2013 개인정보 보호를 위한
데이터베이스 보안 세미나

IBM

한국IBM 정보관리사업부
조가원 차장
2013/10/29

개인정보보호법에 대응하는 우리의 자세

© 2013 IBM Corporation

개인정보 공개에 대한 항목별 거부감

개인정보 공개항목	전혀 거부감이 들지 않는다	거부감이 들지 않는다	거부감이 드는 편이다	매우 거부감이 든다		거부감이 드는 편이다+ 매우 거부감이 든다	
• 주민등록번호	0.5	2.3	13.4	83.8	(1)	97.2	(1)
• 휴대폰번호	0.9	11.7	38.6	48.8	(2)	87.4	(2)
• 자택전화번호	1.2	11.5	42.6	44.7	(3)	87.3	(3)
• 소득정보	1.7	13.1	40.8	44.2	(5)	85.0	(4)
• 부동산정보	1.8	13.7	38.1	46.2	(4)	84.3	(5)
• 자택주소	2.3	17.3	50.3	30.1		80.4	(6)
• 신체정보	1.6	19.3	38.8	40.2	(6)	79.0	(7)
• 회사전화번호	2.4	20.1	46.3	30.9	(10)	77.2	(8)
• 의료정보	2.5	22.9	41.6	32.9	(8)	74.5	(9)
• 아이디	4.8	23.4	33.4	38.5	(7)	71.9	(10)
• 직장주소	3.4	25.3	48.8	22.3		71.1	
• 생일	3.7	26.2	37.3	32.8	(9)	70.1	
• 메일주소	3.9	27.8	43.2	25.1		68.3	
• 직장명	3.7	28.1	43.7	24.3		68.0	
• 직업	4.4	36.7	38.4	20.4		58.8	
• 이름	7.1	37.4	39.2	16.3		55.5	
• 나이	7.7	40.7	35.7	15.8		51.5	

출처 : 2012년 개인 인터넷 이용자 정보보호 실태조사(한국인터넷진흥원, 2012)

© 2013 IBM Corporation

개인정보 유형별 중요도 인식

개인정보유형	전혀 중요하지 않음	별로 중요하지 않음	보통	다소 중요함	매우 중요함	다소 + 매우 중요함
일반정보	0.9	1.0	9.9	15.7	72.5	88.2
가족정보	4.3	4.8	16.3	21.7	52.9	74.6
신용정보	11.6	4.5	14.5	16.0	53.5	69.5
소득정보	11.9	6.8	17.1	15.8	48.4	64.2
부동산정보	12.0	6.8	19.1	17.7	44.4	62.1
법적정보	11.6	5.3	21.7	13.6	47.8	61.4
기타 수익정보	13.5	7.2	19.5	20.0	39.7	59.7
의료정보	10.0	5.2	27.0	14.1	43.7	57.8
교육 및 훈련정보	8.7	7.6	26.2	19.0	38.4	57.4
고용정보	12.9	5.4	25.9	20.4	35.4	55.8
신체정보	12.4	7.8	28.5	15.8	35.5	51.3
통신정보	12.8	6.9	29.4	15.2	35.8	51.0
위치정보	13.6	7.6	28.3	15.1	35.4	50.5
병역정보	13.7	8.7	30.7	15.5	31.4	46.9
조직정보	13.3	6.8	35.7	17.7	26.5	44.2
습관 및 취미정보	12.2	10.1	33.8	16.8	27.1	43.9

출처 : 2012년 민간기업 정보보호 실태조사(한국인터넷진흥원, 2012)

© 2013 IBM Corporation

개인정보 보호법 대응 방안 요약

개인정보보호법은 전 산업 분야에 걸쳐 많은 영향을 줄 것으로 판단되며 이를 대응하기 위해, 개인정보의 수집 이용 제공 등 처리 단계에 따른 법적 요구사항을 면밀히 분석하여 법률 위반 사항이 없도록 만반의 준비와 더불어 개인정보보호법 세부 시행령, 규칙, 표준 지침 등의 발표에 따른 구체적 기준 및 절차 마련 및 대응 필요

1. 개인정보보호책임자 지정 및 전담조직 강화

- 임원급 개인정보 책임자 지정
- 지속적 개인정보보호업무 수행을 위한 전담조직 구성
- 개인정보보호법 시행관리를 위한 TF 팀 조직 대응

2. 개인정보보호 정책 지침 등 규정 정비

- 법령을 반영하여 개인정보보호 정책, 지침 등 관련 규정 재정비
- 개인정보 처리 수탁업체 및 서비스 제휴업체 등과의 계약서를 재 검토하여 법령 요구 사항 반영
- 개인정보보호법만이 아닌 개별법에서 규정한 개인정보보호 관련 내용도 함께 검토하여 모두 포함한 정책 수립, 준수관리 누락 리스크 최소화

3. 개인정보보호 컴플라이언스 활동 강화

- 개인정보 보안사고 및 법령 준수 대응을 위한 법률, 정책, 지침 요건 일상 점검 컴플라이언스 활동 강화
- 컴플라이언스 결과의 시정활동을 통한 개인정보 관리 수준 향상
- 기존 준법감시, 감사부서등의 역할 재정립

4. 전사적인 개인정보보호 관리체계 수립 및 이행

- 개인정보의 체계적이고 지속적 관리를 위한 전사 개인정보보호 관리체계 운영 수립
  - 사내 개인정보 유형 식별, 정의, 개인정보의 흐름, 업무 처리 프로세스 등 개인정보 생명 주기 각 단계별 현황 관리 강화 및 위험 관리를 통한 적절한 보호 대책 수립 적용

