관리 진단 5 기 C 반

수행계획서

작성자 : 오희창

목차

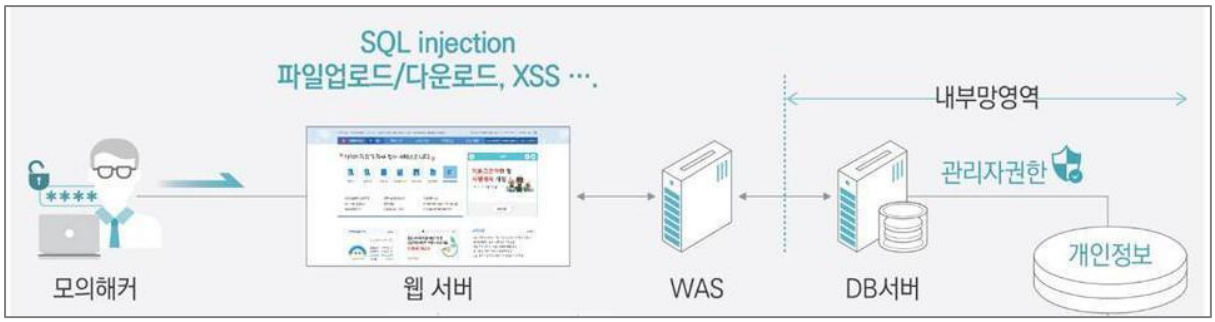
1 모의해킹

- 주제 : (구)KISEC 웹사이트 모의해킹을 통한 보안 점검

1-1 배경 및 목적

- 본 취약점 진단은 (구)KISEC 의 웹사이트에 대해 "주요 정보통신 기반시설 기술적 진단 가이드" 진단 항목을 기준으로 존재하는 취약점을 발견하고 취약점을 증명함으로써 해킹 위협으로부터 안전성 여부를 판단함과 동시에 보안 대응책 강구를 목적으로 한다.

1-2 수행 범위



[그림 1-1] 모의해킹 수행 범위

팀명	진단 사이트
1팀	(구)KISEC 웹 사이트 (10.10.0.165)
2팀	(구)KISEC 웹 사이트 (10.10.0.166)

[표 1-1] 모의해킹 수행 범위

1-3 수행 전략

- 작업의 효율성을 위해 취약점 진단 시 2 인 1 조로 구성하여 한 조당 하나의 취약점을 작업하도록 한다.
- 미리 취약점별 공격 스크립트를 작성하여 목록화하고, 프로젝트를 수행하는 시간에는 목록화된

코드를 대입하여 수행 시간을 최소화한다.

- 매일 프로젝트 수행 전, 전 날 파악된 취약점을 기반으로 팀원 한 명당 2 개의 시나리오를 계획한다.

1-4 수행 일정

<2020. 10. 26(월) ~ 2020. 11. 4(수)>

수행일정	26(월)	27(화)	28(수)	29(목)	30(금)	2(월)	3(화)	4(수)
수행계획서 작성								
정보 수집								
취약점 진단								
모의 침투								
보안대책 수립								
결과 보고서 작성								
프로젝트 발표								

[표 1-2] 모의해킹 수행 일정

1-5 수행 인원

팀	성명	비고
모의해킹 1팀	박기택	PL, 팀장
	김일한	
	강경훈	
	임승원	
	함도윤	
모의해킹 2팀	정형수	팀장
	김재원	
	이호웅	
	김상훈	

[표 1-3] 모의해킹 수행 인원

1-6 수행 내용

1-6-1 수행기준

점검항목	항목 중요도	항목코드
버퍼 오버플로우	상	BO
포맷스트링	상	FS
LDAP 인젝션	상	LI
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
SSI 인젝션	상	SS
XPath 인젝션	상	XI
디렉터리 인덱싱	상	DI
정보 누출	상	IL
악성 콘텐츠	상	CS
크로스사이트 스크립팅	상	XS
약한 문자열 강도	상	BF
불충분한 인증	상	IA
취약한 패스워드 복구	상	PR
CSRF	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE

[표 1-4] 주요정보통신기반시설 기술적 취약점 분석 상세 가이드

1-6-2 수행 내용 상세

1 - 6 - 2 - 1 정보수집

- OSINT 를 활용한 웹 정보를 수집한다.

