# CISSP®

# Practice Exams

## Fifth Edition

Fully revised for the 2018 CISSP Body of Knowledge

■

Hundreds of practice questions covering all 8 Certfied Information Systems Security Professional exam domains

■

Written by leading IT security certification and training experts

Digital content includes:

1000+ multiple-choice practice exam questions

■

Hotspot and drag-and-drop practice exam questions

SHON HARRIS, CISSP
JONATHAN HAM, CISSP, GSEC, GCIA, GCIH

# CISSP®
# Practice Exams

# ABOUT THE AUTHORS

**Shon Harris, CISSP,** was the founder and CEO of Shon Harris Security LLC and Logical Security LLC, a security consultant, a former engineer in the Air Force's Information Warfare unit, an instructor, and an author. Shon owned and ran her own training and consulting companies for 13 years prior to her death in 2014. She consulted with Fortune 100 corporations and government agencies on extensive security issues. She authored three best-selling CISSP books, was a contributing author to *Gray Hat Hacking: The Ethical Hacker's Handbook* and *Security Information and Event Management (SIEM) Implementation*, and a technical editor for *Information Security Magazine*.

**Jonathan Ham, CISSP, GSEC, GCIA, GCIH, GMON,** is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through team selection and training, to implementing scalable prevention, detection, and response technologies and techniques. With a keen understanding of ROI and TCO (and an emphasis on real-world practice over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small startups to the Fortune 50, and the U.S. Department of Defense across multiple engaged forces.

Mr. Ham has been commissioned to teach investigative techniques to the NSA, has trained NCIS investigators how to use intrusion detection technologies, has performed packet analysis from a facility more than 2,000 feet underground, and has chartered and trained the CIRT for one of the largest U.S. civilian federal agencies.

In addition to his professional certifications, Mr. Ham is a Principal Instructor and Author with the SANS Institute, and is a member of the GIAC Advisory Board. He has also consistently been the highest rated trainer at Black Hat events, teaching his course on Network Forensics. His groundbreaking textbook on the topic established him as a pioneer in the field.

A former combat medic with the U.S. Navy/Marine Corps, Mr. Ham has spent over a decade practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross, as both a Senior Patroller and Instructor and a Professional Rescuer.

### A Note from Jonathan

Shon and I never met in person, though my career has been inextricably linked to hers for more than a decade. The first time I was ever asked to teach a class for the SANS Institute was because Shon was scheduled and couldn't make it. I went on to teach SANS' extremely popular CISSP prep course (Mgt414) dozens of times, and my students routinely brought her books to my classroom.

As a result, I've gone on to teach thousands of students at both the graduate and post-graduate level, across six continents and in dozens of countries, and involving content ranging from hacking techniques to forensic investigations. Thanks to Shon, I am truly living the dream and giving it back in every way that I can.

I am also extremely honored to have been asked by McGraw-Hill Education to continue her work. We had so very many friends in common that nearly everyone I know professionally encouraged me to do it. She will be remembered with the respect of thousands of CISSPs.

And mine.

## About the Technical Editor

**Daniel Carter, CCSP, CISSP, CISM, CISA,** is currently working as a senior systems engineer at Johns Hopkins University & Medicine. An IT security and systems professional for almost 20 years, Daniel has worked extensively with web-based applications and infrastructure, as well as LDAP and federated identity systems, PKI, SIEM, and Linux/Unix systems. He is currently working with enterprise authentication and single sign-on systems, including cloud-base deployments. Daniel holds a degree in criminology and criminal justice from the University of Maryland and a master's degree in technology management, with a focus on homeland security management, from the University of Maryland, University College.

*This page intentionally left blank*

# CISSP®
# Practice Exams

## Fifth Edition

Shon Harris
Jonathan Ham


New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-1-26-014266-2
MHID: 1-26-014266-3

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-014267-9,
MHID: 1-26-014267-1.

eBook conversion by codeMantra
Version 1.0

It has been at the expense of my tribe that I have managed to continue Shon's work. I honor them by name here, as elsewhere:

436861726C6965204D617269652048616D0D0A
56696F6C65742044616E67657220576573740D0A
5468756E646572204772657920576573740D0A
50616F6C6120436563696C6961204761726961204A756172657A0D0A

They are beautiful and brilliant each, and ~~are~~ *continue to be* loved more than they may ever know, *through each of these revisions, and their own*.

