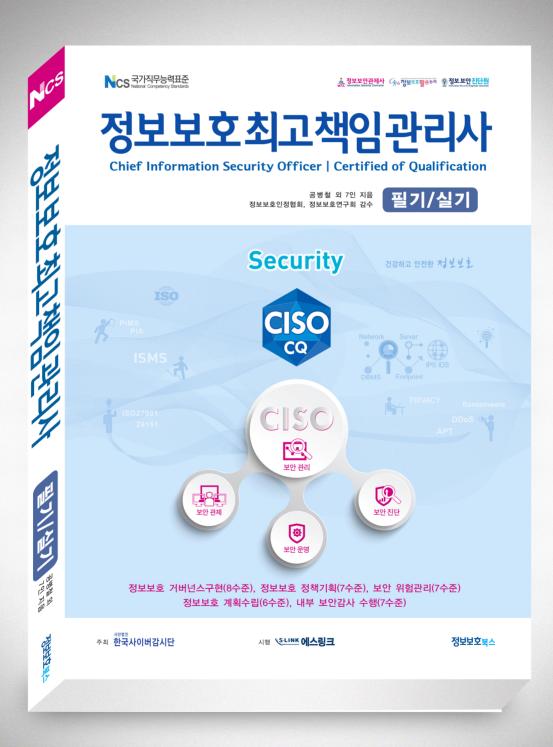
## 국내 최초 **정보보호 분야** 인재양성 전문출판사



- 2018. 11 -

## Security 정보보호복스 신간도서 안내





#### ■ 정보보호북스 신간 보도자료

### NCS 정보보호 부문 적용 민간자격 도서

# 정보보호최고책임관리사(필기/실기)



● 도서명 : 정보보호최고책임관리사 필기/실기

● 지은이 : 공병철 외 7인 공저

● 분 야 : 수험서 / 컴퓨터 자격증 수험서

● 쪽 수: 320쪽

● 판 형 : 사륙배판 변형(188\*256)

● 제 본: 무선

● 정 가:30,000원

● 컬 러 : 본문 2도

● 출간일 : 2018년 11월 15일

● ISBN: 979-11-964448-2-2 (93560)

● 출판사 : 정보보호북스

## NCS(국가직무능력표준) 기반 직무수행능력평가 교재

정보보호(정보보호 거버넌스 구현 8수준) 적용도서



우)06221) 서울시 강남구 테헤란로 216 신웅타워 12층 (역삼동 719-1) **Tel** 02)555-0816 **Fax** 070)7614-2221 **e-mail** sponet@nate.com

#### ■■■ 책 소개

#### NCS(국가직무능력표준) 기반 직무수행능력평가 교재!

이 책은 2015년 제정된 국가직무능력표준(NCS:National Competency Standards) 기반 채용 흐름은 2016년에 이르러 대부분의 공공기관으로 확산되어 향후 직무능력에 기반한 채용 제도가 확산되고는 추세이며, 2018년 대다수 공기업과 대기업들이 NCS와 블라인드 채용 제도에 동참하고 있으며, 정보보안산업계 또한 직무능력 중심의 채용제도로 전환하고 있습니다.

최근 국가 기반시설에 대한 사이버 위협의 증가와 공공기관과 기업의 중요정보(산업기밀, 영업정보, 인사정보, 개인정보)의 유출사고가 늘어나고 있으며, 정보시스템에 대한 랜섬웨어, DDoS, APT 공격 등 지능화된 사이버 공격이 확산됨에 따라 지능형 사이버위 협으로부터 침해대응을 위한 실시간 정보보안관제와 정보시스템 취약점 진단 등 정보자산의 안정적인 운영과 정보보호거버넌스 구현을 총괄 운영하는 데 필요한 전문인력의 필요성이 날로 증대되고 있습니다.

정부는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제45조의3(정보보호 최고책임자의 지정 등) 제1항에 의거 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호최고책임자를 지정하고 과학기술정보통신부장관에게 신고하고, 제3항에 의거 지정 및 신고 된 정보보호최고책임자는 다른 업무를 겸직할 수 없도록 명시하고 있습니다.

