* 알기사 (알기쉬운 정보보안기사)
- cafe.naver.com/algisa
- sec.algisa.com

출제기준(필기)

직무 분야	정보통신	중직무분야	정보기술	자격종목	정보보안기사	적용기간	2019. 1. 1. ~ 2022.12.31.
○직무내용 : 정보보호에 대한 지식과 운용 경험을 바탕으로 실무적인 시스템과 서버, 네트워크 장비 및 보안시스템 운용을 통해, 보안업무 및 보안정책수립과 보안대책 구현, 정보보호 관련 법규 준수 여부를 판단하는 등의 업무 수행							
필기검정방법	객관식	문제수	100문	시험시간	2시간30분		

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
시스템 보안	20문	1.클라이언트 보안	1. 클라이언트 보안 관리	1. 운영체제 이해 및 관리 2. 인증·접근통제의 이해 및 관리 3. 파일시스템 이해 및 관리 4. 공격기술의 이해 및 대응관리 5. 최신 유·무선 단말기의 보안(공격기술 및 대응기술, 보안이슈 등) 이해 및 관리
		2. 서버 보안	1. 서버 보안 관리	1. 운영체제 이해 및 관리(레지스터, 웹 브라우저, 보안도구 등) 2. 인증·접근통제의 이해 및 관리 3. 파일시스템 이해 및 관리 4. 공격기술의 이해 및 대응관리 5. 최신 유·무선 서버의 보안(공격기술 및 대응기술, 보안이슈 등) 이해 및 관리
			2. 서버 보안 활용	1. 운영체제 설치 및 활용 2. 시스템 최적화 활용 3. 시스템 로그 설정 및 활용 4. 공격 대응기술의 활용 5. 점검도구 활용(취약점, 무결성 등) 6. 로깅 및 로그분석 기술 활용 7. 백업 기술 활용
			3. 서버 보안용 S/W 설치 및 운영	1. 서버 접근통제 2. 시스템 취약점 점검도구 활용 3. 서버보안시스템의 설치 및 운영 4. 무결성 점검도구 설치 및 운영 5. 로깅 및 로그분석도구의 설치 및 운영

이전과 차이 나는 부분

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
네트워크 보안	20문	1. 네트워크 일반	1. 네트워크 개념 이해	1. 네트워크의 개요(OSI 7 Layers 및 TCP, UDP, IP, ICMP 등 네트워크 프로토콜) 2. 네트워크의 종류별 동작 원리 및 특징(Ethernet, LAN, Intranet, Extranet, Internet, CAN, WAN, HAN, SDN 등) 3. 네트워크 주소의 개요 (IPv4, IPv6 Addressing, Subnetting, CIDR, VLSM, 데이터 캡슐화, Multicast, Broadcast 등) 4. 네트워크 주소의 종류별 동작원리 및 특징(공인주소, 사설주소, 정적주소, 동적주소, NAT 등) 5. 포트(Port)의 개요
			2. 네트워크의 활용	1. 네트워크 장비별 원리 및 특징 (NIC, Router, Bridge, Switch, Hub, Repeater, Gateway, VLAN 등) 2. 네트워크 공유(Share)의 동작원리와 특징(Netbios, Netbeui, P2P 등) 3. 유·무선 네트워크 서비스의 개요와 종류별 특징 4. 네트워크 도구(ping, arp, rarp, traceroute, netstat, tcpdump 등)의 이해와 활용
		2. 네트워크 기반 공격기술의 이해 및 대응	1. 서비스 거부(DoS) 공격	1. 서비스 거부(DoS) 공격 유형별 동작원리 및 특징 2. 각종 서비스 거부(DoS) 공격에 대한 대응 방법
			2. 분산 서비스 거부(DDoS) 공격	1. 분산 서비스 거부(DDoS) 공격 유형별 동작원리 및 특징 2. 각종 분산 서비스 거부(DDoS) 공격에 대한 대응 방법
			3. 스캐닝	1. 포트 및 취약점 스캐닝의 동작원리와 특징 2. 포트 및 취약점 스캐닝의 대응 방법

