KiRi Weekly

2015.4.27 제330호

KiRi 보험연구원
Korea Insurance Research Institute

이슈와 포커스는 연구자 개인의 의견이며, 보험연구원의 공식 견해가 아님을 밝힙니다.

서울시 영등포구 국제금융로 6길 38 (여의도동 35-4) 8층 보험연구원 (문의 : 변철성 수석담당역 / 02-3775-9115)

KiRi Weekly 2015.4.27

이슈

미국 정부 ERM 도입의 시사점

최창희 연구위원

요약

- 정적(Static) 리스크 관리 방법의 경우 정해진 법규와 규정에 따라 경제주체의 활동을 규제하는데 반해 민간에서 자주 활용되는 ERM은 순환적 프로세스에 따라 리스크를 관리하고 리스크 관리 체계 자체가 환경 변화에 적응해 가도록 이를 지속적으로 개선시키는데 초점을 맞추는 동적(Dynamic) 리스크 관리 방법임.

- 미국 정부는 911 사태와 허리케인 카트리나 이후 기존의 정적 리스크 관리 방법에 한계가 있음을 인식하고, 변화하는 환경에 신속하고 능동적으로 대처하기 위해 ERM 기반의 리스크 관리 표준을 제정하는 한편 이를 동적 국가 리스크 관리 체계 구축에 활용하고 있음.

- 현재 미국 정부는 국토안보부, 국방부, 교육부, 항공우주국, 환경보건국, 원자력규제위원회, 예산관리국, 과학기술국, 식품 · 의약품국 등 정부 기관 리스크 관리에 ERM을 활용하고 있으며 유럽, 캐나다, 호주, 일본, 싱가포르 등도 ERM 이용해 국가 리스크를 관리하고 있음.

- 세월호 사고 이후 정부 당국은 기존 재난관리 체계의 문제점을 개선하기 위해 국민안전처 신설, '안전혁신 마스터플랜' 수립, '국가안전대진단'과 같은 다양한 방안을 제시하였음.

- 정부의 포괄적 안전혁신 계획인 '안전혁신 마스터플랜'은 순환적 리스크 관리 프로세스와 의사소통 채널 운영 등 ERM 개념을 부분적으로 포함하고 있으나 외국 사례와 같이 큰 틀에서 리스크 관리 체계 자체를 지속적으로 발전시키는 ERM을 이용한 동적 리스크 관리 체계 구축은 포함하고 있지 않은 것으로 보임.

- 정부당국은 재난사고의 효과적인 방지와 신속한 대응을 위해 미국의 ERM 도입 사례를 고려하여 리스크 관리 체계 표준을 제정하고 이를 활용해 동적 리스크 관리 체계를 구축하는 방안을 모색할 필요가 있음.

1. 배경

■ 한국은 지금까지 대형 재난 사고[1] 발생 후 유사 사고를 방지하기 위해 새로운 제도를 도입하는 등 정적인 방식으로 재난사고 리스크를 관리해 왔음.

- 대형사고 이후 유사한 사고를 방지하기 위해 도입된 제도들은 다음과 같음.
  - 1973년 대연각호텔 화재사고 이후 화재로 인한 『재해보상과보험가입에 관한 법률』 제정
  - 1993년 서해페리호 침몰사고 이후 '유도선사업자배상책임보험가입' 의무화
  - 1999년 화성씨랜드 사고 이후 '수련시설배상책임보험가입' 의무화
  - 2014년 세월호 사고 이후 『세월호 특별법』 제정

■ 세월호 사고 이후 정부는 기존의 재난관리 체계의 한계점을 인식하고 국민안전처 신설, '안전혁신 마스터플랜' 수립, '국민안전대진단' 등 다양한 대책을 내놓았음.

