정보보호 능력은 필수적인 '기업의 핵심 경쟁력이다'

국제 정보보호 표준

ISO/IEC 27001:2013 Guideline

Information security management systems — Requirements

(정보보호 경영시스템 ISO 27001:2013)

KQA
Q.Assurance

☑ ISO 27001:2013 Framework Overview

1. 국제 정보보호 ISO 27001:2013 Framework

- ISO27001:2013은 부속서 SL(Annex SL)의 부록 2(Appendix 2) 규격으로 개정되어 High Level Structure의 구조로 구성 되어 있으며 조직에게 정보보호 경영시스템 프레임워크를 제공한다.

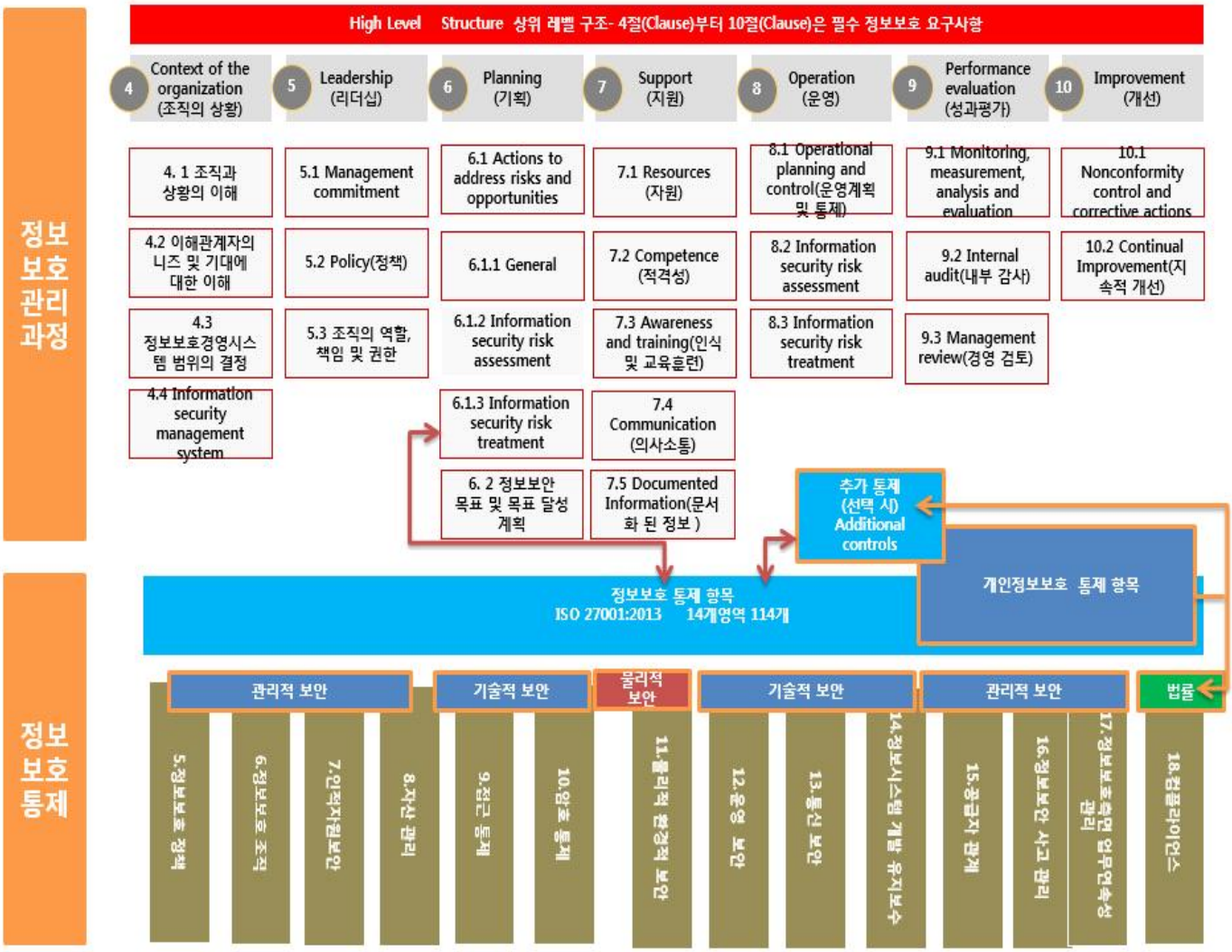
- ISO/IEC 27001:2013은 ISO/IEC 270001, 27002, 27003, 27005 등과 중복되거나 충돌이 발생되는 부분을 줄이도록 하는 요구사항과 모든 ISO 경영시스템이 공통된 구조를 갖도록 동일 구문에 동일 텍스트 사용요구를 반영하기 위해 최초 제정 이후 8년 만에 개정되었다.

