# 새로운 개인정보보호 규격 BS 10012:2009

By BSI Korea (SONG ILSEOB)

July 2, 2009

*raising standards worldwide™*

BSI Management Systems

# Agenda

- Data Protection Act 1998
- Data Protection Principles
- Overview of BS 10012
  - 1. Scope
  - 2. Terms and definitions
  - 3. Planning for a PIMS
  - 4. Implementing the PIMS
  - 5. Monitoring and reviewing the PIMS
  - 6. Improving the PIMS
- PDCA Cycle applied to the management of personal information

# Data Protection Act 1998

- 1998년 개정되어 2000년 3월에 발효된 영국의 개인정보보호법(Data Protection Act 1998)
- 정부기관이나 개인기업들이 보유하는 개인과 관련된 정보의 취득, 유지, 사용, 공개하는 등의 활동을 포함한 새로운 처리 규범의 수립을 위한 법률
- Information Commissioner(정보감독관)가 DPA를 규제하고 집행

※ Data Protection Act 1998 (http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)

※ Information Commissioner's Office (http://www.ico.gov.uk/)

*raising standards worldwide™*

BSI Management Systems

DPA는 영국의 개인정보보호법으로 Information Commissioner Office가 독립기관으로 존재하고 Information Commissioner(정보감독관)이 DPA를 규제하고 집행한다.

서문, 개인정보 소유자(즉, 개인)의 권리, 데이터 관리자에 의한 통보, 예외조항, 집행 등과 부칙으로 구성되어있다.

# Data Protection Principles

- Data Controller(데이터관리자)는 다음의 8개의 데이터 보호 원칙을 준수해야 한다.
  - fairly and lawfully processed;
  - processed for compatible and specified purposes;
  - adequate, relevant and not excessive;
  - accurate and up-to-date;
  - not kept for longer than is necessary;
  - processed in line with the rights afforded to individuals under the legislation, including the right of subject access;
  - kept secure;
  - not transferred to countries outside the European Economic Area (EEA)2 without adequate protection.

*raising standards worldwide™*

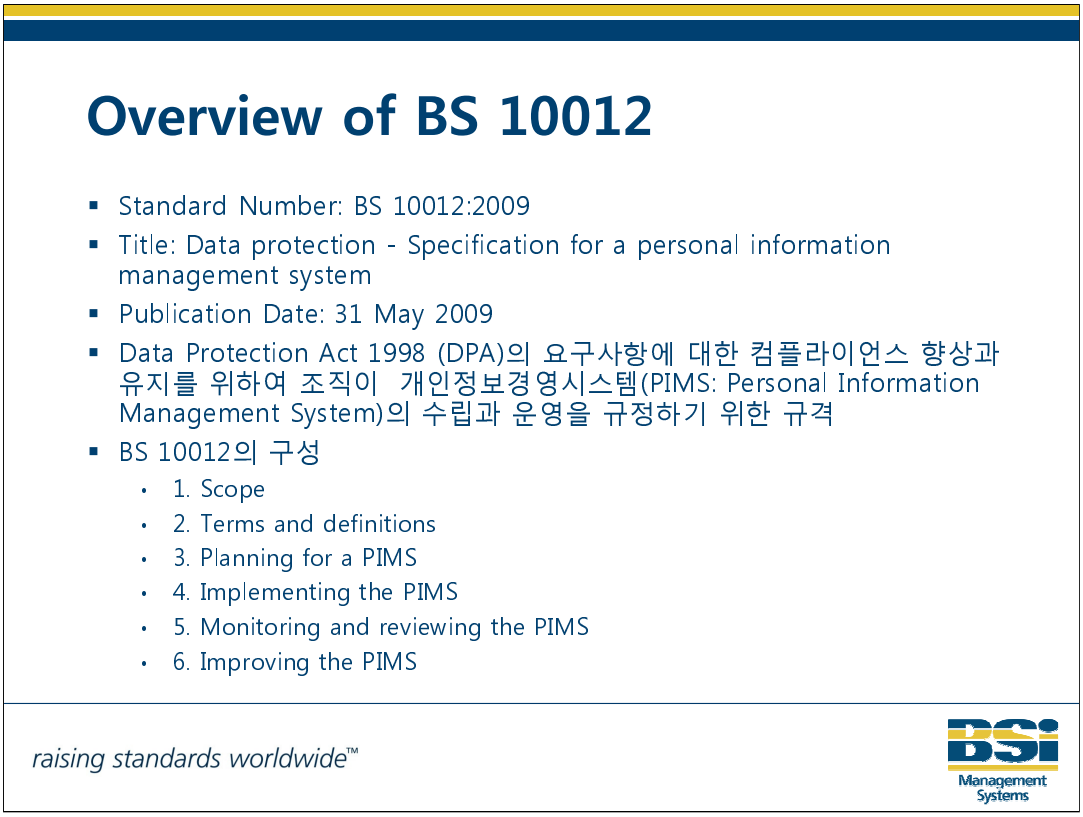
BSI Management Systems

Data Controller(데이터 관리자): 개인 데이터를 어떤 목적, 어떤 방법으로 처리할 것인지 또는 처리해야 하는지를 (단독이나 합작 또는 공동으로) 결정하는 사람 - DPA에서 정의하고 있으며, BS 10012에서도 서문에 언급하고 있음

Data Protection Principle

1. 개인 데이터는 공정하고 적법하게 처리되어야 한다.
2. 개인 데이터는 하나 이상의 명시된 적법한 목적으로만 취득되어야 하며, 그와 같은 목적과 부합되지 않는 방식으로 처리되어서는 안 된다.
3. 개인 데이터는 처리되어야 하는 목적에 대하여 적합해야 하며, 그 목적과 관련이 있어야 하며, 이를 넘어서서는 안 된다.
4. 개인 데이터는 정확하고 가능한 한 최신의 상태로 보존되어야 한다.
5. 개인 데이터는 그 목적상 필요한 기간 이후에 보존되어서는 안 된다.
6. 개인 데이터는 본 법령에 따른 데이터 주체의 권리와 일치하게 처리되어야 한다.
7. 개인 데이터의 무자격 또는 불법적 처리와 사고로 인한 손실, 파괴나 훼손에 대해서는 적절하고 조직적인 조치가 취해져야 한다.
8. 유럽 경제 구역 밖의 나라나 지역에서 개인 데이터의 처리에 데이터 주체의 권리와 자유를 적절한 수준으로 보장하지 않는다면 개인 데이터는 그 국가나 지역으로 이동시킬 수 없다.

