Secure Learn

Introduction to CISSP

Trainer: Daniel Mahanty

CISSP, CISA, CRISC, CIPM, CIA, ISO 27001 LA, ITIL (Found.)

Agenda

- **Part I**
  - Trainer information, background
- **Part II**
  - Origins of ISC2 and CISSP
  - Exam pattern, CAT (Computerized Adaptive Testing)
  - How to prepare for the exam
- **Part III**
  - Why you should choose my training program

PART I: TRAINER INFO

Trainer Introduction

Daniel Mahanty, Banker, Cybersecurity Professional & Trainer
Worked at senior levels in leading banks in India and overseas

Trainer Certifications: CISSP, CISA, CRISC, CIPM, CIA, ISO 27001 LA, ITIL (Found.)

CISSP programs for:

- MasterCard
- Target
- Indian Navy
- Deloitte
- Comcast
- Société Générale

https://www.linkedin.com/in/daniel-sunil-mahanty-cisa-cissp-crisc-cia-caiib/

CISA programs for:

- Standard Chartered Bank
- US Govt Accountability Office
- T-Systems, subsidiary of Deutsche Telekom
- Janalakshmi Financial Services (now Jana Bank)

Others:

- Cybersecurity programs for Emirates Institute for Banking & Financial Studies, UAE
- Various banks in India and overseas
- Mentor for young UAE bankers recruited under ETHRAA program of CB-UAE

Daniel Mahanty - Testimonial

FOR TEAMS

Daniel’s expert instruction ensured over 100 employees in a Fortune 500 financial services institution attained their CISSP certification. His students always share positive feedback on how he connects the material to his extensive real-word experience managing large scale data security programs. Students love how he breaks down complex topics into simple concepts. We can’t wait to work with him again!”

-Cybrary, Inc.

Daniel’s CISSP Training

Joseph Rose

Daniel is a very capable and patient trainer, with a keen wit. He was able to effectively explain the CISSP study material, often dealing with a very mixed audience.

I am grateful for his training and his support throughout the study and exam preparation process.

Jason Marilla

Daniel is an exceptional educator. I have worked with him and have been trained by him so i have a unique perspective on his teaching style and effectiveness.

If you are looking to get your CISSP, his cohort is a great place to start.

Theodore Naunheim

I had the pleasure of studying under Daniel for a CISSP bootcamp. He has an exceptionally broad base of knowledge and a talent for breaking down complex security topics into simple, manageable concepts.

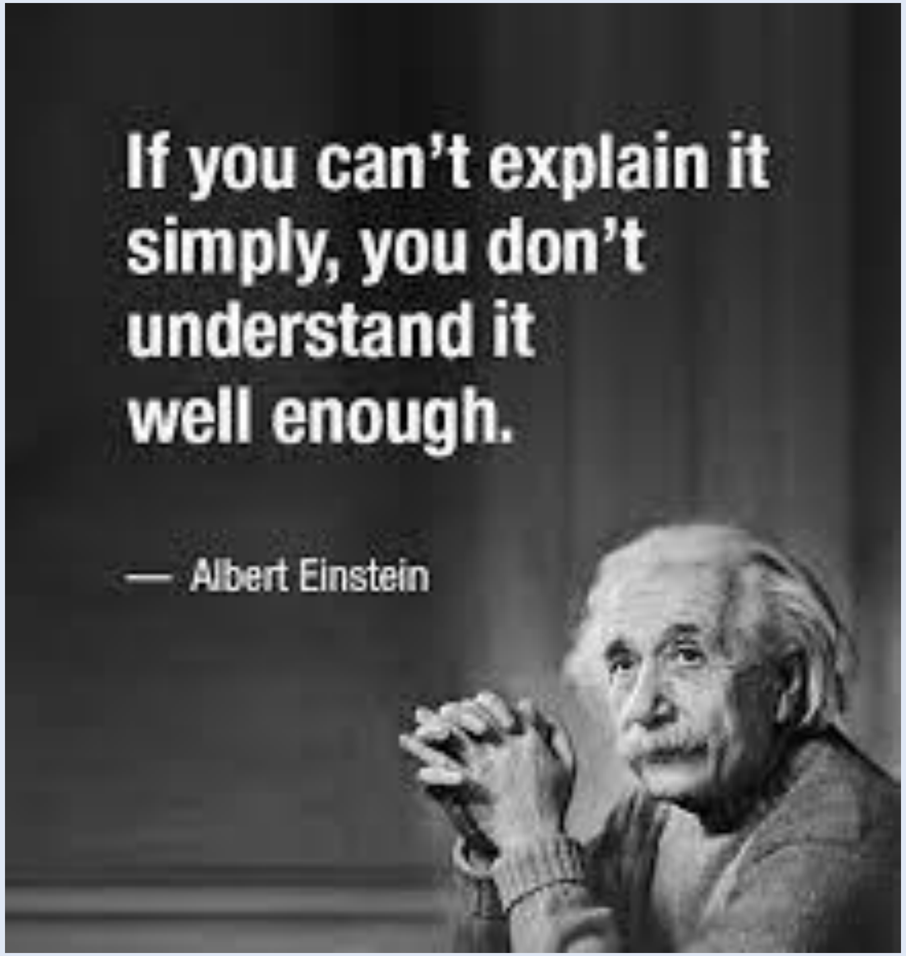
With his guidance I was able to pass the CISSP examination on my first attempt, and I recommend him highly.

Kate O’Loughlin

I recently participated in a CISSP Bootcamp taught by Daniel and without a doubt he helped me pass. Provided a thorough and clear explanation of the material and great guidance on how to best tackle each domain.