- 올해 1월 국민안전처는 안전혁신을 위해 아래와 같은 정책방향 제시[2]
  - 제도 개선: 재난안전관리 컨트롤 기능 강화, 신속한 재난대응 체계 확립
  - 점검 강화: 국민참여 안전대진단, 취약계층 위해요소 선제적 점검
  - 인프라 보강: 안전산업 육성, 지자체 재정 지원 및 책임 강화
  - 교육 확대: 생애주기별 안전교육, 범국민 안전 문화운동
- 정부의 '안전혁신 마스터플랜'은 아래와 같은 5대 추진전략 제시[3]
  - 재난안전 컨트롤 기능 확립: 재난현장 통합지원 컨트롤 타워 기능 강화, 재난대응표준체계 확립, 안정정책 총괄관리 · 개선체계 구축, 국가재난안전 정책방향 및 표준 설정
  - 재난현장 대응역량 강화: 지자체 재난대응 역량 및 책임성 강화, 재난대비 교육 · 훈련 강화, 현

1) 『재난 및 안전관리 기본법』은 재난을 국민의 생명 · 신체 · 재산과 국가에 피해를 주거나 줄 수 있는 것으로 자연재난(태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 낙뢰, 가뭄, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해)과 사회재난(화재 · 붕괴 · 폭발 · 교통사고(항공사고 및 해상사고를 포함한다) · 화생방사고 · 환경오염사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 에너지 · 통신 · 교통 · 금융 · 의료 · 수도 등 국가기반체계의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산 등으로 인한 피해)을 통칭하는 것으로 정의하고 있음.

2) 분야별로 2개 과제 제시, http://www.mpss.go.kr/main/2015plan.html

3) 국무총리실 보도자료(2015. 3. 30), "제54차 중앙안전관리위원회, 안전혁신 마스터플랜 심의 확정" 참조.

장대응 역량 강화, 오염방제 역량 강화

- 생활 속 안전문화 확산: 국민안전교육 강화, 범국민 안전문화 확산, 주민참여 민관협력 거버넌스 구축, 안전복지 정책 강화
- 재난 안전예방 인프라 확산: 재난 조사 및 평가·환류체계 강화, 예방을 통한 기능·업무연속성 강화
- 분야별 안전관리 추진: 학교, 에너지, 산업단지, 감염병, 의료서비스, 유해화학물질, 산업현장, 시설물, 교통, 해양, 원자력, 가축질병, 정보통신, 기타(14개) 분야에 대해 추진

- 올해 2월~4월 정부는 제도의 사각에 있는 리스크를 발견하기 위해 '국가안전대진단'[4]을 진행하고 있음.
- 이와 같은 노력은 재난사고 방지와 대응 체계 개선에 기여할 것으로 예상되나 외국과 같이 ERM을 이용해 동적 리스크 관리 체계를 구축하는 방안은 제시되지 않은 것으로 보임.

■ ERM[5]은 특정 기관의 효과적 목적 달성을 위해 활용되는 리스크 관리 방법으로서 일반적으로 순환적 리스크 관리 프로세스, 의사소통 채널, 지속적 관리 체계 개선 방안 등으로 구성됨('2. 해외 ERM 표준 소개' 참조).

- 기존 정적 리스크 관리 체계가 제도와 법규를 통해 경제주체의 활동을 규제하는데 중점을 두는데 반해 ERM은 지속적으로 인적·물적 리스크 관리 체계를 운영·평가·보완하는데 중점을 둠.

■ 미국 정부는 911 사태와 허리케인 카트리나 이후 기존의 정적 리스크 관리 체계가 새로운 리스크를 식별하고 이에 대처하는데 효과적이지 못하다는 것을 인식하였으면, 이에 ERM을 도입하여 동적 국가 리스크 관리 체계를 구축하였음.[6]

- 미국 감사원은 국토안보부와 같은 국가 기관의 ERM 시행 실적을 평가함.[7]
- 미국 정부기관 중 국토안보부, 국방부, 교육부, 항공우주국, 환경보건국, 원자력규제위원회, 예산관리국, 과학기술국, 식품·의약품국 등이 ERM을 활용하고 있음.[8]

---

4) '안전혁신 마스터플랜'의 일환임.
5) Enterprise risk management, '전사적 위험관리'라고도 함.
6) https://www.rims.org/resources/ERM/Documents/Risk%20in%20Government.pdf
7) http://www.gao.gov/assets/130/120506.pdf
8) http://www.gao.gov/products/GAO-06-91,
http://csis.org/files/publication/110314_Murdock_RiskManagement_Web.pdf

■ 미국뿐 아니라 유럽, 캐나다, 호주, 일본 정부들도 ERM을 국가 리스크를 관리하는데 활용하고 있음.