또한,「전자금융거래법」제21조의2(정보보호최고책임자 지정) 제1항에 의거 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하며, 제3항에 의거 총자산, 종업원 수 등을 감안하 여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 다른 정 보기술부문 업무를 겸직할 수 없도록 명시하고 있습니다.

이 책은 NCS 학습모듈에 의거 정보보호진단분석 세분류 능력단위인 정보보호 거버 넌스 구현(8수준), 정보보호 정책 기획(7수준), 보안 위험관리(7수준), 정보보호 계획 수립(6수준), 내부 보안 감사 수행(7수준) 등을 기반으로 하고있는 정보보호최고책임관리사 자격증 취득을 가장 체계적인 표준 수험서 교재로써 각 분야별 정보보호 및 정보보안 최고전문가가 참여하여 정보보호 & 개인정보보호 거버넌스구현, 정보보호 정책기획, 정보보호 계획수립, 보안 위험관리, 기술적(네트워크/애플리케이션/시스템)/관리적/물리적 보안운영, 보안 장비운용, 보안성 검토, 내부 보안감사 수행, 외주/협력사 보안관리등의 최신 경향분석을 기반으로 정보보호 전략, 정보보호 정책, 정보보호 계획, 위험관리 전략, 보안 감사 계획 등 총 5과목 필기시험 이론과 '정보보호 거버넌스 구현' 실무형 실기시험을 대비할 수 있도록 구성했습니다.



#### ■■■ 출판사 서평

#### 정보보호최고책임자 부문 국내 최초 NCS 적용 민간자격 수험서!

'정보보호최고책임자'는 조직의 정보 자산을 안정적으로 운영하는 데 필요한 관리적, 물리적, 기술적 보안 대책 수립과 안정적으로 운영하는데 필요한 지식 능력을 갖추었는지를 평가하고, 위험관리에 기반을 둔 정보보호 전략 및 정책, 활동 대책 도출, 내부 보안감사 수행 등 정보보호를 위한 자원을 확보하며 정보보호의 성과를 검토하고 관리하는 실무업무를 수행하는 능력을 가진 자를 말하며, 이러한 업무를 수행하는 이가 '정보보호최고책임관리사' 입니다.

'정보보호최고책임관리사(Chief Information Security Officer | Certified of Qualification)'는 정보시스템의 사이버 공격에 대한 예방과 신속한 대응을 위한 정보보안에 대한 전문지식과 운용 능력을 갖추고, 정보보호 관련 법률과 규제를 만족하는 조직의 정보보호관리체계 정책 기획수립 및 정보보호를 위한 자원 확보, 성과 검토, 주요 정보자산의 기밀성·무결성·가용성·관리 적정성을 점검 등의 거버넌스 구현하고 관리하는 업무 수행 능력을 가진 자를 말합니다.

정보보호최고책임관리사 자격검정은 조직의 주요 정보시스템 등 정보자산을 안정적으로 운영하기 위해 필요한 업무 수행 지식 능력을 갖추었는지를 평가하고, 정보보호 & 개인정보보호 거 버넌스구현, 정보보호 정책기획, 정보보호 계획수립, 보안 위험관리, 기술적(네트워크/애플리케이션/시스템)/관리적/물리적 보안운영, 보안 장비운용, 보안성 검토, 내부 보안감사 수행, 외주/협력사 보안관리 등 조직의 정보보호를 위한 자원 확보와 정보보호의 성과를 검토하고 관리하는 업무 수행에 필요한 지식, 기술, 태도에 대하여 전반적인 내용에 대한 시험문제가 출제 됩니다.

정보보호최고책임관리사 자격검정 시험은 필기시험과 실기시험으로 나누어지며, △응시자격은 기사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에 10년 이상 실무에 종사한 사람, 시험과목은 △이론 시험은 제1과목 정보보호 전략, 제2과목 정보보호 정책, 제3과목 정보보호 계획, 제4과목 위험관리 전략, 제5과목 보안 감사 계획으로 총 5과목을 평가하며 객관식 4지선다 100문항이 출제, △실무 시험은 주관식 필답형으로, 단답형 20문항(40점), 서술형 3문항(30점), 작업형 2문항(30점)으로 출제되며, 과목별로 주어진 사례 중심의문제해결을 통한 현장실무 능력을 평가, △시험시간은 90분 △합격기준은 100점 만점기준 60점이상 득점하여야 합니다.

