CISSP
Getting your CISSP

June 2020

Jeff Hoskins

CISSP, CISM, MBA, PMP

Agenda

- What is the CISSP?
- Why?
- How?
- Cheap?

Disclaimer: the presentation is for informational purposes only and is meant to provide a head start on pursuing certification. To pursue certification, you should read the materials directly from ISC^2. All opinions expressed are those of the speaker and do not necessarily represent the views of any organization.

- Save Money
- Save Time
- Be Confident

Who is this presentation for?

- Are you thinking about the CISSP?
- Are you concerned about passing?
- Are you concerned about funding?
- Are you considering the CISSP for developing others?

So… What now? Where do I start?

What is the CISSP?

Certified Information Systems Security Professional

Founded in 1988, the International Information System Security Certification Consortium, or (ISC)², is a non-profit organization which specializes in training and certifications for cybersecurity professionals. It has been described as the "world's largest IT security organization". The most widely known certification offered by (ISC)² is the Certified Information Systems Security Professional certification.

Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program. With a CISSP, you validate your expertise and become an (ISC)² member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

Descriptions from https://www.isc2.org/

What is the CISSP?

Certified Information Systems Security Professional

Founded in 1988, the International Information System Security Certification Consortium, or (ISC)², is a non-profit organization which specializes in training and certifications for cybersecuri ionals. It has been described as the "world's large ion". The most widely known certifica rtified Information Systems S .

Earni what it takes to effectively design, imple best-in-class cybersecurity program. With a CISSP, idate your expertise and become an (ISC)² member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

Blah Blah

- Shows experience and exposure
- Could be a “Checkbox” to apply
- Gold Standard InfoSec Cert
- Security Advisor
- Broad – not deep
- Does not indicate expertise
- Not technical

Descriptions from https://www.isc2.org/

Why the CISSP?

- Self Growth
- Position Requirement
- Skills Gap
- Opportunities
- Confidence

How to get the Cert?

- 5 Years Experience including 2 or more Domains

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

- Book knowledge – Broad not Deep

- No magic needed

What does the Cert Cost?

1. Books
2. Bootcamp
3. Travel, Lodging, Food
4. Missed Work
5. Test Cost
6. Hassle
7. Fees to ISC^2

The path people recommended to me would have cost over $7,000.

I spent less than $900 (which includes $825 in fees to ISC^2)

How do I get certified?

1. Confirm you have the required experience
2. Register for the test ($699)
3. Pass the test
4. Contact a Sponsor (current CISSP, or apply for ISC^2 to sponsor you)
5. Submit the Sponsor's Information
6. Allow time for processing (A very long 6 weeks)
7. Received Acceptance Notification
8. Pay Fee ($125) (Credential is made official immediately upon payment)
9. Continue to Pay Annual Fee until Retirement
10. CPEs
11. Advance the profession – help others

CISSP Experience Requirements

Candidates must have a **minimum of five years** cumulative paid work experience in **two or more of the eight domains.** Your work experience must fall within two or more of the eight domains of the (ISC)² CISSP CBK:

Domain 1. Security and Risk Management
Domain 2. Asset Security
Domain 3. Security Architecture and Engineering
Domain 4. Communication and Network Security
Domain 5. Identity and Access Management (IAM)
Domain 6. Security Assessment and Testing
Domain 7. Security Operations
Domain 8. Software Development Security

You may satisfy one year of required experience via a relevant 4-year degree or another approved security credential.

You can pass the exam without the experience to obtain the Associate level credential.

What experience is relevant? – See ISC² requirements at - https://www.isc2.org/Certifications/CISSP/Experience-Requirements

How does the test work?

CISSP (English)

- Register and Pay $699 for the test (not cheap – this is the biggest fee and is unavoidable)
- Up to 3 Hours
- 100 – 150 multiple choice and advanced innovative items (some multi-select questions)
- 25 of the first 100 questions are for research only

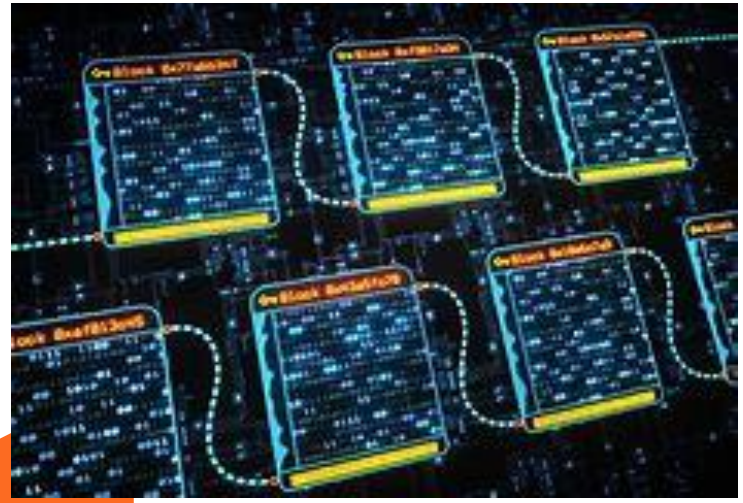
- Adaptive Format (cannot go back)
  - Answer questions right – test moves on to a new topic faster
  - Answer questions wrong – get more questions from the same topic
  - Test is looking for mastery of the topic before moving on