- EU는 방재[9], 세관[10], 심리사회적 리스크 관리[11]에 ERM 활용
- 캐나다 재무위원회 사무국은 ERM 표준을 기업과 금융기관에 제공[12]
- 호주는 국방[13], 교육[14], 금융[15] 등에서 ERM 활용
- 일본은 후생노동성[16], 정부의 정보보안 체계 관리, 지자체 리스크 관리[17], 일본 농림수산성 식품 리스크 관리[18] 등에 ERM 활용
- 싱가포르는 국무총리실을 중심으로 RAHS[19]라는 ERM 도구를 활용하여 리스크를 인식하고 이를 관리함.[20]

2. ERM의 특징 및 장점

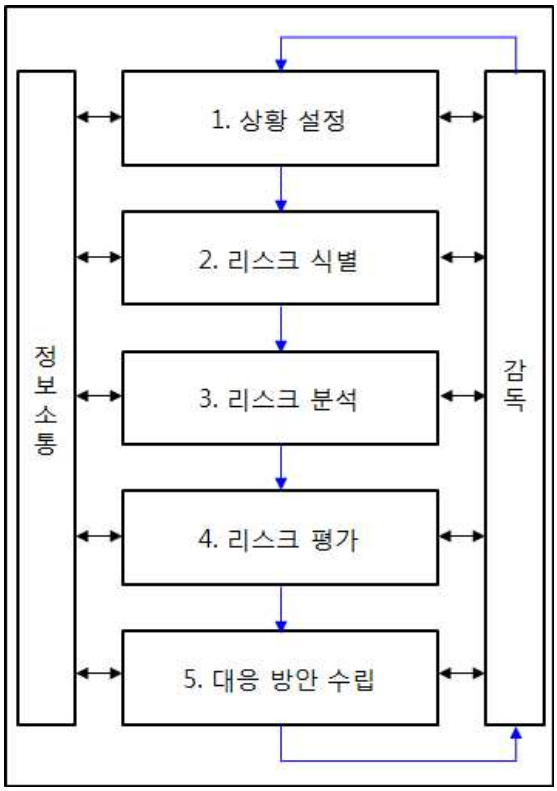
■ ERM을 이용한 동적 리스크 관리는 보험, 금융, IT, 환경 보호 등 민간에서 자주 활용되어 왔으며 다음과 같은 특징을 가지고 있음.

- ERM은 정해진 법규와 규정으로 경제주체의 활동을 규제하기보다 변화하는 환경에 적응하는 리스크 관리 체계를 구축하는데 중점을 둠.
  - ERM은 리스크 관리를 위한 인적·물적 체계 구성, 리스크 관리자의 책임과 권한 정의, 순환적 리스크 관리 프로세스의 운영과 평가, 관련 커뮤니티 정보 공유 네트워크 운영, 그리고 이들을 고려한 리스크 관리 체계의 지속적인 개선 등을 정함.

9) http://www.preventionweb.net/files/35805_02efdrr06oct2014spaineceuframework.pdf
10) http://ec.europa.eu/taxation_customs/resources/documents/framework_doc.pdf
11) http://www.prima-ef.org/uploads/1/1/0/2/11022736/prima-ef_ebook.pdf
12) Treasury Board of Canada Secretariat, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422
13) http://dtic.mil/dtic/tr/fulltext/u2/a434592.pdf
14) http://deta.qld.gov.au/corporate/pdf/enterprise-risk-management-framework.pdf
15) http://www.finance.gov.au/sites/default/files/commonwealth-risk-management-policy_0.pdf
16) http://www.mhlw.go.jp/topics/bukyoku/iyaku/syoku-anzen/dl/pamph01_03.pdf
17) 일본의 경우 Sompo Japan과 같은 민간 기관이 지자체의 리스크 관리 체계 구축을 지원하고 있음. http://www.sjnk-rm.co.jp/service/rm_system/rm_admini.html 참조.
18) http://www.maff.go.jp/j/syouan/seisaku/risk_analysis/sop/index.html
19) Risk Assessment and Horizon Scanning.
20) http://csis.org/files/publication/110314_Murdock_RiskManagement_Web.pdf, pp. 74 참조.