  * SHODAN : https://www.shodan.io/

  * Censys : https://censys.io/

- 정보 수집 도구를 활용하여 웹 정보를 수집한다.

수집 도구	사용 목적
whatweb	서버의 구성요소 및 사용된 기술 식별
Nmap	네트워크 스캐닝

[표 1-5] 모의해킹 정보 수집 도구

1 - 6 - 2 - 2 취약점 진단

- 주요정보통신기반시설 취약점 가이드를 기반으로 웹 취약점 진단을 수행한다.
- 취약점 진단을 통해 확인된 취약점을 목록화한다.

1 - 6 - 2 - 3 모의 침투

- 파악된 취약점 목록을 활용하여 시나리오를 수립한다.
- 수립한 시나리오를 기반으로 모의 침투를 진행한다.
- 침투 결과에 따른 웹 서비스 안전성 확보 방향을 제시한다.

1-7 기대효과

- 홈페이지 모의해킹을 통한 데이터 유출 가능성을 사전탐지 및 예방한다.
- 주요정보통신기반시설 취약점 가이드의 웹 해킹 취약점 해소를 통해 안전성 확보한다.
- 개인정보 유출 등의 해킹 사고 발생시 법적 책임을 완화한다.
- 고객에게 안정적 서비스를 제공하여 기업 이미지를 향상한다.

2 취약점 진단

2-1 배경 및 목적

- "주요 정보통신 기반시설 기술적 진단 가이드(버전 2017.12)" 진단 항목을 기준으로 IT 인프라 장비를 점검하여 취약점을 찾아내어 취약점을 보완하고 위험을 수용할 수 있도록 감소시키는 것을 목적으로 한다.

2-2 수행 범위

- 고객사 보유 IT 인프라에 대한 취약점 점검한다.
- 리눅스 서버 7 대, 윈도우 서버 5 대, DBMS 3 대의 자산을 점검한다.

- 취약점 점검 항목

대분류	NO	자산식별	Hostname	IP	OS Ver.	용도
Server	LIN01	SV-74	NS-Master	210.222.32.74	Cent OS 5.5	DNS 서버
	LIN02	SV-182	serv-182	210.222.32.182	Cent OS 5.6	광고서버
	LIN03	SV-101	NDB-101	192.168.0.101	Cent OS 6.3	뉴스기사 DB
	LIN04	SV-141	web-01	210.222.32.141	Cent OS 5.6	뉴스웹서비스
	LIN05	SV-215	mobile-01	210.222.32.215	Cent OS 5.6	모바일서비스
	LIN06	SV-31	serv34	210.222.32.31	Red Hat Linux 7.3	메일서버
	LIN07	SV-94	Nserv-94	210.222.32.94	Cent OS 6.3	이미지서버
	WIN01	SV-19	LMSDB	192.168.0.240	Windows Server 2003 SE	LMSDB
	WIN02	SV-21	LMSWEB	210.222.32.241	Windows Server 2003 SE	LMS 웹서비스
	WIN03	SV-08	BACKUP	192.168.0.250	Windows Server 2012 R2	백업서버
	WIN04	SV-14	NMS	192.168.0.179	Windows Server 2012 R2	관리서버
	WIN05	SV-05	PAY2012	210.222.32.230	Windows Server 2012 R2	전자결제
Network	NW02	NT_01	MKDC-3750G-Active	210.222.32.74	ver. 15.2	L3Switch
DBMS	DB01	DB_01	NDB-101	192.168.0.101	11g Release 11.1.0.6.0	MainDB
	DB02	DB_02	LMSDB	192.168.0.240	SQL Server 2017	LMSDB
	DB03	DB_03	serv-182	210.222.32.182	5.1.41	광고서버

[표 2-1] 취약점 진단 점검 항목

2-3 수행 전략

- **협업**

  파트별로 분야를 나누었지만 필요에 따라 함께 협력하며 업무를 수행한다.