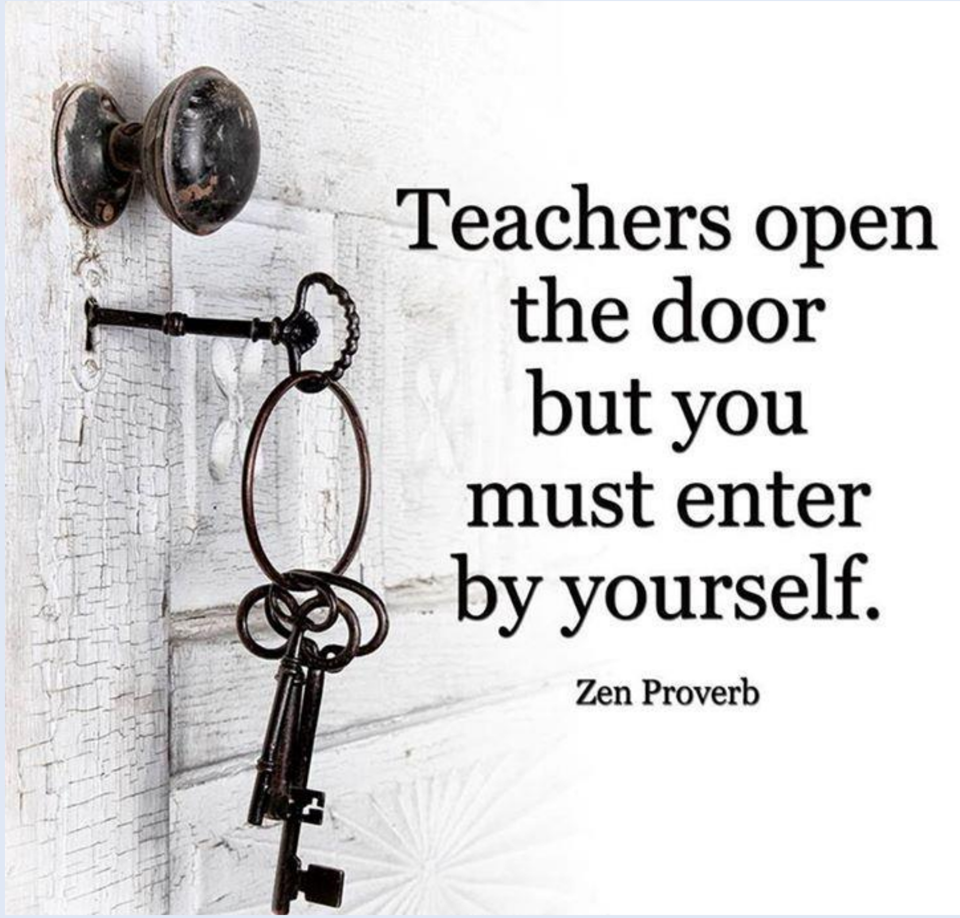
Secure Learn

My Precepts for Teaching



If you can't explain it simply, you don't understand it well enough.

— Albert Einstein



Teachers open the door but you must enter by yourself.

Zen Proverb

Part II: Origins of CISSP

Good News: The good guys are getting better.
Bad News: The bad guys are getting badder, faster.

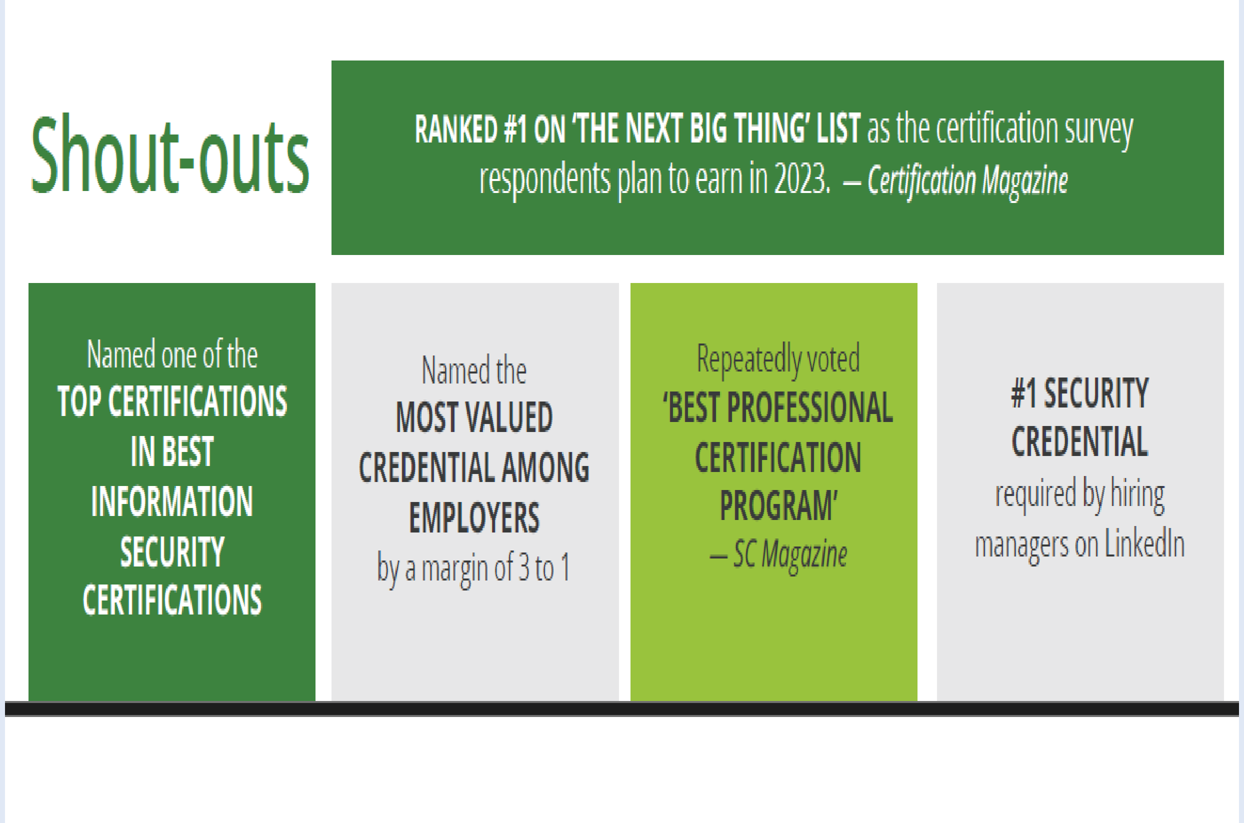
Stuart Madnick, Emeritus Prof MIT Sloan School of Management