- ERM을 활용한 동적 리스크 관리는 참여자의 자발적 노력과 감독자의 전문성을 필요로 하기 때문에 구축 · 운영에 더 많은 시간 · 노력 · 예산을 필요로 하나 끊임없이 변화하는 환경에 능동적이고 신속하게 대처할 수 있다는 특징을 가지고 있음.

〈그림 1〉 ISO 31000의 리스크 관리 프로세스



대표적인 ERM 국제 표준인 ISO 31000은 다음과 같은 내용을 포함하고 있음.[21)]

- ISO 31000은 리스크를 '기관의 목적 달성에 영향을 미치는 불확실성'으로 정의함.
- 적용 범위, 용어 및 정의, 관리 원칙
- 관리 체계의 구축 및 운영: 프레임워크 설계, 권한과 책임, 리스크 관리 실행, 체계 모니터링과 리뷰, 지속적인 개선
- 리스크 관리 프로세스 구축 및 운영: 의사소통 채널 구축, 조직 현황 조사 및 확정, 리스크 평가, 리스크 대응, 프로세스 운영 현황 기록, 프로세스 모니터링 및 리뷰(〈그림 1 참조〉)

21) 외국 정부와 공공기관이 제시하는 ERM 표준은 부록 참조.

- ISO 31000은 리스크 관리에 대해 다음 11가지 원칙 제시
  1. 조직의 목표 달성 및 가치 창조에 기여해야 함.
  2. 조직의 모든 운영 프로세스와 통합되어야 함.
  3. 경영의사결정에 있어 선택 및 집중의 우선순위를 제공해야 함.
  4. 불명확성을 구체화하는 기능을 해야 함.
  5. 체계성, 구조성, 적시 적용 가능성을 가져야 함.
  6. 활용 가능한 최선의 정보에 기반을 두어야 함.
  7. 조직의 특성에 맞추어 조율되어야 함.
  8. 조직의 인적, 문화적 요소를 고려하여 구축되어야 함.
  9. 투명하고 전체 조직원이 적극 참여할 수 있도록 만들어져야 함.
  10. 새로운 리스크에 동적이고 빠르게 적응할 수 있도록 만들어져야 함.
  11. 조직의 지속적인 발전을 지향할 수 있도록 만들어져야 함.
- ISO 31000은 '상황설정→리스크 식별→리스크 분석→리스크 평가→대응방안 수립'의 과정을 반복하는 순환적인 리스크 관리 프로세스를 제시함(〈그림 1〉 참조).
  - 상황 설정: 조직의 내부 · 외부 환경 분석, 평가 기준 및 판단 기준 수립, 리스 관리 목표 수립
  - 리스크 식별: 발생 가능한 리스크를 발견
  - 리스크 분석: 리스크의 발생 가능성과 심도 등 리스크를 분석
  - 리스크 평가: 조직의 환경을 고려하여 리스크가 조직에 미치는 영향을 분석
  - 대응방안 수립: 회피(Avoid), 경감(Reduce), 분배(Share), 보유(Retain) 등의 다양한 방법을 고려한 대응 방안 수립
  - 정보소통 채널: 각 기능을 수행하는 부서간의 투명 · 정확 · 신속한 효율적인 정보 전달은 리스크 관리 체계 성공에 있어 필수적인 요소임.
  - 감독: 리스크 관리 체계의 운영을 위해서는 각 부분의 감독 책임자를 정하고 감독 책임자의 권한과 의무를 명확히 하여야 함.
  - 지도부의 역할: 지도부는 리스크 관리체계가 원활하게 운영되는지 주기적으로 평가하고 평가 내용을 바탕으로 리스크 관리 체계를 수정 · 보완하는 역할을 수행해야 함.

