데이터 보안 점검사항

통제 영역		통제 목표	통제항목	설 명
보안기획 및 관리	1. 기획 및 조사	1.1 DB보안 정책의 수립	1.1.1 DB보안 정책 및 세부 정책 수립	보안 정책은 상위 정책(규정)과 일관성을 유지하고, DB보안의 목적 및 범위를 포함하여 문서화 하여야 한다. 또한 보안 정책을 지원하기 위한 DB보안절차 및 지침 등을 문서화 하여야 한다.
			1.1.2 컴플라이언스 준수	보안정책은 관련 법.규제 대응을 포함하여야 한다.
			1.1.3 DB보안 조직의 구성	DB보안을 전담하는 조직을 구성하고, 역할 및 책임을 명확히 하여야 한다. DB보안 담당자는 개발자나 시스템관리자와 직무가 분리되어야 하며, 여건상 직무 분리가 어렵다면 관리 강화 대책이 마련되어야 한다.
			1.1.4 경영층 승인	보안정책은 경영진의 승인을 득하여야 한다.
			1.1.5 DB보안 정책 배포 및 관리	DB보안 정책 및 지원 문서들의 제/개정 및 변경, 배포 등을 통제하기 위한 절차가 문서화 또는 시스템화 되어 있어야 한다.
		1.2 위험평가	1.2.1 위험평가 방법 결정	위험평가 방법을 선정하고 위험평가 계획을 수립 하여야 한다.
			1.2.2 DB자산 식별	위험 평가 계획에 의거 DB자산을 식별하고 목록화 하여야 하며, DB자산 목록의 항목에는 DB자산에 대한 등급/소유자/관리자를 명시 하여야 한다.
			1.2.3 위험분석	위협과 취약점을 평가 하여야 하며, 취약성은 관리적 기술적인 부문을 포함하여야 한다.
			1.2.4 위험평가	위험분석 결과를 바탕으로 위험도를 산정하고 우선순위를 부여한 목록이 작성되어야 한다..
		1.3 DB보안요구사항 정의	1.3.1 수용 위험수준 선정	관련자 검토를 통하여 수용 가능한 위험수준을 선정하여야 한다.
			1.3.2 DB보안 요구사항 정의(보호대책)	수용 수준을 넘어서는 위험에 대하여 보호대책을 선정하고 DB보안 요구사항으로 정의 하여야 한다.
	2. 보안 및 보호	2.1 DB보안 구축	2.1.1 DB보안 구축 로드맵 수립	조직의 역량에 따라 장.단기 계획을 수립하고 로드맵으로 관리하여야 한다. 로드맵은 관련자와 검토를 거치고 경영자의 승인을 득하여야 한다.
			2.1.2 DB보안 구축 예산 확보	로드맵은 장.단기를 구분하여 예산에 반영하여야 한다.
			2.1.3 DB보안 구축 조직 구성	구축 담당자를 지정하고, 보안 솔루션 구축은 외부 인원이 수행하므로 보안서약서 징구 및 관리 대책을 함께 수립하여야 한다.
		2.2 DB보안 교육	2.2.1 DB보안 교육 계획 수립	조직의 각 역할에 맞는 보안 인식 교육 계획을 수립하고 시행하여야 한다.
			2.2.2 DB보안 교육 실시	정해진 계획에 의거 교육을 실시하고, 교육 참석 확인 및 교육 피드백을 받아 차기 교육에 반영 하여야 한다.
	3. 모니터링 및 감사	3.1 DB보안 모니터링	3.1.1 모니터링 계획 수립	상시 모니터링 및 정기점검 계획을 수립하여야 하고, 점검 항목에는 내/외부 환경의 변화와 DB보안관리체계 운영현황, 보안 기술요소 운영 상태를 포함하여야 한다.
			3.1.2 모니터링 수행	모니터링 결과를 문서화 하고 이력을 관리하여야 한다.
			3.1.2 모니터링 결과 분석	모니터링 결과를 분석하고 정기적으로 보고하여야 한다.
		3.3 DB보안 감사	3.2.1 감사 계획 수립	내부 감사 계획을 수립하고 시행하여야 한다. 감사 내용은 정책서 점검, 관리활동 점검, 보안 시스템 점검, 점검활동 점검 등을 포함하여야 한다.
			3.2.2 감사 수행	감사 결과를 문서화하고 이력을 관리하여야 한다.