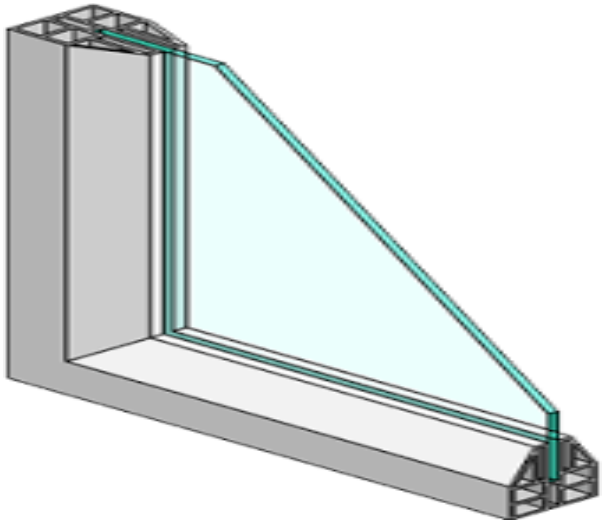
- Test ends somewhere at 100 to 150 questions
  - Prove mastery = test ends
  - Prove statistically that you will not pass = test ends

Next Up – How do you pass the exam?

★If you prefer the 250 question, 6 hour test – Look into the Non-English exam offerings.

I developed a Next Gen Solution



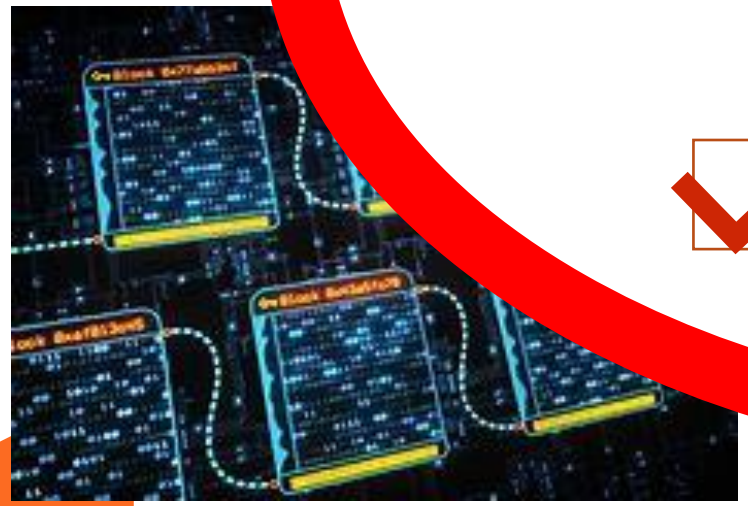


Using –

- AI
- Deep Learning
- Blockchain

All in a single pane of glass

I developed a Next Gen Solution



This is not true!

Conference Buzz Word
Requirement Completed

ng

of glass

Prepare for the Test – First thing – Know the Code

(ISC)² Code Of Ethics

Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons (order is important):

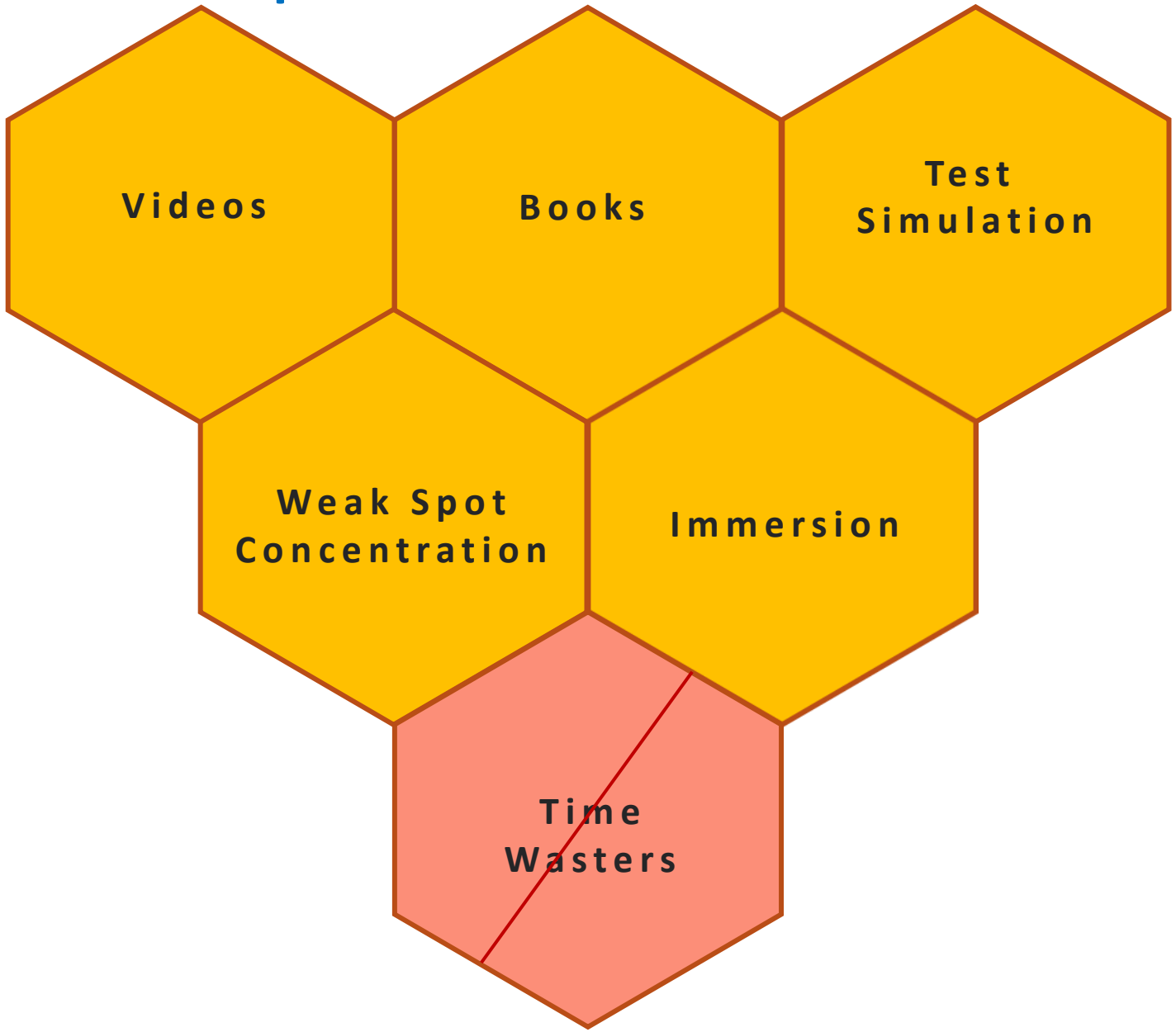
- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