—*Jonathan Ham*, ~~April 13, 2016~~ August 1, 2018

*This page intentionally left blank*

# CONTENTS

# PREFACE

The preface for the previous edition of this book began as follows:

> *Computer, information, and physical security are becoming more important at an exponential rate. Over the last few years, the necessity for computer and information security has grown rapidly as cyber attacks have increased, financial information is being stolen at a rapid pace, cyber warfare is affecting countries around the world, and today's malware is growing exponentially in its sophistication and dominating our threat landscape. The world's continuous dependency upon technology and the rapid increase in the complexities of these technologies make securing them a challenging and important task.*

That was published roughly two years ago but still holds true today. If anything, the problems confronting information security professionals are more daunting than ever before.

A lot has happened in the world of information security since the previous edition was published in 2016, including some of the most notorious incidents and events in our sordid history. In the summer of 2016 an organization of Russian state-affiliated malicious actors calling themselves The Shadow Brokers (TSB) emerged publicly, and by March 2017 began pedaling zero-day exploits and hacking tools ostensibly stolen from the U.S. National Security Agency (NSA). Most famous among these involved a very old but previously unannounced vulnerability in version 1 of Microsoft's Server Message Block implementation (SMBv1), dubbed "EternalBlue." Microsoft immediately issued a patch for the issue (MS17-010)—out of cycle in order to try to assist its customers in getting ahead of the threat—but adoption was slow, and EternalBlue remains a nightmare of rather epic proportions.

The first widespread exploitation of this flaw was with the DoublePulsar back-door implant, which began spreading rapidly by April 2017 and which compromised at least 100,000 systems worldwide, though to very little fanfare. In May 2017, however, the WannaCry ransomware attack emerged targeting the same largely unpatched flaw. In December 2017 the U.S. government formally placed the blame for this campaign on North Korean actors, and some estimates of the worldwide damage from it top US$4B.

Somewhat predictably, the NotPetya attack followed in June 2017, again leveraging the same vulnerability, but used only one minor vector as its initial means of intrusion. This malware more notably stole credentials for lateral movement throughout compromised organizations, leveraging tools commonly used by Active Directory domain administrators to "live off the land" as it spread internally. Initially assumed to be another ransomware effort, the NotPetya attack is now widely understood to have been a supply-chain-based denial-of-service (DoS) attack on Ukraine that was nation-state sponsored, with worldwide collateral damage. Shipping transport companies FedEx and Maersk have reputedly suffered over US$300M in damages each.

But perhaps the most notorious event in our recent history was the Equifax breach, which in hindsight was instructive on just about every conceivable level. This time the vulnerability was in the Internet-facing use of the Apache Struts web app framework, for which patches had been available for months. The result was the loss of sensitive personal and financial records of over

145 million consumers—most likely just about any U.S. citizen with a credit score, and many millions of others. Through the details of this event we were able to see failures in executive leadership, security processes and procedures for defensive posture, intrusion detection, incident response, and ultimately gross failures in public relations as well. Everything that could have gone wrong, at any stage, went wrong.

Among the ultimate results of this event were the departure of the CEO and other top-level executives of Equifax, and federal criminal indictments of several Equifax executives by the U.S. government for insider-trading violations, for allegedly dumping company stock upon learning of the breach but prior to its public announcement. The departed CEO, Richard Smith, was called by the U.S. Congress to testify publicly on the matter. This was followed by Facebook's founder and CEO Mark Zuckerberg's public U.S. Senate testimony in April 2018 about yet another (unrelated) very high-profile data breach involving Facebook.

On and on it goes, and we've only just scratched the surface.

So what is to be done? What is required is a better educated, better informed, and hence better prepared workforce of information security professionals to lead the charge, and to implement the changes that we as an industry—apparent evidence to the contrary—actually *do* know how to effect. The task falls to every last one of us to rise to this challenge, and to make a difference in the equation, everywhere we possibly can. It starts and ends with us.