8원칙이 적용되지 않는 경우(개인이 동의한 경우, 계약상의 조건, 공익을 위해 필요할 때, 개인의 중요한 이익을 보호할 때 등)




BS 10012, was developed by a panel of experts including representatives from industry, government, academia and consumer groups.

3개월 동안 DPC(draft for public comments)가 진행되었으며, 지난 5월 31에 규격 발표

규격이 DPA를 기반으로 하고 있는 관계로, 국내에서는 규격에서 요구하는 많은 부분을 충족시키기 어렵다.

하지만 본 규격에서 제시한 Framework과 요구사항이 DPA 컴플라이언스 준수를 위해 구성되었으나, 국내에서도 활용이 가능할 것으로 판단된다.

일부 용어가 DPA와는 다르게 정의되어 있는 부분도 있다. 예를 들어 DPA에서는 개인정보를 'Personal Data'로 표현하고 있으나, BS 10012에서는 'Personal Information'으로 표기한다.

# 1. Scope

- 개인정보관리를 위한 기본 체계 및 신뢰를 제공하고, DPA 컴플라이언스에 대한 평가를 위해 내부 및 외부 평가가 효과적으로 이루어질 수 있도록 함
- 조직 내 PIMS에 대한 수립, 책임, 구현 및 유지를 위함
- 공공 및 민간 부문 등 조직 규모에 제한 없이 모든 조직에 적용 가능한 규격
- "Plan-Do-check-Act"(PDCA) cycle을 적용
- DPA외 법규(예: Freedom of Information Act 2000 - 영국정보공개법)참조

*raising standards worldwide™*

BSI Management Systems

본 규격의 적용 범위는 민간, 공공 등에 제한이 없으며, 조직의 규모에도 제한이 없다.

ISO 27001처럼 PDCA Cycle이 적용되어 있으며, BS 10012에는 명시되어 있지 않으나, 'DPA외의 법규(예: 영국정보공개법 등)에 대해서도 반드시 확인해야 한다'라고 되어 있다.

## 2. Terms and Definitions

- Personal information management system
  - 전반적인 경영 시스템의 일부로 개인정보 관리 체계의 구현, 운영, 모니터링, 검토, 유지 및 개선을 위한 시스템 (개인정보경영시스템)
- Personal Information (DPA 정의)
  - 신원을 확인할 수 있는 실제적인 사람과 관련된 데이터
  - Sensitive personal information: 개인의 민족 또는 인종적 출신 사항, 정치적 견해, 종교적 믿음(또는 유사한 성격의 믿음), 노동조합의 가입 여부, 정신적, 육체적 건강 상태, 성생활, 법률 위반 사실 또는 추정된 위반 사실, 법률 위반이나 추정된 위반에 대해 소송 여부, 해당 소송의 처리재판 결과 받은 판결

*raising standards worldwide™*

BSI Management Systems

PIMS: part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves the management of personal information

Personal Information

- 해당 데이터

- 데이터 관리자가 보유하고 있거나 앞으로 관리할 가능성이 많은 기타 데이터나 정보

- 해당 개인에 대해 표현된 의견이나 데이터 관리자의 모든 지시사항, 그 사람과 관계 있는 모든 타인에 관한 의견도 포함

Sensitive personal information (2.1.12)에 정의되어 있으며., 위험관리 등의 요구사항에서 민감한 개인정보에 대한 관리는 보다 중요하게 관리하도록 규정하고 있다.

This British standard uses the term “personal information” in place of the term “personal data”.

Organization(조직)은 정보를 처리하는 법적 단체로 정의하고 있다. (Natural persons, sole traders, companies, partnerships, bodies corporate, public sector bodies, voluntary associations and charities)

# 2. Terms and Definitions

- Processing
  - 개인 정보의 취득, 기록, 보존하거나 해당 정보나 데이터에 대한 작업 또는 일련의 과정을 이행함
- Data controller
  - 데이터 관리자: 개인 데이터를 어떤 목적, 어떤 방법으로 처리할 것인지 또는 처리해야 하는지를 (단독, 합작 또는 공동)결정하는 사람
- Data processor
  - 데이터 처리자: 개인 데이터에 대해서 데이터 관리자를 대신하여 데이터를 처리하는 모든 사람(데이터 관리자 제외)
- Individual (Data subject)
  - 개인 데이터의 주체가 되는 개인을 의미



Data Controller, Data Processor, Data Subject는 BS 10012의 2. Terms and Definitions에서는 정의하지 않고 있다.

Workers (employees, temporary staff, contractors, volunteers, consultants)

# 3. Planning for a PIMS

- 조직은 다음 사항에 따라서 문서화된 PIMS의 개발, 구현, 유지 및 지속적인 개선을 해야 한다.
- **Scope and objectives of the PIMS**
  - 개인정보 관리를 위한 요구사항들
  - 조직의 목표와 의무 사항들
  - 조직의 수용 가능한 위험 수준
  - 법규, 규제, 계약상 의무 등
  - 주요 이해 관계자의 요구사항
- **Personal information management policy**
  - Senior Management Team (대표이사, 이사회, 부서장, 파트너社 등)을 구성함으로써 PIMS Policy(DPA 준수, 명확한 Framework 확립, 지원 활동 및 의지 표명 등이 포함된)수립과 운영을 확인

*raising standards worldwide™*

BSI Management Systems

다음을 고려하여 PIMS의 Scope과 개인 정보 관리 목적을 정의한다.

- 개인정보 관리를 위한 요구사항들 (requirements for the management of personal information;)
- 조직의 목표와 의무 사항들 (organizational objectives and obligations;)
- 조직의 수용 가능한 위험 수준 (organization's acceptable level of risk;)
- 법규, 규제, 계약상 의무 등 (statutory, regulatory and contractual duties; and)
- 주요 이해 관계자의 요구사항 (interests of its key stakeholders.)

특히 주요 이해관계자에 대한 부분이 Senior management team에 포함되어 있음을 주목해야 한다. (협력사, 관계사, 자영업자 등)

개인 정보를 공유하는 관련 조직(기업)과의 관계를 PIMS에 반영하고 정책을 수립할 필요가 있다.