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
			4. 스푸핑 공격	1. 스푸핑 공격의 동작원리 및 특징 (Spoofing) 2. 스푸핑 공격의 대응 방법
			5. 스니핑 공격	1. 스니핑 공격의 동작원리 및 특징 (Sniffing, Session Hijacking 등) 2. 스니핑 공격의 대응 방법
			6. 원격접속 공격	1. 원격접속 공격의 동작원리 및 특징 (Trojan, Exploit 등) 2. 원격접속 공격의 대응 방법
		3. 대응기술 및 응용	1. 보안 프로토콜 이해	1. 보안 프로토콜별 동작원리 및 특징(SSL, IPSec 등) 2. 보안 프로토콜 응용 사례
			2. 보안 솔루션 이해	1. 보안 솔루션의 종류별 동작원리 및 특징 (Firewall, IDS, IPS, VPN, ESM, UTM, NAC, 역추적시스템 등) 2. 보안 솔루션의 활용(Snort, 탐지툴, Pcap 등) 3. 로그 분석 이해 및 응용 4. 패킷 분석 이해 및 응용 5. 역추적 이해 및 응용 악성코드 분석 도구의 이해 및 응용
		4. 최신 네트워크 보안 동향	1. 네트워크 보안 신규 위협 이해	1. 네트워크 보안 신규 위협 분석
			2. 네트워크 보안 신기술 이해	최신 네트워크 보안 기술과 솔루션

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
어플리케이션 보안	20문	1. 인터넷 응용 보안	1. FTP 보안	1. FTP 개념 2. FTP 서비스 운영 3. FTP 공격 유형 4. FTP 보안방안
			2. 메일 보안	1. 메일 개념 2. 메일 서비스 운영 3. 메일 서비스 공격 유형(스팸 메일, 악성 메일, 웜 등) 과 대책 4. 메일 보안 기술
			3. 웹 보안	1. 웹 개념 2. 웹 서비스 운영 3. 웹 서비스 장애 분석 및 대응 4. 웹 서비스 공격 유형 5. 웹 보안 기술
			4. DNS 보안	1. DNS 개념 2. DNS 서비스 운영 3. DNS 공격 유형 4. DNS 보안 기술
			5. DB 보안	1. DB 보안 개념 2. DB 공격 유형 3. DB 보안 기술
		2. 전자 상거래 보안	1. 전자상거래 보안 기술	1. 전자지불 수단별 보안요소 2. 전자상거래 보안 프로토콜 3. 전자상거래 인증기술 4. 무선플랫폼에서의 전자상거래 보안
		3. 기타 어플리케이션 보안 기술	1. 어플리케이션 보안취약점 대응	1. 취약점/버그 유형 2. 취약점/버그 방지 개발 방법
			2. 기타 어플리케이션 보안 응용	1. SSO 기술 개념 및 활용 2. DRM 기술 개념 및 활용(워터마킹, PKI기반 불법복제 방지, DOI 등) 3. 디지털 포렌식의 개념과 절차 4. 최신 어플리케이션 보안 동향

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
정보보안 일반	20문	1. 보안요소 기술	1. 인증	1. 사용자 인증 방식 및 원리 2. 메시지에 대한 인증 방식 및 핵심 기술 3. 디바이스에 대한 인증 기술의 원리 4. 생체인증 등 신규 인증기술
			2. 접근통제	1. 접근통제 정책의 이해 및 구성 요소 2. 접근통제 정책의 특징 및 적용 범위(임의적, 강제적, 역할 기반 등) 3. 접근통제 기법과 각 모델의 특징
			3. 키 분배 프로토콜	1. 대칭 키 기반 분배 방식의 원리 및 운영 2. 공개 키 기반 분배 방식의 원리
			4. 전자서명	1. 전자인증서 구조 및 주요 특징 2. 전자서명의 이해(종류, 보안 요구 조건, 특징, 서명 방식 등) 3. PKI 구성방식 및 관리(계층구조, 네트워크 구조, 복합형 구조 등) 4. CRL 사용 목적 및 구조 5. OCSP의 구조 및 동작 절차 6. 전자서명 응용 원리 및 구조(은닉서명, 이중서명 등) 7. 전자서명을 이용한 최신 응용프로그램의 특징 및 이해
		2. 암호학	1. 암호 알고리즘	1. 암호 관련 용어 및 암호 시스템의 구성 2. 암호 공격의 유형별 특징 3. 대칭키 암호시스템 특징 및 활용(종류, 구조, 운영 모드, 공격 기술 등) 4. 공개키 암호시스템의 특징 및 활용(종류, 구조, 특징) 5. 인수분해 기반 공개키 암호방식 6. 이산로그 기반 공개키 암호방식 7. 암호 알고리즘을 이용한 최신 응용 기술
			2. 해시함수	1. 해시함수의 개요 및 요구사항 2. 해시함수별 특징 및 구조 3. 메시지 인증 코드(MAC)의 원리 및 구조