- **분석 및 평가**

  취약점을 상세 분석을 하고 평가하여 팀원들과 함께 보고서를 작성한다.

- **소통**

  업무를 진행하면서 어려운 부분에 대해 상의하고 피드백을 통해 프로젝트를 수행한다.

2-4 수행 일정

<2020. 10. 26(월) ~ 2020. 11. 4(수)>

수행일정	26(월)	27(화)	28(수)	29(목)	30(금)	2(월)	3(화)	4(수)
자료조사								
아이디어 구상								
분석								
인터뷰								
위험 분석 및 평가								
D.o.A 결정								
취합								
보고서 제작								
발표 준비								

[표 2-2] 취약점 진단 수행 일정

2-5 수행 인원

팀	성명	비고
취약점 진단 1 팀	심인철	팀장
	나지혜	
	배세진	
	김건영	
	조선경	
	최근호	
취약점 진단 2 팀	백인걸	팀장
	한지예	PL

	오희창	PM
	김한호	
	최재혁	
	반정원	

[표 2-3] 취약점 진단 수행 인원

2-6 수행 내용

2-6-1 수행기준

- 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드 (2017)를 기반으로 한 체크리스트 형식의 진단을 진행한다.

- UNIX 서버 취약점 분석 및 평가 항목 (참고. 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드 (2017))

구 분		점 검 항 목
1. 계정 관리	U-1	root 계정 원격 접속 제한
	U-2	패스워드 복잡성 설정
	U-3	계정 잠금 임계값 설정
	U-4	패스워드 파일 보호
	U-44	root 이외의 UID 가 '0' 금지
	U-45	root 계정 su 제한
	U-46	패스워드 최소 길이 설정
	U-47	패스워드 최대 사용기간 설정
	U-48	패스워드 최소 사용기간 설정
	U-49	불필요한 계정 제거
	U-50	관리자 그룹에 최소한의 계정 포함
	U-51	계정이 존재하지 않는 GID 금지
	U-52	동일한 UID 금지
	U-53	사용자 shell 점검
	U-54	Session Timeout 설정

2.파일 및 디렉터리 관리	U-05	root 홈, 패스 디렉토리 권한 및 패스 설정
	U-06	파일 및 디렉토리 소유자 설정
	U-07	/etc/passwd 파일 소유자 및 권한 설정
	U-08	/etc/shadow 파일 소유자 및 권한 설정
	U-09	/etc/hosts 파일 소유자 및 권한 설정
	U-10	/etc/(x)inetd.conf 파일 소유자 및 권한 설정
	U-11	/etc/syslog.conf 파일 소유자 및 권한 설정
	U-12	/etc/services 파일 소유자 및 권한 설정
	U-13	SUID, SGID, Sticky bit 설정 파일 점검
	U-14	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
	U-15	world writable 파일 점검
	U-16	/dev 에 존재하지 않는 device 파일 점검
	U-17	$HOME/.rhosts, hosts.equiv 사용 금지
	U-18	접속 IP 및 포트 제한
	U-55	hosts.lpd 파일 소유자 및 권한 설정
	U-56	NIS 서비스 비활성화
	U-57	UMASK 설정 관리
	U-58	홈 디렉토리 소유자 및 권한 설정
	U-59	홈 디렉토리로 지정한 디렉토리의 존재 및 관리
	U-60	숨겨진 파일 및 디렉토리 검색 및 제거(dot file)
3.서비스 관리	U-19	finger 서비스 비활성화
	U-20	Anonymous ftp 비활성화
	U-21	r 계열 서비스 비활성화
	U-22	cron 파일 소유자 및 권한 설정
	U-23	DoS 공격에 취약한 서비스 비활성화
	U-24	NFS 서비스 비활성화
	U-25	NFS 접근 통제
	U-26	automountd 제거
	U-27	RPC 서비스 확인
	U-28	NIS, NIS+ 점검