# 3. Planning for a PIMS

- Policy Content: DPA 및 관련 규제의 준수와 조직의 commitment와 함께, 다음의 사항들을 포함한 Policy를 수립해야 한다.
  - 엄격하게 정의된 장소에서만 개인 정보 관리(처리) 업무 수행
  - 업무상 필요로 하는 최소한의 개인 정보 수집
  - 수집된 개인 정보가 누구에 의해 어떻게 사용되는지에 대해서 개개인에게 명확한 정보를 제공
  - 관련되고 목적에 적합한 개인 정보만을 처리
  - 필요한 장소에 개인정보는 정확하고 최신의 정보로 유지
  - 적법한 범위 내에서 조직의 목적 또는 법규 요구사항의 범위 내에서만 개인정보를 보유



Policy는 a) 조직 전체, 또는 b) 조직의 일부 정의된 부분을 커버해야 한다.

적법하고 공정한 개인정보 관리가 이루어질 수 있도록 Policy를 수립하는 것이 필요하다.

Policy에 대한 부분이 실제 PIMS 구현에 반영되는 부분이기 때문에 4. Implementing the PIMS 에서 자세한 내용으로 확인할 수 있다.

# 3. Planning for a PIMS

- Individual access의 권한을 포함하여 본인의 개인정보에 대한 권한을 가지고 있는 개인 권리에 대한 존중 (Subject access request)
- Personal information management Policy가 운영되고 유지될 수 있도록 PIMS를 개발하고 구현
- 모든 개인 정보는 안전하게 보관
- DPA에 의해 허용 가능한 예외 사항들
- 내부 및 외부의 이해관계자 들이 조직 PIMS의 거버넌스 구조에 관련된 정도를 파악
- 특별 권한 (책임 및 의무에 대한 사항)이 부여된 개인을 식별
- 적절한 보호 상태에서만 EEA(European Economic Area) 외부로 개인정보 전송

*raising standards worldwide™*

BSI Management Systems

Subject access request(DPA에서 사용하는 용어)는 데이터 관리자로부터 데이터 주체인 개인 데이터가 데이터 관리자에 의해 처리되고 있는지, 또는 데이터 관리자를 대신하여 처리되고 있는지 보고 받을 수 있는 권리

DPA - 개인정보를 자동화된 도구로 다룰 때, 개인에 대한 사항을 평가하기 다루는 경우(예: 업무 수행 능력, 신용, 신뢰성이나 품행 등)에 어떤 부분에서 그 사람에게 중대한 영향을 미치는 결정이 관계되어 있는지에 대한 논리 근거를 제공해야 한다.

국내에서는 해당 사항이 없는(그러나 요구사항을 일반적인 부분으로 해석을 해보면 적용 가능한) 부분이 EEA 외부로 개인정보가 전송되는 부분이다.

# 3. Planning for a PIMS

- **Responsibility and accountability**
  - A member of the senior management team
    - PIM Policy 승인
    - PIMS의 개발과 구현
    - PIM Policy와 함께 관련된 컴플라이언스에 대한 보안과 위험 관리
  - 조직의 컴플라이언스에 대한 책임을 갖는 숙련되고 경험이 많은 담당자 지정
  - 모든 직원(worker)은 PIM Policy를 준수해야 한다.
- **Provision of Resources**
  - 조직은 PIMS의 수립, 구현, 운영, 유지를 위해 필요한 모든 자원에 대하여 결정하고 제공해야 한다.



Responsibility and accountability

- Senior management team의 멤버는 DPA 및 기타 관련 법규와 규제에 대한 컴플라이언스 이행을 위하여 개인 정보 관리를 위한 책임을 갖는다.

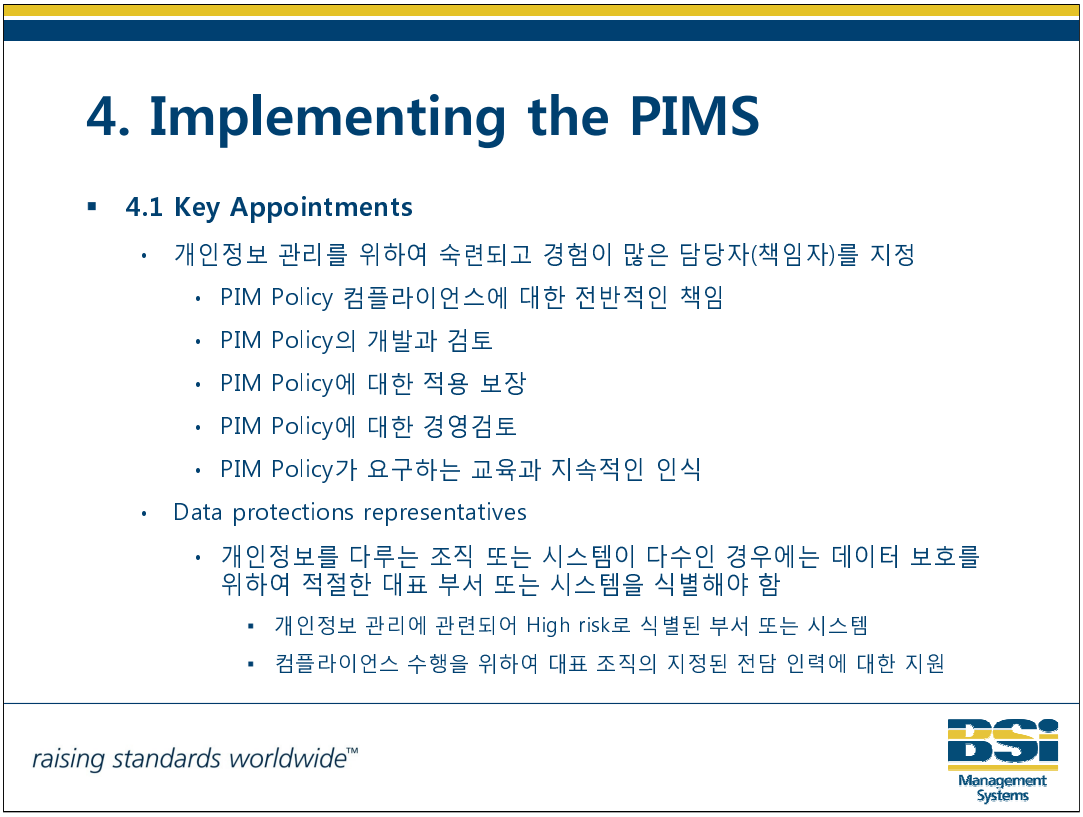
- 조직의 컴플라이언스에 대한 책임을 갖는 숙련되고 경험이 많은 담당자 지정 (Day-to-day)