자격시험과 관련한 더 자세한 내용은 홈페이지(www.ciso-cq.com)에서 확인할 수 있습니다.

구 분	과 목 명	문항수	검정시간	문제유형	합격기준
필기시험	1. 정보보호 전략	20문	90분	객관식 4지 택일형	60점
	2. 정보보호 정책	20문			
	3. 정보보호 계획	20문			
	4. 위험관리 전략	20문			
	5. 보안감사 계획	20문			
실기시험	정보보호 거버넌스 구현 실무	25문	120분	주관식 필답형	60점~ B레벨 85점~ A레벨



#### ■■■ 저자 소개

저자 : 공병철

(사)한국사이버감시단 대표이사, 정보보호인정협회 회장, ㈜에스링크 대표이사 ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : 김형구

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : 박종문

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자: 송병룡

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : 이원연

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : 오법영

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : **여동균** 

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : 조규호

정보보호인정협회 이사, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : **이근혁** 

정보보호연구회 부회장, ISMS-P 선임인증심사원, ISO 국제 인증심사원

저자 : **한철동** 

정보관리 기술사, ISMS-P 인증심사원, ISO 국제 인증 선임심사원

저자 : **김기환** 

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : 오원철

정보보호인정협회 부회장, ISMS-P 인증심사원, ISO 국제 인증심사원

저자 : **마기평** 

정보보호인정협회 이사, ISMS-P 인증심사원, ISO 국제 인증심사원

저자: **장진섭** 

정보보호인정협회 이사, ISMS-P 인증심사원, ISO 국제 인증심사원



#### ■■■이 책의 차례

#### 1편 정보보호 전략

1장 정보보호 전략 수립

1.1 거버넌스의 정의

chapter 1. 거버넌스의 개요 및 이해 chapter 2. 정보보호 거버넌스의 개요 및 프로세스 이해

1.2 전사적 정보보호 역할 및 책임

chapter 1. 정보보호 조직의 개념 및 구성

chapter 2. 정보보호 조직의 역할 및 책임

1.3 정보보호 환경 분석 및 요구사항 정의

chapter 1. 정보보호 환경 분석

chapter 2. 정보보호 요구사항 정의 및 분석

2장 정보보호 자원 할당

2.1 예산 및 인력 계획 수립

chapter 1. 정보보호 예산 수립

chapter 2. 정보보호 인력 구성 계획 수립

2.2 투자관리 및 사업대가 산정

chapter 1. 투자관리

chapter 2. SW 사업 대가

chapter 3. 컨설팅 사업 대가산정

2.3 조직편성 및 인적자원 관리

chapter 1. 조직 편성 및 협의체

chapter 2. 인적자원 관리

3장 정보보호 성과관리

3.1 정보보호 성과관리 개요

chapter 1. 성과 관리 이해

chapter 2. 정보보호 성과관리 이해

3.2 정보보호 성과 측정지표 및 평가

chapter 1. 정보보호 성과 측정지표

chapter 2. 정보보호 성과 측정지표의 사례

chapter 3. 정보보호 성과 측정 및 평가

#### 2편 정보보호 정책

1장 정보보호 정책 수립

1.1 정보보호 정책 개요

chapter 1. 정보보호 정책 체계

chapter 2. 정보보호 정책의 필요성

1.2 정보보호 정책 요구사항

chapter 1. 요구사항

chapter 2. 환경 분석

chapter 3. 정보보호 정책 요구사항 도출

1.3 정보보호 정책 수립

chapter 1. 정보보호 정책 수립 시 고려사항

chapter 2. 정보보호 정책 수립 절차

2장 정보보호 정책 유지 관리

2.1 정책 시행문서 이력관리

chapter 1. 정보보호 정책의 승인

chapter 2. 정보보호 정책의 공표

chapter 3. 정보보호 정책 관리 절차 수립