You have in your hand a whole lot of answers. There are an equal number of questions posed to you as well, but it is the answers you need to understand, and why the correct ones are correct, and the incorrect ones are not. If you can master the questions and answers in this volume, you should have little difficulty passing the CISSP certification exam (also newly revised) to demonstrate your knowledge to others in a somewhat shorthand manner, as a CISSP.

That, however, is just another step in a longer journey of what is required of you. Accomplish that step, then take the next, which is to get back out into the field, share what you have learned, and put what you know to work.

# INTRODUCTION

The objective of this book is to prepare you for the CISSP exam by familiarizing you with the more difficult types of questions that may come up on the exam. The questions in this book delve into the more complex topics of the CISSP Common Body of Knowledge (CBK) that you may be faced with when you take the exam.

This book has been developed to be used in tandem with the *CISSP All-in-One Exam Guide, Eighth Edition*, both of which have been thoroughly revised since their last editions to reflect the most recent revision of the CISSP exam in 2018. The best approach to prepare for the exam using all of the material available to you is outlined here:

1. Review the questions and answer explanations in each chapter.
2. If further review is required, read the corresponding chapter(s) in the *CISSP All-in-One Exam Guide, Eighth Edition.*
3. Review all of the additional questions that are available. See the "Additional Questions Available" section at the end of this introduction.

Because the primary focus of this book is to help you pass the exam, the questions included cover all eight CISSP exam domains. Each question features a detailed explanation as to why one answer choice is the correct answer and why each of the other choices is incorrect. Because of this, we believe this book will serve as a valuable professional resource after your exam.

## In This Book

This book has been organized so that each chapter consists of a battery of practice exam questions representing a single CISSP exam domain, appropriate for experienced information security professionals. Each practice exam question features answer explanations that provide the emphasis on the "why" as well as the "how-to" of working with and supporting the technology and concepts.

## In Every Chapter

Included in each chapter are features that call your attention to the key steps of the testing and review process and that provide helpful exam-taking hints. Take a look at what you'll find in every chapter:

- Every chapter includes practice exam questions from one **CISSP CBK Security Domain**. Drill down on the questions from each domain that you will need to know how to answer in order to pass the exam.
- The **Practice Exam Questions** are similar to those found on the actual CISSP exam and are meant to present you with some of the most common and confusing problems that

you may encounter when taking the actual exam. These questions are designed to help you anticipate what the exam will emphasize. Getting inside the exam with good practice questions will help ensure you know what you need to know to pass the exam.

- Each chapter includes a **Quick Answer Key**, which provides the question number and the corresponding letter for the correct answer choice. This allows you to score your answers quickly before you begin your review.
- Each question includes an **In-Depth Answer Explanation**—explanations are provided for both the correct and incorrect answer choices and can be found at the end of each chapter. By reading the answer explanations, you'll reinforce what you've learned from answering the questions in that chapter, while also becoming familiar with the structure of the exam questions.

## Additional Questions Available

In addition to the questions in each chapter, there are more than 1,500 multiple-choice practice exam questions available to you. Also available are simulated hotspot and drag-and-drop questions. For more information on these question types and how to access them, please refer to the appendix.

CHAPTER

# Security and Risk Management

This domain includes questions from the following topics:

- Security terminology and principles
- Protection control types
- Security frameworks, models, standards, and best practices
- Computer laws and crimes
- Intellectual property
- Data breaches
- Risk management
- Threat modeling
- Business continuity and disaster recovery
- Personnel security
- Security governance

A security professional's responsibilities extend well beyond reacting to the latest news headlines of a new exploit or security breach. The day-to-day responsibilities of security professionals are far less exciting on the surface but are vital to keeping organizations protected against intrusions so that they don't become the next headline. The role of security within an organization is a complex one, as it touches every employee and must be managed companywide. It is important that you have an understanding of security beyond the technical details to include management and business issues, both for the CISSP exam and for your role in the field.