# 3. Planning for a PIMS

- **Embedding the PIMS in the organization's culture**
  - 개인 정보 관리가 조직의 핵심가치의 일부로써, 그리고 효과적인 관리를 위하여 조직은 다음을 수행해야 한다.
    - 모든 임직원을 대상으로 지속적인 교육, 인식전환 프로그램을 통하여 PIMS의 인식 강화
    - PIMS 인식 전환 활동에 대한 효과성 평가 프로세스 마련
    - 임직원간의 PIM의 목적, PIM Policy 이행, PIM Policy의 지속적인 개선의 중요성 공유
    - 모든 임직원들이 조직의 PIM 목적 달성을 위하여 노력할 수 있도록 함



PIMS 인식 전환 활동에 대한 효과성 평가 프로세스가 마련되어야 한다. (교육 후 평가, 설문, 교육 이후에 수행된 감사 결과와 시정 조치 활동 등)




4. Implementing the PIMS가 본 규격의 상당 부분을 차지하고 있다.

개인정보 책임자
- 공정한 관리와 커뮤니케이션에 대한 공지
- Subject access 요청 처리
- 개인정보 수집과 처리
- 심사 요청
- 불만사항 처리
- 아웃소싱 또는 오프쇼어링(Off-shoring)
- 조직 내의 위험관리 및 보안 이슈 책임자와의 연락
- DPA 문제에 대한 안내와 전문가적인 조언 지원
- 개인정보처리에 적절한 다양한 예외 사항들에 대한 판단과 적용
- 데이터가 오프사이트에 위치한 경우의 보안 이슈를 포함한 데이터 공유 프로젝트(Data Sharing Project) 등과 관련된 -사항에 대한 지원
- DPA 관련한 적절한 가이드와 개정된 법률 사항에 대한 조직의 이용 보장
- DPA에서 요구되는 사항에 대하여 정보보호 감독관(Information Commissioner)에게 보고 사항 관리 및 제출 등
- 적절한 사례로서 개인 정보의 처리는 조직에 적용되는 모든 의무 또는 권고 sectoral code에 명시된 관련 코드

(implementing as appropriate the practices related to the processing of personal information outlined in any mandatory or advisory sectoral codes which apply to the organization.)

# 4. Implementing the PIMS

- **4.2 Identifying and recording uses of personal information**
  - 개인정보의 카테고리 별 목록 관리
    - 목록에는 각 개인정보 카테고리 별 사용 목적을 문서화
    - 조직 전반의 프로세스 내의 개인정보 흐름을 문서화
    - High Risk로 분류된 정보에 대하여 식별하고 문서화
      - DPA Section2에서 정의된 민감한 개인 정보
      - 개인 은행 계좌 및 다른 금융 정보
      - National identifiers

*raising standards worldwide™*

BSI Management Systems

문서화하여 관리하도록 요구하고 있는 부분이 있는데, 개인정보의 카테고리 별(위험 등급 별 등으로 분류) 목록 관리 등이다.

High Risk로 분류된 개인정보는 다음을 포함한다.
- DPA Section2에서 정의된 민감한 개인 정보
- 개인 은행 계좌 및 다른 금융 정보
- National identifiers (주민등록번호, 영국의 경우 National insurance numbers)
- 상처 입기 쉬운 성인 및 어린이에 관련된 정보
- 상세한 개인 프로필
- 다량의 개인정보 또는 민감한 개인 정보
- 어떤 부정적인 영향을 미칠 수 있는 민감한 개인 협상 내용

# 4. Implementing the PIMS

- **4.3 Training and awareness**
  - 개인정보 처리 및 책임, 그리고 보안 요구사항에 대한 교육이 이행되어야 하며, 이행 여부를 확인할 수 있어야 함
- **4.4 Risk assessment**
  - 데이터 처리자의 업무 프로세스를 포함하여, 개인정보 처리에 관련된 사항(Data subjects)에 대한 위험 수준을 평가할 수 있는 체계 마련
  - 식별된 위험을 감소시키기 위한 위험 관리 요구
  - **ICO의 가이드** (http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx)

*raising standards worldwide™*

BSI Management Systems

교육과 인식

-교육 대상자는 모든 임직원, 계약직, 임시직, 계약자, 자원봉사자, 컨설턴트 등이 포함됨

단순히 개인정보 자체 뿐만 아니라, 처리에 관련된 프로세스도 위험평가를 수행하고, 이에 따른 위험을 감속시키기 위한 활동을 수행해야 한다. (자체 위험평가 방법론 참조 또는 ICO의 가이드 참조)

참고: BS 10012에는 Data processor, Data subject에 대한 정의가 포함되어 있지 않다.

# 4. Implementing the PIMS

- **4.5 Keeping PIMS up-to-date**
  - DPA 및 기타 관련된 법규, 규정에 대한 준수 여부와 Best practice를 통한 개선 활동을 위한 점검을 지속적으로 수행한다.
    - 조직의 요구사항 또는 기술적 사항에 대한 변경이 발생되는 경우에는 PIMS 검토가 포함되어야 한다.
- **4.6 Notification**
  - DPA 요구사항에 따른 Notification 절차



4.6 Notification에 대한 부분: DPA에서는 Information Commissioner(정보감독관)에게 매년 개인정보 처리에 대한 사항을 보고하도록 되어 있음

# 4. Implementing the PIMS

- 4.7 Fair and lawful processing
  - 개인정보는 명확하게 식별되고 법적 기준에 따라 처리되어야 한다.
  - 4.7.1 Collection and processing of personal information
    - 정의된 장소에서 DPA를 준수하여 개인정보를 처리
    - 조직의 요구사항에 따라 필요한 부분만을 처리
    - Privacy Notice 또는 Online privacy statement 제공
    - 새로운 개인정보 수집방법을 적용하는 경우, 적절한 담당자(qualified and experienced person)에 의해 관련 법규가 준수되고 있는지, 검토되고 승인되어야 함