chapter 4. 상위 정책과의 연계성 및 정책시행 문서 수립

2.2 정책의 타당성 검토와 제/개정

chapter 1. 정보보호 컴플라이언스

chapter 2. 정보보호 정책의 타당성 및 영향도 부서

chapter 3. 정책의 유지관리

#### 3편 정보보호 계획

1장. 정보보호 목표 설정

1.1 정보보호 정책과 관리체계

chapter 1. 정보보호 정책 및 시행 문서 분석 chapter 2. 정보보호 관리체계 내의 관리대상

chapter 3. 관리적, 물리적, 기술적 정보보호 목표 설정

2장 정보보호 대상 범위 설정하기

2.1 정보보호 대상 범위 설정

chapter 1. 정보자산의 식별

chapter 2. 정보자산별 영향도 분석

chapter 3. 정보자산의 관리방안 수립

3장 정보보호 중장기 계획 수립하기

3.1 정보보호 중장기 계획 수립

chapter 1. 정보보호 중장기 목표 설정

chapter 2. 정보보호 대책 수립

chapter 3. 중장기 계획 수립

4장 정보보호 세부 실행 계획 수립하기

4.1 정보보호 세부 실행 계획 수립

chapter 1. 정보보호 실행 목표 설정

chapter 2. 정보보호 대책 및 지원 방안 수립

chapter 3. 정보보호 세무 실행 계획 수립

#### 4편 위험관리 전략

1장. 위험관리 계획 수립

1.1 위험관리 개요

chapter 1. 위험관리 원칙

chapter 2. 위험관리 프레임워크



chapter 3. 위험관리 프로세스

1.2 위험 식별

chapter 1. 위협, 취약점 및 위험

chapter 2. 위험의 상관관계

1.3 위험관리 계획 수립

chapter 1. 위험관리

chapter 2. 위험관리 계획 수립

#### 2장 위험분석

2.1 위험분석 관리 및 조사방법론

chapter 1. 위험분석 모델

chapter 2. 위험도 산정

2.2 위험분석 방법론

chapter 1. 브레인 스토밍

chapter 2. 인터뷰 (구조화 또는 반 구조화 인터뷰)

chapter 3. 델파이 기법

chapter 4. 체크리스트

chapter 5. HAZOP

chapter 6. SWIFT (Structured "What-if"

#### Technique)

chapter 7. 시나리오 분석

chapter 8. 비즈니스 영향 분석

chapter 9. 고장 모드 및 영향 분석 (FMEA)

chapter 10. 인과 관계 분석

chapter 11. 인간 신뢰도 평가 (HRA)

3장 위험분석 결과 조치

3.1 위험분석 결과 조치 방법론

chapter 1. 위험 처리

3.2 위험전략 소요비용 편익 분석

chapter 1. 비용 편익 분석(Cost-Benefit

### Analysis)

#### 5편 보안 감사 계획

1장. 보안감사 계획 수립

1.1 보안감사 기획

chapter 1. 보안감사의 정의 및 목적

chapter 2. 보안감사의 분류 및 정책 수립

chapter 3. 보안감사의 필요성 증가

1.2 감사대상과 범위 선정

chapter 1. 보안감사 대상과 범위 설정

chapter 2. 사전 예비 조사 수행

chapter 3. 보안감사 계획 수립

1.3 중점점검 항목 도출

chapter 1. 중점점검 항목 도출 프레임워크

chapter 2. 중점점검 항목 도출 및 작성

2장 보안감사 실행

2.1 보안감사 수행 체크리스트

chapter 1. 최종 체크리스트 작성 및 감사 자료 요청

2.2 인터뷰 및 감사일지 작성

chapter 1. 감사 일정을 고려한 범위 관리 방법 chapter 2. 감사 지적 사항의 정리 기법

2.3감사증적 수집 및 분석

chapter 1. 감사 목적 및 시정 조치 가능성을 고려한 컨설팅 기법

3장 보안감사 결과 보고

3.1 표준 감사보고서

chapter 1. 감사보고서 작성 기법

chapter 2. 시정 조치 관련 의사소통 방법

3.2 감사결과보고서 및 시정조치 보고서 요구

chapter 1. 감사결과보고서 작성 기법 3.3 감사 수행 결과에 대한 평가 및 교육

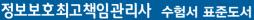
chapter 1. 시정 조치 결과의 적정성 판단 기법

#### 6편 부록

- 정보보호서비스 표준계약서
- 비밀유지 계약서
- 청렴계약 이행각서
- 개인정보의 안전 조치 기준 법률간의 주요내용 비교
- 정보보호시스템 및 네트워크 구성도
- 국제·국내 정보보호 인증제도 현황
- 해킹과 침해사고 및 정책 흐름 History Map