			3.2.3 감사 후속 조치	감사 결과에 대한 후속 조치를 수행하고 조치결과를 경영진에 보고하여야 한다.
접근제어	4. 구축기획	4.1 DB보안 구축계획 수립	4.1.1 DB보안 구축계획 수립	DB보안 구축 범위를 정의하고 수행 조직의 역할 및 책임을 명시하여야 하며, 구축 완료를 승인하는 절차를 포함하여야 한다.
		4.2 DB보안솔루션 도입	4.2.1 제품선정	도입 제품은 보안요구 기능, 비상대응 기능 및 인증요구 등을 만족하여야 한다.
			4.2.2 제품설치	구축 계획에 따라 우회접근 방지, 접근제어 서버 보안대책 및 접근제어 서버 이중화를 포함하여 제품이 설치되어야 한다.
		4.3 운영 정책의 수립	4.3.1 운영 정책의 수립	DB접근제어 시스템에 대한 운영 절차를 수립하여야 한다. 운영 절차에는 운영자에 대한 역할 및 책임 명시, 보안 규칙 변경, 보안 경보 모니터링, 장애 및 사고 대응을 포함하여야 한다.
	5. 설계	5.1 DB보안설계	5.1.1 DB사용자 식별	DB사용자는 유일하게 식별할 수 있어야 하며 패스워드의 복잡도는 컴플라이언스 기준을 충족하여야 하고, 초기 패스워드 변경 및 변경 주기를 강제할 수 있도록 시스템화 하여야 한다.
			5.1.2 DB보안 규칙 설계	DB보안 규칙은 DB보안 요구사항을 만족하여야 한다.
		5.2 DB보안 시험계획 수립	5.2.1 DB보안 시험계획 수립	시험범위, 일정, 시험 환경 및 세부 절차를 포함하는 시험계획을 수립하여야 한다.
	6. 구축	6.1 DB보안 규칙 적용	6.1.1 DB보안 규칙 적용	DB보안 규칙은 DB에 접속하는 모든 세션에 적용되어야 한다.
		6.2 DB보안 시험	6.2.1 DB보안 시험 수행	시험계획서 상의 시험 항목은 누락 없이 모두 수행하여야 하며, 미 충족 항목이 없어야 한다.
	7. 시스템 운영	7.1 DB보안 시스템 운영	7.1.1 통제	다음의 항목에 대한 통제 및 관련 조치가 적용되어야 한다. - 로그인 통제 - SQL 수행 통제 (통제 사유 제공) - 개인정보/민감정보 접근 통제 - IDLE 상태 통제 - 보안 위반에 대한 경보 - 중요한 테이블에 대한 접근 및 관찰 대상 SQL 수행 시도에 대해 경보 - SQL 마스킹 통제
			7.1.2 로깅	다음의 항목에 대한 로깅 및 관련 조치가 적용되어야 한다. - DB접속 및 SQL 수행 이력 저장 - SQL 변수값 및 조회 결과 저장 - 보안규칙 변경 이력 저장
			7.1.3 운영기록의 수집 및 검토	운영기록이 수집 및 검토되어야 한다. - 이벤트 발생 이력 및 내용 - 로그 수집 내용 - 퇴사자 규칙을 포함하여 미사용규칙을 제거 이력 - 백업 이력 및 내용 - 보안 시스템 상태 정보
			7.1.4 운영 현황 보고	수집 및 검토한 운영 현황을 주기적으로 관리자에게 보고하여야 한다.
암호화	4. 구축기획	4.1 DB보안 구축계획 수립	4.1.1 DB보안 구축계획 수립	DB보안 구축 범위를 정의하고 수행 조직의 역할 및 책임을 명시하여야 하며, 구축 완료를 승인하는 절차를 포함하여야 한다.
		4.2 DB보안솔루션 도입	4.2.1 제품선정	도입 제품은 보안요구 기능, 비상대응 기능 및 인증요구(검증필 암호 모듈 사용) 등을 만족하여야 한다.
			4.2.2 제품설치	구축 계획에 따라 우회접근 방지, 암호화키 서버 보안대책, 암호화키 서버 이중화를 포함하여 제품이 설치되어야 한다.
