ISMS인증 이후 정보자산관리를 위한 보안실태 사례

대한병원정보협회장 한기태(건국대학교병원)
(kthan@kuh.ac.kr)

2018 의료기관 개인정보보호&정보보안 컨퍼런스

- 목 차 -

1. ISMS 최초심사 과정

2016년	2017년				
9월 ~ 11월	1월 ~ 5월	6월	7월~9월	10월	11월
ISMS 컨설팅	**ISMS 운영**	**최초심사**	**결함이행 조치**	**현장실사**	**인증위원회**
컨설팅 투입인력 3개월 10MM	증적자료 작성 취약점 개선 [서버 취약점 개선] . 패치관리 . 계정관리 . 불필요한 서비스	5일간 5명 심사	22개 결함	결함이행 확인	인증마크 게재 (홈페이지, HIS)

2. 결함 이행 과정

구 분	기 간	세부 업무
단기 이행	**1개월 ~ 3개월**	**. 최초심사 이후 3개월 내 이행**
중기 이행	**1년 ~ 2년**	**. 위험 수용** **- 예산 및 개발 기간 필요 항목** **- 정보보호 최고책임자/병원장 승인**
장기 이행	2년 이상	**. 위험 수용** **- 예산 및 개발 기간 필요 항목** **- 정보보호 최고책임자/병원장 승인** **예) 망분리, 개발보안(시큐어 코딩)**

3. ISMS 인증 획득 과정

[인증마크, HIS화면, 홈페이지 화면]