5. 개인정보처리시스템의 안전성 강화

- 개인정보 처리 시스템의 접근 권한 통제, 접근 이력 보관, 접근 기록 위변조 방지 및 백업, 개인정보 암호화, 보안 서버 구축, 악성 프로그램 방지, 패스워드 설정 강화 등
- 보안 솔루션 도입 검토 - 개인정보 유출 방지 시스템 등
- 개인정보보호법에서 추후 제시될 관리적, 기술적, 물리적 보호 조치 요건 주시 관리

6. 개인정보취급에 대한 관리 감독 및 교육 강화

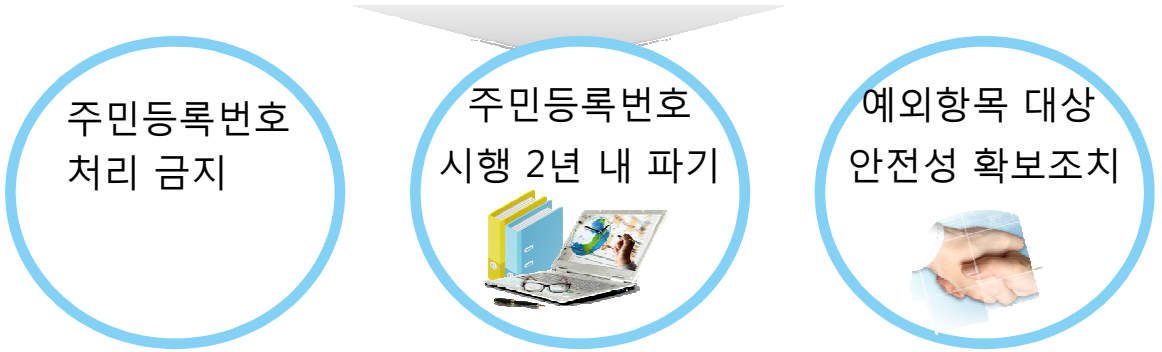
- 내부자에 의한 개인정보보안 사고를 최소화 하기 위해 개인정보취급자들에 대한 처리 권한 최소화 통제 관리
- 주기적 감사를 통한 관리 감독 강화
- 연2회 이상 개인정보보호 강화 교육 수행으로 개인정보보호에 대한 직원 의식 제고

© 2013 IBM Corporation

개인정보 보호법 개정안 의결

개인정보에 대한 기술적 보호 조치 (개인정보 – 고유식별정보 에 대한 암호화 조치) 의무화에 대한 준수 및 기업의 가장 소중한 자산인 고객정보(DB)에 대한 유출 통제 및 차단 방안 마련이 필요

구분	게정안
주민등록번호 수집이용	**주민등록번호 원칙적 처리금지 및 법 시행 2년 내에 파기해야 함** **단,예외적용:** **-법령에 구체적인 근거 있는 경우** **-정보주체 또는 제3자의 급박한 생명,신체,재산의 이익을 위해 명백히 필요한 경우** **-안전행정부령으로 정하는 경우**
과징금 제도	**주민등록번호 분실,도난,유출,변조,훼손 시** **최대 5억원 과징금 부과** **단, 안전성 확보조치를 모두 이행한 경우 제외**
CEO 징계권고	**책임 있는 자에 해당 기관 대표자 및 책임 있는 임원이 포함된다는 것을 명확화**



© 2013 IBM Corporation

개인정보의 기술적 관리적 보호조치 방안

과거 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 대한 개인정보의 기술적·관리적 보호조치기준 고시를 통해, 개인정보처리시스템에 접근하는 개인정보취급자 접근통제규칙의 상세화, 침해대응을 위해 개인정보취급자 접속기록의 관리·감독의 강화, 민감한 개인정보의 불법사용을 방지하기 위한 개인정보의 암호화 강화 등 보호 조치 사례

통제 항목	보호 조치 내역
제3조 내부관리계획의 수립·시행	이용자 개인정보의 안전한 취급을 위한 내부관리계획의 수립·시행의 보호조치
제4조 접근통제	이용자 개인정보에 대한 불법적인 접근을 차단하기 위한 접근통제 규칙, 침입차단시시스템 및 침입탐지시스템의 설치·운영 등 보호조치
제5조 접속기록의 위·변조방지	개인정보취급자의 개인정보처리시스템에 대한 접속기록의 위조·변조 방지를 위한 보호조치
제6조 개인정보의 암호화	이용자의 개인정보가 안전하게 저장·전송될 수 있도록 보호조치
제7조 악성프로그램 방지	악성 프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어의 설치·운영 등 보안 조치
제8조 출력·복사	출력 복사 통제시 용도 지정 및 사전 승인 통제
제9조 개인정보 표시 제한	개인정보 조회, 출력시 개인정보 마스킹 처리