Origins of ISC^2 & CISSP

- ISC^2 was created in 1989 pursuant to felt need for a **comprehensive, vendor-neutral** information security program that demonstrated **competence** and enjoyed **global acceptance**.

- Since its introduction in 1994, CISSP has emerged as the **gold standard** for information security and commands universal recognition – **across industries and geographies.**
- Do a keyword search in job portals anywhere in the world and see for yourself!

CISSP Career Prospects



Shout-outs

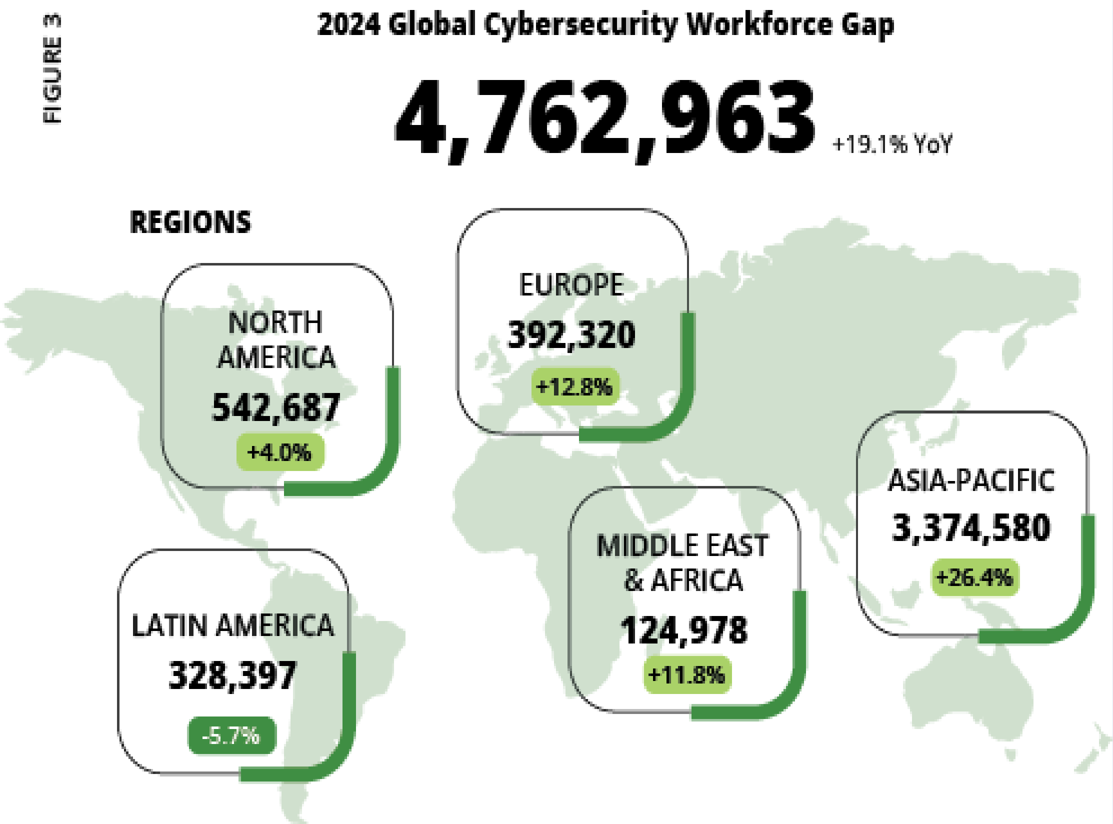
RANKED #1 ON ‘THE NEXT BIG THING’ LIST as the certification survey respondents plan to earn in 2023. – *Certification Magazine*