- ISO 27001 정보보호 경영체계는 **비즈니스 목표**를 달성하기 위해 조직의 정보보안을 수립하고, 구현하고, 운영하고, 모니터링하고, 검토하고, 유지하고, 지속적인 개선을 위한 체계적인 Process Approach (Plan -> Do -> Check -> Act) 접근 방법이다.(조직의 전략적인 선택을 위한 경영 시스템이다.)

- 그림은 ISO 27001:2013 High Level Structure 정보보호 경영 프레임워크이다.
  - HLS 구조(Clause)는 총 1절부터 10절로 구성되어 있으며 4절(Clause)부터 10절(Clause)은 필수 요구사항이다.
    참고로 1절 Scope(범위), 2절 Normative references(참고 문헌), 3절 Terms and definitions(용어 및 정의) 구성이다.
  - 정보보호 관리과정은 HLS 상위 레벨 구조 7개 필수 요구사항으로 구성되어 있다.
  - 정보보호 통제과정은 14개 영역 114개 통제항목으로 구성되어 있다.
  - 추가적인 통제 항목 선택 및 구현 시 개인정보보호 통제 항목을 추가적으로 구현 할 수 있다.

- Annex SL (previously ISO Guide 83) structure는 high level structure(상위 레벨 구조), identical core text(동일한 핵심 본문), common terms and core definitions(공통 용어 및 정의) 로 구성되어 있다.

- ISO 27001:2013 structure 는 **①조직의 상황**(Context of the organization) **② 리더십**(Leadership) **③기획**(Planning) **④지원**(Support) **⑤운영**(Operation) **⑥성과평가**(Performance evaluation) **⑦개선**(Improvement) **7개 관리과정 요구사항 HLS(High Level Structure, common framework)**로 구성되어 있다.