## QUESTIONS

1. Which of the following best describes the relationship between COBIT and ITIL?
   - **A.** COBIT is a model for IT governance, whereas ITIL is a model for corporate governance.
   - **B.** COBIT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.
   - **C.** COBIT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.
   - **D.** COBIT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals.
2. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?
   - **A.** Committee of Sponsoring Organizations of the Treadway Commission
   - **B.** The Organisation for Economic Co-operation and Development
   - **C.** COBIT
   - **D.** International Organization for Standardization
3. Steve, a department manager, has been asked to join a committee that is responsible for defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What committee is he joining?
   - **A.** Security policy committee
   - **B.** Audit committee
   - **C.** Risk management committee
   - **D.** Security steering committee
4. Which of the following is not included in a risk assessment?
   - **A.** Discontinuing activities that introduce risk
   - **B.** Identifying assets
   - **C.** Identifying threats
   - **D.** Analyzing risk in order of cost or criticality
5. The integrity of data is not related to which of the following?
   - **A.** Unauthorized manipulation or changes to data
   - **B.** The modification of data without authorization
   - **C.** The intentional or accidental substitution of data
   - **D.** The extraction of data to share with unauthorized entities

6. As his company's CISO, George needs to demonstrate to the board of directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?

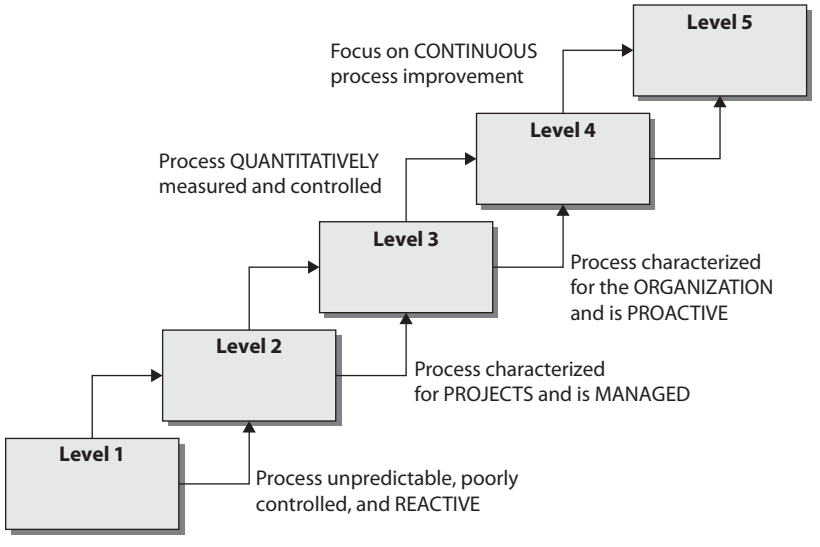
   **A.** threats × vulnerability × asset value = residual risk

   **B.** SLE × frequency = ALE, which is equal to residual risk

   **C.** (threats × vulnerability × asset value) × controls gap = residual risk

   **D.** (total risk – asset value) × countermeasures = residual risk

7. Capability Maturity Model Integration (CMMI) came from the software engineering world and is used within organizations to help lay out a pathway of how incremental improvement can take place. This model is used by organizations in self-assessment and to develop structured steps that can be followed so an organization can evolve from one level to the next and constantly improve its processes. In the CMMI model graphic shown, what is the proper sequence of the levels?