Named one of the TOP CERTIFICATIONS IN BEST INFORMATION SECURITY CERTIFICATIONS

Named the MOST VALUED CREDENTIAL AMONG EMPLOYERS by a margin of 3 to 1

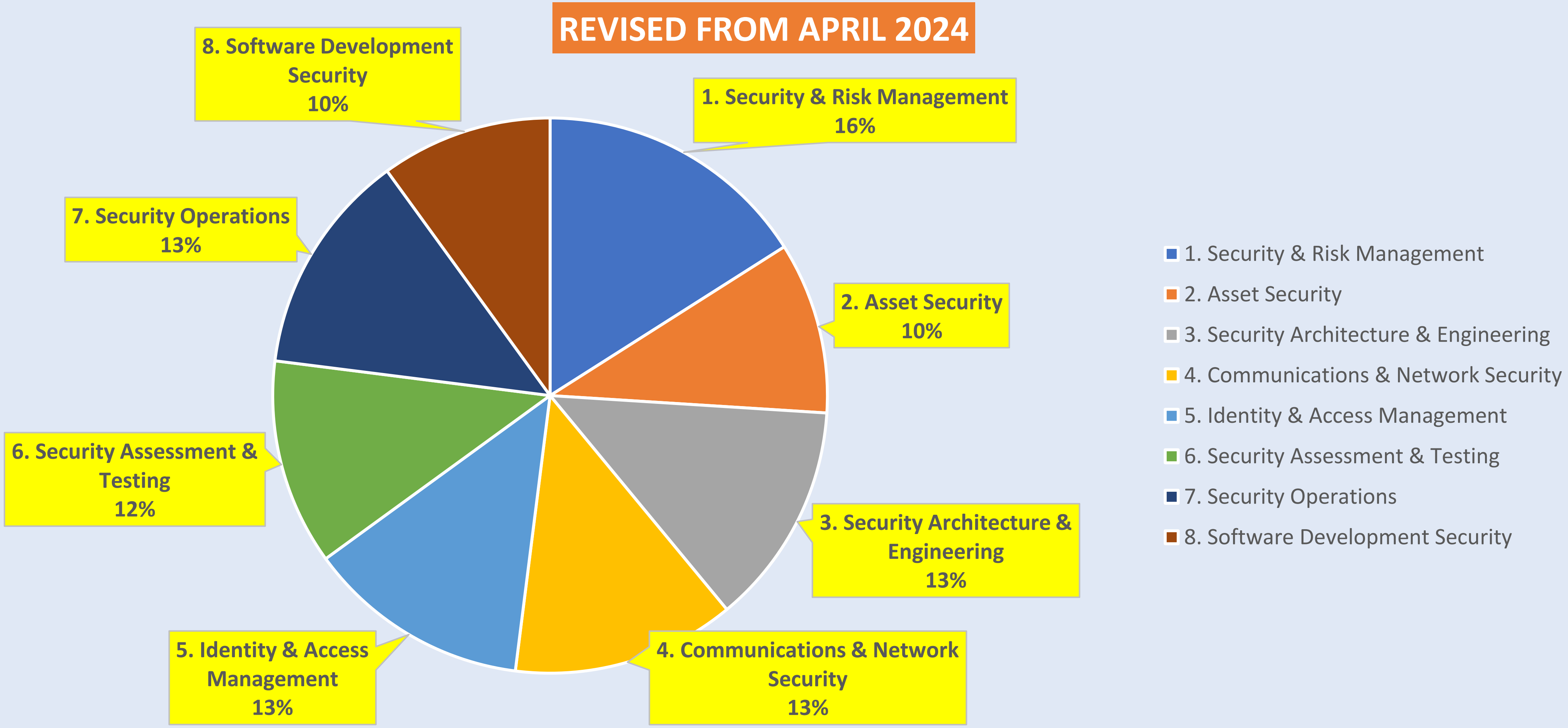
Repeatedly voted ‘BEST PROFESSIONAL CERTIFICATION PROGRAM’ – *SC Magazine*

#1 SECURITY CREDENTIAL required by hiring managers on LinkedIn



CISSP Domain Weights

REVISED FROM APRIL 2024



Common Body of Knowledge (CBK)

- The CISSP CBK is divided into eight domains, each of which covers a broad spectrum of security topics. Here what we should remember about the CBK:
- The eight domains encompass all aspects of IT, but not necessarily at great depth. In the words of Shon Harris: *The CBK is a mile wide and an inch thick*.
- CISSP is a **managerial**, not a core technical, certification: Candidates are expected to have an *understanding of the concepts, risks involved and the controls implemented to mitigate them to an acceptable level.*
- CISSP CBK is *vendor*- and *platform*-agnostic.
- Remember this mantra: *Security transcends technology*. CISSP candidate should be able to apply the principles you learn here in various scenarios, regardless of platform or technology.

CISSP Exam

Computerized Adaptive Testing

- **Exam duration:** Maximum 3 hours
  - Exam can end sooner if the algorithm determines with 95% confidence level that the candidate possesses / does not possess the required ability.
- **Number of Questions:** 100 to 150
  - Candidates will have to answer between 100 to 150 questions.
- **Pretest / Research Questions: 25**
  - Within the first 100 questions, there will be 25 questions for which the candidate will not be evaluated.
  - **Catch:** You cannot distinguish between scored and unscored questions!
- **You cannot skip questions, nor revise answers later.**
  - When in doubt, make an educated guess. You have a 25% chance of getting it right!

Understanding the CISSP Exam Pattern

- **Shon Harris:**
- *Remember that these questions are formatted and asked in a certain way for a reason.*
- *The CISSP exam asks questions at a conceptual level.*
- *Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.*
- **Types of Questions:**

i. *Multiple-choice questions – choose the best of four options*

ii. *Scenario-based questions*

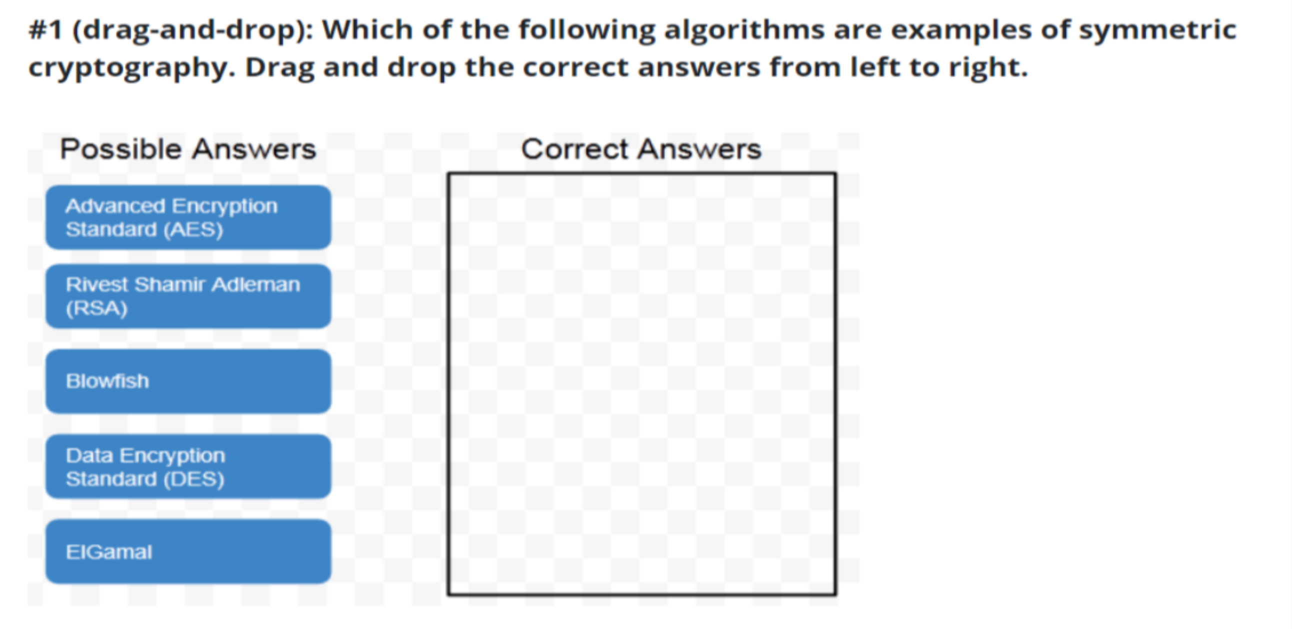
iii. *Advanced innovative questions: Hotspot, Drag-and-Drop*