© 2013 IBM Corporation

개인정보의 기술적 관리적 보호조치 방안

통제 항목	세부 내역
제3조 내부관리계획의 수립·시행	**① 개인정보 보호조직의 구성 및 운영** **② 개인정보보호 교육** 교육 계획 수립, 연 2회 이상 실시 **③ 이하 개인정보 보호조치 이행을 위한 세부적인 추진방안 수립**
제4조 접근통제	**① 개인정보처리시스템 접근권한 제한** – 서비스 제공을 위해 필요한 개인정보관리책임자 또는 개인정보취급자에게만 허용 **② 개인정보 취급자 전보, 퇴직시 시스템 접근 권한 즉시 변경** **③ 시스템 접근 권한 관리 이력 기록 및 5년 보관** **④ 외부 네트워크로부터 시스템 접근시 공인인증서 등 안전한 인증 수단 적용**(정보통신망을 통해 외부) **⑤ 네트워크 불법적인 접근, 침해사고 방지 목적 시스템 설치·운영** 1.개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한 (미안가 접근 제한) 2.접속한 IP주소 등을 재분석, 불법적인 개인정보 유출 시도 탐지 **⑥ 이용자의 안전한 비밀번호를 작성규칙 수립, 이행** **⑦ 개인정보취급자의 비밀번호 작성규칙 수립, 적용, 운용** 1. 다음 중 2종류 이상을 조합, 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 가. 영문 대문자(26개)/나. 영문 소문자(26개)/다. 숫자(10개)/라. 특수문자(32개) 2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 금지 권고 3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 **⑧ 개인정보 유출 방지 조치 적용 - 개인정보 처리시스템 및 개인정보취급자 PC** - 인터넷 홈페이지, P2P, 공유설정 등을 통한 개인정보 유출 차단

© 2013 IBM Corporation

개인정보의 기술적 관리적 보호조치 방안

통제 항목	세부 내역
제5조 접속기록의 위·변조방지	① **접속한 로그 월 1회 이상 정기적으로 확인·감독, 접속로그 6개월 이상 보존·관리** ②「**전기통신사업법**」**제5조의 규정에 따른 기간통신 사업자는 2년 보관** ③ **로그는 별도의 물리적인 저장 장치에 보관 및 백업을 수행** (로그 위·변조 방지 목적)
제6조 개인정보의 암호화	① **비밀번호 및 바이오정보 일방향 암호화 저장 (복호화 방지)** ② **주민등록번호, 신용카드번호 및 계좌번호 암호화 저장** (안전한 암호 알고리듬) ③ **개인정보 및 인증정보 네트워크 전송시, 통신 암호화 적용 - 보안서버 구축** 1. 웹서버에 **SSL(Secure Socket Layer) 인증서 설치**, 통신 데이터 암호화 2. 웹서버에 **암호화 응용프로그램을 설치**하여 통신 데이터 암호화 ④ **이용자의 개인정보 개인용컴퓨터(PC) 저장시 암호화 처리**
제7조 악성프로그 램 방지	**백신 소프트웨어를 월 1회 이상 갱신·점검** **악성 프로그램관련 경보가 발령된** 경우 및 백신소프트웨어 또는 운영체제 제작업체에서 업데이트 공지가 있는 경우에는 **응용프로그램과 정합성을 고려하여 최신 소프트웨어로 갱신·점검**

© 2013 IBM Corporation

개인정보의 기술적 관리적 보호조치 방안

통제 항목	세부 내역
제8조 출력·복사	**① 개인정보의 출력 시 용도 지정, 용도에 따라 출력 항목을 최소화** **② 개인정보 종이 인쇄, 이동시 저장 매체 복사시 아래 정보 기록, 사전 개인정보관리책임자의 승인 처리** 1. 출력·복사물 일련번호 2. 출력·복사물의 형태 3. 출력·복사 일시 4. 출력·복사의 목적 5. 출력·복사를 한 자의 소속 및 성명 6. 출력·복사물을 전달 받을 자 7. 출력·복사물의 파기일자 8. 출력·복사물의 파기 책임자 **③ 2항 출력/복사물에는 정보통신서비스 제공자의 명칭 및 일련번호 표시** - 우편 발송, 고지서 발급 등, 개인단위 종이에 인쇄 경우는 일련번호를 표시 예외 **④ 제2항의 사전승인시 위법 여부 확인 법에 위배되는지 여부를 확인하고, 개인정보불법 유출에 따른 책임을 개인정보취급자에게 주지**
제9조 개인정보 표시 제한	**개인정보 마스킹 처리 원칙** 1. 성명 중 이름의 첫 번째 글자 이상 2. 생년월일 3. 전화번호 또는 휴대폰 전화번호의 국번 4. 주소의 읍·면·동 5. 인터넷주소는 버전 4의 경우 17~24비트 영역, 버전 6의 경우 113~128비트 영역

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

개인정보에 대한 안전성 확보 조치에 관한 세부 기준의 제시

개인정보보호법 제 29조, 개인정보 보호법 시행령 제 30조 제 3항 및 개인정보의 안전성 확보조치 기준 준수(안전행정부 고시 제 2011-43호, 2011/9/30 발령.시행)

구분	주요내용
내부관리계획 수립·시행(제3조)	• 보호책임자 지정 및 역할과 책임, 취급자 교육 등
접근권한 관리(제4조)	• 업무수행에 필요한 최소한의 범위로 차등 부여 • 접근권한 부여기록은 최소 3년간 보관
비밀번호 관리(제5조)	• 비밀번호 작성규칙 수립 의무화
접근통제시스템(제6조)	• 방화벽 등 접근통제시스템 설치 · 운영 • 업무용 컴퓨터만을 이용해 개인정보 처리시, 접근통제시스템 설치의무 면제 (O/S, 보안프로그램의 접근통제기능 이용)
암호화(제7조)	• 암호화 대상 : 고유식별정보, 비밀번호, 바이오정보 • 암호화 기준 -(전송시) 정보통신망 송수신 등의 경우 암호화 -(저장시) ① 비밀번호 및 바이오정보 암호화 (비밀번호 일방향 암호화) ② 고유식별정보는 인터넷구간, DMZ구간 저장시 암호화하고 내부망 저장시 위험도 분석에 따라 암호화 적용여부, 적용범위 결정
접속기록 보관(제8조)	• 최소 6개월 이상 보관
보안프로그램(제9조)	• 백신 등 보안프로그램 설치, 자동 또는 일1회 이상 업데이트
물리적 접근방지(제10조)	• 개인정보 물리적 보관장소에 대한 출입통제절차 등