	U-29	tftp, talk 서비스 비활성화
	U-30	sendmail 버전 점검
	U-31	스팸 메일 릴레이 제한
	U-32	일반 사용자의 sendmail 실행 방지
	U-33	DNS 보안 패치
	U-34	DNS Zone Transfer 설정
	U-35	Apache 디렉토리 리스팅 제거
	U-36	Apache 웹 프로세스 권한 제한
	U-37	Apache 상위 디렉토리 접근 금지
	U-38	Apache 불필요한 파일 제거
	U-39	Apache 링크 사용 금지
	U-40	Apache 파일 업로드 및 다운로드 제한
	U-41	Apache 웹 서비스 영역의 분리
	U-61	ssh 원격 접속 허용
	U-62	ftp 서비스 확인
	U-63	ftp 계정 shell 제한
	U-64	ftpusers 파일 소유자 및 권한 설정
	U-65	ftpusers 파일 설정
	U-66	at 파일 소유자 및 권한 설정
	U-67	SNMP 서비스 구동 점검
	U-68	SNMP 서비스 커뮤니티 스트링의 복잡성 설정
	U-69	로그온 시 경고 메시지 제공
	U-70	NFS 설정 파일 접근 권한
	U-71	expn, vrfy 명령어 제한
	U-72	Apache 웹 서비스 정보 숨김
4. 패치 관리	U-42	최신 보안 패치 및 벤더 권고사항 적용
5. 로그 관리	U-43	로그의 정기적 검토 및 보고
	U-73	정책에 따른 시스템 로깅 설정

[표 2-4] 취약점 진단 수행 상세 내용(UNIX)

- Windows 서버 취약점 분석 및 평가 항목 (참고. 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드 (2017))

구 분		점 검 항 목
1. 계정 관리	W-01	Administrator 계정 이름 바꾸기
	W-02	Guest 계정 장비
	W-03	불필요한 계정 제거
	W-04	계정 잠금 임계값 설정
	W-05	해독 가능한 암호화를 사용하여 암호 저장 해제
	W-06	관리자 그룹에 최소한의 사용자 포함
	W-46	Everyone 사용권한을 익명 사용자에 적용 해제
	W-47	계정 잠금 시간 설정
	W-48	패스워드 복잡성 설정
	W-49	패스워드 최소 암호 길이
	W-50	패스워드 최대 사용 기간
	W-51	패스워드 최소 사용 기간
	W-52	마지막 사용자 이름 표시 안함
	W-53	로컬 로그온 허용
	W-54	익명 SID/이름 변환 허용 해제
	W-55	최근 암호 기억
	W-56	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한
	W-57	원격터미널 접속 가능한 사용자 그룹 제한
2. 서비스 관리	W-07	공유 권한 및 사용자 그룹 설정
	W-08	하드디스크 기본 공유 제거
	W-09	불필요한 서비스 제거
	W-10	IIS 서비스 구동 점검
	W-11	IIS 디렉토리 리스팅 제거
	W-12	IIS CGI 실행 제한
	W-13	IIS 상위 디렉토리 접근 금지
	W-14	IIS 불필요한 파일 제거
	W-15	IIS 웹프로세스 권한 제한
	W-16	IIS 링크 사용 금지

	W-17	IIS 파일 업로드 및 다운로드 제한
	W-18	IIS DB 연결 취약점 점검
	W-19	IIS 가상 디렉토리 삭제
	W-20	IIS 데이터파일 ACL 적용
	W-21	IIS 미사용 스크립트 매핑 제거
	W-22	IIS Exec 명령어 쉘 호출 진단
	W-23	IIS EWebDAV 비활성화
	W-24	NetBIOS 바인딩 서비스 구동 점검
	W-25	FTP 서비스 구동 점검
	W-26	FTP 디렉토리 접근 권한 설정
	W-27	Anonymous FTP 금지
	W-28	FTP 접근 제어 설정
	W-29	DNS Zone Transfer 금지
	W-30	RDS(Remote Data Services) 제거
	W-31	최신 서비스팩 적용
	W-58	터미널 서비스 암호화 수준 설정
	W-59	IIS 웹 서비스 정보 숨김
	W-60	SNMP 서비스 구동 점검
	W-61	SNMP 서비스 커뮤니티스트링의 복잡성 설정
	W-62	SNMP Access control 설정
	W-63	DNS 서비스 구동 점검
	W-64	HTTP/FTP/SMTP 배너 차단
	W-65	Telnet 보안 설정
	W-66	불필요한 ODBC/OLE-DB 데이터소스와 드라이브 제거
	W-67	원격터미널 접속 타임아웃 설정
	W-68	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검
3. 패치 관리	W-32	최신 HOT FIX 적용
	W-33	백신 프로그램 업데이트
	W-69	정책에 따른 시스템 로깅설정
4. 로그 관리	W-34	로그의 정기적 검토 및 보고