3. 미국 정부의 ERM 적용 사례

■ 최근 미국 정부는 기존 정적 리스크 관리 체계의 한계를 인식하고 ERM을 이용해 동적으로 리스크를 관리하는 체계를 구축하였음.[22]

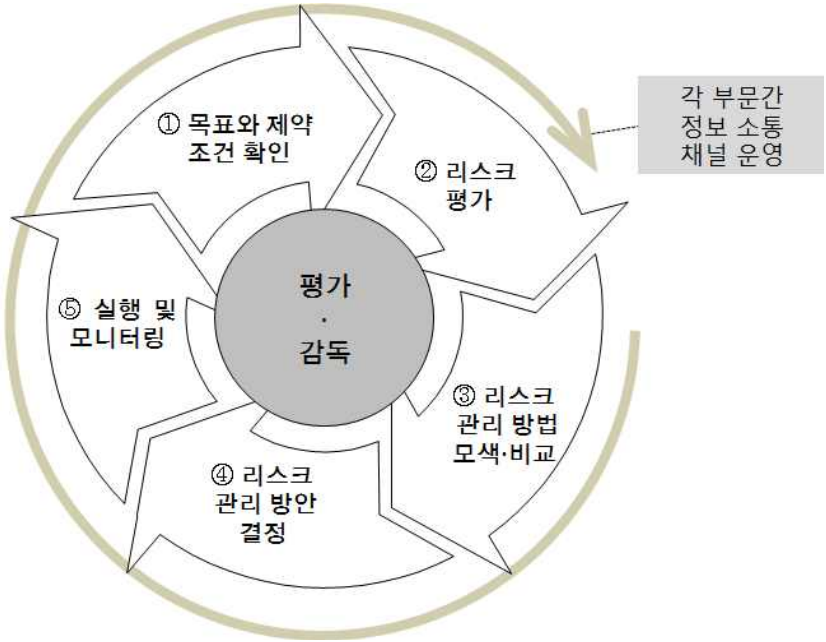
- 미국 정부는 정부성과결과법[23], 정부회계감사표준[24], 감사원 연방정부 내부규제표준[25], 관리예산처[26] 의견, 대통령 리스크 관리 자문 위원회 의견[27], COSO[28] ERM 표준, 민간 자문 위원단 의견 등을 고려하여 ERM 표준을 정하고 이를 토대로 리스크 관리 체계를 구축·운영함.

〈그림 2〉 미국 정부의 지속적 ERM 개선 체계

- 미국 정부는 〈그림 2〉와 같이 리스크 관리 체계를 평가하고 이를 지속적으로 개선해 나아가는 체계를 구축하였음.
  - 미국 국토안보부는 ERM을 하위 기관의 리스크 관리에 적용하고 감사원은 이를 평가하고 개선사항을 지적함.
  - 미국 국회의 리스크 감독 위원회는 국토안보부의 리스크 관리가 예산낭비 없이 기관의 목적에 부합하도록 운영되고 있는지 감독하는 역할을 수행함.

22) http://www.gao.gov/assets/160/157672.pdf, pp. 100 참조.
23) the Government Performance and Results Act(GPRA) 1993.
24) the Government Auditing Standards 2003.
25) GAO's Standards for Internal Control in the Federal Government.
26) the Office of Management and Budget (OMB).
27) the President's Commission on Risk Management.
28) COSO(The Committee of Sponsoring Organizations of the Treadway Commission)는 5개 민간단체(AICPA, AAA, FEI, IIA, IMA)가 결성한 민간기구로서 기관에 다양한 분야의 경영 자문 제공

〈그림 3〉 미국 정부의 ERM 프로세스



자료: "RISK MANAGEMENT: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure", 미국 감사원, pp. 102 참조.
http://www.gao.gov/assets/160/157672.pdf