통제항목별 증적자료 문서

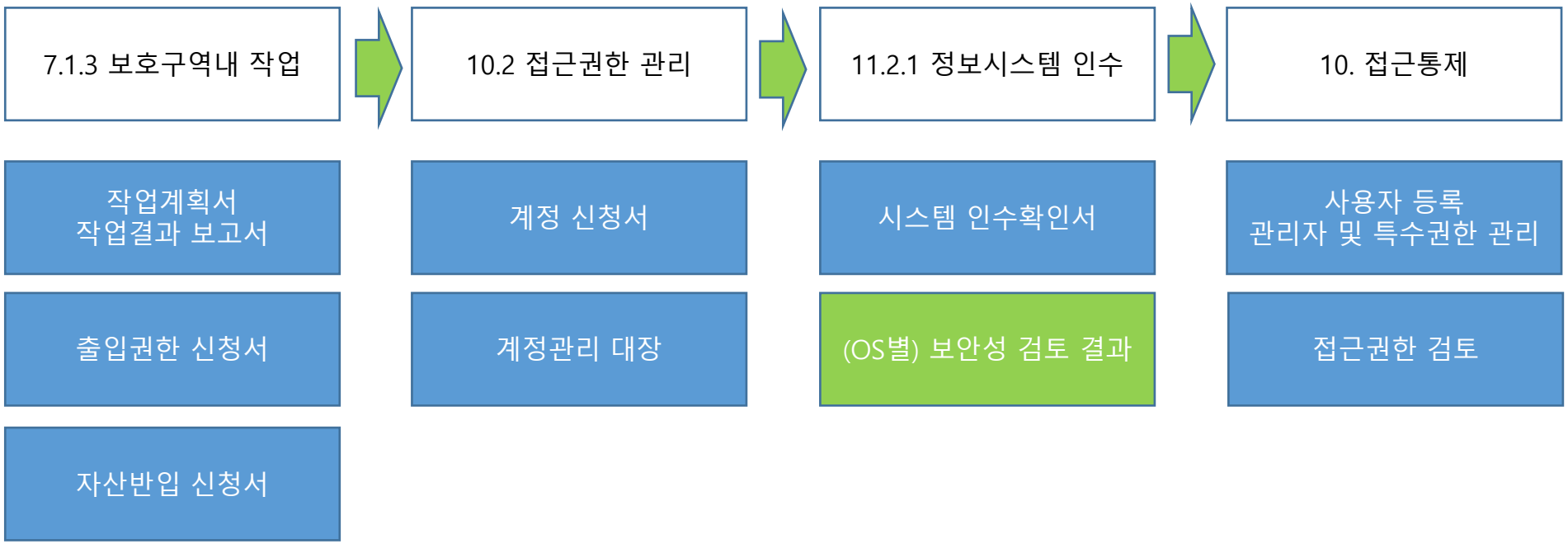
구분	ISMS기준	관련문서(증적)
[1] 정보보호정책	1.1.1 정책의 승인	(1.1.1) 정책의 승인(증적) o 정책/지침 제개정안
	1.1.2 정책의 공표	(1.1.2) 정책의 배포(증적)
	1.2.1 상위정책과의연계성	(1.2.1) 정보보호법률 및 상위 규정검토서
[2] 정보보호조직	2.1.1 CISO지정	(2.1.1) CISO 인사명령
	2.1.2 실무조직구성	(2.1.2) 정보보호 조직도
	2.1.3 정보보호위원회	(2.1.3) 정보보호위원회
	2.2.1 역할 및 책임	(2.2.1) 직무기술서
[3] 외부자보안	3.1.1외부자계약시보안요구사항	(3.1.1) 외부자_계약서
	3.2.1 외부자보안이행관리	(3.2.1) 외부자 보안 점검 (3.2.1) 외부자_정보보호서약서
	3.2.2 외부자계약만료시보안	(3.2.2) 외부인력_퇴사자점검표 o 외부인력 퇴직 프로세스 증적 o 외부인력 퇴직 보안서약서
[4] 정보자산 분류	4.1.1 정보자산 식별	(4.1.1) 정보자산관리대장
[5] 정보보호교육	5.1.1 교육계획	(5.1.1) 정보보호교육계획서
	5.1.3 교육내용 및 방법	(5.1.3) 교육내용 및 방법 o 정보보호교육자료