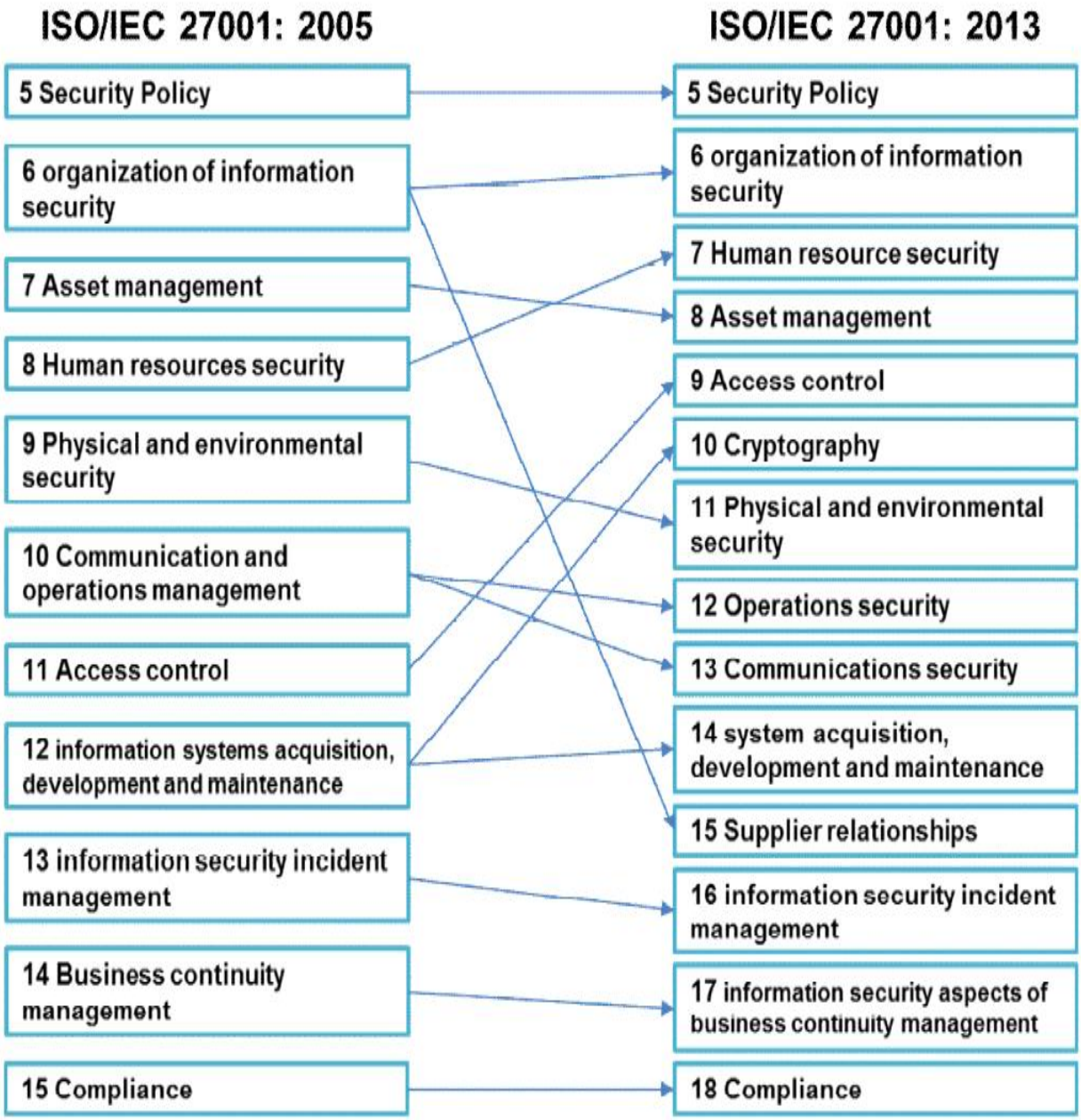
• ISO/IEC 27001:2013은 3개 도메인이 확대되었으며, 통제목표와 통제항목은 각각 4개 및 19개로 축소됨

구 분	ISO/IEC 27001:2005	ISO/IEC 27001:2013	비고
Domains (통제분야)	11	14	3개 증가
Control objectives (통제목적)	39	35	4개 축소
Controls (통제항목)	133	114	19개 축소

[질문] ISO27001:2005(PDCA) and ISO 27001:2013(High Level Stucture) 차이점을 설명하세요?

[질문] ISO 9001:2015(High Level Stucture)와 ISO27001:2013 High Level Stucture 차이점을 설명하세요?

〈 Annex A 각 도메인 비교 〉



2. 국제 정보보호 ISO 27001:2013 표준 및 적용 메커니즘

- ISO Guide 72 에서는 경영시스템을 “방침과 목표를 수립하고 그 목표를 달성하기 위한 시스템” 으로 정의하고 있다.
- ISO Guide 72 는 경영시스템 표준의 PDCA 모델이나 프로세스(Input-output)모델에 따른 구조를 제시해 면서 6개 “공통 경영요소(방침, 기획, 실행 및 운영, 성과평가, 지속적 개선, 경영검토)를 포함하는 것을 요구하고 있다.
- ISO Guide 83, Annex SL High level structure, identical core text, common terms and core definitions

Q Mapping the clauses ISO 27001:2013 과 ISO 27001:2005 **관리과정** 비교해 주세요?

A ISO 27001:2013 은 **①조직의 상황, ② 리더십, ③ 기획, ④ 지원, ⑤ 운영, ⑥ 성과평가, ⑦ 개선 7개 관리과정 요구사항** HLS(High Level Structure)로 변경되었다.

3. ISO 27001:2013 관리 과정 Requirements

1. 국제 정보보호 표준 Framework

- ISO 27001 은 ①조직의 상황, ② 리더십, ③ 기획, ④ 지원, ⑤ 운영, ⑥ 성과평가, ⑦ 개선으로 7개 관리과정 요구사항으로 구성되어 있으며, 정보보호 통제 요구사항은 부속서 A ‘통제 목적 및 통제’ 로 14개 영역 114개 통제 항목으로 구성되어 있다.
- Process Approach(PACA 접근): Plan -> Do -> Check -> Act
- HLS(High Level Structure): 조직 상황, 리더십, 기획, 지원, 운영, 성과평가, 개선의 7개 구조로 구성
- Risk-based Approach: ISO 31000 기반 원칙, 프레임워크, 프로세스 3가지 축으로 구성된다.