- 미국 정부의 ERM 표준은 ① 목적과 제약조건 확인 ② 리스크 평가 ③ 리스크 관리 방법 모색 · 비교 ④ 리스크 관리 방안 결정 ⑤ 실행 및 모니터링을 주기적으로 반복하는 ISO 31000과 유사한 순환적 리스크 관리 프로세스를 제시함(〈그림 3〉 참조).
  - ① 기관의 목표와 제약조건 확인: ERM은 조직의 목표를 성취하는 것을 목적으로 하므로 조직의 목표와 이를 수행하기 위해 취할 수 있는 대응방안을 모색하기 위해 기관의 제약조건을 확인해야 함.
  - ② 리스크 평가: 리스크의 존재를 확인하고 리스크가 기관의 목표를 달성하는데 미치는 부정적인 영향을 평가하는 과정
  - ③ 리스크 관리 방법 모색 · 비교: 리스크를 관리하기 위한 대응 방안을 구상하고 대응방안들의 장단점과 각각의 기대 효과와 비용을 분석
  - ④ 리스크 관리 방안 결정: 분석 결과를 토대로 기관의 특성에 맞는 리스크 관리 방안 결정
  - ⑤ 실행 및 모니터링: 수립된 방안에 따라 리스크 관리를 수행하고 이를 평가
  - 각국의 리스크 관리 표준들도 이와 유사한 프로세스를 제시함.

〈그림 4〉 미국 주요 기간시설 · 자원보호계획 조직 체계

부분	부문별 담당 기관	주요 기간시설 협력체 자문 위원회		
		무문조정위원회	정부조정위원회	지역컨소시엄
화학	국토안보부	√	√	
민간시설		√	√	
통신		√	√	
주요생산시설		√	√	
댐		√	√	
응급대응서비스		√	√	
IT기간시설		√	√	
핵발전소		√	√	
식품 · 농업	농무부, 보건사회복지부	√	√	
국방산업기지	국방부	√	√	
에너지	에너지부	√	√	
건강관리 · 공공위생	보건사회복지부	√	√	
금융	재무부	별도로 운영	√	
기상	환경보호청	√	√	
정부시설	국토안보부, 총무청	없음	√	
교통	국토안보부, 교통부	부문별 운영	√	

범 부문 위원회 | 연방 고위 위원회 | 주 · 지방정부 조정 위원회 | 지방 컨소시엄 조정 위원회

자료: NIPP(2013), "NIPP 2013 Partnering for Critical Infrastructure Security and Resilience", Homeland Security, pp. 11. http://www.dhs.gov/national-infrastructure-protection-plan 참조.

■ 미국 국토안보부는 ERM을 적용하여 주요 국가 기반시설을 파악하고 비상시 공공 · 민간의 인적 · 물적 자원을 이용하여 이들을 보호하는 국가기간시설 · 자원보호계획(NIPP)을 수립 · 운영하고 있음.[29]

- NIPP는 공공 · 민간 협력체계를 통해 주요 기간시설 · 자원을 보호하는 계획임(〈그림 4〉 참조).
- 본 계획은 각 부분의 담당하는 부문 조정 위원회(Sector Coordinating Council), 정부 조정 위원회(Government Coordinating Council), 부문별 담당 기관(Sector-Specific Agencies), 여러 부분을 통합적으로 관리하는 범 부문 위원회(Cross-Sector Council), 연방 고위 위원회(Federal Senior

29) NIPP(2013), pp. 1 참조.

Leadership Council), 지자체 조정 위원회(State, Local, Tribal, and Territorial Government Coordinating Council), 지역별 컨소시엄 조정 위원회(Regional Consortium Coordinating Council), 정보 공유 및 분석 기관(Information Sharing and Analysis Organizations), 자문 위원회(Critical Infrastructure Partnership Advisory Council) 등의 조직으로 운영됨.

