【정보보안관리 및 법규】

1. 물리적 보안에 해당하는 내용으로 가장 적절하지 **않은** 것은?
① 운영 서버 시스템의 도난 방지 또는 파괴 방지
② 정보시스템과 네트워크장비들의 위치 공간 분리
③ 조직 구성원의 보안구역 출입 통제
④ 조직 내 정보보안의 정책과 절차 수립

2. 정보보호 대책 수립을 위한 대응 전략으로 가장 적절하지 **않은** 것은?
① 위험전가는 위험이 발생하는 원인을 제3자를 통해 제거한다.
② 위험감소는 위험을 줄일 수 있는 대책을 채택하여 구현한다.
③ 위험회피는 위험이 존재하는 프로세스나 사업을 수행하지 않는다.
④ 위험수용은 식별된 위험을 받아들이고 비용을 감수한다.

3. ISO 27001에서 제시한 정보보안관리 PDCA 모델의 단계별 이행내용으로 가장 적절하지 **않은** 것은?
① Plan 단계에서 보안 정책, 목적, 프로세스 및 절차를 수립한다.
② Do 단계에서 정책, 통제, 위험처리 프로세스를 구현하고 수행한다.
③ Check 단계에서 프로세스 수행을 모니터링하고 점검한다.
④ Approve 단계에서 프로세스 진행에 대한 최고경영진의 승인을 획득한다.

4. 정보보호 위험관리를 위한 요소와 설명으로 가장 적절하게 짝지어진 것은?

<요소>

(가) 자산 (Asset)　(나) 위험 (Risk)
(다) 위협 (Threat)　(라) 취약점 (Vulnerability)

<설명>

㉠ 보호 대상에 손실 및 피해를 유발할 가능성
㉡ 악의적인 공격이 발생하기 위한 조건 및 상황
㉢ 조직에서 보호해야 할 가치가 있는 자원
㉣ 보호 대상에 악영향을 미칠 수 있는 사건·행위

	(가)	(나)	(다)	(라)
①	㉢	㉣	㉠	㉡
②	㉡	㉠	㉣	㉢
③	㉢	㉠	㉣	㉡
④	㉡	㉣	㉠	㉢

5. BCP(Business Continuity Planning) 5단계 접근방법론을 통한 복구 프로세스 개발 절차이다. ㉠~㉢에 들어갈 단계들이 가장 적절한 순서로 배열된 것은?

BCP 정책 및 계획수립 → ㉠ → ㉡ → ㉢ → 수행테스트 및 유지보수

	㉠	㉡	㉢
①	사업영향평가	복구전략개발	복구계획수립
②	복구전략개발	사업영향평가	복구계획수립
③	사업영향평가	복구계획수립	복구전략개발
④	복구전략개발	복구계획수립	사업영향평가

6. 재해복구 수준별 핵심 지표에 대한 설명으로 가장 적절한 것은?
① RTO는 복구 완료가 필요한 기능의 우선순위이다.
② RPO는 서비스 중단에 따른 데이터 보호 계획이다.
③ RP는 실제 업무 기능 복구까지 걸리는 시간이다.
④ MTD는 서비스를 중단할 수 있는 최소시간이다.

7. TCSEC(Trusted Computer System Evaluation Criteria)에 제시된 보안 등급과 보호 수준에 대한 연결이 가장 적절한 것은?
① A 등급 – 통제된 보호(Controlled Protection)
② B 등급 – 검증된 보호(Verified Protection)
③ C 등급 – 임의적 보호(Discretionary Protection)
④ D 등급 – 최대 보호(Maximum Protection)

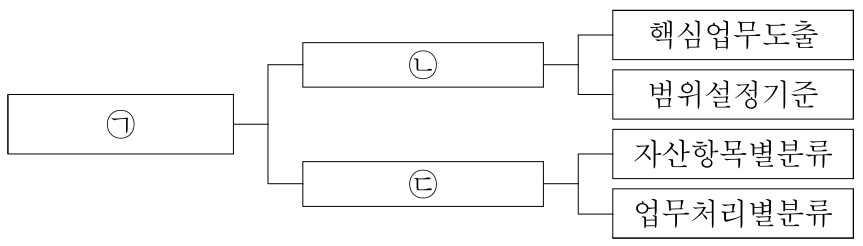
8. ISMS-P 인증의 '관리체계 수립 및 운영' 분야와 항목에 대한 연결이 가장 적절하지 **않은** 것은?
① 관리체계 기반 마련 – 경영진 참여, 최고책임자 지정, 조직 구성, 정책 수립, 자원 할당
② 위협관리 – 정책의 유지관리, 조직의 유지관리, 외부자 보안 이행관리, 개인정보 수집제한
③ 관리체계 운영 – 보호대책 구현, 보호대책 공유, 운영현황 관리
④ 관리체계 점검 및 개선 – 법적 요구사항 준수 검토, 관리체계 점검, 관리체계 개선

9. 정보보호 정책 구현 요소와 관련된 ㉠~㉣ 설명의 연결이 가장 적절한 것은?

㉠ 정보보호에 대한 상위 수준의 목표 및 방향을 제시한다.
㉡ 선택적이거나, 권장 혹은 권고적인 내용으로 예측할 수 없는 상황에 유연성을 제공한다.
㉢ 정책을 만족하기 위해 수행되는 단계적인 작업으로 구체적이고 세부적인 방법을 기술한다.
㉣ 정책을 만족하기 위한 의무적 활동, 행위, 또는 규칙으로 요구사항에 관해 정의한다.