- Don't Steal Training Materials

- Know the Code of Ethics – and the order of the canons
- More detail at https://www.isc2.org/Ethics
- I will not tell you the questions I saw or how they were written.

https://www.isc2.org/Ethics

Use multiple sources for well-rounded test preparation



3 Free Video Series (about 50 hours)

CYBRARY

FRSECURE®

CBTnuggets

These are 3 video sources that take you through all domains to prep for the CISSP exam.

- *Cybrary – Kelly Handerhan CISSP Series https://app.cybrary.it/browse/course/cissp
- FRSecure – CISSP Mentor Program https://frsecure.com/cissp-mentor-program/
- **CBT Nuggets – CISSP Series https://www.cbtnuggets.com/certification-playlist/(ISC)2/cissp-2018

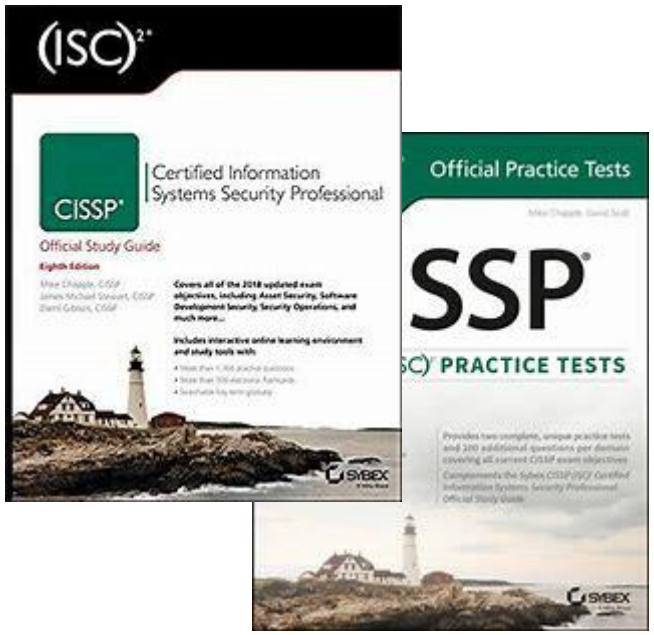
Don’t pay for bootcamp!

*Since the original date for this conference, I have heard that Cybrary may have removed Kelly’s videos from their free offerings, but check the site. Also, note that Cybrary is always running discounts.

**At CBT Nuggets – the first 7 days is free. You must provide a credit card and elect for auto-renewal, but you can cancel easily at anytime by turning off auto-renewal.

The books you need

Many people recommend various books – these are the ones I bought and I recommend.

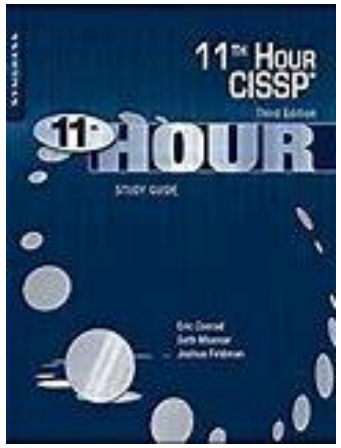


~$50 (package of 2 books)

CISSP Official Study Guide 8th Edition plus Official Practice Tests

Mike Chapple, James Michael Stewart, Darill Gibson

Pros – "official source", comes with instruction for online test simulator
Con – Sleeping aid



~$20

11th Hour CISSP Study Guide 3rd Edition

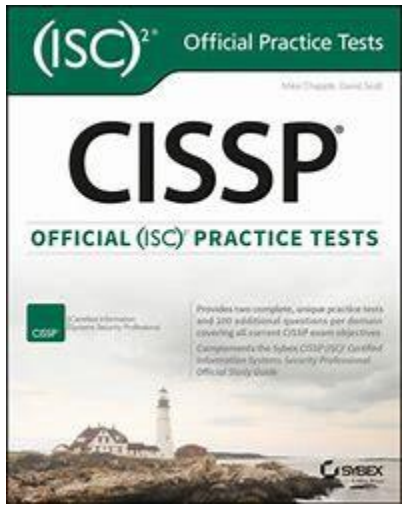
Eric Conrad, Seth Misenar, Joshua Feldman

Pros – Concise and readable
Con – Is it too brief?