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
정보보안 관리 및 법규	20문	1. 정보보호 관리	1. 정보보호 관리 이해	1. 정보보호의 목적 및 특성 2. 정보보호와 비즈니스 3. 정보보호 관리의 개념
			2. 정보보호 거버넌스 체계 수립	1. 정보보호 전략(정보보호 요구사항 분석, 전략 및 중장기 계획 수립) 2. 조직 체계와 역할/책임(정보보호 최고책임자의 지정, 실무조직 구성, 정보보호위원회 구성, 책임 및 역할, 자원 확보(예산 및 인력) 등) 3. 정보보호 정책의 수립(정책의 승인, 정책의 공표, 상위 정책과의 연계성, 정책관련 하위 문서 수립, 정책의 주기적 검토, 정책 문서의 이력 관리 등)
			3. 정보보호 위험평가	1. 위험분석 및 계획수립 2. 정보자산 식별 및 분석 3. 위험분석 및 평가
			4. 정보보호 대책 구현 및 운영	1. 정보보호 대책 선정 및 계획서 작성 2. 관리적 보호대책 구현 및 운영(내·외부 인력보안, 교육 및 훈련, 내부감사, 침해사고 예방·대응, 업무연속성관리 등) 3. 물리적 보호대책 구현 및 운영 (출입통제, 개인 및 공용 환경 보안 등) 4. 기술적 보호대책 구현 및 운영(시스템 및 SW개발 보안, 서버·네트워크·DB·어플리케이션 보안, IT 시스템 및 정보보호시스템 운영 보안 등)
			5. 정보보호 인증제도 이해	1. 국제/국가 정보보호 표준 2. 정보보호 인증 체계

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
		2. 정보보호 관련 윤리 및 법규	1. 정보보호 및 개인정보보호법 체계	1. 사이버 윤리(보안윤리 개념, 디지털 저작권 침해 및 보호기술, 유해정보유통, 사이버 폭력, 사이버 사기 등 범죄행위) 2. 정보시스템 이용자 및 개인정보취급자의 금지행위
			2. 정보보호 관련 법제	1. 정보보호 관련 법제 용어의 정의 2. 주요 정보보호 관련 법제 개요 파악(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신기반 보호법 등) 3. 기타 정보보호 관련 법제 개요 파악(클라우드컴퓨팅법, 전자정부법 등)
			3. 개인정보보호 관련 법제	1. 개인정보보호 관련 용어의 정의 2. 개인정보보호 관련 법제 파악(개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률)

출제기준(실기)

직무 분야	정보통신	중직무 분야	정보기술	자격종목	정보보안기사	적용 기간	2019. 1. 1. ~ 2022.12.31.

○직무내용 : 정보보호에 대한 지식과 운용 경험을 바탕으로 실무적인 시스템과 서버, 네트워크 장비 및 보안시스템 운용을 통해, 보안업무 및 보안정책수립과 보안대책 구현, 정보보호 관련 법규 준수 여부를 판단하는 등의 업무 수행