		4.3 운영 정책의 수립	4.3.1 운영 정책의 수립	DB암호화에 대한 범위, 절차 및 방법을 포함하는 암호화 운영 절차를 수립하여야 한다. 또한 안전한 암호화키 관리를 위한 운영 절차를 수립하여야 한다. - 마스터키 백업 및 안전한 장소 보관 등 - 암호화 솔루션이 보유(사용)하는 DB계정의 과도한 권한제한으로 시스템 취약점 방어
	5. 설계	5.1 DB보안설계	5.1.1 DB사용자 식별	DB사용자는 유일하게 식별할 수 있어야 하며 패스워드의 복잡도는 컴플라이언스 기준을 충족하여야 한다.
			5.1.2 DB보안 규칙 설계	DB보안 규칙은 DB보안 요구사항을 만족하여야 한다. - 개인정보보호법 충족 등
		5.2 DB보안 시험계획 수립	5.2.1 DB보안 시험계획 수립	시험범위, 일정, 시험 환경 및 세부 절차를 포함하는 시험계획을 수립하여야 한다.
	6. 구축	6.1 DB보안 규칙 적용	6.1.1 DB보안 규칙 적용	DB보안 규칙의 적용은 관련 부서와 협의 후 진행하여야 한다. - 원본데이터 삭제 (인덱스/뷰, 임시 테이블, 백업 데이터 포함) - 참조 무결성관계 유지 - 제약조건 정상 동작 - 암호화키, 데이터와 물리적 분리, 암호화 키 백업 및 복구
		6.2 DB보안 시험	6.2.1 DB보안 시험 수행	시험계획서 상의 시험 항목은 누락 없이 모두 수행하여야 하며, 미 충족 항목이 없어야 한다.
	7. 시스템 운영	7.1 DB보안 시스템 운영	7.1.1 통제	다음의 항목에 대한 통제 및 관련 조치가 적용되어야 한다. - 사용자 식별 및 인증 - 복호화 권한 통제 - 비인가 암호키 접근 통제 - 패스워드 단방향 암호화
			7.1.2 로깅	다음의 항목에 대한 로깅 및 관련 조치가 적용되어야 한다. - 암호키 사용이력 저장 (생성/삭제/변경 이력 포함) - 암호화 시스템의 시작/정지 이력 - 초기 암호화 수행이력 (테이블 및 칼럼 변경이력 포함) - 보안규칙 변경 이력 저장 - 복호화 수행 정보 (사용자, 해당 SQL 포함)
			7.1.3 운영기록의 수집 및 검토	다음의 운영기록이 수집 및 검토되어야 한다. - 이벤트 발생 이력 및 내용 - 로그 수집 내용 - 보안규칙 변경 이력 - 백업 이력 및 내용 - 보안 시스템 상태 정보
			7.1.4 운영 현황 보고	수집 및 검토한 운영 현황을 주기적으로 관리자에게 보고하여야 한다.
작업결재	4. 구축기획	4.1 DB보안 구축계획 수립	4.1.1 DB보안 구축계획 수립	DB보안 구축 범위를 정의하고 수행 조직의 역할 및 책임을 명시하여야 하며, 구축 완료를 승인하는 절차를 포함하여야 한다.
		4.2 DB보안솔루션 도입	4.2.1 제품선정	도입 제품은 보안요구 기능, 비상대응 기능 및 인증요구 등을 만족하여야 한다.
			4.2.2 제품설치	구축 계획에 따라 우회접근 방지, 작업결재 서버 보안대책 및 작업결재 서버 이중화를 포함하여 제품이 설치되어야 한다.
		4.3 운영 정책의 수립	4.3.1 운영 정책의 수립	DB작업결재에 대한 범위, 절차 및 방법을 포함하는 작업결재 운영 절차를 수립하여야 한다.
	5. 설계	5.1 DB보안설계	5.1.1 DB사용자 식별	DB사용자는 유일하게 식별할 수 있어야 하며 패스워드의 복잡도는 컴플라이언스 기준을 충족하여야 하고, 초기 패스워드 변경 및 변경 주기를 강제할 수 있도록 시스템화 하여야 한다.
			5.1.2 DB보안 규칙 설계	DB보안 규칙은 DB보안 요구사항을 만족하여야 한다. - 다양한 결재경로 관리, 위임 결재 등
		5.2 DB보안 시험계획 수립	5.2.1 DB보안 시험계획 수립	시험범위, 일정, 시험 환경 및 세부 절차를 포함하는 시험계획을 수립하여야 한다.