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 3조 내부 관리 계획 수립/시행

내부관리계획에 포함할 사항

개인정보의 안전성 확보조치 기준(고시)(안) 제3조

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 제4조 내지 제10조에 따른 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 그 밖에 개인정보 보호를 위하여 필요한 사항

내부관리계획 수립 · 운영 방법

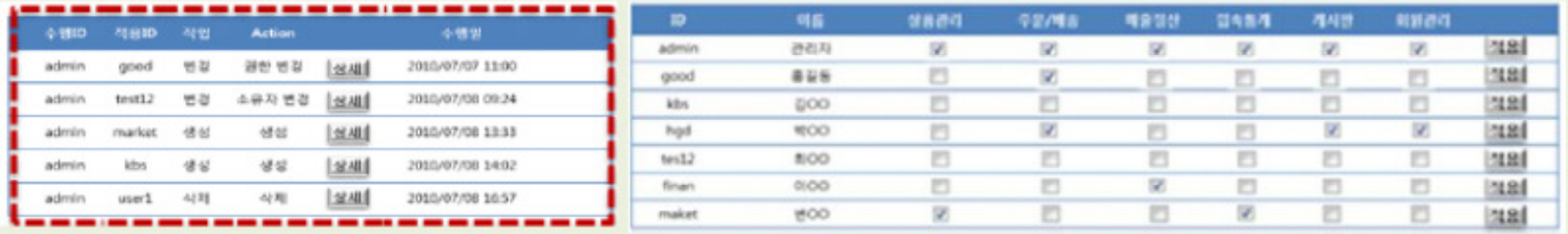
- 유출통지처리 및 피해구제 절차, 담당자 명시
- 취급자 PC에 고유식별정보가 저장되지 않도록 조치
- 저장이 필요한 경우 암호화하도록 수립하여 운영
- 정보주체 이외로부터 수집하는 개인정보 관리방안 수립
- 정보주체의 요구에 대한 수집출처 고지 절차 수립 및 처리 담당자를 지정하여 운영
- 개인정보 불필요 여부 점검, 파기 절차 • 방법 수립 및 관련 담당자를 지정하여 운영
- 개인정보를 처리하는 임직원, 파견 및 시간제 근로자, 수탁업체 관리 · 감독 절차, 방법, 담당자 역할, 점검항목 등 체계 수립 · 운영
- 내부관리계획, 개인정보처리방침에 보호책임자 공개

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 4조 접근권한 관리

<예시>



- ◆ 개인정보처리시스템 **접근권한**을 업무수행에 필요한 **최소한 범위**로 업무담당자별 **차등부여**
  - 예) 개인정보 보호책임자에게는 전체권한(읽기/쓰기/변경)을 부여하거나, 개인정보 취급자에게는 읽기 권한만 제공하는 등 권한에 차등
- ◆ 개인정보취급자 변경 시 지체 없이 개인정보처리시스템의 접근권한 변경 또는 말소
- ◆ 권한부여, 변경, 말소 내역 기록 및 최소 3년간 보관
- ◆ 개인정보취급자별 한개의 사용자 계정 발급 및 공유금지

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 5조 비밀번호 관리

◆ 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정할 수 있도록 비밀번호 작성 규칙 수립 및 적용

- 비밀번호 최소 길이
  - 최소 10자리 : 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상으로 구성
  - 최소 8자리 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성
- 추측하기 어려운 비밀번호
  - love, happy, 12345678,qwerty (X)
- 비밀번호의 주기적인 변경
  - 유효기간 설정 및 6개월마다 변경
- 2개 비밀번호 교대 사용 제한

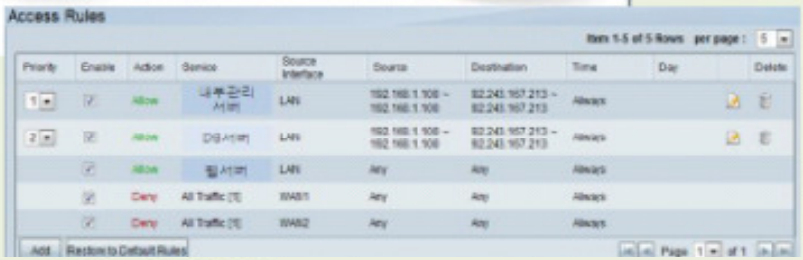
© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 6조 접근통제 시스템

◆ **접근통제(IP주소 등) 및 불법유출시도 탐지 기능 포함 시스템 설치 및 운영**

- 침입차단시스템(Firewall), 침입방지 시스템(IPS)
- 웹방화벽, Secure OS, 네트워크장비 ACL 기능 이용
- IDC, 클라우드 서비스에서 제공하는 보안서비스 활용



〈예시〉

☞www.privacy.go.kr 사이버 교육 동영상
- 개인정보 안전성 확보조치, 업무용 PC에서 개인정보보호조치 설정방법

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준
제 7조 암호화

◆ **안전한 암호 알고리즘으로 암호화 저장**

➢ 미국NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 기관 및 국내외 암호 연구기관에서 권고하는 알고리즘