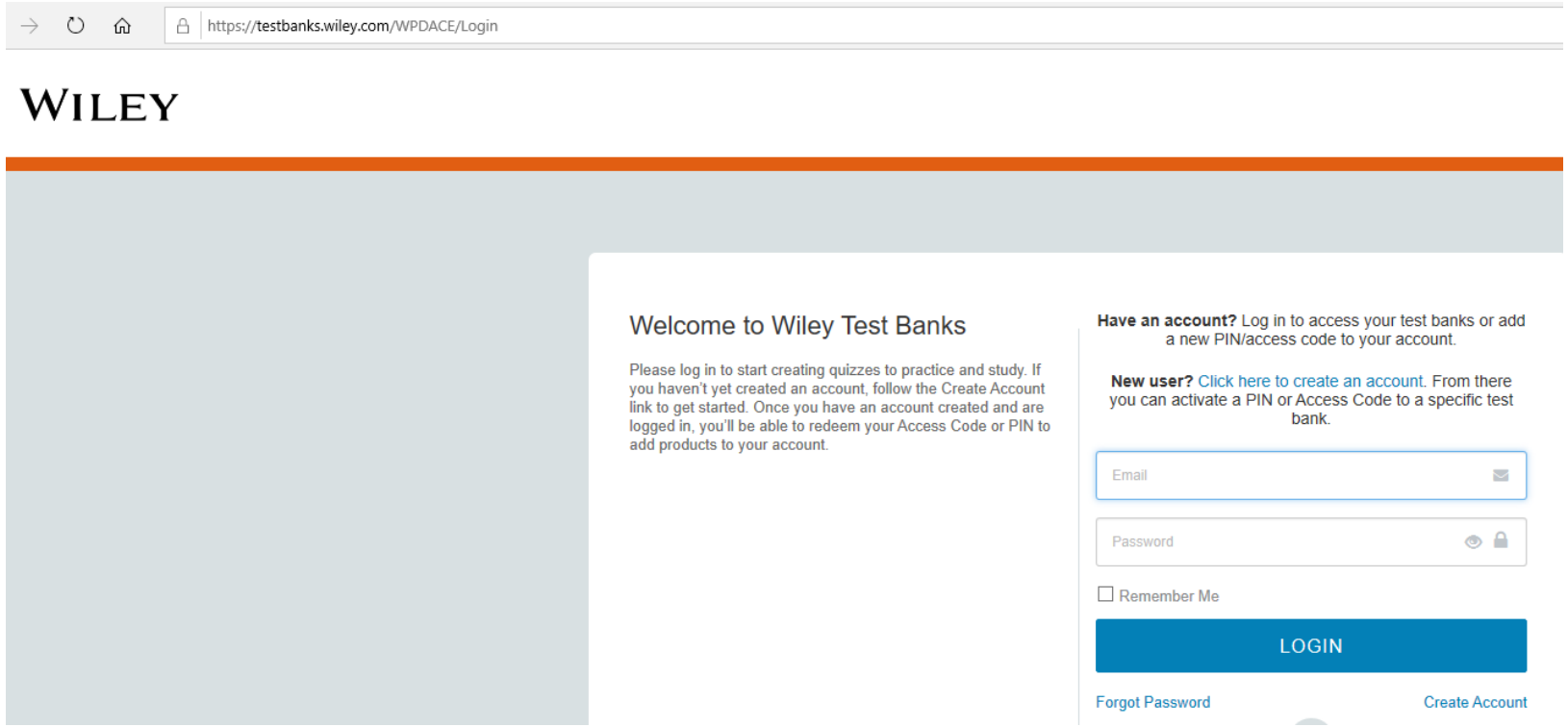
Note – I bought from Amazon. I don't have an affiliate code and I do not benefit in anyway from your purchases.

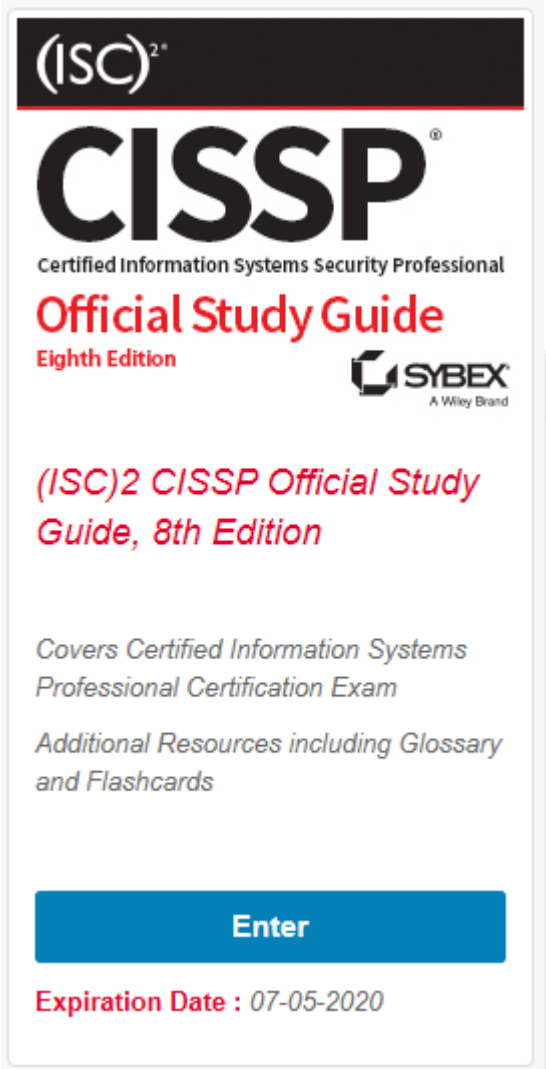
Block your time and distractions for practice tests