#### ■■■ 표지 이미지



조진의 주요 정보시스템 등 정보자산을 안정적으로 운영하기 위해 필요한 업무 수행 지식 능력을 갖추었는지를 평가하고 정보보호 거버넌스구현, 정책기획, 계획수립, 보안 위험관리, 기술적(네트워크/애플리케이션/시스템)/관리적/물리적 보안운영. 보안 장비운용, 보안성 검토, 내부 보안감사 수행, 외주/협력사 보안관리 등 조직의 정보보호를 위한 자원 확보와 정보보호의 성과를 검토하고 관리하는 업무를 수행하기 위한 이해 능력을 갖추고 있는지에 대한 실무기능 평가

#### 「정보통신망 이용촉진 및 정보보호 등에 관한 법률

제45조의3 (정보보호 최고책임자의 지정 등) 제1항에 의거 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호최고책임자를 지정하고 과학기술정보통신부장관에게 신고하고, 제3항에 의거 지정 및 신고 된 정보보호최고책임자는 다른 업무를 겸직할 수 없다.

#### 『전자금융거래법

제21조의2 (정보보호최고책임자 지정) 제1항에 의거 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 임원급의 정보보호최고책임자를 지정하며, 제3항에 의거 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 다른 정보기술부문 업무를 겸직할 수 없다.

주최 한국사이버감시단 시형 **오나마 에스링크** 후원 승민간사이버안전지원센터

감수 @ 정보보호인정협의 등 정보보호인구의 및 지능정보**보안아카데미** 



NCS 국가직무능력표준

Ncs

♣ 정보보안관계사 (g)⇔정보보호합용## 및 정보보안진단원

Chief Information Security Officer | Certified of Qualification

공병철 외 7인 지음 필기/실기 정보보호인정협회, 정보보호연구회 감수



주최 한국사이버감시단 시행 (SLINK 에스링크 저나나하늘人







NCS 국가직무능력표준

☆ 정보보안관제사 영화 South Controller Grant Specific S

## 정보보호최고책임관리사

Chief Information Security Officer | Certified of Qualification

공병철 외 7인 지음 정보보호인정협회, 정보보호연구회 감수





필기/실기

정보보호북스



<sup>사단법인</sup> 주최 **한국사이버감시단** 

시행 **& LINK 에스링크** 

정보보호북스

### ■■■ 도서 구입처

- http://www.yes24.com/24/Goods/66913143
- https://www.aladin.co.kr/shop/wproduct.aspx?ltemId=174002253
- http://www.kyobobook.co.kr/product/detailViewKor.laf?ejkGb=KOR&barcode=9791196444822
- $\ http://book.interpark.com/product/BookDisplay.do?\_method=detail\&sc.shopNo=0000400000\&sc.dispNo=001\&sc.pr\\ \ dNo=296747694$

NCS(국가직무능력표준) 기반 민간자격 수험서!

## 정보보호최고책임관리사 필기/실기

2018년 11월 09일 초판 1쇄 인쇄 2018년 11월 12일 초판 1쇄 발행

지 은 이 : 공 병 철 외 7인

**펴 낸 이** : 공 병 철

진 행: 정보보호북스 출판기획팀

**펴 낸 곳**: 정보보호북스 (info@ciso-cq.com)

홈페이지: www.ciso-cq.com

**주 소**: 06221) 서울시 강남구 테헤란로 216 신웅타워 12층 (역삼동 719-1)

전 화: 02) 555-0816 팩 스: 070) 7614-2221

**발행자번호**: 964448

Copyright ⓒ 공병철, 김형구, 박종문, 송병룡, 이원연, 오법영, 여동균, 조규호 2018, Printed in Seoul, Korea

본 도서는 저작권법에 의해 보호를 받는 저작물이므로 내용을 무단으로 복사, 복제, 전제 및 발췌하는 행위는 저작권법에 저촉되며, 민형사상의 처벌을 받게 됩니다.

정가 30,000원

ISBN 979-11-960000-2-2 (93560)