HLS 구조(Clause)		PACA	ISO 27001:2013 요구사항
1	Scope (범위)		이 국제표준은 조직의 Context 내에서 정보보호 경영시스템의 수립, 구현, 유지 및 지속적인 개선을 위한 요구사항을 규정하고 있다. 이 국제표준은 조직의 요구에 맞게 정보보호위험 평가 및 조치하기 위한 요구사항을 포함하고 있다.
2	Normative references (참고 문헌)		ISO/IEC27000 - 정보보호경영시스템-개요 및 용어
3	Terms and definitions (용어 및 정의)		ISO/IEC27000 에서 주어진 용어 및 정의가 적용된다.
4	Context of the organization	Plan (계획)	4. Context of the organization(조직의 상황)

	(조직의 상황)		4.1 Understanding of the organization and its context (조직과 그 상황의 이해) 4.2 Understanding the needs and expectations of interested parties(이해관계자의 니즈 및 기대에 대한 이해) 4.3 Determining the scope of the information security management system(정보보호경영시스템 범위의 결정) 4.4 Information security management system
5	**Leadership (리더십)**		5. Leadership(리더십) 5.1 Management commitment(경영진의 의지) 5.2 Policy(정책) 5.3 Organizational roles, responsibilities and authorities(조직의 역할, 책임 및 권한)
6	**Planning (기획)**		6. Planning(기획) 6.1 Actions to address risks and opportunities (위험과 기회에 대한 대처 활동) 6.1.1 General 6.1.2 Information security risk assessment (정보보호 위험평가) 6.1.3 Information security risk treatment (정보보호 위험처리) → Annex A control objectives and controls (부속서 A. 통제 목표 및 통제) 6.2 Information security objectives and planning to achieve them (정보보안 목표 및 목표 달성 계획)
7	**Support (지원)**	Do (실행)	7. Support(지원) 7.1 Resources(자원) 7.2 Competence(적격성) 7.3 Awareness and training(인식 및 교육훈련) 7.4 Communication(의사소통) 7.5 Documentation(문서화) 7. 5. 1 일반 7. 5. 2 생성 및 갱신 7. 5. 3 문서화된 정보의 통제
8	**Operation (운영)**		8. Operation(운영) 8.1 Operational planning and control(운영계획 및 통제) 8.2 Information security risk assessment (정보보호 위험평가) 8.3 Information security risk treatment (정보보호 위험처리)
9	**Performance evaluation (성과평가)**	Check (점검)	9. Performance evaluation (성과평가) 9.1 Monitoring, measurement, analysis and evaluation (모니터링, 측정, 분석 및 평가) 9.2 Internal audit(내부 감사)

			9.3 Management review(경영진의 검토)
10	**Improvement (개선)**	Action (조치)	10. Improvement(개선) 10.1 Nonconformity control and corrective actions (부적합사항에 대한 통제 및 시정조치) 10.2 Continual Improvement(지속적 개선)

[표. ISO 27001 정보보호 관리과정 요구사항]

구분	ISO 27001:2013/KS ISO 27001:2014 요구사항		통제항목
통제 목적 및 통제	A.5 Information security policies	정보보호 정책	2
	A.6 organization of information security	정보보호 조직	7
	A.7 Human resource security	인적 자원 보안	6
	A.8 Asset management	자산 관리	10
	A.9 Access control	접근 통제	14
	A.10 Cryptography	암호화	2
	A.11 Physical & environmental security	물리적 환경적 보안	15
	A.12 Operations security	운영 보안	14
	A.13 Communications security	통신 보안	7
	A.14 System acquisition, development & maintenance	정보 시스템 개발 유지보수	13
	A.15 Supplier relationships	공급자 관계	5
	A.16 Information security incident management	정보보안 사고 관리	7
	A.17 Information security aspects of business continuity management	정보보호 측면 업무 연속성 관리	4
	A.18 Compliance	컴플라이언스	8
		14개 영역 통제 항목	**114 개**

aspect 측면	통제	설 명
개인정보보호 분야 클라우드 보안 분야	additional controls (추가 통제)	조직 상황(Context), 보안 요구사항, 정보보호, 개인정보보호 목표 수준에 따라 추가 통제 선택 및 적용을 고려할 수 있음 **예시(ISO 27009: CD 단계로 국제 표준화 예정)** - 국내 정보보호 통제(ISMS), 개인정보보호 통제(PIPL, PIMS) - ISO 27009 + ISO 29151(개인정보보호 통제) - ISO 27009 + ISO 27007, 27008 (클라우드 정보보호 및 개인정보보호 통제)