Scenario-Based Questions

- A passage details a particular scenario, on which the next few multiple-choice questions will be based.
- Same four-option multiple-choice question
- Only difference is that the questions pertain to the scenario.
- *Challenge is to grasp the relevant information and ignore irrelevant information.*

Advanced Innovative Questions: Drag-and Drop

- The Drag-and-Drop is the only question type that requires multiple answers
- Drag-and-Drop questions are a newer type of question that typically requires moving items from one column to another column
- Simple list-based or category questions work especially well in this format



#1 (drag-and-drop): Which of the following algorithms are examples of symmetric cryptography. Drag and drop the correct answers from left to right.

Possible Answers

- Advanced Encryption Standard (AES)
- Rivest Shamir Adleman (RSA)
- Blowfish
- Data Encryption Standard (DES)
- ElGamal

Correct Answers

Computerized Adaptive Testing (CAT)

- **Questions are weighted**
- **Scaled scores are used to be able to directly compare scores from one exam to another.**
    - A candidate’s raw score (number of items answered correctly) is converted to a number within a predefined score range. All raw scores are converted to scaled scores of 0-1000, with the passing scaled score of 700.
- **Advice:** Never place speed before accuracy, but be mindful of the clock ticking away on your screen.

To determine success or failure, the algorithm will apply one of the following 3 rules in order.

How does CAT determine pass or fail?

Confidence Interval Rule

- Once the minimum length of the exam (100 questions) is completed, the exam will end if the algorithm estimates with 95% confidence that the candidate's ability *exceeds* or *falls below* the passing standard.

Maximum Length Rule

- If the first rule is not invoked, the exam may be extended up to a maximum of 150 questions.
- Algorithm will stop the exam at any time between 100 and 150 questions when it estimates with 95% confidence level that the candidate's ability *exceeds* or *falls below* the passing

Run Out of Time (ROOT)

- If a candidate does not answer seventy-five (75) *operational* items within the maximum time of the examination (3 hours), the candidate will automatically fail the exam.

Popular Sources for CISSP

- **Official CISSP CBK Reference,** Arthur Deane & Aaron Kraus
- **CISSP All-in-One Exam Guide,** Shon Harris (updated by Fernando Maymi)
- **Sybex Official Study Guide,** Mike Chapple & Others
  - Crisp, but does not proceed according to CISSP domains. Chapter to domain mapping provided.
- **Boson Practice Exams**
- **O'Reilly**
- *All books have some grey areas. You may need to refer to more than one.*
- Go with the latest edition.
- YouTube channels:
  - Destination Certification
  - Mike Chapple
- Learnzapp for CISSP is a good source for questions. http://www.learnzapp.com/apps/cissp/index.html

Examination Process

- Pearson Vue is the exclusive, global administrator of all (ISC)^2 exams.
- Create a user account in Pearson Vue, select the CISSP exam and schedule the exam and testing location. **Exam fee is $749.**
- From time to time, (ISC)^2 offers **“Peace of Mind”** protection: **Pay $199 extra** and get a second shot at the exam if you are not successful at the first attempt. *Terms & conditions apply – specified time frames within which to appear / re-appear.* Please check the (ISC)^2 website for current offers.
- After two extensive pilot programs, ISC2 abandoned the online proctoring model because of *irregular exam results, clear violations of exam administration rules and cheating attempts.*

Secure Learn

Certification Requirements

- Candidates must pass the exam before certification.
- A **minimum of five years** of cumulative paid work experience in **two or more of the eight domains** of the CISSP CBK is necessary for certification.

➢ *A four-year college degree or regional equivalent or an additional credential from the (ISC)^2 approved list will satisfy one year of the required experience.*

➢ A candidate who doesn't have the required experience to become a CISSP may become an **Associate of (ISC)^2** by successfully passing the CISSP examination. The Associate of (ISC)^2 will then have six years to earn the five years required experience.

➢ In the certification process, an existing CISSP should sign the endorsement form. *In case of need, (ISC)^2 will itself endorse your form.*

- Endorsement should be completed within 90 days of the advice of passing the exam.
- **Certification cycle is three years. Members will be re-certified for a new three-year certification cycle, subject to two conditions:**

i. Payment of Annual Maintenance Fee (AMF) of $135; and

ii. Fulfilling CPE requirements

Continuing Professional Education (CPE)

Annual Maintenance Fee of $135 & CPE

Type –	Suggested Annual –	3-year Total
Group A	– 30 hours	– 90 hours
Group B	– 10 hours	– 30 hours
Total	- 40 hours	– 120 hours

- CPE credits are subject to random audit – keep proof and brief description.
- Retain record of CPEs claimed in case of audit.