	5.2.1 교육시행 및 평가	(5.2.1) 정보보호교육결과 o 교육사진 및 출석 증적 o 정보보호 교육 결과보고
[6] 인적보안	6.1.1 주요직무자지정및감독	(6.1.1) 주요직무자 목록 ※ 정보자산관리대장 참조(내부인력 및 PC)
	6.1.3 비밀유지서약서	(6.1.3) 정보보호서약서
	6.2.1 퇴직및직무변경관리	(6.2.1) 퇴직 및 직무 변경관리 o 내부인력 퇴직 프로세스 증적 o 퇴직보안서약서
	6.2.2 상벌규정	(6.2.2) 개인업적평가기준(KPI)
[7] 물리적보안	7.1.2 보호설비	(7.1.2) 보호설비점검일지 o UPS 점검 결과보고서 o 소방점검 o CCTV 관리대장
	7.1.3 보호구역 내 작업	(7.1.3) 보호구역내작업 계획서
	7.1.4 출입통제	(7.1.4) 전산실_출입권한 관리 o 15층 서버실 출입권한 리스트
		(7.1.4) 전산실_출입기록 점검
		(7.1.4) 전살실_출입대장 o 서버실_반출입관리대장
	7.2.2 시스템배치 및 관리	(7.2.2) 시스템 배치도
	7.3.1 개인업무환경보안	(7.3.1) PC보안점검 결과 o 클리닝 데이 점검 o Privacy-I 점검 결과
	7.3.2 공용업무환경보안	(7.3.2) 공용 및 모니터링 PC보안점검 결과