	6. 구축	6.1 DB보안 규칙 적용	6.1.1 DB보안 규칙 적용	DB보안 규칙의 적용은 관련 부서와 협의 후 진행하여야 한다. - 조직도를 반영한 결재 프로세스 적용
		6.2 DB보안 시험	6.2.1 DB보안 시험 수행	시험계획서 상의 시험 항목은 누락 없이 모두 수행하여야 하며, 미 충족 항목이 없어야 한다.
	7. 시스템 운영	7.1 DB보안 시스템 운영	7.1.1 통제	다음의 항목에 대한 통제 및 관련 조치가 적용되어야 한다. - 사전결재/즉시결재/사후결재 등 적절한 결재 방법 구현 - 중요 정보에 대한 결재 처리 - 결재자 관리 및 결재자 상태 관리 - 승인된 내용으로만 로그인 & SQL 수행 가능 여부
			7.1.2 로깅	다음의 항목에 대한 로깅 및 관련 조치가 적용되어야 한다. - 결재 이력 - 결재받은 계정에 대한 접근 및 SQL 수행 이력 - 보안규칙 변경 이력 저장 - 결재자 자신이 결재한 이력만 조회 - 특정 SQL에 대한 수행 전후 데이터 저장
			7.1.3 운영기록의 수집 및 검토	다음의 운영기록이 수집 및 검토되어야 한다. - 이벤트 발생 이력 및 내용 - 로그 수집 내용 - 보안규칙 변경 이력 - 백업 이력 및 내용 - 보안 시스템 상태 정보
			7.1.4 운영 현황 보고	수집 및 검토한 운영 현황을 주기적으로 관리자에게 보고하여야 한다.
취약점분석	4. 구축기획	4.1 DB보안 구축계획 수립	4.1.1 DB보안 구축계획 수립	DB보안 구축 범위를 정의하고 수행 조직의 역할 및 책임을 명시하여야 하며, 구축 완료를 승인하는 절차를 포함하여야 한다.
		4.2 DB보안솔루션 도입	4.2.1 제품선정	도입 제품은 보안요구 기능을 만족하여야 한다.
			4.2.2 제품설치	구축 계획에 따라 지정 PC에 제품이 설치되어야 한다.
		4.3 운영 정책의 수립	4.3.1 운영 정책의 수립	취약점 분석 운영 절차를 수립하여야 한다. 운영 절차에는 운영자에 대한 역할 및 책임 명시, 보안 규칙 변경, 보고서 검토 및 이력관리를 포함하여야 한다.
	5. 설계	5.1 DB보안설계	5.1.1 DB사용자 식별	취약점 분석용 DB사용자는 별도로 지정하여야 하며 다른 용도로 사용할 수 없다. 패스워드의 복잡도는 보안관리자 패스워드와 동일 수준으로 설정하여야 하고, 주기적으로 변경하여야 한다.
			5.1.2 DB보안 규칙 설계	DB보안 규칙은 DB보안 요구사항을 만족하여야 한다.
		5.2 DB보안 시험계획 수립	5.2.1 DB보안 시험계획 수립	시험범위, 일정, 시험 환경 및 세부 절차를 포함하는 시험계획을 수립하여야 한다.
	6. 구축	6.1 DB보안 규칙 적용	6.1.1 DB보안 규칙 적용	DB보안 규칙의 적용은 관련 부서와 협의 후 진행하여야 한다.
		6.2 DB보안 시험	6.2.1 DB보안 시험 수행	시험계획서 상의 시험 항목은 누락 없이 모두 수행하여야 하며, 미 충족 항목이 없어야 한다. - 모의해킹, 내부감사 수행 및 조치
	7. 시스템 운영	7.1 DB보안 시스템 운영	7.1.1 통제	다음의 항목에 대한 통제 및 관련 조치가 적용되어야 한다. - 취약점 최신 정보 수집 - 주기적인 취약점 분석 수행 - 취약점 제거 - 취약점 항목의 배포 및 회수에 관한 통제
			7.1.2 로깅	다음의 항목에 대한 로깅 및 관련 조치가 적용되어야 한다. - 취약점 결과 보고서 관리 - 취약점 이력 관리
			7.1.3 운영기록의 수집 및 검토	다음의 운영기록이 수집 및 검토되어야 한다. - 취약점 분석 결과 - 미조치 취약점 목록 - 보안규칙 변경 이력
			7.1.4 운영 현황 보고	취약점 분석 현황을 주기적으로 관리자에게 보고하여야 한다.