	W-35	원격으로 액세스 할 수 있는 레지스트리 경로
	W-70	이벤트 로그 관리 설정
	W-71	원격에서 이벤트 로그파일 접근 차단
5. 보안 관리	W-36	백신 프로그램 설치
	W-37	SAM 파일 접근 통제 설정
	W-38	화면보호기 설정
	W-39	로그온 하지 않고 시스템 종료 허용 해제
	W-40	원격 시스템에서 강제로 시스템 종료
	W-41	보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제
	W-42	SAM 계정과 공유의 익명 열거 허용 안함
	W-43	Autologin 기능 제어
	W-44	이동식 미디어 포맷 및 꺼내기 허용
	W-45	디스크 볼륨 암호화 설정
	W-72	Dos 공격 방어 레지스트리 설정
	W-73	사용자가 프린터 드라이버를 설치할 수 없게 함
	W-74	세션 연결을 중단하기 전에 필요한 유휴시간
	W-75	경고 메시지 설정
	W-76	사용자별 홈 디렉토리 권한 설정
	W-77	LAN Manager 인증 수준
	W-78	보안 채널 데이터 디지털 암호화 또는 서명
	W-79	파일 및 디렉토리 보호
	W-80	컴퓨터 계정 암호 최대 사용 기간
	W-81	시작 프로그램 목록 분석
6. DB 관리	W-82	Windows 인증 모드 사용

[표 2-5] 취약점 진단 수행 상세 내용(Windows)

- DBMS 취약점 분석 및 평가 항목(참고. 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드 (2017))

구분		점검 항목
1. 계정 관리	D-01	기본 계정의 패스워드, 권한 등을 변경하여 사용
	D-02	scott 등의 Demonstartion 및 불필요 계정을 제거하거나 잠금 설정 후 사용
	D-03	패스워드의 사용시간 및 복잡도를 기관 정책에 맞도록 설정
	D-04	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
	D-12	패스워드 재사용에 대한 제약이 설정되어 있는가?
	D-13	DB 사용자 계정 개별적 부여하여 사용하고 있는가?
2. 접근 관리	D-05	원격에서 DB 서버로의 접속 제한
	D-06	DBA 이외의 인기되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정
	D-07	오라클 데이터베이스의 경우 리스너의 패스워드를 설정하여 사용
	D-14	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거하고 사용하고 있는가?
	D-15	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정되어 있는가?
	D-16	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask 를 022 이상으로 설정하여 있는가?
	D-17	데이터베이스의 주요 설정 파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한 설정되어 있는가?
	D-18	관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경이 가능하지 않는가?
3. 옵션 관리	D-08	응용프로그램 또는 DBA 계정의 Role 이 Public 으로 설정되지 않도록 설정
	D-09	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 를 FALSE 로 설정
	D-19	패스워드 확인함수가 설정되어 적용되는가?
	D-20	인가되지 않은 Object Owner 가 존재하지 않는가?
	D-21	grant option 이 role 에 의해 부여되도록 설정되어 있는가?
	D-22	데이터베이스의 자원 제한 기능을 TRUE 로 설정하고 있는가?
4. 패치 관리	D-10	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용
	D-11	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정
	D-23	보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?
5. 로그 관리	D-24	Audit Table 은 데이터베이스 관리자 계정에 속해 있도록 설정되어 있는가?

