주의(2단계)는 재난 상황에 해당되지 않으며 초기 대응으로 복구가 가능하다고 본다. 경계(3단계)와 심각(4단계)은 재난 상황에 해당되며 전자기록 장기보존 기관책임자가 재난으로 선포하며 비상대책조직을 소집하도록 한다. 재난은 전자기록 장기보존 기관책임자(국가기록원장)가 다음과 같은 내용으로 가능한 모든 커뮤니케이션 방안(유선전화, 휴대폰, 사내 메신저, SNS, 재난 관리 시스템, 포털 등)을 활용하여 선포하여야 한다.

> "200*년 00월 00일 00시 00분 다수의 매체에서 다수건의 전자기록에 무결성 손실이 발생하여 전자기록 장기보존 업무 수행에 심각한 영향이 예상됩니다. 이에 200*년 00월 00일, 00시 00분을 기준으로 전자기록 장기보존 업무의 비상상황을 선포합니다."

NR04 '기록정보의 무결성 손실' 위험으로 인한 재난에 대비하여 〈그림 4〉와 같은 개인임무카드를 작성하였다.

〈그림 4〉 NR04 '기록정보의 무결성 손실' 재난 시 개인임무카드 사례

5. 맺음말

위험관리 기법은 지속적인 실행을 통해 효과를 얻을 있다. 이 논문에서 살펴본 사례의 경우도 국가기록원이 최소 연 1회 정기적으로 관련 업무의 위험평가를 수행하고 그에 따른 조치를 취할 때 의미가 있는 것이다. 동일한 위험요소의 위험도는 외부적 환경요인에 의해서도 변화하며, 내부적 업무 및 시스템 준비도에 의해서도 변화한다. 위험은 사전예방조치가 우선이므로 조직 내에서 고위험도의 위험요소를 관리하는데 자원배분을 먼저할 수 있도록 매년 정기적으로 평가를 수행해야 한다.

정기적인 위험평가 과정에서 전자기록 장기보존 업무 평가 프레임워크가 가진 다음과 같은 한계점들을 지속적으로 개선해 나가야 할 것이다. 첫째, 본 논문의 사례에서 제시한 전자기록 장기보존 업무의 평가 프레임워크는 위험요소별로 발생 사례가 충분히 확보되지 못하였다. 왜냐하면, 아직 국가기록원이 대량의 전자기록 보존업무를 본격화하지 않았기 때문이다. 2015년 이후에는 매년 대량의 전자기록을 이관받으면서 누적되는 기록을 보존하기 위한 도전적인 과제를 부여받게 될 것이다. 안정적인 업무가 정착되기까지의 여러 시행착오들을 위험요소와 연결하여 사고하고 위험의 발생사례로 위험관리등록부에 누적해 간다면 도움이 될 것이다. 둘째, 본 논문의 사례에서 제시한 위험요소에서 속성을 정의할 때 사용한 용어가 국가기록원의 전자기록 관리업무에 정확히 부합하지는 못하고 있다. 이는 DRAMBORA의 산출물을 응용하는 과정에서 상당수의 위험요소가 국가기록원 입장에서는 잠재적인 위험으로만 인식할 뿐이므로 내부 조직의 언어로 기술하기에는 시기상조였기 때문이다. 향후 보존업무가 본격화되면서 업무활동 기술서를 작성하고 이를 위험관리등록부에 반영하는 과정을 거쳐야 할 것이다.

2010년 국가기록원이 평가한 44개의 위험요소 중 위험도 상위 10위에

속했던 위험요소는 〈표 16〉과 같다. 각각 4, 5, 6, 8, 9위에 해당하는 NR42, NR43, NR12, NR41, NR17은 보존과정이라기 보다는 입수과정에서의 위험요소에 해당한다. 입수 시의 오류는 보존과정에서 복구할 수 없으므로 효과적인 보존이 되려면 입수시 문제점이 없어야 한다. 2015년 본격적 대량 전자기록 이관을 앞두고 입수 과정에 대해 세밀하게 점검해봐야 한다는 업무담당자들의 인식이 위험도 평가에 반영된 것으로 이해할 수 있다.