Groups A and B

- **Group A**: Areas directly covered by the domains, e.g.: *Taking a self-paced, blended or instructor-led educational course; publishing an article, book or whitepaper; attending a conference, seminar or presentation (physical or virtual); teaching information security; self-study or preparation for a certification course; higher educational course.*
- **Group B:** *General professional development, education, knowledge outside the domains, e.g., attending non-security industry conference; non-security education courses; non-security training;*

CPE Resources

- ISC2 offers several resources free to members.
- *Professional Development Institute, Webinars, Center for Cyber Safety & Education, Exam Development, Infosec magazine*
- *https://www.isc2.org/Membership/CPE-Opportunities*

Secure Learn

Acing CISSP

What to remember about CISSP

- Understanding the concepts is important. Learning by rote without understanding the concepts will not help.
- No single option may be entirely right or wrong. Choose the best option in the given scenario.
- This is a managerial, not a core technical, certification.
- **Remember:** The benefits of the knowledge you acquire in this program will extend beyond the exam. You will understand the rationale behind the controls and processes that we follow every day

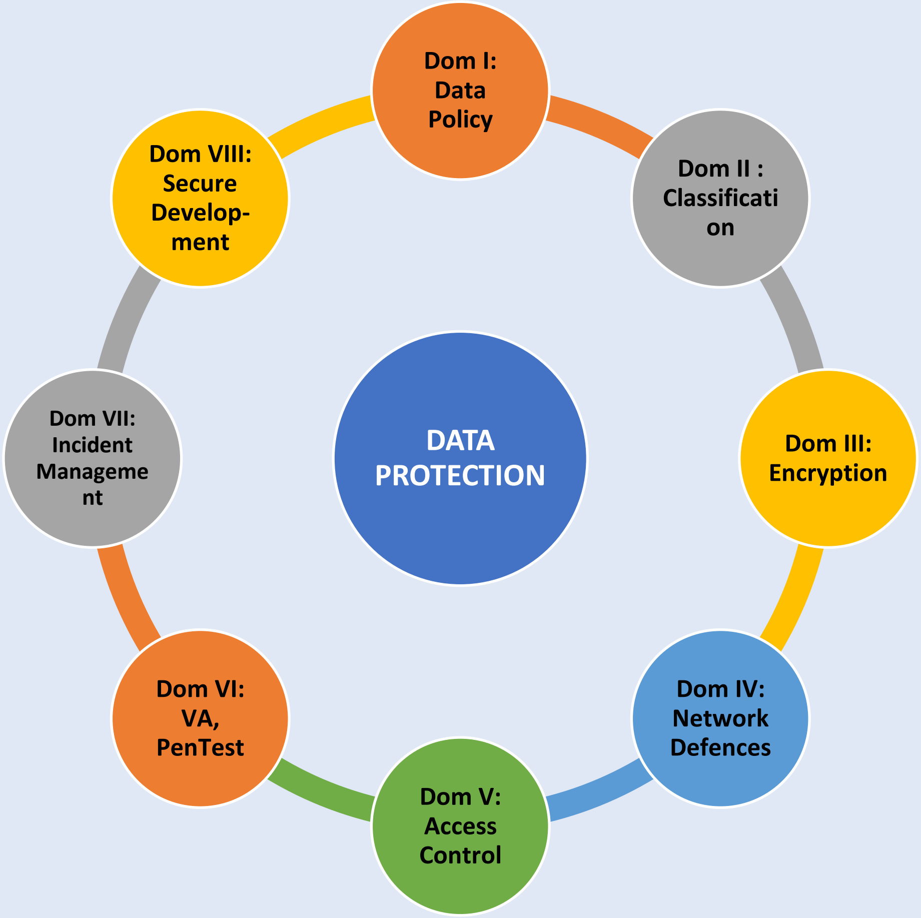
Domains are Interconnected

Domains

- Division of CBK into domains is for convenience.
- Much like the human body, domains impact each other.

Interconnected

- Domains are interconnected.
- Any major security concern has CBK-wide ramifications.



Top CISSP Tips

- **Remember your role**
- Risk advisor.
- Balance security with business needs and resources.
- **Risk permeates all decisions**
- RM basics. Quantitative and qualitative risk analysis.
- Impact and likelihood
- Know your assets – sensitivity of data!

- **Not technical exam but …**
- You must know enough about technology to understand the risk – *encryption, EDR, incident management, BCP, network defences, SoC audits.*
- **Security Transcends Technology**
- Platform-, vendor-agnostic
- You cannot be an expert in every technology used in the organization.

Top CISSP Tips (contd.)

Aim for the sky and you’ll reach the ceiling.
Aim for the ceiling and you’ll stay on the floor.
-- Bill Shankly

- **Ethics are important**
- ISC^2 Code of Ethics
- **Who is responsible for security?**
- We all are!
- **What is most important?**
- Human life and safety
- Business continuity
- Fixing the process
- All the information you need to answer the question is the question itself. *Don’t assume anything beyond that.*

- **Things to remember**
- Security starts at the beginning, not an add-on
- Don’t put all your eggs in one basket – *layered defence*
- Security depends on *people, processes* and *technology* – in that order!
- Understand the exam format, budget your time
- Understand the concepts
- Read questions carefully.

More on Exam Preparation

- The CBK may look intimidating but is eminently doable for serious contenders.
- **Start from Day 1:** Overcome the temptation to start studying in earnest **after** the cohort is over. Play an active role in class, make notes, ask questions.
- **Prepare a schedule:** Study a domain a week even if it is not an intense study.
- **Make / use flashcards:** Creating flash cards or notes in bullet points is recommended. *Active vs passive learning.*
- **Consult more than one source** if necessary – for a different perspective or fuller explanation.
- **Alternate reading and testing** to relieve monotony and keep your brain receptive.
- Always read questions and alternatives carefully. Never place speed before accuracy.
- Always read the explanations, even if you got it right: *Understand not only why one alternative is right but also why the other three are wrong!*
- Read the CBK at least once, twice for domains that are new to you.
- Take time off before the big day if you can. “Bang-for-the-buck” cramming.