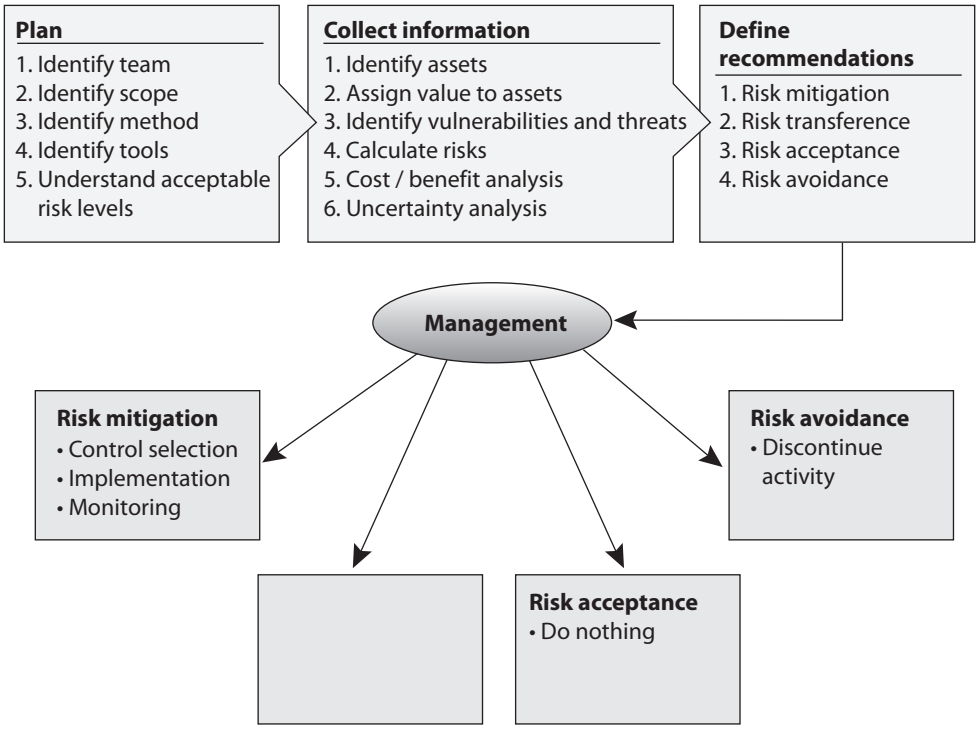

   **A.** Initial, Defined, Managed, Quantitatively Managed, Optimizing

   **B.** Initial, Defined, Quantitatively Managed, Optimizing, Managed

   **C.** Defined, Managed, Quantitatively Managed, Optimizing

   **D.** Initial, Repeatable, Defined, Quantitatively Managed, Optimizing

8. Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?
   - **A.** FAP
   - **B.** OCTAVE
   - **C.** AS/NZS 4360
   - **D.** NIST SP 800-30
9. Which of the following is not a characteristic of a company with a security governance program in place?
   - **A.** Board members are updated quarterly on the company's state of security.
   - **B.** All security activity takes place within the security department.
   - **C.** Security products, services, and consultants are deployed in an informed manner.
   - **D.** The organization has established metrics and goals for improving security.
10. There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?



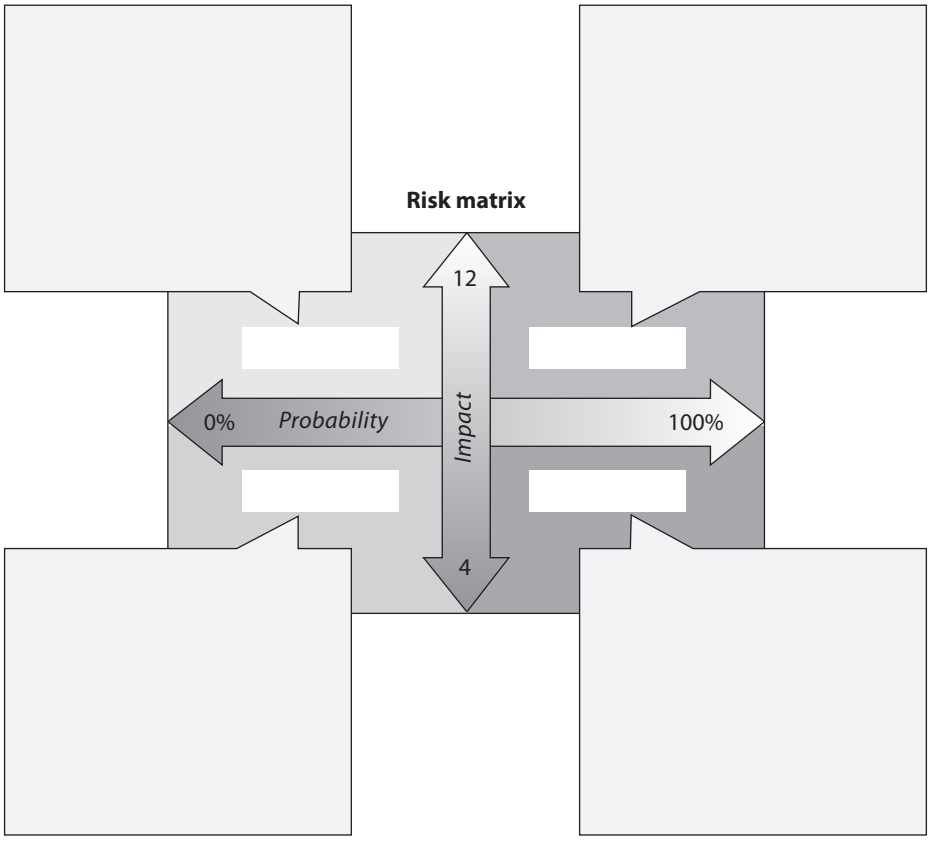
**A.** Risk transference. Share the risk with other entities.