민간기관

국내외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)의 권고를 중심으로 구성

분류	암호알고리즘
대칭키 암호 알고리즘	SEED ARIA-128/192/256 AES-128/192/256 Blowfish Camelia-128/192/256 MISTY1
공개키 암호 알고리즘	RSA KCDSA(전자서명용) RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/256/384/512 Whirlpool 등

공공기관

국가정보원(IT보안인증사무국) 검증대상 암호알고리즘 목록

분류		암호알고리즘
블록암호		ARIA , SEED
해쉬함수		SHA-224/256/384/512
메시지 인증코드	해쉬함수 기반	HMAC
	블록암호 기반	GCM(GMAC), CCM, CMAC
난수 발생기	해쉬함수/ HMAC기반	Hash_DRBG HMAC_DRBG
	블록암호 기반	CTR_DRBG
키 설정 방식		DH, ECDH
공개키 암호		RSAES
전자서명		RSA-PSS, KCDSA, ECDSA, EC-KCDSA

공통 권고 사항

❖ 대칭키 암호 알고리즘 : 키 길이 128 비트 미만 사용 X

❖ 일방향 암호 알고리즘 : 해쉬값 길이 112 비트 이하 사용 X

개인정보 암호화 조치 안내서(1210, 안행부) 기준 참고

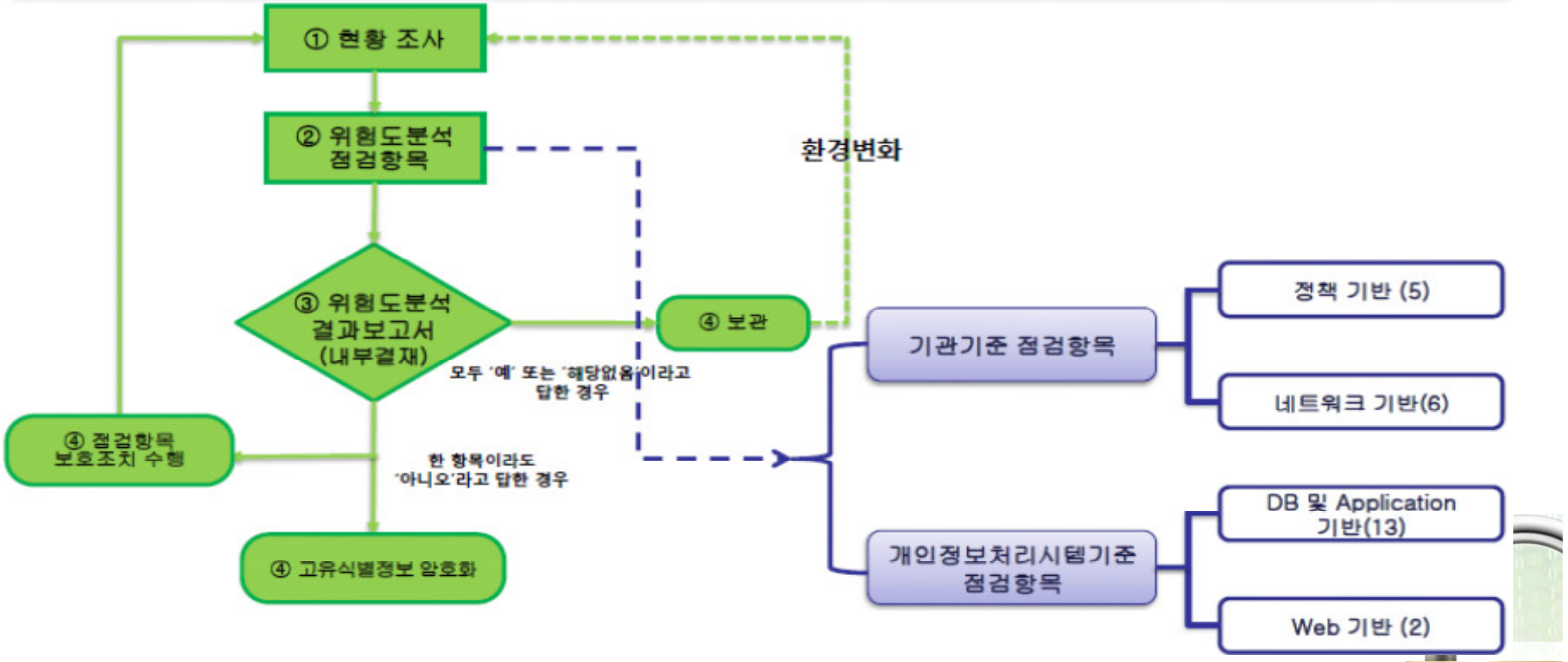
© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 7조 암호화

위험도 분석 절차 및 주요항목 구성

「위험도 분석」은 내부망에 고유식별정보를 암호화하지 않고 저장하는 경우 개인정보처리자가 이행하여야 할 최소한의 보호조치 기준으로 어느 하나의 항목이라도 '아니오' 에 해당하는 경우 암호화 대상이다.



© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 8조 접속기록 보관

◆ 개인정보취급자 **접속 기록** 최소 **6개월** 이상 **보관** · 관리

필수기록 항목	설명
ID	개인정보취급자 식별정보
날짜 및 시간	접속 일시
접속자 IP 주소	접속지 정보
수행업무	열람,수정,삭제,인쇄,입력 등

◆ 접속기록 위 · 변조, 도난, 분실되지 않도록 **안전하게 보관**

◆ (소상공인) 개인정보취급자가 1인(Root, Admin 등)인 경우 전자적 로그 남기지 않고 접속기록 수기 작성 후 상급자 승인 가능

<예시>

1 접속로그 기록

ID	접속자 IP	접속일시	수행업무
Admin	172.16.3.x	20XX/07/07 12:00	사용자 추가 작업
Admin	172.16.3.x	20XX/07/07 12:20	권한 추가 작업
상담1	172.16.4.x	20XX/07/07 14:00	사용자 수정
상담2	172.16.4.x	20XX/07/07 14:00	사용자 열람
개발자	172.16.5.x	20XX/07/07 19:00	게시판 삭제

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 9조 보안프로그램

- **백신** 소프트웨어 등의 보안 프로그램 설치·운영
- **자동 업데이트** 기능 사용 또는 일 1회 이상 업데이트
- 보안 업데이트 공지가 있는 경우, 즉시 업데이트 실시

<예시>

© 2013 IBM Corporation

개인정보의 안전성 확보조치 기준

제 10조 물리적접근방지

- 별도의 물리적 보관장소(전산실, 자료보관실)에 대한 출입통제 절차 수립 및 운영
- 개인정보 문서, 보조저장매체 등은 잠금장치가 있는 안전한 장소 보관

© 2013 IBM Corporation

개인정보 영향 평가

1. 개인정보 영향평가 개념

- 개인정보 영향평가 (PIA : Privacy Impact Assessment)

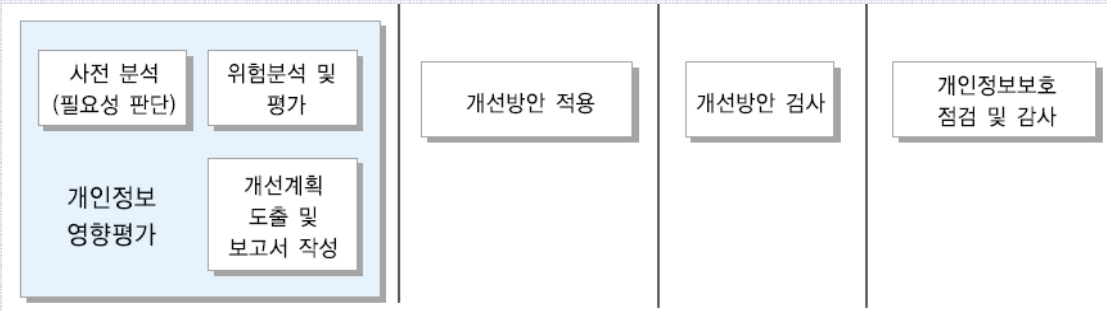
- 개인정보를 활용 하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보 시스템의 중대한 변경시 동 시스템의 구축·운영·변경 등이 프라이버시에 미치는 영향(impact)에 대하여 사전에 조사·예측·검토하여 개선 방안을 도출하는 체계적 절차

2. 개인정보 영향평가의 목적

- 개인정보 취급 정보화 사업 구축 완료전, 실제 사업 추진 상에 이를 반영함으로써 개인정보 침해 발생을 사전예방
- 사전적 평가 수행을 통해, 시스템 구축 이후 개인정보 보호조치 적용 대비 획기적 비용을 절감 유도

3. 개인정보 영향평가 대상 기업

- 사전분석 → 개인정보 관리 현황 분석 → 영향 평가 결과 정리의 단계를 거침
- 각 단계별 점검 체크리스트 및 평가 방법론에 근거하여 수행



© 2013 IBM Corporation

고객 성공 사례 > 해외 금융권

고객사: 뉴욕 증권 거래소
요건: SOX 규제 준수(Compliance) 및 내부 접속자 감사

- 1단계: 모든 특권 사용자의 활동 및 DB 변경 모니터링
- 2단계: 데이터 프라이버시에 중점

환경: 4개의 데이터 센터 , 100개 이상의 서버에 122개의 DB 인스턴스

- DBMS: Oracle, IBM DB2, Sybase, SQL Server,
- O/S: AIX, HP-UX, Solaris, Windows
- PeopleSoft plus 75 사내 애플리케이션

검토된 대안: Native 감사

- 과도한 퍼포먼스로 인해 비실용적; DB서버용량의 99%

Guardium 적용 결과: 현재 일일 백 만개 이상의 세션 감사(GRANTS, DDLs, etc.)

- DBA의 엑셀이나 공유 권한으로 DB 접근 감지
- SOX를 위한 리포트를 매일 자동으로 작성; DB 관리 팀과 정보보안 팀의 결제
- 티켓ID를 사용한 자동화된 변경 관리
- 2개의 외부 감사 통과

© 2013 IBM Corporation

고객 성공 사례 > 해외 금융권

고객사: Northwestern Mutual

요건: 자산 데이터베이스 감사와 모니터링

- SOX(Sarbanes-Oxley compliance)규제 대응을 위해 가디움 제품 도입

환경: 4개의 데이터 센터 , 100개 이상의 서버에 122개의 DB 인스턴스

- 15 collectors, plus 3 aggregators, central management
- 120 databases: DB2, Sybase, Oracle, SQL Server
- 51 database servers
- Implemented in corporate data center

