한국심사자격인증원 [KAR]	점 수	
ISO/IEC 27001 자격확대 연수과정 [모의] 필기시험	성 명	
문 제 [답 안]	응시번호	

[주의] '* 참고'는 출제 근거를 제시한 것으로 실제 시험지에는 참고가 없음.

Ⅰ. 다음 문제를 읽고 그 내용이 맞으면 'o', 틀리면 'x'를 빈칸에 기입하시오.

(각2.5점/6개/총15점)

1~2. '기밀성(confidentiality)'이란 정보를 비인가 개인, 기관, 프로세스가 사용할 수 없게 하거나, 이들에게 공개되지 않게 하는 성질을 말한다. (**o**)

*** 참고 : ISO/IEC 27000:2018 "3.10"의 내용**

3~6. 이 표준은 내부 및 외부 당사자가 조직의 자체 정보보안 요구사항을 충족하려는 조직의 능력을 평가하는 데 사용할 수 없다. (**x**)

*** 참고 : ISO/IEC 27001:2022 "개요"의 내용**

Ⅱ. 다음 문제를 읽고 빈칸에 옳은 보기의 번호를 입하시오.

(각2.5점/14개/총35점)

7~8. 다음은 '정보보호 사건(information security incident)'에 대한 용어를 설명한 것이다. (a)에 들어갈 단어로 가장 적절한 것을 고르시오. (**3**)

정보보안 사건(information security incident)은 기업 운영을 저해하고 정보보안을 위협할 확률이 상당한, 하나의 혹은 일련의 원치 않은, 혹은 예기치 않은 정보보안 (a)이다.

① a: 사건
② a: 인시던트
③ a: 이벤트
④ a: 사고

*** 참고 : ISO/IEC 27000:2018 "3.31"의 내용**

9~20. 조직이 정보보안 위험처리 프로세스를 정의하고 적용하여야 하는 사항과 가장 거리가 먼 것을 고르시오. (**4**)

① 위험평가 결과를 감안한 적절한 정보보안 위험처리 방안의 선택
② 선택한 정보보안 위험처리 방안의 실행에 필요한 모든 통제의 결정
③ 적용성보고서(Statement of Applicability)의 작성
④ 정보보안 위험평가 계획의 수립

*** 참고 : ISO/IEC 27001:2022 "6.1.3"의 내용**

Ⅲ. 문제 유형은 A형과 B형으로 구성되어 있습니다.

(각 2.5점 / 총 8문항 / 총 20점)
A형: 각 2.5점 × 4문항 = 총 10점
B형: 각 2.5점 × 4문항 = 총 10점

Ⅲ-A형. 다음에 제시된 상황의 적합성 여부를 합리적으로 결정하기 위하여 귀하는 ISO/IEC 27001 표준의 어떠한 조항번호를 근거로 부적합 또는 부적합 아님으로 판단하는지를 결정하고 ( )에 해당번호를 기재하시오.

(각2.5점/4개/총10점)

21~24. 한국정보(주)에서 ISMS를 심사하던 중에 심사원은 한달 전에 퇴사한 직원의 계정관리에 대하여 검토하고 있었다. 퇴사자가 생기면 그 계정은 본인이 업무를 수행하였던 ERP 정보시스템을 포함하여 모든 서버에 접근을 중지하도록 규정이 있는 것을 확인하였다. 그런데 퇴사자 계정으로 회사의 업무 보안 정보가 있는 내부 서버에 접속을 시도하였더니 아직도 이 계정이 유효하게 작동하고 있음을 발견하였다. (**2**)

① 8.2 정보보안 위험평가
② 8.3 정보보안 위험처리
③ 부속서 A 인원통제
④ 부적합 아님

*** 이유 : 8.3 정보보안 위험처리**
조직은 정보보안 위험처리 계획을 실행하여야 한다. (부 5.18 참조)

Ⅲ-B형. 다음에 제시된 상황의 적합성 여부를 객관적으로 결정하기 위하여 귀하는 부적합으로 지적 또는 추적조사를 하여 판단하고자 한다. 질문에 가장 적절한 답을 골라서 ( )에 해당번호를 기재하시오. (각2.5점/4개/총10점)