구분	ISMS기준	관련문서(증적)
[8] 시스템개발 보안	8.1.1 보안 요구사항 정의	(8.1.1) 보안 요구사항 정의 o 개발보안 가이드 o 개발 표준 및 절차메뉴얼 o 프로세스 정의서
	8.2.1 구현 및 시험	(8.2.1) 구현 및 시험 o 개발프로세스 증적
	8.2.4 시험데이터보안	(8.2.4) 시험데이터관리 o 운영데이터 무효화 규칙 절차
	8.2.5 소스프로그램보안	(8.2.5) 소스프로그램보안 o 소스관리 접근권한 검토 o CVS+SVN계정관리대장
	8.3.1 외주개발 보안	(8.3.1) 외주개발 계약서
[9] 암호통제	9.1.1 암호정책 수립	(9.1.1) 암호정책수립 증적
	9.2.1 암호키 관리	※ (내화금고 보관)
[10] 접근통제	10.2.1 사용자 등록 및 권한부여 10.2.2 관리자 및 특수 권한 관리	(10.2.1) 접근권한 부여 o 시스템권한부여현황 o 방화벽신청내역
	10.2.3 접근권한 검토 10.3.3 사용자 패스워드 관리	(10.2.3) 접근권한 검토 o 정보시스템 계정관리대장 o 네트워크 및 정보보호시스템 계정관리대장 o 어플리케이션 계정관리대장
	10.4.1 네트워크 접근	(10.4.1) 네트워크 접근 o 방화벽 정책 검토 o IP 신청서 o 네트워크구성도
	10.4.3 응용 프로그램 접근	(10.4.3) 응용 프로그램 접근 o 응용프로그램 접근권한 검토
	10.4.4 데이터베이스 접근	(10.4.4) DB접근제어 정책관리 o DB접근제어 접근권한 검토 o DB접근제어 계정관리대장
	10.4.5 모바일 기기 접근	(10.4.5) 모바일기기 접근차단 정책 증적
	10.4.6 인터넷 접속	(10.4.6) 인터넷접속제어 정책 설정 o 웹메일 발신 통제 가이드

구분	ISMS기준	관련문서(증적)
[11] 운영보안	11.1.2 변경관리	※ (11.2.2) 월간 운영보고서 참조
	11.2.1 정보시스템 인수	(11.2.1) 정보시스템 인수 o 클라운드 전환 o 보안 솔루션 도입
	11.2.2 보안시스템 운영	(11.2.2) 시스템 월간 운영보고 o IDC 월 운영보고서 o 보안시스템 운영현황 보고서 및 증적
	11.2.3 성능 및 용량관리	(11.2.3) 성능 및 용량 관리 o 성능 및 용량 현황 보고 증적 ※ (11.2.2) 월간 운영보고서 참조
	11.2.4 장애관리	(11.2.4) 장애관리 o 장애관리 프로세스 증적 ※ (11.2.2) 월간 운영보고서 참조
	11.2.5 원격운영관리	(11.2.5) VPN운영 관리 o VPN 사용 정책 o VPN 발급 프로세스 증적
	11.2.9 백업관리	(11.2.9) 백업관리 o 백업프로세스 증적 o 백업 및 소산 관리대장 ※ (11.2.2) 월간 운영보고서 참조
	11.2.10 취약점 점검	※ 취약점진단 결과 참조
	11.4.1 정보시스템 저장매체 관리	(11.4.1) 정보시스템 저장매체폐기 증적
	11.4.2 휴대용 저장매체 관리	(11.4.2) 휴대용저장매체 통제정책 (증적)
	11.5.1 악성코드 통제	(11.5.1) 악성코드 관리 o V3 백신 통제정책
	11.5.2 패치관리	※ (11.2.2) 월간 운영보고서 참조
	11.6.2 로그 기록 및 보존	(11.6.2) 로그 기록 및 보존 o 정보시스템 로그 검토 결과 o 보안시스템 로그 검토 결과 o 응용그로그램 로그 검토 결과
	11.6.4 침해시도 모니터링	(11.6.4) 침해시도 모니터링 o SDS 관제보고서 o 보안관제티켓
[12] 침해사고 관리	12.2.1 침해사고 훈련	(12.2.1) 침해사고 훈련 결과
	12.2.2 침해사고 보고	(12.2.2) 침해사고 보고
[13] IT재해복구	13.2.1 영향분석에따른복구대책 수립	(13.2.1) IT재해복구 계획서 o 업무영향분석서 o 비상연락망
	13.2.2 시험 및 유지관리	(13.2.2) IT재해복구 모의훈련계획서 (13.2.2) IT재해복구 모의훈련결과 보고서