[표 2-6] 취약점 진단 수행 상세 내용(DBMS)

2-6-2 수행상세내용

- **취약점 진단 결과 분석**
  각 자산 점검결과를 토대로 취약점 별 위험 평가를 하고, 진단 결과를 상세 분석을 한다.
- **인터뷰**
  인터뷰가 필요한 항목에 대해서 담당자와 인터뷰를 한다. D.o.A 를 결정한다.
- **위험 분석 및 평가**
  자산에 대한 평가와 취약점을 이용하여 위험을 분석하고 평가한다.
- **D.o.A 결정**
  고객사가 수용 가능한 D.o.A 를 결정하기 위한 지원을 한다.
- **마스터플랜 제작**
  고객사의 상황에 맞게 보안 방법의 우선순위를 정하는 마스터플랜을 제시한다.

2-7 기대효과

- 취약점 보완은 ROI 를 증가시켜 위험 감소한다.
- IT 인프라의 취약점 현황 파악한다.
- 전문적인 컨설팅을 통한 작업시간을 감소시킨다.
- 전문인력이 상주할 필요가 없기에 인건비가 감소한다.

3 관리 진단(정보)

3-1 배경 및 목적

- 본 프로젝트는 정보보호 법적 준거성 확보, 침해사고 및 집단소송 등에 따른 사회 · 경제적 피해 최소화의 중요성 대두를 배경으로, 관리체계 구축을 통한 온라인 쇼핑몰의 서비스 비즈니스 연속성 확보를 위한 정보보호 체계 수립을 목적으로 한다.

3-2 수행 범위

- KISA 가 운영하는 ISMS(Information Security Management System) 인증 기준을 따라 기업의 전체적인 관리체계를 구축한다.

3-3 수행 전략

3-3-1 정보수집

- '예/아니오'로 대답할 수 있는 단순한 질문이 아닌 기업의 상황을 충분히 이해할 수 있는 답변이 나오도록 인터뷰 자료를 구성한다.

3-3-2 관리 진단(개인)팀과 협업을 통한 개선 방향 설정

- 필요에 따라 관리 진단(개인)팀과 협력하여 미비한 부분을 보충한다.

3-3-3 관리 체계 구축

- KISA 의 ISMS 인증 체계를 구성하는 80 개의 기준이 모두 적절하게 수행될 수 있도록 4 명의 팀원의 20 개씩 기준을 받아 정책을 수립한다.
- 정책을 수립한 후 팀원들과 피드백을 주고 받는다.

3-4 수행 일정

<2020. 10. 26(월) ~ 2020. 11. 4(수)>

수행 일정	26(월)	27(화)	28(수)	29(목)	30(금)	2(월)	3(화)	4(수)
수행 계획서 작성								
정보 수집								
GAP 분석								
정책 수립								
결과 보고서 작성								
프로젝트 발표								

[표 3-1] 관리 진단(정보) 수행 일정

3-5 수행 인원

팀	성명	비고
관리 진단(정보)	주홍희	PL, 팀장
	정유진	
	장희나	
	윤하영	

[표 3-2] 관리 진단(정보) 수행 인원

3-6 수행 내용

3-6-1 수행기준

KISA 가 제공하는 ISMS-P 인증기준 안내서(2019.1.18)을 수행 기준으로 한다.

영역	분야	항목 (개)
관리체계 수립 및 운영 (16 개)	**관리체계 기반 마련**	6
	위험 관리	4
	관리체계 운영	3
	관리체계 점검 및 개선	3
보호대책 요구사항 (64 개)	**정책, 조직, 자산 관리**	3
	인적 보안	6
	외부자 보안	4
	물리보안	7
	인증 및 권한관리	6
	접근통제	7
	암호화 적용	2
	정보시스템 도입 및 개발 보안	6
	시스템 및 서비스 운영관리	7
	시스템 및 서비스 보안관리	9
	사고 예방 및 대응	5
	재해복구	2

[표 3-3] 관리 진단(정보) 수행 기준

3-6-2 수행 내용 상세

<관리체계 구축>

- **정보 수집**

  회사의 소개자료를 토대로 파악 후 인터뷰할 질문을 작성한다.

  질문을 통해 회사의 담당자와 인터뷰를 진행하여 정보 수집한다.