Do the questions – read the explanations where you responded correctly or incorrectly.



Instructions in the book tell you how to get a 12 month account at Wiley.

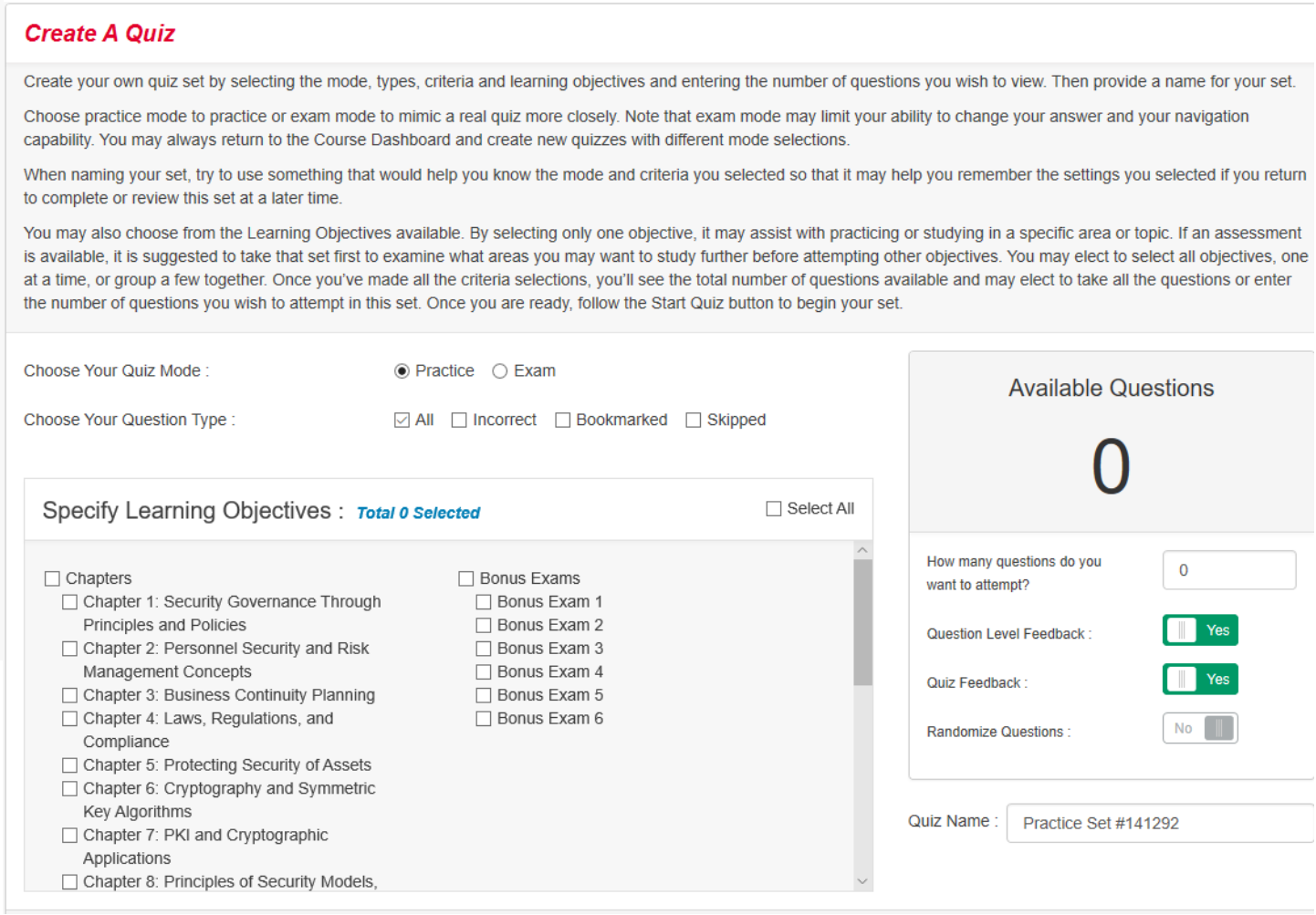




Wiley/Sybex Test Simulator

Pros – Good questions, similar difficulty to exam, “official”

Cons – Explanations of the right answer are not enough



Example of explanations of answers (Wiley/Sybex Test Simulator)

Question – Your company has sent you overseas to conduct a security assessment on a vendor that processes PHI for your company.

What is the first thing you should do upon arrival to the hotel?