○수행준거 : 1. 보안정책 운영을 위해 운영체제별, 프로토콜별, 서비스별, 보안장비 및 네트워크 장비별 보안 특성을 파악하고 설정 및 점검 등을 수행할 수 있다.
2. 운영체제, 서비스, 보안장비 및 네트워크 장비 등의 취약점 점검을 통해 원인파악, 보완 및 이력사항을 관리할 수 있다.
3. 시스템 로그 및 패킷 로그를 분석하여 침입 원인을 파악하고 보완할 수 있다.
4. 조직의 비즈니스 특성을 고려하여 정보보호 목표를 설정하고 정보보호 및 법적 요구사항을 포함하여 정보보호 계획을 수립할 수 있다.
5. 조직의 정보자산을 식별하고 내·외부 위협요인을 분석·평가하여 적절한 정보보호대책 선정 및 이행계획을 수립할 수 있다.
6. 조직의 목표 달성을 위한 정보보호 정책을 수립하고 종합(법률, 관리, 기술, 물리)적 정보보호 대책을 구현하고 운영할 수 있다.

실기 검정방법	필답형	시험시간	3시간

실 기 과목명	주요 항목	세부 항목	세세항목
정보보안실무	1. 시스템 및 네트워크 보안특성 파악	1. 운영체제별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도를 파악할 수 있다. 2. IT환경을 구성하고 있는 개인용 PC 또는 서버에 설치된 운영체제 및 버전정보를 파악할 수 있다. 3. 운영체제 및 버전별로 제공되는 보안서비스, 보안정책 설정, 보안 취약점들을 파악할 수 있다. 4. 내부 사용자와 네트워크 사용자에게 공유되는 객체들의 정보를 수집하고 보안목표에 따라 보안정책이 적절히 설정되었는지 점검할 수 있다. 5. 운영체제별로 동작하는 악성코드의 종류 및 특징을 파악할 수 있다. 6. 운영체제에서 생성되는 로그파일관리가 되고 있는지 점검할 수 있다. 7. 보안 운영체제(SecureOS)가 제공하는 보안서비스를 이해하고, 접근 통제정책 등을 적용할 수 있다.
		2. 프로토콜별 보안특성 파악하기	1. OSI 7계층과 TCP/IP 프로토콜의 구성 그리고 각 계층별 기능, 동작 구조를 이해할 수 있다. 2. TCP/IP 각 계층에서 처리하는 PDU 구조 및 PDU 헤더별 필드 기능을 이해할 수 있다. 3. IP, ARP, RARP, ICMP 그리고 각 Routing 프로토콜 동작절차 및 취약점을 이해할 수 있다. 4. TCP, UDP, SSL, IPSec 프로토콜의 동작절차와 취약점을 이해할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
			5. 서비스 거부 공격 및 DDoS, DRDoS 공격 절차를 이해할 수 있다. 6. 무선 프로토콜 동작 구조 및 보안 취약점을 이해할 수 있다.
		3. 서비스별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 파악할 수 있다. 2. FTP 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 3. 메일 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 4. 웹 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 5. DNS 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 6. DB 서비스와 환경 설정, 보안 취약점을 이해할 수 있다. 7. 전자서명, 공개키 기반 구조 구성과 보안 특성을 이해할 수 있다.
		4. 보안장비 및 네트워크 장비별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 파악할 수 있다. 2. NIC, Hub, Switch, Bridge 장비의 역할과 동작을 이해할 수 있다. 3. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다. 4. Router 설정 절차 및 트래픽 통제 기능을 이해할 수 있다. 5. Firewall, IDS, IPS 보안 장비의 보안 서비스 및 설정 방법을 이해할 수 있다. 6. NAT 종류 및 동작 절차를 이해할 수 있다. 7. VPN 구현 방법 및 동작 절차를 이해할 수 있다. 8. 조직의 보안대상 관리시스템과 네트워크 장비를 파악할 수 있다. 9. 네트워크 구성도를 분석하여 사용 중인 IP 주소, 서브넷 등의 네트워크 정보를 파악할 수 있다. 10. SNMP를 이용한 원격관리기능과 스캐닝 도구를 이용한 관리대상시스템의 제공 서비스를 파악할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