- NIPP 비전: 취약점 감소, 사고 영향 극소화, 리스크의 확인 및 중단, 사고 시 신속한 대응과 회복을 통해 물리적 또는 사이버 상의 국가기반시설이 안전하게 관리되는 나라
- NIPP 미션: 민관의 협력을 통해 기간시설·자원의 보안과 사고에 대한 저항력을 강화
- NIPP 목표: ① 기간시설·자원의 취약점과 기간시설·자원에 대한 리스크를 평가·분석하고 리스크 관리, ② 지속가능한 비용의 효과적인 투자로 기간시설·자원을 인적·물적·사이버 리스크로부터 보호, ③ 사고가 기간시설·자원에 미치는 영향 최소화, ④ 관련 주제간 효과적 정보 공유, ⑤ 훈련 및 사고 전후 리스크 관련 교육 촉진
- NIPP의 리스크 인자: 기상재해, 전염병, 테러, 시설·장비 고장, 사이버 공격 위협
- NIPP의 핵심 원칙: ① 자원의 효과적인 활용을 위해 리스크의 확인·관리는 조직 체계에 의해 이루어져야 함, ② 기간시설·자원 보안 강화를 위해 조직간 종속성과 상호의존도를 이해해야 함, ③ 기간시설·자원의 리스크와 부문별 상호의존도를 이해하기 위해 조직 체계간의 정보 공유가 필요함, ④ 민·관 협력체계의 다양성과 고유한 의견은 기간시설·자원 보안 관리에 강점을 제공함, ⑤ 지역별 관리 체계간의 협력은 리스크 관리 체계 개선을 위해 필수적임, ⑥ 주요 기간시설·자원 보호를 위해서는 국경과 지역간 경계를 초월한 협력과 상호지원을 필요로 함, ⑦ 자산·체계·네트워크 구축 시 보안과 안정성이 고려되어야 함.
- NIPP는 〈그림 5〉와 같이 순환적 리스크 관리 프로세스를 제시
- 미 국토안보부는 NIPP의 성공적인 정착과 운영을 위해 다양한 교육 프로그램을 운영함.[30]

〈그림 5〉 미국 국토안보부 기간시설·자원 관리 프로세스

자료: NIPP(2013), pp. 15.

30) NIPP 홈페이지(http://www.dhs.gov/national-infrastructure-protection-plan) 참조.

4. 미국 사례의 시사점

〈표 1〉 국민안전처 안전혁신 마스터플랜과 미국 정부의 리스크 관리 체계 비교

구분	국민안전처 안전혁신 마스터플랜	미국 국토안보부 NIPP
국가 ERM 표준	없음	제공
ERM 표준 적용	순환적 리스크 관리 프로세스 등에 부분적 적용	부처 운영과 하위기관 및 관련 민간 기관 리스크 관리에 적극 활용
ERM 체계 구축 지원	없음	교육 프로그램 운영 및 자문 제공
지속적 리스크 관리 체계 개선 방안	없음	국회와 감사원이 기관의 ERM 체계를 지속적으로 감독하고 개선 사항 제시, 각 부분에서 자발적·지속적으로 개선되는 리스크 관리 체계 구축
민간 참여 방안	안전 점검, 리스크 관리 컨설팅 확대, 재난보험 확대 등의 민간 참여 촉진	지역별 부문별 조직에 민간 참여 장려, 민간 자원 중 비상 시 활용 가능한 자원을 파악하고 활용 계획 수립
고려하는 사고 범위	물리적 사고(자연재해, 전염병, 화재, 안전사고 등)를 중점적으로 관리	물리적 사고 이외에 사이버·테러 리스크 관리

■ 정부의 '안전혁신 마스터플랜'은 ERM의 개념을 일부 도입해 현행 리스크 관리 체계를 개선하는 다양한 방안을 제시하고 있으나 ERM을 적용해 환경 변화에 동적으로 대응하는 리스크 관리 체계를 구축하는 방안은 제시하지 않음.