① 절차 – ㉠　② 비전 – ㉡　③ 지침 – ㉢　④ 표준 – ㉣

10. 자산식별 과정의 일부 중 ㉠~㉢에 들어갈 내용으로 가장 적절한 것은?



	㉠	㉡	㉢
①	자산조사	자산목록 작성	자산범위 설정
②	자산목록 작성	자산조사	자산범위 설정
③	자산조사	자산범위 설정	자산목록 작성
④	자산목록 작성	자산범위 설정	자산조사

11. 다음의 위험분석 방법에 대한 설명으로 가장 적절한 것은?

전문가 지식과 경험을 활용하여 위험분석을 수행하므로 상대적으로 신속한 결과를 도출할 수 있는 장점이 있다. 하지만 전문가의 개인적 지식 및 주관적 판단에 지나치게 의존하기 때문에 분석 결과가 일관성이 부족하거나 왜곡될 가능성이 있다. 따라서 전문성이 높은 인력이 수행하지 않으면 위험분석 결과의 완전도가 낮을 수 있으며 심지어 실패할 위험이 존재한다.

① 기준선 접근법(Baseline Approach)
② 비정형화된 접근법(Informal Approach)
③ 상세 위험 분석 접근법(Detailed Risk Analysis Approach)
④ 복합 접근법(Combined Approach)

12. 「개인정보 보호법」상 개인정보처리자가 개인정보를 수집할 수 있는 경우로 가장 적절하지 **않은** 것은?

① 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
② 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
③ 개인정보처리자가 법에서 정한 방법을 통해 정보주체의 동의를 받는 경우
④ 법률에 특별한 규정이 없지만, 사회 통념상 관행을 준수하기 위한 경우

13. 「개인정보 보호법」상 개인정보 보호 원칙에 대한 설명으로 가장 적절하지 **않은** 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최대한의 개인정보를 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

14. 「개인정보 보호법」상 다음과 같은 경우로 법원이 배상액을 정할 때에 고려해야 하는 사항으로 가장 적절하지 **않은** 것은?

> 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.

① 개인정보처리자의 재산상태
② 개인정보주체가 취득한 경제적 이익
③ 고의 또는 손해 발생의 우려를 인식한 정도
④ 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

15. 「전자서명법」 제2조(정의)의 일부이다. ㉠~㉣에 들어갈 용어로 가장 적절하게 짝지어진 것은?

> · (㉠)라 함은 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말한다.
> · (㉡)라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
> · (㉢)라 함은 공인인증기관으로부터 전자서명생성정보를 인증받은 자를 말한다.
> · (㉣)라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

	인증서	서명자	가입자	전자서명 검증정보
①	㉡	㉣	㉢	㉠
②	㉠	㉣	㉢	㉡
③	㉡	㉠	㉣	㉢
④	㉠	㉣	㉡	㉢

16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자가 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근권한이 필요한 경우를 두 가지로 설명하고 있다. 이 두가지 경우에서 이용자의 동의를 받기 위해 이용자가 명확하게 인지할 수 있도록 알려야 하는 것 중 공통사항으로만 가장 적절하게 짝지어진 것은?

> ㉠ 접근권한이 필요한 이유
> ㉡ 접근권한이 필요한 정보 및 기능의 항목
> ㉢ 접근권한이 필요한 서비스의 과금 정보
> ㉣ 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실

① ㉠㉡ ② ㉠㉢ ③ ㉠㉡㉢ ④ ㉠㉡㉢㉣

17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 통신과금서비스제공자가 재화등의 판매·제공의 대가가 발생한 때 및 대가를 청구할 때 통신과금서비스이용자에게 고지하여야 하는 사항으로 가장 적절하지 **않은** 것은?

① 통신과금서비스 이용일시
② 통신과금서비스를 통한 구매·이용 금액과 그 명세
③ 통신과금서비스제공자의 이용자 개인정보보호 대책
④ 이의신청 방법 및 연락처

18. 「위치정보의 보호 및 이용 등에 관한 법률」상 개인위치정보를 대상으로 하지 아니하는 위치정보사업만을 하려는 자가 대통령령으로 정하는 바에 따라 방송통신위원회에 신고해야 하는 사항으로 가장 적절하지 **않은** 것은?

① 위치정보서비스 이용자 수와 매출액
② 위치정보사업의 종류 및 내용
③ 주된 사무소의 소재지
④ 위치정보시스템을 포함한 사업용 주요 설비

19. 「개인정보 보호법」상 보호위원회에 대한 내용으로 가장 적절하지 **않은** 것은?

① 위원장은 보호위원회를 대표하고, 보호위원회의 회의를 주재하며, 소관 사무를 총괄한다.
② 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행한다.
③ 보호위원회는 상임위원 2명(위원장과 부위원장)을 제외한 9명으로 구성한다.
④ 보호위원회의 위원장과 부위원장은 정무직 공무원으로 임명한다.

20. 「전자금융거래법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 다음에서 설명하는 업무를 수행 및 총괄하는 자로 가장 적절한 것은?

<전자금융거래법>
· 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
· 정보기술부문의 보호
· 정보기술부문의 보안에 필요한 인력관리 및 예산편성
· 전자금융거래의 사고 예방 및 조치

<정보통신망 이용촉진 및 정보보호 등에 관한 법률>
· 정보보호관리체계의 수립 및 관리·운영
· 정보보호 취약점 분석·평가 및 개선
· 침해사고의 예방 및 대응
· 사전 정보보호대책 마련 및 보안조치 설계 및 구현 등
· 중요 정보의 암호화 및 보안서버 적합성 검토

① 개인정보처리자 ② 클라우드컴퓨팅서비스 제공자
③ 정보보호최고책임자 ④ 개인위치정보사업자