A) Immediately begin attempting to hack the vendor, since your IP address will be local
B) Wash your hands
C) Take a nap
D) Text your next of kin to advise of safe arrival

Not an actual test question!

Example of explanations of answers (Wiley/Sybex Test Simulator)

Question – Your company has sent you overseas to conduct a security assessment on a vendor that processes PHI for your company.

What is the first thing you should do upon arrival to the hotel?

A) Immediately begin attempting to hack the vendor, since your IP address will be local
B) Wash your hands
C) Take a nap
D) Text your next of kin to advise of safe arrival

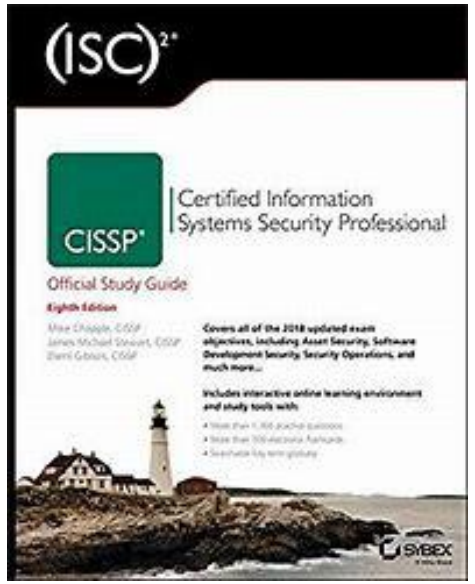
Answer B – Explanation

-The first thing you should do upon arrival to the hotel is wash your hands.

Not an actual test question!

Extra Concentration for YOUR Weak Spots

Depending on your work experience – you will have different weak spots. Spend some extra time here.



Read the in-depth material on the domains that are less familiar to you.

– you might spend extra time on –

- Memorizing some ports
- Encryption Algorithm stats
- OSI Model
- What is a …
  - Router
  - Switch
  - Bridge

Look for the basics on specific topics – like networks or business continuity. Be careful with generic searches for CISSP videos.

Immerse yourself in Information Security

Dive into the Information Security world and get exposure beyond your job/company and even your country.

Community Groups

- ISC^2 Chapters
- ISACA Chapters
- ISSA Chapters
- B-Sides

Podcasts

- Unsecurity
- Smashing Security
- SecurityNow

News and Blogs

- Krebs
- Schneier
- Naked Security

How to waste time…

I made mistakes looking for material in these locations. There is nothing there except other digital identities to share your hardship. Stay productive with your time by using the other recommended sources.