인증수준

레벨1

레벨2

레벨3

레벨4

데이터 보안인증

DataQuality Certification -Security

데이터 보안 인증(DQC-S)이란 공공·민간에서 구축·활용 중인 데이터베이스를 대상으로 DB접근제어, DB암호화, DB작업결재, DB취약점분석등 데이터베이스 보안에 대한 기술요소 전반을 심사하여 인증하는 것을 의미합니다.

정보 보안과 데이터 보안

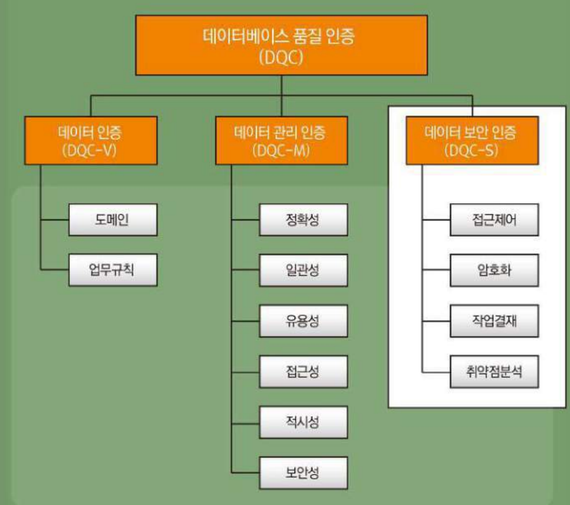
① Applicaton 보안
② Network 보안
③ Server 보안
④ DB 보안
① ② ③ ④ 정보보안

"데이터베이스 보안 가이드라인" P.48 참조

데이터 보안 프레임워크

	DB 접근제어	DB 암호화	DB 작업결재	DB 취약점분석
기획	DB 보안 정책수립			
설계	접근제어 규칙 정의	복호화 권한 통제	작업결재 규칙 정의	취약점 분석 계획
		암호화 키 및 알고리즘 정의		
구축	우회 접근 방지	원본 데이터 삭제	우회 결재 방지	모의 해킹
		제약 사항 유지		
		암호화 키 관리		
	환경보완			내부보안 감사
	보안 적용 시험			
운영	보안규칙관리			취약점 수집
	사용자 로그 관리			취약점 제거
	모니터링			취약점 개선 분석 비교
	운영 리뷰			

데이터베이스 품질 인증의 구성



관련문의

서광래 연구원
skr@kdata.or.kr 02-3708-5426
http://www.dqc.or.kr

한국데이터진흥원 Korea Data Agency