- 정부의 '안전혁신 마스터플랜' 중 다음은 ERM의 개념이 일부 적용된 것으로 볼 수 있음.
  - 정보소통채널확보: 재난현장과 국민의 수요와 요구를 반영하는 상향식, 안전관리 계획 등을 전달하는 하향식 정보체계 운영(pp. 2)
  - 순환적 프로세스 운용: 역량 개선 프로세스(pp. 16, 20), 『안전기준 등록·심의제』 운영(pp. 19), 예산 사전협의-사업평가 관리 체계 구축(pp. 19), 지자체 지역안전진단 지원(pp. 23), 재난안전사고 원인조사 및 이력관리 체계 구축(pp. 37)
  - 리스크 관리자의 책임과 권한 강화
- 그러나 '안전혁신 마스터플랜'의 주요 내용은 대부분 정적인 제도 도입이고 ERM 도입을 통해 지속적으로 개선되는 동적 리스크 관리 체계를 구축·운영하는 방안은 제시되지 않음.

■ 정부 당국은 대형 재난사고가 정적으로 운영되는 제도의 사각에서 발생한다는 것을 고려하여 ERM 도입을 통해 지속적으로 개선되는 동적 리스크 관리 체계를 수립하는 방안을 모색할 필요가 있음.

- 재난관리를 위한 ERM의 도입과 적용을 위해 다음과 같은 노력이 필요함.
  - 국내 실정이 맞는 국가 ERM 표준 제정[31]
  - ERM 표준을 이용한 동적 리스크 관리 체계 구축·운영 방안 모색
  - ERM 교육 프로그램 개설과 전문가 파견 등을 통해 하위 기관·지자체·민간에 동적 리스크 관리 체계 구축·운영 지원
- 또한 정부당국은 리스크 관리 표준과 함께 이를 이용하여 관리될 필요가 있는 리스크(예를 들어 NIPP의 사이버 공격 또는 테러)를 파악하여 이를 리스크 관리 체계에 포함시키는 방안도 모색할 필요가 있음. KiRi

부록: 외국 ERM 표준

■ 해외 정부·공공기관과 민간은 다음과 같은 ERM 표준을 제시함.

- 해외 정부·공공기관의 ERM 표준
  - 미국 감사원 ERM 표준[32]: 정부·민간의 리스크 관리 체계 구축을 위해 제공
  - 캐나다 재무위원회 사무국 ERM 표준[33]: 기업과 금융기관의 재무 리스크 관리에 적용
  - 일본 농림수산성 ERM 표준[34]: 기관 실무자를 위한 리스크 관리 표준
- 해외 민간 기관의 ERM 표준
  - COSO 리크스 관리 체계[35]: 인적 요소 구성과 책임의 중요성 강조하는 리스크 관리 체계
  - OCEG Red Book 2.0[36]: 관리자들의 실적 평가 기준과 정부 규제를 고려한 리스크 관리 체계

31) 국가기술표준원이 사이버 보안, 금융 및 기업 정보 보안, 사고대비 운영 영속성, 기록 관리 등 특정 분야에 대한 ERM 표준을 정하고 있으나 ERM 국가 표준은 없는 것으로 보임. 나라표준 인증(http://standard.go.kr/KSCI/) 참조.
32) U.S. Government Accountability Office(http://www.gao.gov).
33) Treasury Board of Canada Secretariat(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422).
34) http://www.maff.go.jp/j/syouan/seisaku/risk_analysis/sop/index.html
35) COSO(The Committee of Sponsoring Organizations of the Treadway Commission)는 5개 민간단체(AICPA, AAA, FEI, IIA, IMA)가 결성한 민간기구로서 기관에 다양한 분야의 경영 자문 제공
36) 미국의 비영리 싱크탱크(http://www.oceg.org/resources/grc-capability-model-red-book).

- ISO 31000[37]: 세계 리스크 관리 표준
- BS 31100[38]: 영국 리스크 관리 실무 가이드
- 유럽 리스크평가연합(FERMA) 리스크 관리 표준[39]
- JIS Q31000: 일본 리스크 관리 표준[40]
- AS/NZS 31000: 호주/뉴질랜드 리스크 관리 표준[41]

37) http://www.iso.org/iso/home/standards/iso31000.htm
38) http://shop.bsigroup.com/ProductDetail/?pid=000000000030228064
39) http://www.ferma.eu/risk-management/standards/risk-management-standard
40) http://kikakurui.com/q/Q31000-2010-01.html
41) http://sherq.org/31000.pdf