	2. 취약점 점검 및 보완	1. 운영체제 및 버전별 취약점 점검, 보완하기	1. 불필요한 계정 존재 및 악성코드 설치여부에 대하여 점검·보완할 수 있다. 2. 운영체제별 보호 대상 객체(파일, 폴더) 권한 설정이 보안목표에 따라 설정되어 있는지 점검.보완할 수 있다. 3. 운영체제별 이벤트 로그정보 생성과 관리가 보안목표에 따라 설정되어 있는지 점검.보완할 수 있다. 4. 운영체제 종류 및 버전 정보가 불필요하게 노출되어 있는지 점검·보완할 수 있다. 5. 원격접속 및 원격관리 기능이 보안목표에 따라 설정되어 있는지 점검.보완할 수 있다. 6. 운영체제의 패치관리 또는 패치관리 시스템이 적절히 설정되어 있는지 점검·보완할 수 있다. 7. 보안운영체제(SecureOS)를 적절히 설정하고 운영할 수 있다.
		2. 서비스 버전별 취약점 점검, 보완하기	1. 조직에서 제공하지 않는 서비스가 동작하고 있는지 점검한 후 제거 할 수 있다. 2. 파일서버, FTP서버에 권한이 없는 사용자가 접근할 수 있게 설정되어 있는지, 각 사용자별로 접근할 수 있는 파일/폴더가 적절히 설정되어 있는지 점검할 수 있다. 3. 공유폴더에 적절한 접근통제가 보안목표에 적합한지 점검하며, 폴더가 불필요하게 공유되어 있는지 점검.보완할 수 있다. 4. 메일 서버 설정에서 스팸메일 릴레이가 허용되어 있는지, 메일 송수신 프로토콜(SMTP, POP, IMAP) 보안 설정이 적절한지 점검할 수 있다. 5. 웹 서버 설정에서 다양한 공격 유형들에 대비하여 보안 설정이 적절한지 점검할 수 있다. 6. DNS 서버 설정에서 불필요한 명령어 수행이 허가되어 있지 않은지, DNS 보안 조치가 적절히 설정되어 있는지 점검할 수 있다. 7. DB 서버 설정에서 중요 정보가 암호화되어 저장되고 있는지, DB객체(테이블, 칼럼, 뷰 등)별 접근통제가 적절히 설정되어 있는지 점검할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
		3. 보안장비 및 네트워크 장비 취약점 점검, 보완하기	1. Switch, Router 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다. 2. 침입차단시스템(Firewall) 장비 및 Router의 보안 설정(IP별 통제, Port별 통제, 사용자 ID별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 3. 침입탐지시스템(IDS) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 4. 침입방지시스템(IPS) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 5. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 6. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다. 7. WAF 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 8. AntiDDoS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 9. AntiAPT 또는 Sandbox 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
		4. 취약점 점검 및 보완 사항 이력 관리하기	1. 운영체제별 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 2. 조직에서 사용 중인 주요 서비스에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 3. 네트워크 장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안 취약점 및 보완사항을 기록할 수 있다. 4. 보안장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안 취약점 및 보완사항을 기록할 수 있다.