사례 1

심사원은 ISMS 심사 중에 정보시스템 서버실을 방문하였다. 정보시스템 부서에 소속되어 있지 않은 인원이 보안구역인 서버실 내부에서 작업을 하고 있는 광경을 발견하였다. 심사원은 정보시스템 운영에 필요한 보수 작업을 하는 경우에 외부인에 대한 통제에 대한 질문을 해당 직원에게 하였더니, 최근에 발생한 정보시스템 고장으로 인하여 정보시스템의 조속한 복구가 필요하여 오늘 급히 유지보수 인원을 불러서 작업하고 있다고 답변하였다.

25. 위 상황에 대하여 심사원의 물리적 통제 항목 적용과 가장 거리가 먼 것을 고르시오. (**4**)

① 보안경계는 정보와 그 밖의 관련 자산을 포함하는 구역을 보호하기 위하여 정의되고 사용되어야 한다. (부 7.1)
② 보안 구역은 적절한 출입 통제와 접근 포인트로 보호되어야 한다. (부 7.2)
③ 보안 구역 내에서 작업을 위한 보안 조치는 설계되고 실행되어야 한다. (부 7.6)
④ 장비는 정보의 가용성, 무결성 그리고 기밀성을 보장하도록 정확하게 유지보수되어야 한다. (부 7.13)

.

사례 2

조직의 '책상 정리와 화면 보호' 항목에 대하여 심사하던 중에 점심시간에 불꺼진 사무실에 한 직원의 책상위 개인 용 PC 화면이 업무 정보가 그대로 노출되어 있는 상태로 켜져있는 것이 발견되었다. 부속서 A 통제는 '서류와 이동식 저장 매체를 대상으로 한 책상 정리 규칙과 정보처리 설비에 대한 화면보호 규칙은 정의되고 적절하게 시행되어야 한다'이다.

26. 위 상황에 대하여 심사원이 추적조사를 하는 내용과 가장 거리가 먼 것을 고르시오. (**2**)

① 조직이 '책상 정리와 화면 보호' 항목에 대한 정보보안 위험을 식별하였는지 확인한다.
② 조직이 ISMS에 관련하여 내부 및 외부 의사소통의 필요성을 파악하였는지 확인한다.
③ 조직이 위험평가 결과를 감안한 적절한 정보보안 위험처리 방안을 선택하였는지 확인한다.
④ 조직이 결정한 통제를 부속서 A의 통제와 비교하였는지 확인한다.

27. 위 상황에 대하여 추적조사를 한 후에 부적합으로 지적한다면 다음 조항 중에서 가장 거리가 먼 것을 고르시오. (**3**)

① 6.1.2 정보보안 위험평가
② 6.1.3 정보보안 위험처리
③ 7.4 의사소통
④ 8.1 운영 기획과 통제

사례 3

최고경영진은 다음 사항을 만족하는 정보보안방침을 수립하여야 한다. a) 조직의 목적에 적합 b) 정보보안목표를 포함하거나 정보보안목표를 위한 틀을 제공 c) 정보보안에 관련된 적용 가능한 요구사항을 만족시키도록 하는 의지를 포함 d) 정보보안경영시스템의 지속적 개선을 위한 의지를 포함 정보보안방침은 다음 사항을 만족하여야 한다. e) 문서화된 정보로 이용 가능 f) 조직 내부에 소통 g) 적절하게 이해관계자에게 이용 가능

28. 위 요구사항의 통제에 대하여 심사원의 올바른 행동과 가장 거리가 먼 것을 고르시오. (**1**)

① 정보보안방침이 외부에서 제공되는 프로세스, 제품 또는 서비스가 관리됨을 보장하였는지 확인한다.
② 정보보안방침과 주제별 방침이 정의되고, 경영자에 의하여 승인, 공표되었는지 확인한다.
③ 정보보안방침이 관련된 인원과 관련된 이해관계자에게 소통과 인지되었는지 확인한다.
④ 정보보안방침이 계획된 주기 그리고 중요한 변경 사항이 발생하는 경우 검토되는지 확인한다.

- 수고하셨습니다 -