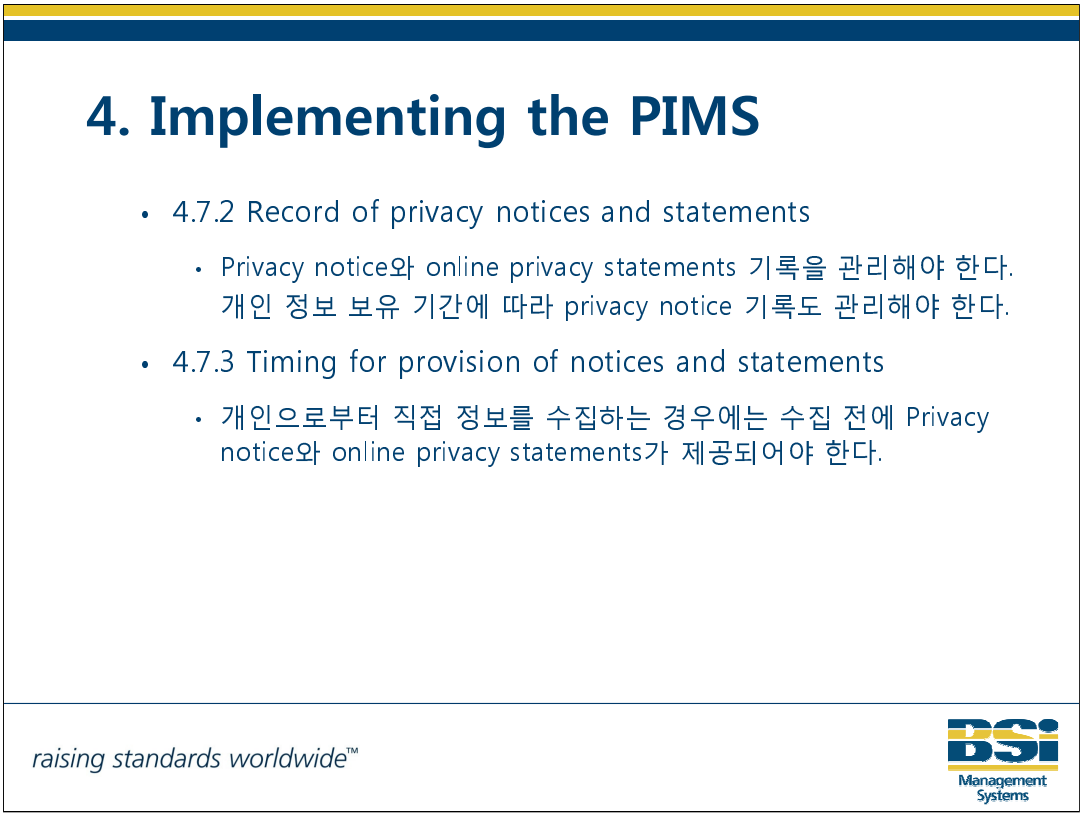
*raising standards worldwide™*

BSI Management Systems

즉, 개인정보는 공정하고 적법하게 처리됨을 보장되고 있음을 Privacy Notice와 Online privacy statement로 제공해야 한다. 국내의 '개인정보취급방침'과 유사하다.

Fair processing notice (FPN 공정처리통지) 제공

- 데이터관리자 명시
- 개인 정보 사용 목적
- 제3자에게 공개할 정보
- 개인정보에 대한 개인 권리
- 개인정보 불만 처리 조직 연락처
- **FPN은 찾기 쉬운 곳에 게시하고, 이해하기 쉽도록 작성을 해야 함**




개인정보 보유기간에 준하여 관련된 privacy notice 등의 기록도 관리해야 한다.

4.7.2 Record of privacy notices and statements

- FPN, 쿠키 사용에 대한 안내, 보유 목적과 보유 기간 (이 부분은 DPC에서는 있었으나, 발행 시에는 제외되었음)

# 4. Implementing the PIMS

- 4.7.4 Accessibility of privacy notices and statements
  - Privacy notice와 online privacy statement는 쉽게 찾아볼 수 있고, 이해하기 쉽게 작성을 해야 한다.
- 4.7.6 Third parties
  - 제3자에 의해 개인정보가 수집되는 경우에 대하여 공정하고 적법하게 수집되었음을 보장하는 절차가 PIMS에 포함되어야 한다.



어린이 또는 학습장애를 가진 사람들도 쉽게 이해하고, 찾아볼 수 있도록 작성해야 한다.

# 4. Implementing the PIMS

- **4.8 Processing personal information for specified purposes**
  - 4.8.1 Grounds for processing
    - 목적을 벗어나 수집된 개인정보 처리는 금지
    - 관련 법규, 규정 또는 계약사항을 벗어난 개인 정보 처리 활동은 할 수 없음
  - 4.8.2 Consent to new purposes
    - 관련 법규에서의 예외사항인 경우를 제외하고, 새로운 목적에 따른 개인정보 처리가 필요한 경우에는 개인의 명시적인 동의를 받아야 한다.



기존의 목적이 아닌 새로운 목적에  따라 개인정보 처리가 필요한 경우에는 개인의 명시적인 동의를 받아야 한다.

# 4. Implementing the PIMS

- 4.8.3 Data Sharing
  - 새로운 제3자와 개인정보 공유 시에는 관련기관에 보고하고, FPN에 포함하여 공지
  - 또는 개인정보 공유를 위한 법적 근거 확인, 개인의 동의
  - 개인 동의 없이 개인정보 공유가 가능한 경우에는 이에 해당하는 법적 요구사항을 위한 증적을 기록, 관리
  - 제3자의 요구(법적 의무 사항 등)로 개인정보를 공유해야 하는 경우에는 개인정보 공유에 대한 규약과 통제에 대한 사항을 문서화하여 관리
- 4.8.4 Data matching
  - 여러 목적으로 수집된 개인정보가 확장된 형태의 개인 정보로 새로이 생성된다면, 이러한 정보에 대하여 공지하고 해당하는 목적에만 이용해야 한다.

*raising standards worldwide™*

BSI Management Systems

FPN(Fair processing notice 공정처리통지 = privacy notice 등)

예외사항에 대한 근거(법적 요구사항 등)를 증적으로 기록 관리해야 한다.

기존 개인정보가 확장된 형태의 새로운 개인 정보로 생성되는 경우에 대해서도 명확한 관리 기준(사용목적 등)을 수립해야 한다.

# 4. Implementing the PIMS

- **4.9 Adequate, relevant and not excessive**
  - 수집된 개인 정보가 조직의 목적에 적절한지에 대한 적절성을 보장해야 한다.
  - 개인정보 처리를 포함하여 관련 시스템과 프로세스가 목적에 부합하는지를 정기적으로 검토해야 한다.
  - 합법적인 비즈니스 목적을 따르기 위해 최소한의 개인정보만을 처리한다.
  - 목적을 벗어나거나 관련이 없는 부가적인 개인 정보는 처리할 수 없다. (해당 정보에 대한 별도의 조항이 언급되어 있거나 개인의 동의가 있다면 가능)
  - 개인정보 처리를 포함하는 새로운 시스템과 프로세스가 위의 사항을 충족하는지 검토해야 한다.
  - 조직의 목적을 위해 관련이 없거나, 추가 정보를 필요로 한 경우(예: 익명의 데이터에 대한 사용 등)에는 해당 사항에 대한 절차를 마련해야 한다.