4. ISMS 인증이후 정보자산 관리 실태

4-1. 정보자산 신규도입(자산 반입)

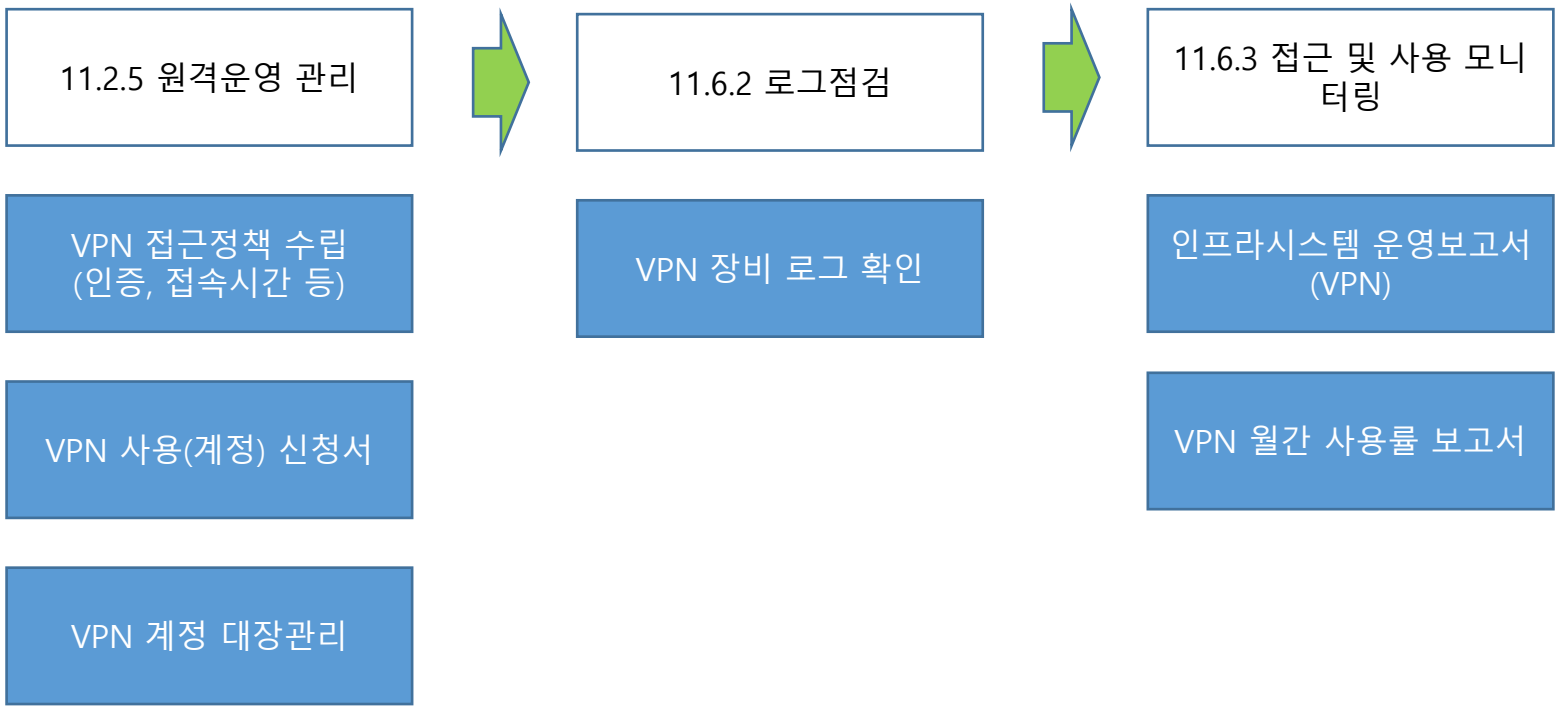


4. ISMS 인증이후 정보자산 관리 실태

4-2. 인적자산 입사 및 퇴사

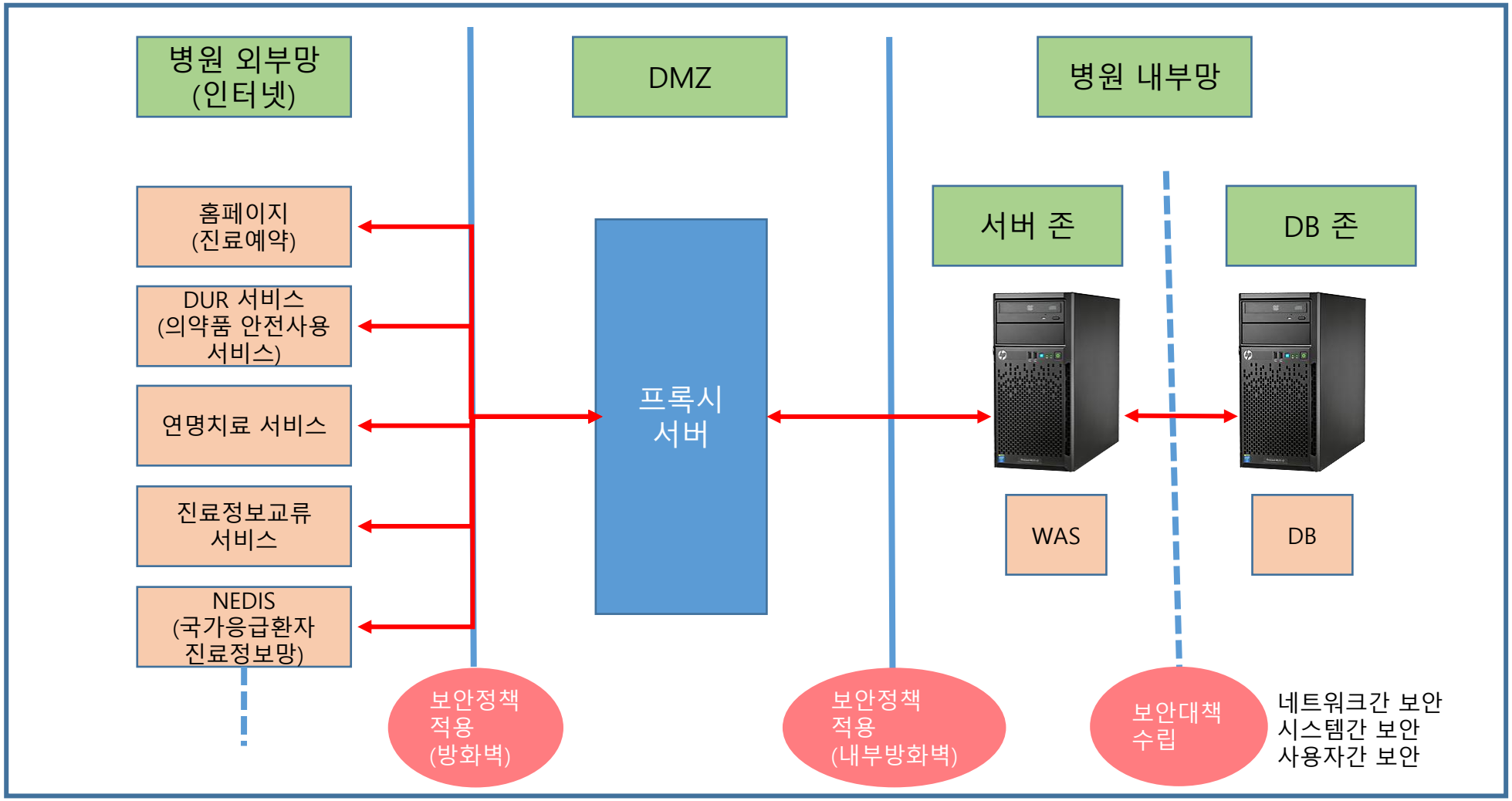
4. ISMS 인증이후 정보자산 관리 실태

4-3. 원격운영(VPN) 관리



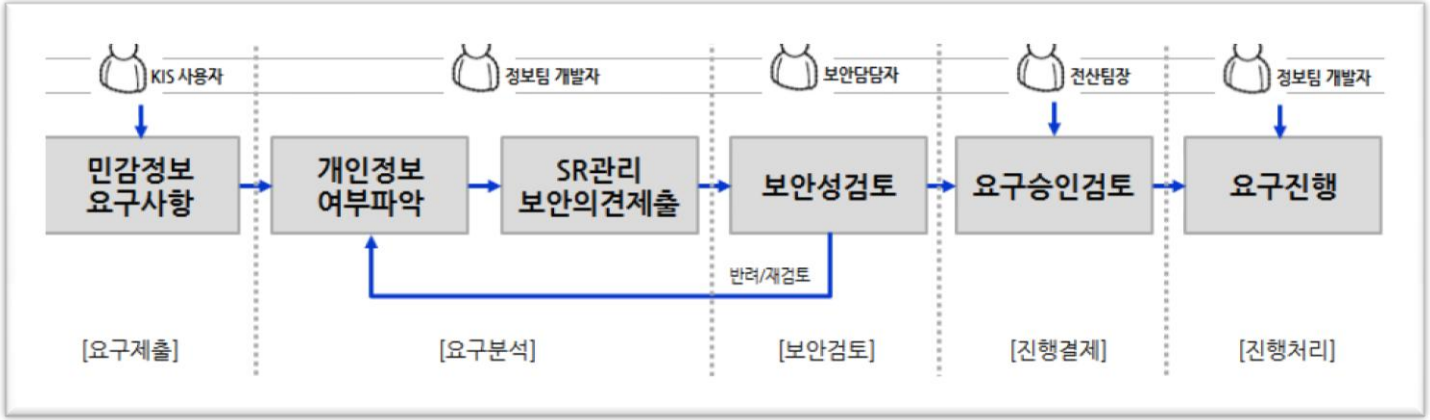