〈표 16〉 2010년 평가 결과 고위험도 상위 10개 위험요소

순위	ID	위험요소명	위험설명	위험도
1	NR03	기록정보의 진본성 손실	기록정보가 위조 또는 변조 되지 않은 원래 그대로의 것이며, 훼손된 바 없는 상태임을 입증할 수 없다.	16.6
2	NR19	메타데이터 변경이력 문서화 불완전 혹은 실패	보존기록패키지에 실행된 보존전략, 보존절차 및 메타데이터 기록 과정이 일부 혹은 전체가 문서화되지 않았거나 부정확하다.	16.0
3	NR05	기록정보의 변경 미식별	기록정보 중 하나 이상의 변경이 발생했음에도 불구하고 어디에서 변경이 발생하였는지를 추적하거나 모니터링할 수 없다.	15.2
4	NR42	입수기록패키지의 불완전성	입수된 입수기록패키지가 보존을 위해 필요한 정보를 포함하지 않고 있다.	14.0
5	NR43	입수 과정에서의 입수기록패키지 변경	입수기록패키지가 생산되거나 입수되는 중에 외부요인의 의해 변경 된다(입수과정은 생산시스템에서 추출된 직후부터 CAMS의 입수모듈에 의해 등록될 때까지의 모든 프로세스).	13.8
6	NR12	입수 과정의 유효성 검증 불가능	이관 대상 전자기록물에 대한 이관 과정 중 무결성과 진본성이 유지되고 있는지를 단정하지 못한다.	13.7

7	NR04	기록정보의 무결성 손실	기록정보가 망실·훼손·손상·변조 등에 의하여 변경되지 않고 완전한 상태를 유지하고 있음을 입증할 수 없다.	13.4
8	NR41	입수기록패키지의 구조적 비유효성과 기형	입수된 입수기록패키지가 보존에 적합한 형태가 아니다.	13.1
9	NR17	입수·보존·배부기록패키지(SIP·AIP·DIP)의 추적 불가능	업무담당자가 기록정보 라이프사이클(information lifecycle)의 특정시점에 해당되는 입수·보존·배부 기록패키지를 추적할 수 없다.	12.2
10	NR33	원격 혹은 로컬지역의 소프트웨어 침입	네트워크 보안 대책을 우회하여 구내 또는 외부에서 소프트웨어에 침입한다.	12.2

최소한 상위 10개의 위험요소에 대해서 만이라도 이 논문에서 살펴본 사례처럼 상세한 관리방안을 빠른 시일 안에 설계해야 할 것이다. 이것이 2015년 이후의 전자기록 대량 이관과 장기보존 업무를 안정적으로 수행해 나갈 수 있는 효과적인 방법 중 하나라고 믿는다.

ABSTRACT

A Case Study on the Risk Management for the Long-term Preservation Business Activities Related to Electronic Records

Yim, Jin-Hee

This paper showed results of the risk management project in detail which was conducted by National Archives of Korea(NAK) in 2010. In the project NAK examined its long-term preservation business of electronic records using DRAMBORA(Digital Repository Audit Method Based on Risk Assessment). NAK has defined 44 different risk elements related to its business activities, assessed and classified them into several grades according to the severity calculated by risk probability score and risk potential impact score, and developed precise management plans for two of the most serious risks. This paper introduced the management plan for one of them. The risk was numbered with NR04 and described by 'Loss of integrity of records information'. This paper explained mitigation strategies, contingency organization, disaster control responsibilities, and personal mission cards for the NR04. This paper planned to give comprehensive understandings to Records Management Organizations about the risk management approaches as an effective way for business management through the case study.

Key words : electronic records, long-term preservation, DRAMBORA, risk management framework, case study