[표. ISO 27001 정보보호 통제 요구사항]

☑ ISO 27001:2013 구축 단계 및 인증 취득 준비 안내

주요 구축 및 심사 준비 내용 설명

• 정보보호경영시스템 구축 단계별 산출물

- Task 1: context 분석(내부, 외부(고객사, 법적), 이해관계자 분석)
- Task 2: 위험분석 및 위험평가
- Task 3: 정보보호 정책 및 지침 등 정보보호경영체계 수립
- Task 4: 정보보호 대책 구현 및 위험 조치 이행
- Task 5: 심사 준비(1단계 문서심사, 2단계 본심사)
- Task 6: 인증 취득 단계(부적합 시정조치 및 완료)

구분	ISO 27001:2013/KS ISO 27001:2014 요구사항		output 산출물
관리 과정	4. Context of organisation	조직의 상황	범위 정의서
	5. Leadership	리더쉽	정보보호 정책(5.2)
	6. Planning	기획	위험평가 지침(6.1.2) 위험평가 보고서(6.1.2) 위험처리 결과보고서(6.1.3) 적용성 보고서 (6.1.3 d) 정보보호 계획서(6.2)
	7. Support	지원	자원, 인식, 의사소통과 관련된 문서화된 정보
	8. Operation	운영	위험평가 보고서(8.2) 위험처리(조치 및 이행) 결과보고서(8.3)
	9. Performance evaluation	성과 평가	정보보호 성과평가 보고서(9.1) 내부감사 계획 및 결과보고서(9.2) 경영 검토에 관련된 문서화 된 정보
	10. Improvement	개선	지속적인 개선과 효과성과 관련된 문서화 된 정보

구분	ISO 27001:2013/KS ISO 27001:2014 요구사항		output 산출물
통제 목적 및 통제	A.5 Information security policies	정보보호 정책	정보보호 정책, 지침
	A.6 organisation of information security	정보보호 조직	정보보호 조직 지침, 절차서
	A.7 Human resource security	인적 자원 보안	인적 보안 지침, 절차서
	A.8 Asset management	자산 관리	자산관리 지침, 절차서
	A.9 Access control	접근 통제	접근 통제 지침, 절차서
	A.10 Cryptography	암호 통제	암호 통제 지침, 절차서
	A.11 Physical & environmental security	물리적 환경적 보안	물리적 보안 지침, 절차서
	A.12 Operations security	운영 보안	운영 보안 지침, 절차서
	A.13 Communications security	통신 보안	네트워크 보안 지침, 절차서
	A.14 System acquisition, development & maintenance	정보 시스템 개발 유지보수	개발 보안 지침, 절차서
	A.15 Supplier relationships	공급자 관계	공급자 보안 지침, 절차
	A.16 Information security incident management	정보보안 사고 관리	정보보안 사고 대응지침, 절차서
	A.17 Information security aspects of business continuity management	정보보호 측면 업무 연속성 관리	정보보호 측면 업무연속성 지침, 절차서
	A.18 Compliance	컴플라이언스	컴플라이언스 지침, 절차서 개인정보보호 지침 내부관리계획, 법적 요구사항 근거 자료

[표. ISO 27001:2013 개정된 문서화 된 정보 예시]

Q & A

Q Mapping the clauses ISO 27001:2013 과 ISO 27001:2005 **관리과정** 비교해 주세요?

A ISO 27001:2013 은 **①조직의 상황, ② 리더쉽, ③ 기획, ④ 지원, ⑤ 운영, ⑥ 성과평가, ⑦ 개선 7개 관리과정 요구사항** HLS(High Level Structure)로 변경되었다.