4. ISMS 인증이후 정보자산 관리 실태

4-4. 외부연계시스템 연동 네트워크 구성도



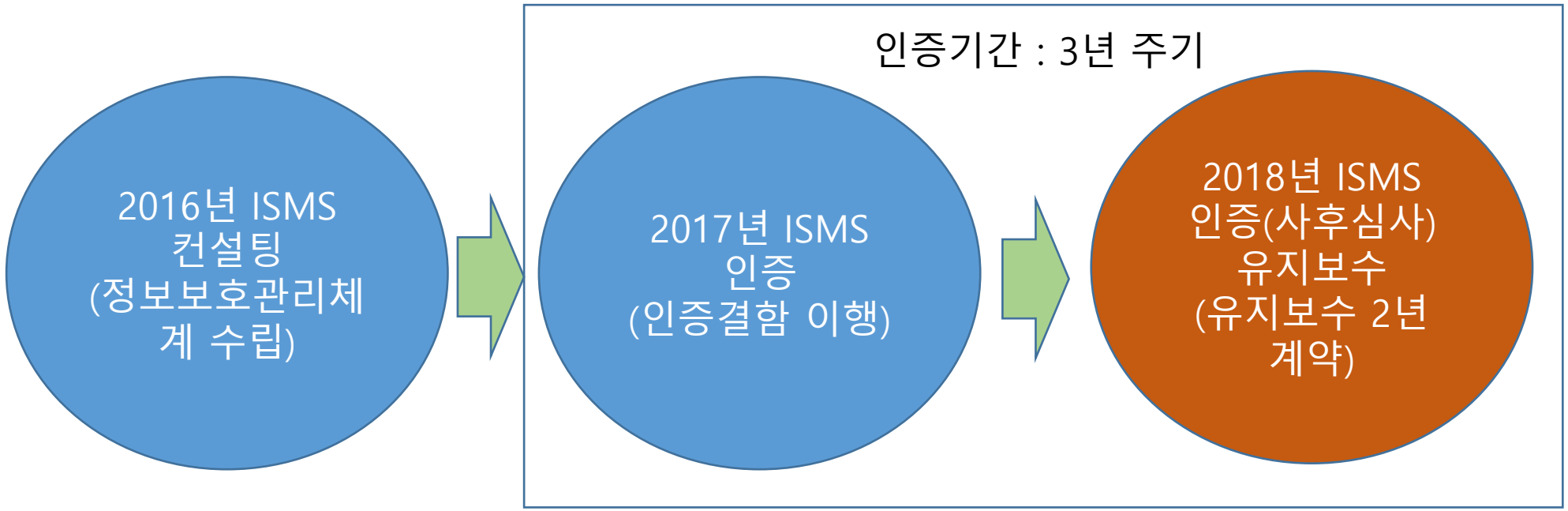
4. ISMS 인증이후 정보자산 관리 실태

4-5. 보안요구사항 처리 프로세스



처리단계	행위자	처리 단계별 상세내용
요구단계	사용자	- 개인정보 등의 민감정보가 포함된 프로그램 개발 요청
요구분석	담당자	- 민감 정보 요구에 대한 존재여부 파악 후 존재 시 해당 요구사항에 대한 담당자 보안처리 의견을 Comment로 등록 보안담당자에게 구두/문서등의 방법으로 보안성 검토 요청
보안검토	보안담당자	해당 요구사항에 대한 요건 검토 해당 요구사항을 처리할 정보개발팀 담당자 의견 검토 보안 요구사항에 대한 위배사항 등을 종합적으로 검토 및 의견
진행결재	전산팀장	보안요건 및 처리방안의 인지 후 개발진행 절차 승인
요구진행	담당자	해당 보안요건이 포함된 요구사항을 검토 지침기반 하에 진행 최소권한의 원칙을 기반으로 사용범위 확정, 사용권한 통제 구현