Reddit – subs for CISSP

Facebook – groups for CISSP

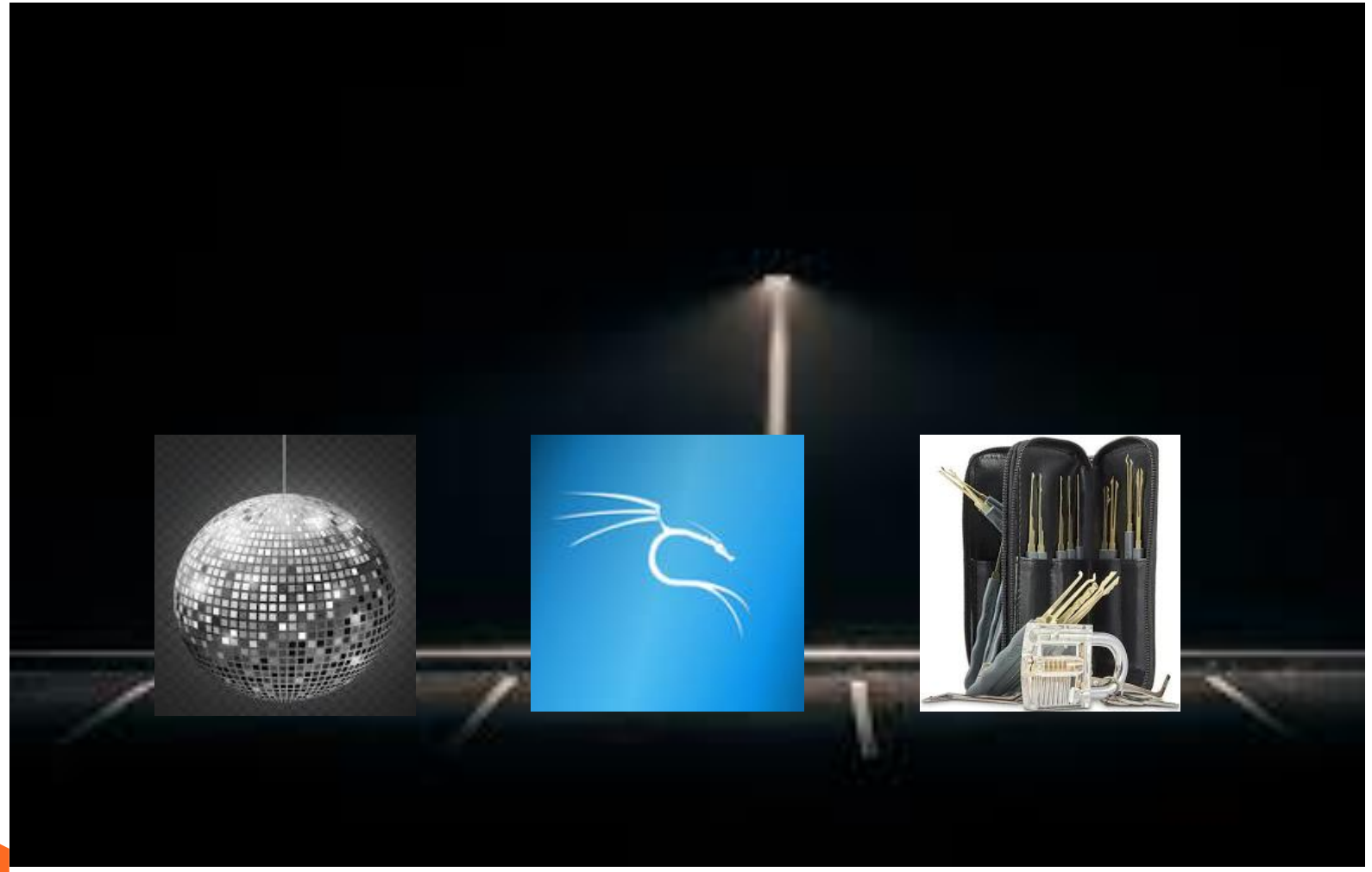
Pocket Prep – App for phone

CISSP

YouTube – General Searches

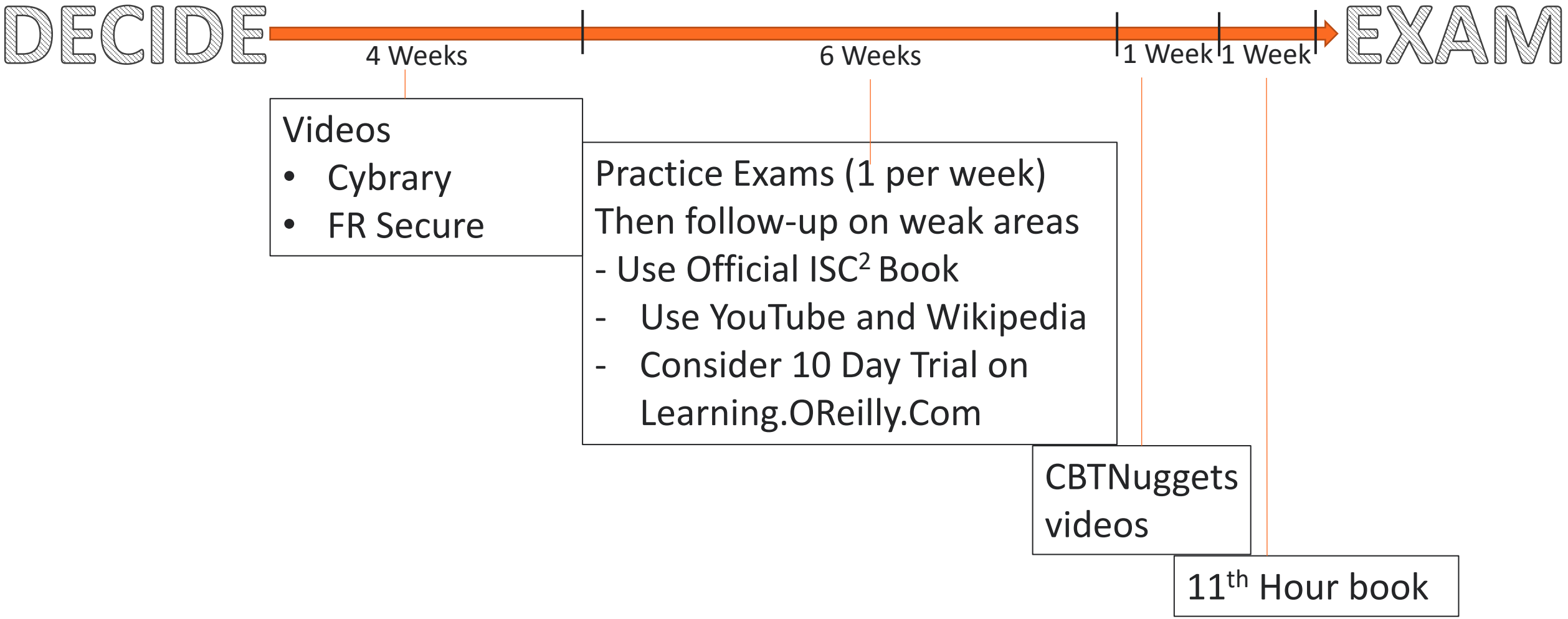
You Tube

Create a Parking Lot for your shiny objects



This test does not require technical in-depth knowledge. Save these interesting topics for after you pass.

12 Week Prep Plan (10-12 hours per week)



Through all 12 weeks – listen to security podcasts, read news, attend local InfoSec group meetings.

Do you want to spend more money?

Additional Sources

Here are a few additional sources that I did not try. I am noting these here as they are highly recommended and the costs seem reasonable. Consider these, if you feel you need just a little more exposure or practice.