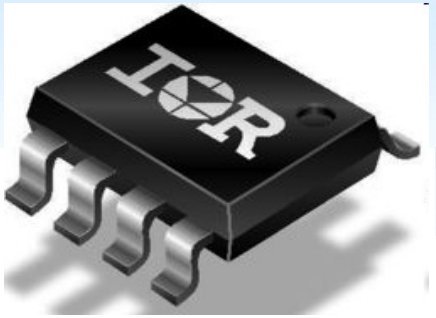
Guardium 적용 결과: SOX 규제 자동 대응 및 데이터 거버넌스를 위한 DB 보안 개선

- 내부/외부 데이터베이스 엑세스 감사
- 일단위 SOX감사 리포트 자동생성

© 2013 IBM Corporation

고객 성공 사례 > 해외 제조사

고객사: 전력 관리 기술 분야의 세계적인 선도업체 International Rectifier



환경 정보:

- 7개 SAP 인스턴스
- 30개 이상의 DB 인스턴스
- 사용 모듈: ECC/SCM/CRM/BW/GTS/PI/Solution Manager

고객 요건

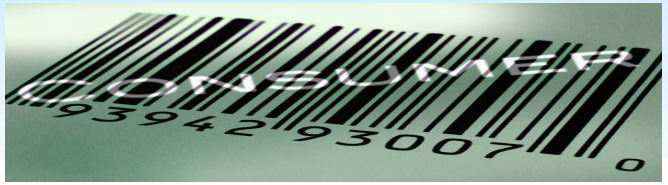
- SAP 암호화
- GRC, Risk Management and Compliance
- Bolton On Applications 지원
  - Sabrix, Tax Accounting Software
  - Business Objects, Business Reporting

주요 성공 요소

- 2일 이내 주장비 암호화 완료
- 운영 환경 변화없이 적용
- 고성능 암호화
- 중앙 관리
  - 키 배포
  - 다수 서버에 대한 정책 통합 관리

© 2013 IBM Corporation

고객 성공 사례 > 해외 유통사



고객사: Global Retail 고객
대상 시스템: ERP 시스템
고객 이슈:

- 기업 정보 거버넌스 관리 정책 부재
- 고객 민감 데이터 보호
- 법적 규제 준수

적용 솔루션: IBM InfoSphere Guardium Data Encryption
고객 가치:

- 운영 인프라 환경 변화없이 빠른 데이터 암호화 시스템 적용
- 비즈니스 요건 변경에 따른 암호화 요건에 따른 빠른 중앙 관제 정책
- 정보 거버넌스 관리 정책의 손쉬운 적용
- 보안 관제 솔루션과의 연동

© 2013 IBM Corporation

귀사의 개인정보는 안전하게 보호되고 있습니까?

구분	점검항목
정책 기반	1. 개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?
	2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?
	3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?
	4. DB 서버에 접속하는 장비에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립/운영하고 있습니까?
	5. DB서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시하고 있습니까?
네트워크 기반	6. 상시적으로 비인가 IP주소의 접근을 통제하고 있습니까?
	7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?
	8. 상시적으로 불법적인 해킹시도를 방지하고, 이에대해 모니터링을 실시하고 있습니까?
	9. 상시적으로 바이러스, 웜 등의 네트워크 유입을차단하고 있습니까?
	10. 주기적으로 네트워크 접속에 대한 로그를 관리하고,분석하고 있습니까?
	11. 네트워크 장비 및 정보보호시스템의 보안패치 발생시 지체없이 업데이트를 수행하고 있습니까?
DB/AP 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?
	13. DB서버내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동발생시 지체없이 DB 접근권한을 변경하고 있습니까?
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?
	20. DB접속자 및 개인정보취급자의 비밀번호 입력시 5회 이상 연속 입력오류가 발생한 경우 계정잠금 등 접근을 제한하고 있습니까?
	21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?
	22. DB 및 DB접속 어플리케이션 서버에서 보조기억 매체(USB 등) 사용시 관리자 승인 후 사용하고 있습니까?
	23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?
	24. HDD등 DB 저장매체의 불용처리시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
웹 기반	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?

© 2013 IBM Corporation

DB 보안 진단 워크샵 > 개요

DB 보안 진단 워크샵 Client Value Engagement (CVE) 는 DB 보안 성숙도 및 위험도에 대해 진단하고 보안 강화를 통해 얻어지는 비용 절감 효과에 대한 비즈니스 이윤을 정량화할 수 있도록 분석하는 워크샵으로서, 전략적인 파트너쉽 고객을 위해 무료로 제공됩니다.

이를 위해 기술 전문가와 함께 고객사의 운영 현황에 대해 살펴보고, 비즈니스 및 기술 요건에 대한 확인 및 제안 구성을 도출합니다.