적절하고 관련된 정보만을 수집하고 처리해야 한다는 요구사항으로, 목적에 부합하는지 그리고 그러한 목적을 달성하기 위하여 이용하는 관리적, 기술적 요인들도 타당한지를 보장할 수 있도록 해야 한다.

# 4. Implementing the PIMS

- **4.10 Accuracy**
  - 개인정보는 필요한 곳에서 최신의 정보로 정확해야 한다.
  - 처리되고 있는 개인정보의 정확성과 무결성을 유지해야 한다.
  - 개인이 자신의 개인정보가 정확하게 유지될 수 있도록 필요한 경우 수정될 수 있도록 해야 한다.
  - 의심되는 부정확함이 실제로 부정확한지를 확인하는 절차가 마련되어야 한다.
  - 중요한 결정을 위하여 최신의 개인 정보를 사용해야 하며, 개인정보의 정확성과 최신성 여부를 직원이 알 수 있어야 한다.



참고: 이력에 대한 기록(historical record)는 수정될 수 없다.

제3자에게 전달되는 정보가 정확하지 않거나, 또는 최신의 정보가 아닌 경우, 이에 대한 사항(정확하지 않고, 최신의 정보가 아님)을 알려줘야 한다.

제3자가 요구하는 경우에는 수정된 정보를 전달해야 한다.

# 4. Implementing the PIMS

- **4.11 Retention and disposal**
  - 개인 정보는 필요 이상 보유해서는 안 된다.
  - 보유 기간을 명시 (최소 보유 기간)
  - 보유 기간에 대하여 명분과 근거를 명확하게 해야 한다.
  - 명시된 최소 보유 기간을 넘어서는 기간 동안 개인 정보를 보유해야 하는 경우(예: 이력 또는 연구 목적), 이에 대한 적용을 정당화한 문서 작성
  - 파기 절차는 파기 승인 프로세스와 함께 개인정보의 민감성에 대한 보안 수준, 조직의 정보보호 위험 평가에 따라 정의되어야 한다.

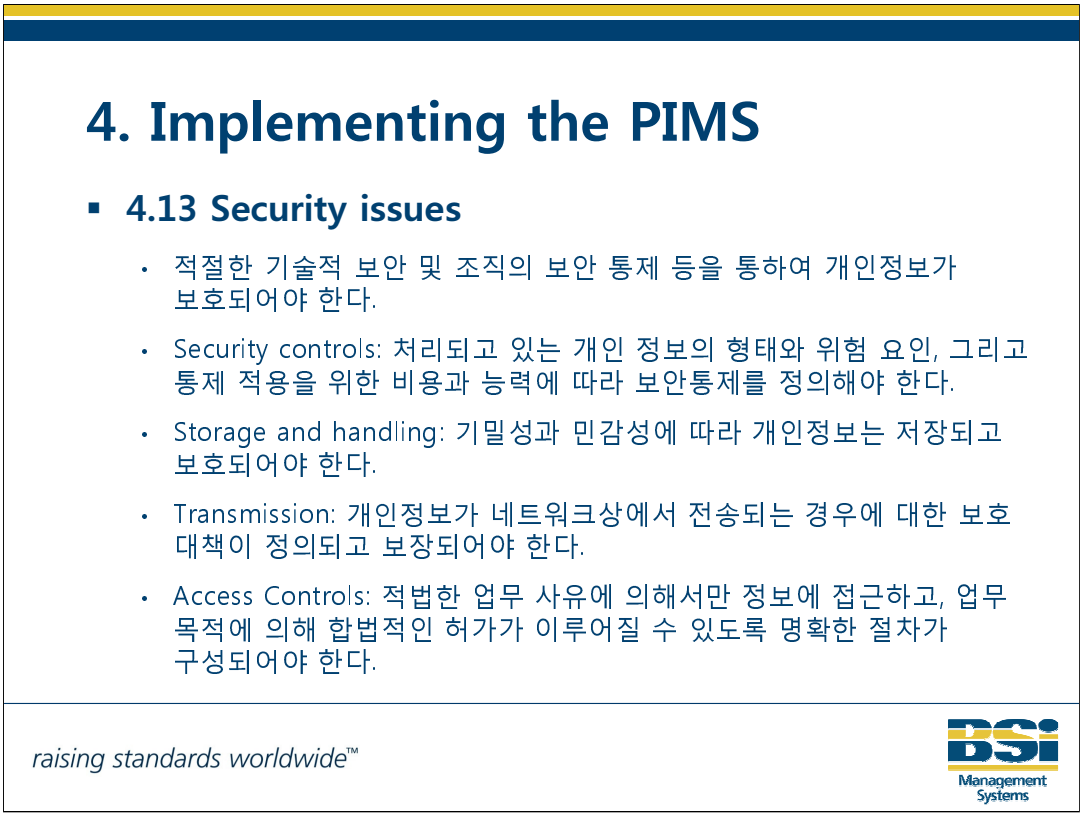
# 4. Implementing the PIMS

- **4.12 Individuals' rights**
  - 개인 정보와 관련하여 개인의 권리가 존중되고, 요청 사항이 법적 제한 시간 이내에 처리되는 등의 모든 법적 권리를 행사할 수 있도록 하는 절차가 포함되어야 한다.
  - 개인정보의 올바른 처리 여부에 대한 고객의 불만사항을 확인할 수 있는 컴플레인 절차가 포함되어야 한다.



Subject = Individual

개인정보 소유자의 권리에 대한 부분으로 개인의 권리가 존중되고, 요청사항이 적절하게 처리될 수 있도록 절차를 구성해야 한다.




4.13.1 Security Controls에 해당되는 부분으로 ISO 27001을 언급하고 있으며, 조직이 필요한 경우에는 ISO 27001을 인증 받음으로써 국제 표준을 따르고 있음을 보여줄 수 있다.

4.13.2 Storage and handling

특히 이동형 저장장치 또는 노트북 등에 대해서는 특별한 주의 필요하다고 이야기 하고 있다.

4.13.4 Access Controls

업무상, 역할 상 필요로 한 정보만을 액세스할 수 있도록 해야 한다.

High risk의 개인정보인 경우에는 해당 정보의 민감성을 고려한 접근 통제를 적용해야 한다.