5. 정보보호 서비스 개념 도입

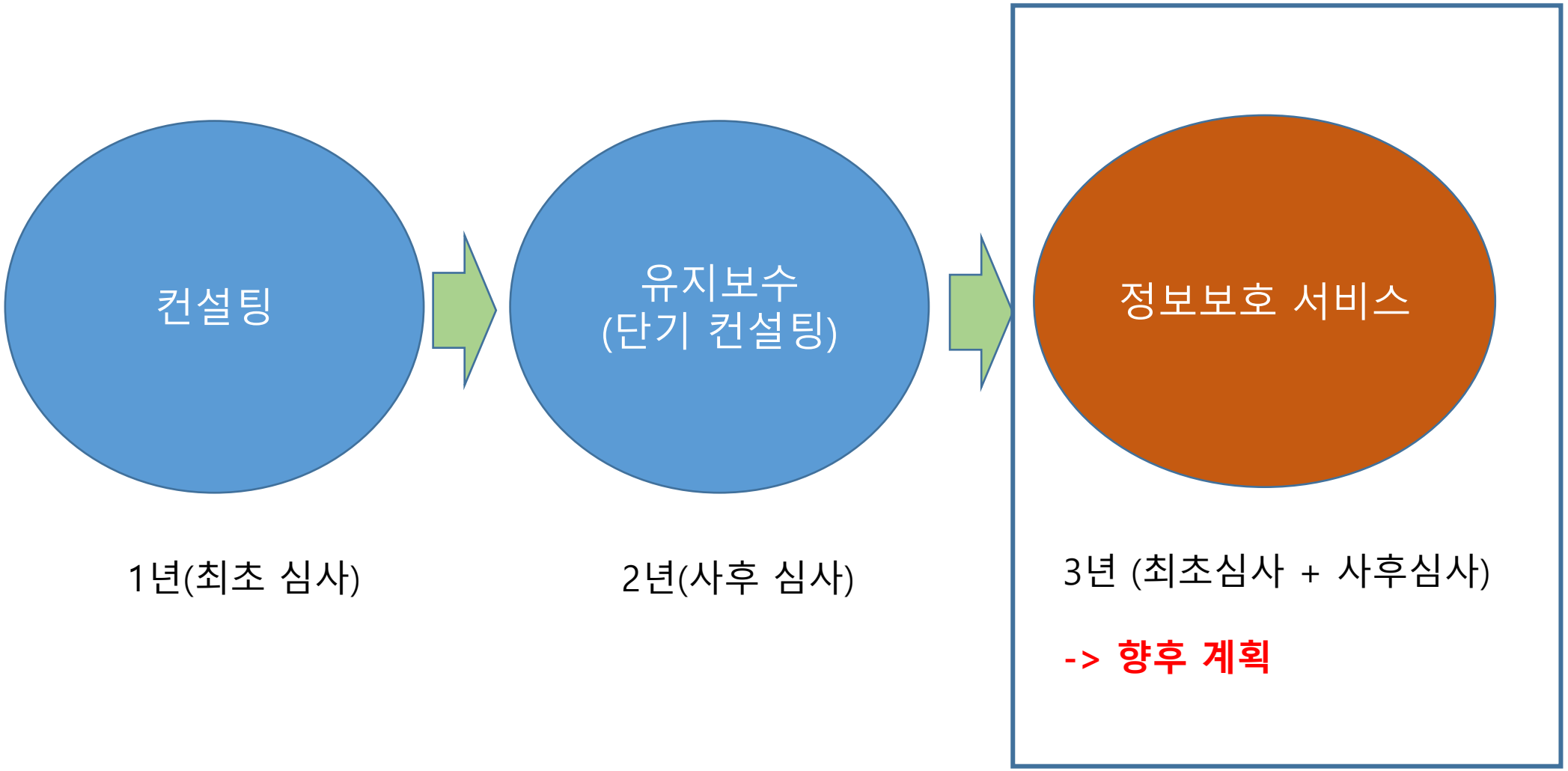


정보보호 년간 활동 계획 수립 + 년간 유지 보수 계획 = 정보보호 서비스 (정보보호 년간 활동 계획)

위험수용 장.단기 계획
감사지적 사항
결함사항/권고사항

정보보호관리체계 유지 활동

5. 정보보호 서비스 개념 도입



5. 정보보호 서비스 개념 도입

◈ 정보보호 년간 계획 샘플

	년간업무 계획	ISMS 심사	정보보호활동	정보보호위원회	교육
1월			자산 현행화 . 보안성 검토		
2월			정보보호 운영활동 점검		
3월			기술적 취약점 진단		주요 직무자 교육 : 정보보호 법령
4월			정보보호 운영활동 점검 위험평가 . 관리/기술/물리/법적		
5월			정보자산대장 확정 기술적 취약점 조치 정책/지침 제개정 등 보호대책 수립		
6월		ISMS 신청 . 신청서 작성	정보보호 운영활동 점검 기술적 취약점 조치	전반기 위원회 . 위험평가 DOA 결정 . 정책/지침 개정 승인	
7월		심사팀장 예비점검	내부 보안감사 침해사고 모의훈련		의사/간호사 . 정보보호 인식 . 개인정보보호
8월	ISMS 사후심사				
9월		결함조치 내역서 작성 결함연장 공문 발송	사후심사 결함조치		행정부서/진료지원부서 . 정보보호 인식 . 개인정보보호
10월			정보보호 운영활동 점검 사후심사 결함조치		
11월		최종 결함조치 내역서 작성 사후심사 인증	사후심사 결함조치		
12월	년간 업무계획 수립 . 인력, 예산 . 위험 수용(장단기 계획) . 감사지적 사항 . 결함이행 사항 . 권고사항		정보보호 운영활동 점검	하반기 위원회 . 년간 업무계획 승인	


Thank
You!