	3. 관제 및 대응	1. 관제하기	1. 조직의 보안목표에 따라 운영체제 및 버전별, 서비스별(FTP, 메일, WWW, DNS, DB 등) 보안 등 생성되는 로그 정보를 파악하고 로그 내용을 모니터링 및 통제할 수 있다. 2. 주요 보안장비(Firewall, IDS, IPS 등), 네트워크 장비(Switch, Router, 무선접속AP 등) 등에서 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성 수준, 구성요소 등을 설정 할 수 있다. 3. 최신 공격 및 대응기술에 대해 이해하고 모니터링 및 통제할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
		2. 대응하기	1. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별, 시간대별로 보안 로그정보를 통합, 분석할 수 있다. 2. 통합 보안로그를 정렬하여 내·외부 공격 시도 및 침투 여부 등 관련 정보를 수집 및 분석할 수 있다. 3. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 비정상 접근과 변경 여부를 확인 및 분석할 수 있다. 4. 업무 연속성을 위한 정보 및 보안 설정 정보를 백업 및 복구 등으로 대응할 수 있다. 5. 최신 공격 및 대응기술에 대해 이해하고, 분석 및 대응 정책을 수립 적용할 수 있다.
	4. 정보보호계획 수립	1. IT현황 및 자산 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 파악할 수 있다. 2. 보호대상 정보자산에 대한 기밀성, 무결성, 가용성 및 법적 준거성 등의 측면으로 중요도를 평가할 수 있다. 3. 보호대상인 정보자산을 식별하고 관리하며, 각 정보자산에 접근할 수 있는 사용자 또는 역할에 대한 정보를 수집, 분석할 수 있다.
		2. 조직의 요구사항 파악하기	1. 조직이 수행하는 핵심 비즈니스 내용 및 목적을 파악, 정리할 수 있다. 2. 컨설팅 대상 조직의 요구사항과 조직을 구성하는 물리적 환경 및 IT환경, 기업정보 및 (개인)정보보호 조직에 대한 정보를 수집할 수 있다. 3. 조직에서 제공하는 주요 서비스 및 네트워크 구조 정보를 수집할 수 있다.
		3. 관련법령 검토하기	1. 조직의 비즈니스 내용 및 보안목표 문서를 파악할 수 있다. 2. 조직의 비즈니스 내용과 관련된 법률 및 규정 정보를 파악할 수 있다. 3. 조직의 비즈니스 수행 중 발생될 수 있는 정보보호 의무사항 위반시 적용되는 법률 및 규정 정보를 수집할 수 있다. 4. 정보보호 관련 법률 및 규정을 준수하기 위해 필요한 조직의 물리적, 관리적 보호대책을 수립할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
	5. 위험분석	1. 조직의 내.외부 위협 요인 분석하기	1. 조직의 비즈니스 목표 및 세부 비즈니스 관련 문서를 파악할 수 있다. 2. 위험분석을 수행하기 위하여 전문인력 구성, 기간, 대상, 방법, 예산 등을 구체화한 위험관리계획을 수립하고 이행할 수 있다. 3. 조직의 IT환경의 시스템 및 네트워크 구성도 등 정보자산 현황을 파악할 수 있다. 4. 조직 내·외부 사용자로부터의 위협 요인을 분석할 수 있다. 5. IT환경을 구성하는 서버, 어플리케이션, DBMS, PC 등으로부터의 위협요인을 분석할 수 있다. 6. 조직의 네트워크를 구성하는 네트워크장비, 보안 장비로부터의 위협요인을 분석할 수 있다. 7. 정보보호 및 개인정보보호 관련 법적 준거성 위험을 식별할 수 있다. 8. 기타 국내외 정보보호 표준 등을 고려하여 기술적, 관리적, 물리적 위험을 식별할 수 있다.
		2. 조직의 H/W, S/W 등 정보 자산 취약점 분석하기	1. 조직의 H/W자산(PC, 서버, 네트워크 및 보안장비), S/W자산(운영체제, 상용 및 자가개발패키지), 정보자산(기업정보 및 고객정보) 및 기타 유무형의 정보(기업이미지 등)를 조사하고 식별할 수 있다. 2. 조직의 비즈니스 목표를 기준으로 보호대상 자산별 중요도를 결정할 수 있다. 3. IT환경을 구성하는 서버, 네트워크, DB, 어플리케이션, PC, 정보자산 등의 취약점을 분석할 수 있다.