# 4. Implementing the PIMS

- 접근 통제는 정보보호 위험평가에 따라 모니터링 되고 평가되어야 한다.
- Security assessments: 정보보호 전문가에 의한 정기적인 보안평가 실시(현재 보안통제 Gap분석과 개선 사항 도출)
- Notification of security incidents: 보안사고에 대한 관리와 보안사고로 인해 발생한 피해를 감소시키기 위한 절차가 구성되어야 한다.
  - 사고 발생 원인, 개선 조치 활동 등에 대한 문서화 기록 관리
  - 알림(또는 보고) 대상에 대한 결정
  - 알림(보고) 기록의 유지
- Contingency plan: 보안 사고 발생 시 이에 대한 연속성 계획이 PIMS에 포함되어야 한다.

*raising standards worldwide™*

BSI Management Systems

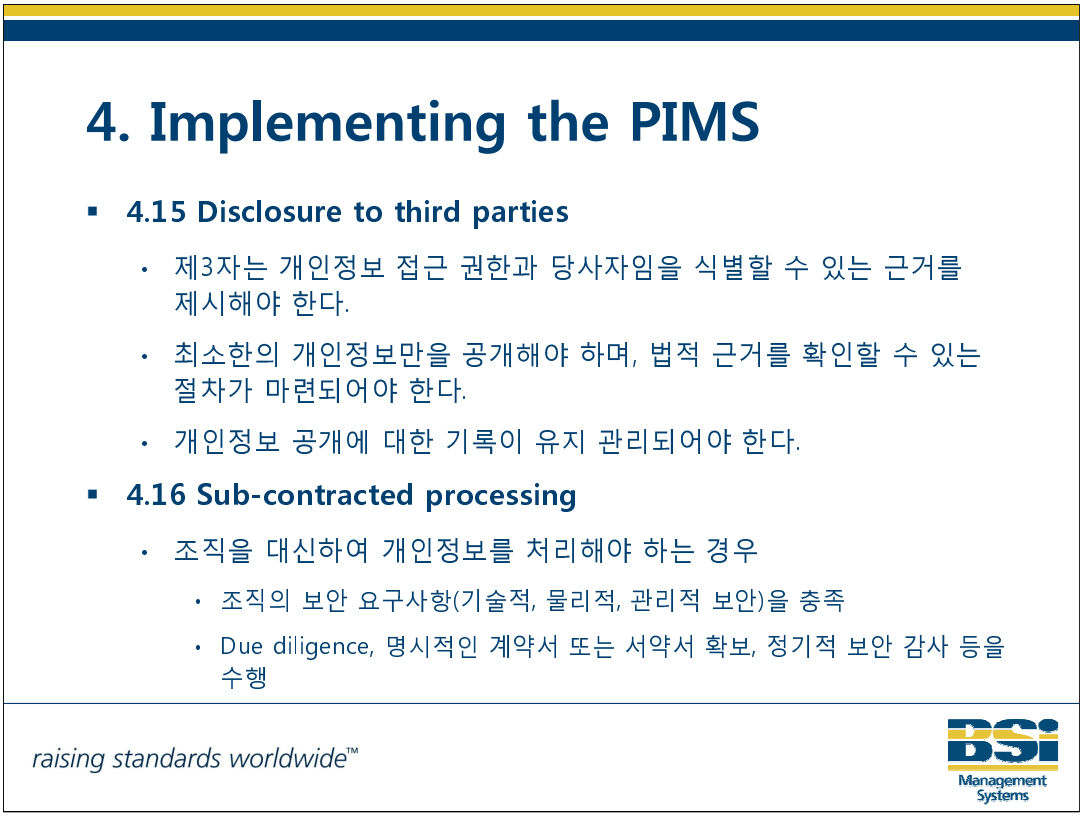
보안 사고가 발생되었을 때, 비즈니스의 연속성을 보장할 수 있도록 Contingency plan을 수립해야 하며, 이러한 계획 수립을 위하여 BS 25999 규격을 참조할 수 있다.

# 4. Implementing the PIMS

- **4.14 Transfer of personal information outside the EEA**
  - 개인정보가 EEA(European Economic Area)밖으로 전송되는 경우에 대하여 적절한 보호 수준에 대한 정의해야 한다.
  - Transfer procedures
    - 계약조건 내에서 보호되고 처리되어야 한다.
    - 제3자의 Security due diligence 수행
    - European Commission에 의하여 승인된 국가



개인정보가 EEA 밖으로 전송되는 경우에 대한 내용으로 국내 환경에는 해당 사항이 없다고 볼 수 있으나, 요구되는 절차를 일반적인 내용으로 이해를 해 본다면 적절한 부분(국외로 전송되는 경우, 제3자에게 전달되는 경우 등)에 적용할 수 있을 것으로 생각한다.




4.15 Disclosure to third parties

제3자에게 개인정보를 공개하는 경우, 제3자를 식별하고 최소한의 정보만을 공개해야 한다.

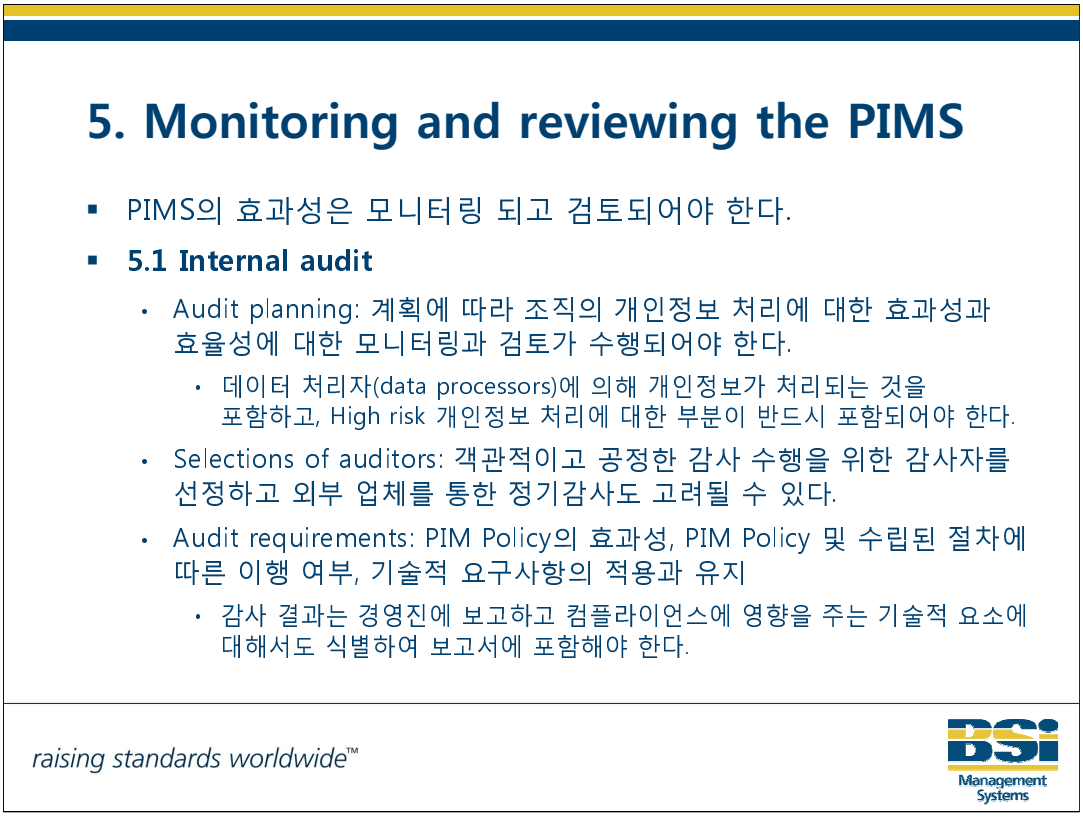
제3자에 개인정보를 공개한 기록은 적법하며, 책임 추적성을 확보할 수 있어야 한다.