ISO 27001: 2013	ISO 27001:2005
1. Scope of the standard	1. Scope of the standard
2. Normative references	2. Normative references
3. Terms and definitions	3. Terms and definitions
4. Context of organisation	4.2.1.a Define the scope & boundaries.
5. Leadership 5. 1 Leadership and commitment 5. 2 Policy 5. 3 Organizational roles, responsibilities and authorities	 5.1 Management Commitment 4.2.1 b) Define an ISMS policy 5.1 c) Establishing roles and responsibilities for information security
6. Planning	4.2.1.b Objectives 4.2.1.c Risk Assessment
7. Support	5.2 Resource Management 4.3 Documentation Requirements
8. Operation	4.2.2 Implement and operate the ISMS
9. Performance evaluation	4.2.3 Monitor and Review the ISMS 6. Internal Audits 7. Management Review
10. Improvement	8. ISMS Improvement

Q Mapping the clauses ISO 27001:2013 과 ISO 27001:2005 **통제항목** 비교해 주세요?

A ISO 27001:20005 **11개 영역 133개 통제항목**에서 ISO 27001:2013 개정판은 **14개 영역 114개 통제항목**으로 변경되었다.

분류	ISO 27001:2005	ISO 27001:2013
통제목적	A5 Security Policy	A5 Security Policies

및 통제항목	A6 Organization of information security	A6 Organization of information security
	A7 Asset management	A7 Human resource security
	A8 Human resource security	A8 Asset management
	A9 Physical and environmental security	A9 Access control
	A10 Communications and operations management	A10 Cryptography
	A11 Access Control	A11 Physical and environmental security
	A12 Information systems acquisition, development and maintenance	A12 Operations security
	A13 Information security incident management	A13 Communications security
	A.14 Business continuity management	A14 System acquisition, development and maintenance
	A15 Compliance	A15 Supplier relationships
		A16 Information security incident management
		A17 Information security aspects of Business Continuity
		A18 Compliance
합계	**11개 영역 133개 통제 항목**	**14개 영역 114개 통제 항목**

Q ISO 27001:2013 **관리과정, 통제항목** 요구사항(심사 기준) 전체를 설명해 주세요?

A • 관리과정은, **①조직의 상황 ② 리더쉽 ③ 기획 ④ 지원 ⑤ 운영 ⑥ 성과평가 ⑦ 개선**으로 7개 정보보호 경영시스템 관리과정 요구사항으로 구성되어 있으며 27개 필수 요구사항이다.

• 정보보호 통제 요구사항은 **부속서 A** '통제 목적 및 통제' 로 **14개 영역 114개 통제 항목**으로 구성되어 있다.

구분	ISO 27001:2013/KS ISO 27001:2014 요구사항		통제항목
관리 과정	4. Context of organisation	조직의 상황	4
	5. Leadership	리더쉽	3
	6. Planning	기획	4
	7. Support	지원	8
	8. Operation	운영	3

	9. Performance evaluation	성과 평가	3
	10. Improvement	개선	2
		7개 관리과정 필수 항목	**27 개**

※ ISO 27001:2013은 7개 경영시스템 HLS 관리과정은 clauses 조항(clauses 4절~10절) 기준으로 27개 항목을 도출함

구분	ISO 27001:2013/KS ISO 27001:2014 요구사항		통제항목
통제 목적 및 통제	A.5 Information security policies	정보보호 정책	2
	A.6 organisation of information security	정보보호 조직	7
	A.7 Human resource security	인적 자원 보안	6
	A.8 Asset management	자산 관리	10
	A.9 Access control	접근 통제	14
	A.10 Cryptography	암호 통제	2
	A.11 Physical & environmental security	물리적 환경적 보안	15
	A.12 Operations security	운영 보안	14
	A.13 Communications security	통신 보안	7
	A.14 System acquisition, development & maintenance	정보 시스템 개발 유지보수	13
	A.15 Supplier relationships	공급자 관계	5
	A.16 Information security incident management	정보보안 사고 관리	7
	A.17 Information security aspects of business continuity management	정보보호 측면 업무 연속성 관리	4
	A.18 Compliance	컴플라이언스	8
		14개 영역 통제 항목	**114 개**

문의 및 연락처

한국품질보증원(KQA)

국내 1호 ISO 27001 인증기관 최초인증팀 남재상 실장 031-469-9001