- **GAP 분석**

  정보 수집 내용을 토대로 ISMS 체크리스트 기반 분석을 실행한다.

  자산, 취약점, 위협 분석을 통해 위험 시나리오를 수립한다.

- **정책 수립**

  GAP 분석 자료를 활용하여 회사 정책의 부족한 부분을 파악한다.

  부족한 부분을 보완하여 ISMS 인증기준에 부합하는 정책을 수립한다.

- **마스터 플랜 작성**

3-7 기대효과

- **종합적 대책수립**

  종합적인(관리/기술/물리)정보보호대책을 수립할 수 있다.

  대외적으로 조직 정보보호 수준에 대한 확신을 제공할 수 있다.

- **비용절감**

  위험관리를 기반으로 비용 효과적인 정보보호대책을 구현할 수 있다.

- **회사 내 경쟁력**

  내부적으로는 각종 입찰 참여시 가점 등의 혜택을 받을 수 있어 사업 경쟁력이 강화된다.

4 관리 진단(개인)

4-1 배경 및 목적

본 프로젝트는 헬스케어를 이용하는 고객사에 대한 정보보호 및 개인정보보호 개선방향을 제시한다. 또한 헬스케어 서비스 내 개인정보 보호를 위한 보호체계를 설계함을 목적으로 한다.

4-2 수행 범위

연동되는 다양한 기기(모바일, 웨어러블, 가정 내 홈 헬스케어)를 통해 축적되는 건강 데이터와 Life-Cycle 패턴 분석 및 의료 정보를 안전하게 보호한다.

4-3 수행전략

4-3-1 개인정보 흐름 분석 및 관련 법적 요구사항 검토

- 개인정보보호법, 정보통신망법을 기반으로 개인정보 처리 단계별 요구사항을 작성한다.
- 인터뷰를 통해 회사 개인정보보호체계에 대한 법적 준거성을 검토한다.

4-3-2 관리 진단(정보)팀과 협업을 통한 개선 방향 설정

- 필요에 따라 관리 진단(정보)팀과 협력하여 미비한 부분을 보충한다.

4-3-3 개선방향 제시

- 법적 요구사항이 지켜지지 않은 사항에 대해 개인정보 보호 개선방향을 제시한다.

4-4 수행일정

<2020. 10. 26(월) ~ 2020. 11. 4(수)>

수행일정	26(월)	27(화)	28(수)	29(목)	30(금)	2(월)	3(화)	4(수)
수행계획서 작성								
현황 분석								
인터뷰								
개인정보 흐름 파악								
개선 사항 도출								
결과 보고서 작성								
프로젝트 발표								

[표 4-1] 관리 진단(개인) 수행 일정

4-5 수행인원

팀	성명	비고
관리 진단(정보)	김가영	팀장
	신정은	
	정민영	

[표 4-2] 관리 진단(개인) 수행 인원

4-6 수행내용

4-6-1 수행기준

- 「개인정보 보호법」을 기반으로 하고, 개인정보의 안전성 확보조치 기준을 참조한다.
- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(약칭: 정보통신망법)을 참조한다.

4-6-2 수행 내용 상세

- **자료 수집**
  담당자에게 관련 자료를 요청하고, 내용을 파악한다.
- **현황조사**
  서비스 로드 맵 및 시행계획을 토대로 현황 조사 진행한다.
- **인터뷰**
  담당자와의 인터뷰를 통해 현재 관리 상황 파악한다.
- **개인정보 흐름 파악**
  개인정보의 흐름을 파악하여 흐름도와 흐름표 작성한다.
- **개선 사항 도출**
  인터뷰와 작성된 개인정보 흐름표를 기반으로 개선사항을 도출한다.
  개인정보보호법과 정보통신망법을 참조하여 개인정보 처리 단계별 요구사항을 도출한다.

4-7 기대효과

- 안전성
  법적 준거성 검토를 통해 개인정보의 안전성 보호를 책임진다.
  정보보호의 신뢰도 향상으로 인한 서비스 이용 증대효과가 있다.
- 효율성
  법에 근거한 개인정보 라이프 사이클을 구축하여 개인정보 관리 효율성을 높인다.