Freedom of Information Act 2000 에 대한 법률적 근거도 확인할 필요가 있다.

Due diligence가 필요하다. (예를 들면 ISO 27001 인증 유지 활동, 내부감사, 경영검토, 교육활동 등)

# 4. Implementing the PIMS

- **4.17 Maintenance**
  - 절차와 기술적 요소 등은 기능 유지를 위해 지속적으로 관리(계획 수립, 정기적 검토 등)되어야 한다.
  - 유지 관리 활동으로 다음의 활동이 포함되어야 한다.
    - 감사 이력과 로그 파일 점검
    - PIMS의 개정과 추가
    - 절차에 따른 컴플라이언스 검토




PIMS의 효과성을 유지하기 위하여 모니터링과 검토가 주기적으로 수행되어야 한다.

감사 시에는 반드시 High Risk로 식별된 개인정보에 대한 관리가 포함되어야 한다.
그리고 감사결과가 경영진에 의해 검토될 수 있도록 해야 한다.

# 5. Monitoring and reviewing the PIMS

- **5.2 Management review**
  - 지속적인 적합성, 적절성, 효과성을 보장하기 위하여 경영검토는 정기적으로 수행되어야 한다.
    - PIMS 사용자의 feedback
    - 식별된 위험
    - 감사 결과
    - 절차 검토 기록
    - 기술적 부문의 향상과 교체에 대한 결과
    - 심사(평가) 요청
    - 불만 처리
    - 발생된 보안사고 또는 위반 사항
  - 주요사항이 변경되어 PIMS에 반영된 후에는 반드시 감사가 수행되어야 한다.



경영검토에 의해 주요 사항이 변경되어 PIMS에 반영되는 경우에는 반드시 해당 부분이 감사에 포함되어 수행되어야 한다.

# 6. Improving the PIMS

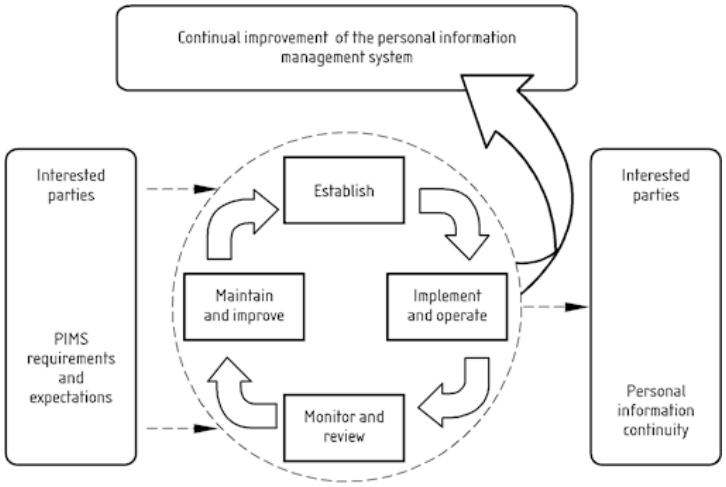
- 개선 활동을 통한 PIMS의 효과성과 효율성을 개선해야 한다.
- **6.1 Preventive and corrective actions**
  - 제안된 변경 또는 개선 사항은 PIM Policy 요구사항에 대한 충족 여부를 보장하기 위해 적용 전에 검토되어야 한다.
  - 예방 및 시정조치 활동에 의한 변경 사항은 문서화되고, 정해진 기간 동안 보유해야 한다.
  - Preventive actions
    - 잠재적 부적합 요인과 원인을 식별
    - 필요한 예방활동 결정과 적용
    - 수행된 활동 결과와 검토를 기록
    - 변경된 위험 식별
    - 알 필요가 있는 사람에게만 잠재적 부적합 사항과 예방 조치 사항을 공유

# 6. Improving the PIMS

- 6.1.3 Corrective actions
  - 부적합 요인을 제거하고,
  - 부적합 수준을 낮추거나
  - 부적합 수준을 감소시킨 것이 보장될 수 없다고 위험평가에서 결정되면, 이러한 내용을 상세하게 문서화하여 기록

- 6.2 Continual improvement
  - 조직은 감사 결과, 예방 및 시정조치 활동과 경영검토를 통하여 PIMS의 효과성을 지속적으로 개선해야 한다.
  - 불만사항, 보안사고, 사용자의 요청 등은 PIMS 효과성을 개선하기 위한 지원사항으로 이용해야 한다.

## PDCA cycle applied to the management of personal information




*raising standards worldwide*™

BSI Management Systems

PDCA 사이클은 ISO 9001, 14001, 27001, 20000 등의 규격에 적용되어 있다. 마찬가지로 BS 10012도 PDCA 사이클을 적용하고 있다.

Tack
Gracias
Vielen Dank
Merci
ありがとうございます
Bedankt
感謝您
Tak
谢谢
Спасибо
Thank You
Kiitos
감사합니다
Takk
Grazie
Dziękujemy
Obrigado

BSI Management Systems Korea
(영국표준협회)
SONG ILSEOB Lead Auditor
(Ilseob.song@bsigroup.com)