How Technical is the Exam?

- An understanding of important technology concepts is necessary, though no hands-on tests are involved.
- *What is the difference between symmetric and asymmetric encryption? What are the pros and cons of each of these?*
- *What is the difference between encryption and hashing? Which provides confidentiality and which provides integrity?*
- *What are the advantages of optic fibre cable?*
- *Why is the use of FTP not encouraged?*
- *How do the responses of IDS and IPS differ with regard to incoming malicious traffic? Which is inline and which is offline?*
- *Layers of the OSI model*
- *TCP vs. UDP? Pros and cons?*

A Personal Note

- I started life as a management trainee (probationary officer) in State Bank of India, India's largest bank and a Fortune 500 company. I graduated in Economics, not technology.
- I spent the first half of my career in business lines in banking: branch management, retail and corporate lending, foreign exchange, NPA management, fraud management cell.
- Chance assignment as Manager of the Data Processing Cell (largely a managerial role) changed the course of my career.
- I got interested in technology and began acquiring certifications one by one. **Passed all exams at first attempt.** Never went back to mainstream banking.
- If I could make the shift from banking to cyber security in mid-career, why can't you?

Part III: Why Would You Choose My Training?

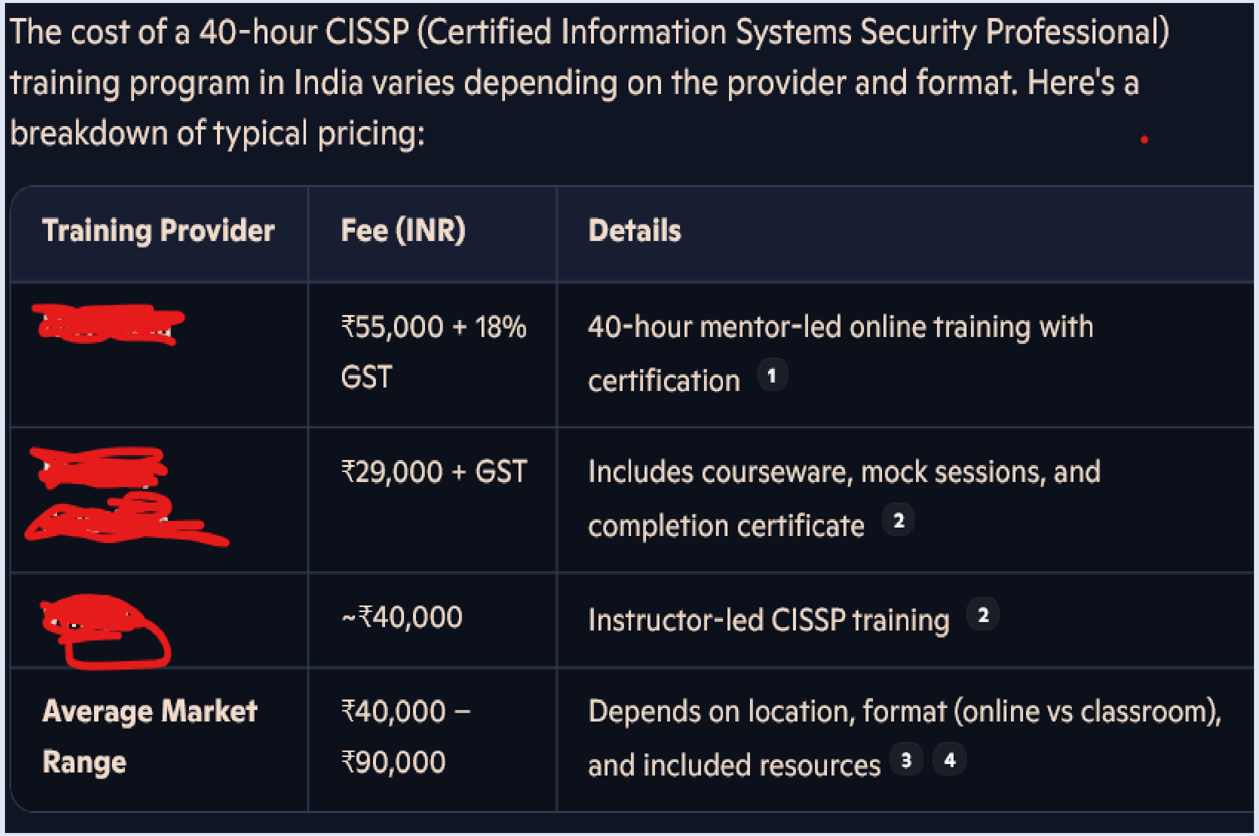
A Training Experience Rooted in Delivering Value

- 💼 **Banker’s Mindset, Trainer’s Heart**
- I price my program at less than half the market rate—because long-term success comes from high volumes and low margins. Not the other way around.
- 🤝 **Service Over Sales**
- Money is a corollary, not the goal.
- 💡 **Value ≠ Cost**
- Value and price are not always directly related. It is possible to provide best-in-class training at an affordable price.
- 📢 **No Cold Calls, No Hype**
- This is a referral-driven, one-man show. Word-of-mouth drives my training

What You Get!