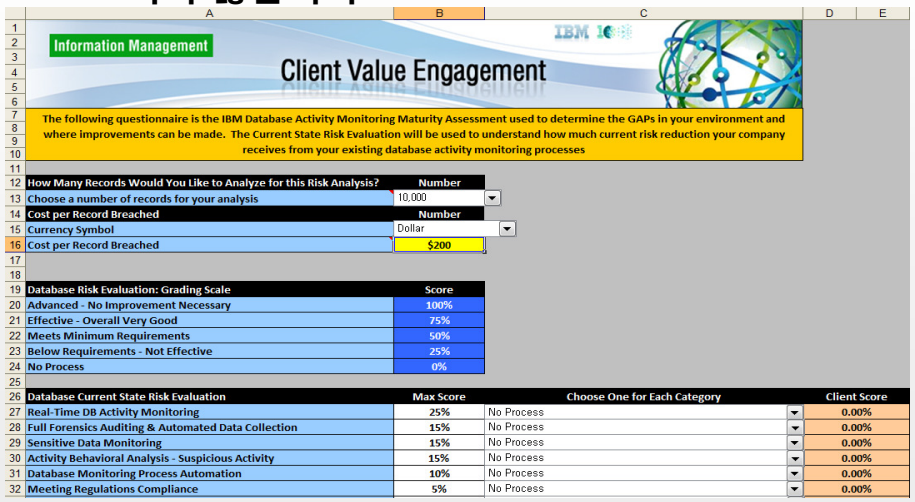
분석 영역

❑ **템플릿을 기반으로 성숙도 기반 진단 결과 및 비용절감을 위한 객관적인 수치를 제공합니다.**

- ✓ 보안 성숙도
- ✓ 위험도
- ✓ 비용 효과

진행 형식

❑ **정형회된 인터뷰지에 대한 답변: 2-4시간 이내의 담당자 인터뷰로 많은 시간이 소요되지 않습니다.**



Information Management

Client Value Engagement

The following questionnaire is the IBM Database Activity Monitoring Maturity Assessment used to determine the GAPs in your environment and where improvements can be made. The Current State Risk Evaluation will be used to understand how much current risk reduction your company receives from your existing database activity monitoring processes

How Many Records Would You Like to Analyze for this Risk Analysis?	Number
Choose a number of records for your analysis	10,000
Cost per Record Breached	Number
Currency Symbol	Dollar
Cost per Record Breached	$200

Database Risk Evaluation: Grading Scale	Score
Advanced - No Improvement Necessary	100%
Effective - Overall Very Good	75%
Meets Minimum Requirements	50%
Below Requirements - Not Effective	25%
No Process	0%

Database Current State Risk Evaluation	Max Score	Choose One for Each Category	Client Score
Real-Time DB Activity Monitoring	25%	No Process	0.00%
Full Forensics Auditing & Automated Data Collection	15%	No Process	0.00%
Sensitive Data Monitoring	15%	No Process	0.00%
Activity Behavioral Analysis - Suspicious Activity	15%	No Process	0.00%
Database Monitoring Process Automation	10%	No Process	0.00%
Meeting Regulations Compliance	5%	No Process	0.00%

© 2013 IBM Corporation

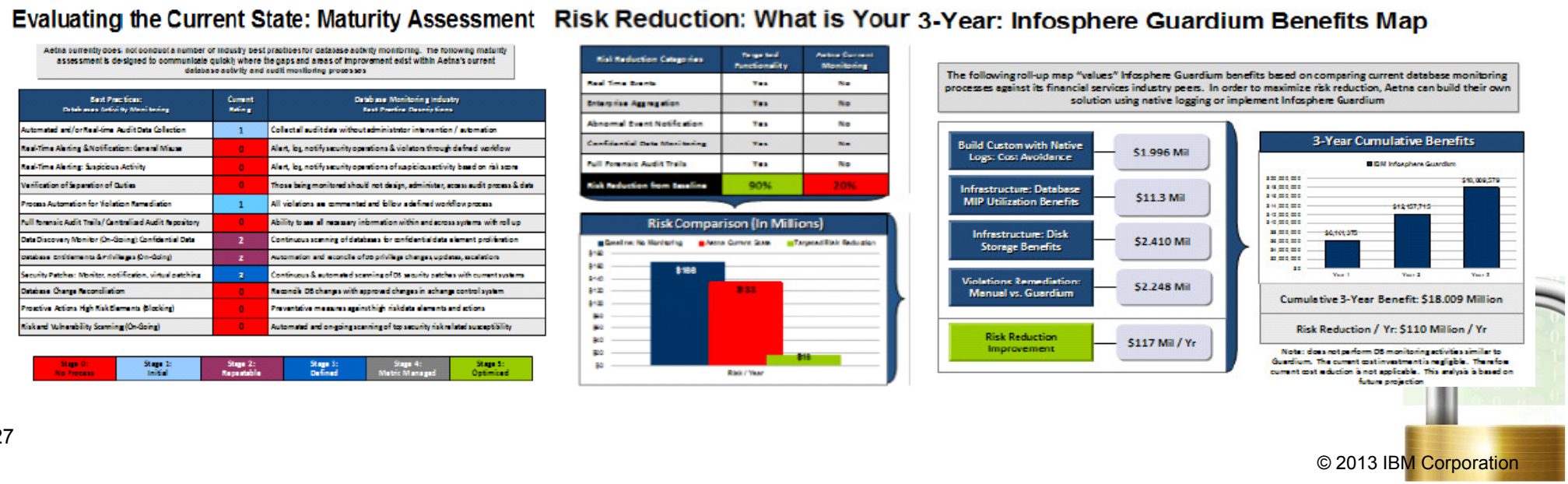
DB 보안 진단 워크샵 > 진행 및 보고서

진행 일정: 평균 2-3주 가량 소요됩니다.

진행 프로세스: DB 보안 진단 워크샵의 주요 진행 단계는 다음과 같습니다.

- Step 1: 주요 관리자와 기술적 업무적 이슈 및 관리 현황 파악
- Step 2: 감사 및 보안 프로세스, 애플리케이션 검토 및 성숙도 진단을 위한 인터뷰 진행
- Step 3: 제안 구성 도출
- Step 4: 담당자와 분석 내용 검토
- Step 5: 비용 절감 효과, 전략 및 제안 구성에 대한 최종 보고서 도출 및 보고

보고서 샘플



© 2013 IBM Corporation

감사합니다

© 2013 IBM Corporation