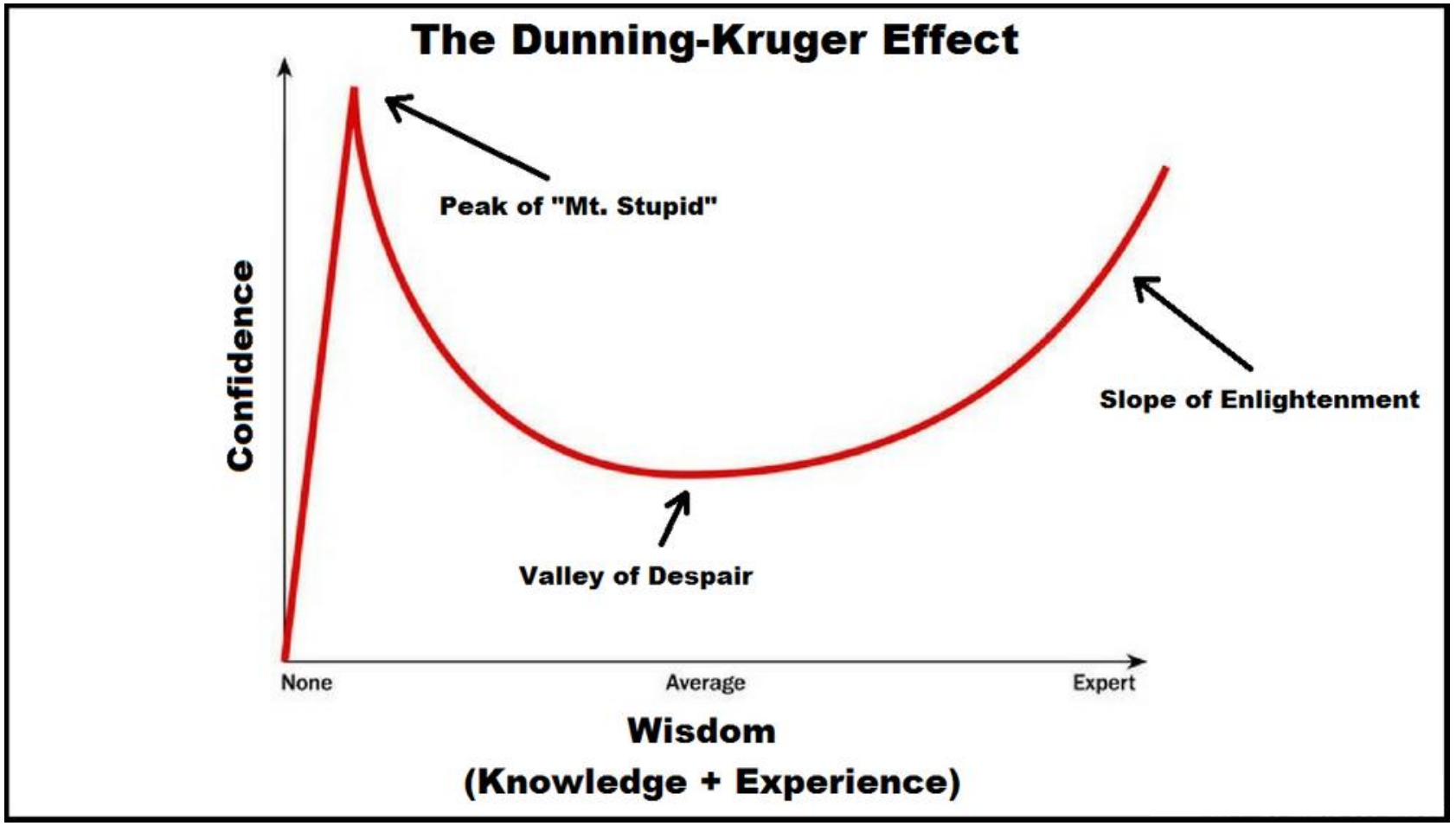
- Shon Harris, CISSP All-in-One Exam Guide, Eighth Edition ~$35
- CBTNuggets – Join for 1 month to unlock Practice Tests ~$60
- Boson – Purchase Practice Tests ~$100
- Learning.Oreilly.Com
  - 10 Day Free Trial – then paid subscription options
  - In Trial - Videos are limited to 1 minute, Books are viewable
  - A few books offer practice questions in written format

Wrap it up!

You must do the work, but you don't have to pay someone just so you can do the work.

Using the sources presented, you can be confident that you have been adequately exposed to all the topics at the proper depth.

If you see an odd question, assume it is a new question that ISC^2 is researching.



- You will be at a different location in each domain.
- Preparing for this test does not make you an actual expert. (breadth not depth)
- On test day, you may feel like you are in the Valley of Despair. That's OK

All the study materials on one slide

Videos

- Cybrary
- FRSecure
- CBT Nuggets

Books

- **CISSP Official Study Guide 8th Edition plus Official Practice Tests**
  Mike Chapple, James Michael Stewart, Darill Gibson
- **11th Hour CISSP Study Guide 3rd Edition**
  Eric Conrad, Seth Misenar, Joshua Feldman
- **CISSP All-in-One Exam Guide, Eighth Edition**
  Shon Harris
- **Learning.Oreilly.Com**
  Many books available in trial mode, including practice tests. Videos in paid mode.

Practice Tests

- **CISSP Official Study Guide 8th Edition plus Official Practice Tests**
  Access the Wiley/Sybex test engine via instructions in your book
- **Boson Practice Tests**
- **CBT Nuggets**
  Paid membership unlocks practice tests

THANK YOU

Questions?

Make this presentation better!

Email me if you find other cheap and awesome sources. Also, let me know if these materials help you pass the exam.

Jeff Hoskins

HoskinsSC@gmail.com