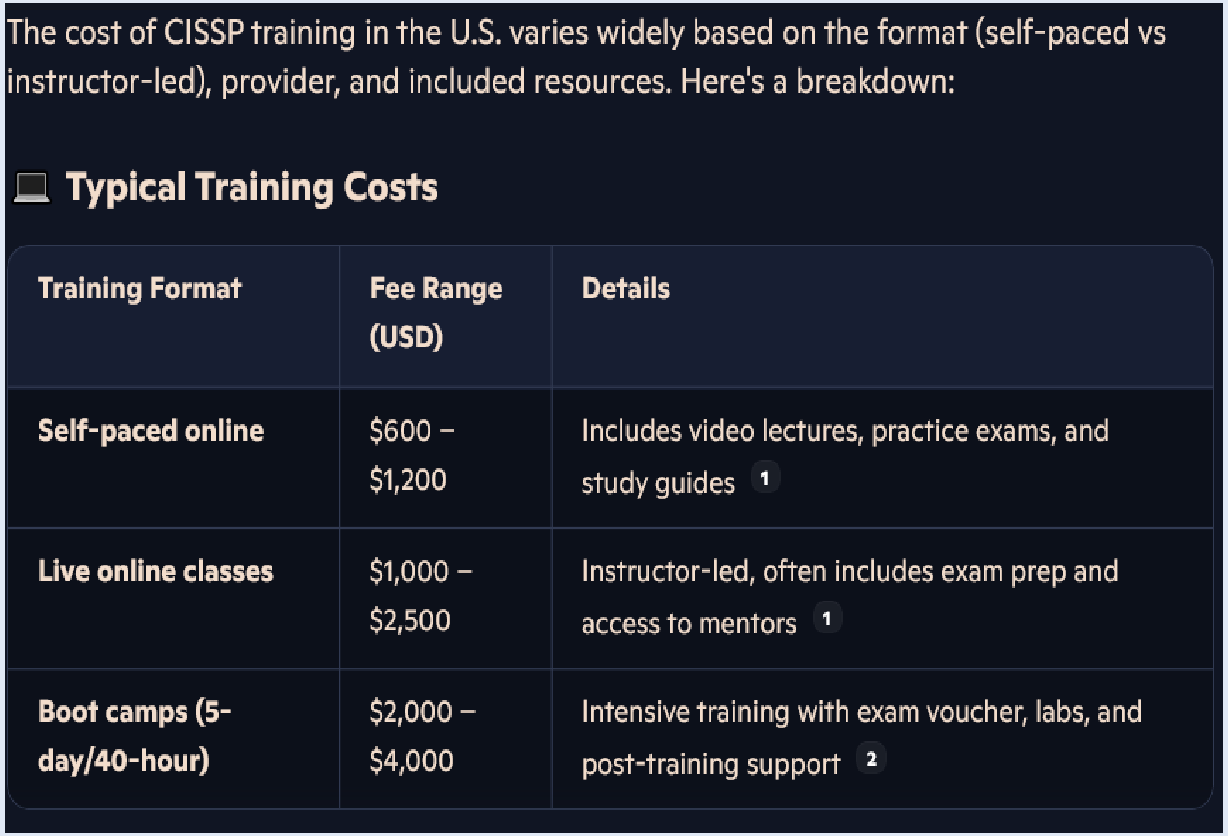
- ⏰ **40 Hours of Live Training**
- Deep-dive sessions designed for clarity, retention, and exam success.
- *Loads of mock questions. Both at the end of each topic and at the end of each domain.*
- 🎥 **Zoom Recordings + PDF Materials**
- Every session is recorded. Training decks will be shared in PDF format.
- 🔄 **Two Free Repeat Sessions**
- Come back, refresh, and reinforce—at no extra cost.
- 📱 **WhatsApp Cohort Groups**
- Stay connected, ask questions, and get support even after the program ends.
- 🧠 **Personal Access to Me**
- No gatekeepers. No bots. Reach out directly to me on phone / email

Prevailing Fees for Similar Training



The cost of a 40-hour CISSP (Certified Information Systems Security Professional) training program in India varies depending on the provider and format. Here's a breakdown of typical pricing:

Training Provider	Fee (INR)	Details
[redacted]	₹55,000 + 18% GST	40-hour mentor-led online training with certification [1]
[redacted]	₹29,000 + GST	Includes courseware, mock sessions, and completion certificate [2]
[redacted]	~₹40,000	Instructor-led CISSP training [2]
Average Market Range	₹40,000 – ₹90,000	Depends on location, format (online vs classroom), and included resources [3] [4]



The cost of CISSP training in the U.S. varies widely based on the format (self-paced vs instructor-led), provider, and included resources. Here's a breakdown:

💻 Typical Training Costs

Training Format	Fee Range (USD)	Details
Self-paced online	$600 – $1,200	Includes video lectures, practice exams, and study guides [1]
Live online classes	$1,000 – $2,500	Instructor-led, often includes exam prep and access to mentors [1]
Boot camps (5-day/40-hour)	$2,000 – $4,000	Intensive training with exam voucher, labs, and post-training support [2]

Training Schedule & Fees

SCHEDULE FOR CISSP PROGRAM

Session	Date	Coverage
	12-Aug-25	Introductory Webinar
1	30-Aug-25	Ice-breaker, Domain I
2	31-Aug-25	Domain I
3	06-Sep-25	Domain II
4	07-Sep-25	Domain III
5	13-Sep-25	
6	14-Sep-25	Domain IV
7	20-Sep-25	Domain V
8	21-Sep-25	Domain VI
9	27-Sep-25	Domain VII
10	28-Sep-25	Domain VIII

- Each session will last 4 hours, from 7 pm to 11pm Indian Standard Time
- Total duration 40 hours.
- PDFs of study / training material will be provied.
- Freedom to attend two further sessions free for recap
- Continued support from trainer even after program concludes

- **Fees**
- Rs 20,000 if you are in India
- USD 250 or equivalent if you are overseas.
- *Trainer account details will be shared by email later.*
- *Fees should be paid before the program commences on 30 Aug 25*

Questions?