**B.** Risk reduction. Reduce the risk to an acceptable level.

**C.** Risk rejection. Accept the current risk.

**D.** Risk assignment. Assign risk to a specific owner.

**11.** The following graphic contains a commonly used risk management scorecard. Identify the proper quadrant and its description.



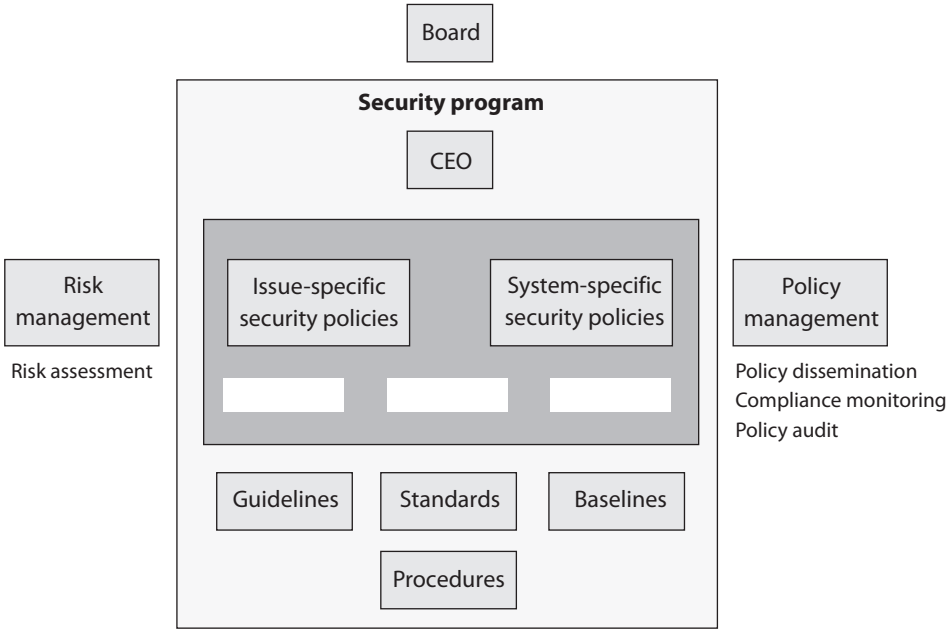

**A.** Top-right quadrant is high impact, low probability.

**B.** Top-left quadrant is high impact, medium probability.

**C.** Bottom-left quadrant is low impact, high probability.

**D.** Bottom-right quadrant is low impact, high probability.

**12.** What are the three types of policies that are missing from the following graphic?




**A.** Regulatory, Informative, Advisory

**B.** Regulatory, Mandatory, Advisory

**C.** Regulatory, Informative, Public

**D.** Regulatory, Informative, Internal Use

**13.** List in the proper order from the table shown the learning objectives that are missing and their proper definitions.

| | **Awareness** | **Training** | **Education** |
|---|---|---|---|
| **Attribute:** | "What" | "How" | "Why" |
| **Level:** | Information | Knowledge | Insight |
| **Learning objective:** | | | |
| **Example teaching method:** | **Media**<br>• Videos<br>• Newsletters<br>• Posters | **Practical instruction**<br>• Lecture and/or demo<br>• Case study<br>• Hands-on practice | **Theoretical instruction**<br>• Seminar and discussion<br>• Reading and study<br>• Research |
| **Test measure:** | True/False<br>Mutiple choice<br><br>(Identify learning) | Problem solving, i.e., recognition and resolution<br><br>(Apply learning) | Essay<br><br>(Interpret learning) |
| **Impact timeframe:** | Short-term | Intermediate | Long-term |

**A.** Understanding, recognition and retention, skill

**B.** Skill, recognition and retention, skill

**C.** Recognition and retention, skill, understanding

**D.** Skill, recognition and retention, understanding