		3. 조직의 정보자산 위협 및 취약점 분석 정리하기	1. 조직의 H/W자산(PC, 서버, 네트워크 및 보안장비)에 대한 중요도, 내.외부위협 및 취약점분석 내용을 정리할 수 있다. 2. 조직의 S/W자산(운영체제, 상용 및 자가 개발패키지)에 대한 중요도, 내.외부 위협 및 취약점분석 내용을 정리할 수 있다. 3. 조직의 정보자산(기업정보 및 고객정보)에 대한 중요도, 내.외부 위협 및 취약점분석 내용을 정리할 수 있다.
		4. 위험평가하기	1. 식별된 위험을 기반으로 위험도를 산정할 수 있다. 2. 조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별할 수 있다. 3. 위험식별 및 위험평가 결과를 경영진에게 보고할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
		5. 정보보호대책 선정 및 이행 계획 수립하기	1. 식별된 위험에 대한 처리 전략(위험감소, 위험회피, 위험전가, 위험수용 등)을 수립하고 위험처리를 위한 정보보호대책을 선정할 수 있다. 2. 정보보호대책의 우선순위를 정한 후에 일정, 예산 등을 포함하여 정보보호대책 이행계획을 수립하고 경영진에게 보고할 수 있다.
	6. 정보보호대책 구현	1. 정보보호 정책 수립 및 운영하기	1. 정보보호정책을 수립하고 경영진에게 승인을 받고 이를 조직원에게 공표하며, 주기적으로 정보보호 정책 및 관련 하위 규정에 대한 검토를 할 수 있다.
		2. 관리적 정보보호 대책 구현 및 운영하기	1. 조직의 주요 직무자를 지정하고 관리하며, 권한의 오남용 등으로 정보보호 이슈가 발생되지 않도록 직무 분리 등의 보안통제를 마련하고 비밀유지에 대한 서약서를 받을 수 있다. 2. 외부 업체 및 외부자와 계약시 보안 요구사항에 대한 사항을 이해하고 외부자가 업무를 수행함에 있어서 보안점검 등을 수행하고 계약 만료 시에 검토해야 할 사항을 이해할 수 있다. 3. 조직의 정보보호 교육 계획을 수립하고 교육의 대상(임직원 및 외부자 등)과 필요한 교육 내용(구현된 정보보호대책 운영 등)을 이해하고 교육 시행(정기, 수시) 및 관련 사항에 대한 평가를 수행할 수 있다. 4. 조직은 정보보호 및 법적 요구사항 등을 효과적으로 운영하고 있는지를 점검하기 위한 내부 감사를 이해할 수 있다.
		3. 물리적 정보보호 대책 구현 및 운영하기	1. 보호해야 할 물리적 보호구역 지정 및 보호설비가 갖추어야 할 요건 등을 이해할 수 있다. 2. 보호구역 내의 출입통제 방법 및 보호구역 내에서 작업 시 주의사항 등을 이해할 수 있다. 3. 물리적 보호구역 내의 중요 시스템 보호에 필요한 케이블 보호, 시스템 배치 및 관리를 이해할 수 있다. 4. 조직이 사용하고 있는 사무실 내의 개인업무 환경 및 공용업무 환경에 필요한 정보보호를 이해할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
		4. 기술적 정보보호 대책 구현 및 운영하기	1. 시스템 및 S/W 개발 시의 분석, 설계, 구현 및 이관의 생명주기에 맞게 필요한 개발과 운영환경 분리, 시험 데이터 보안, 소스 프로그램 보안 등에 관련된 사항을 이해할 수 있다. 2. 조직의 중요 정보를 보호하기 위하여 암호화 대상, 알고리즘, 키관리 등에 관련 기술적 보호대책 및 법적 요구사항을 이해할 수 있다. 3. 비인가자의 접근을 통제할 수 있는 접근통제(사용자 등록, 권한 부여, 접근권한 검토, 사용자 인증, 비밀번호 관리)에 기술적 사항을 이해할 수 있고 서버, 네트워크, 응용프로그램, 데이터베이스, 모바일기기 등에 대한 기술적 접근통제에 대한 사항을 이해할 수 있다. 4. 조직이 운영하고 있는 IT시스템의 도입, 성능 및 용량 관리, 장애관리, 변경관리, 원격운영, 무선네트워크 보안, 백업 관리 등에 시스템 운영에 대한 기술적 보호대책을 이해할 수 있다. 5. 바이러스 등의 악성코드로부터 정보시스템을 보호하고 이에 필요한 패치관리 등에 대한 사항을 이해할 수 있다. 6. 조직이 DDoS, 개인정보유출사고 등의 침해사고에 대하여 대응절차, 대응체계 구축, 침해사고 모의훈련, 침해사고 분석, 처리, 복구 등에 대한 기술적, 관리적 절차를 이해할 수 있다. 7. IT재해복구, 업무연속성 관리에 필요한 체계구축, 영향분석, 복구대책 수립, 모의훈련 등에 대한 사항을 이해할 수 있다.