My CISSP examination preparation experience...!

Things and TIPS, that I followed for preparing CISSP exam.

Sandeep Andhekar
Deputy Manager(IS Audit) at State Bank of India
Sept 29, 2019

It's purely my personal views and request not to share in any media.

Books to be referred: -

1.CISSP Official Study Guide and practise tests:

https://www.amazon.in/Certified-Information-Security-Professional-Official/dp/1119523265/ref=sr_1_1?keywords=cissp&qid=1569683580&s=gateway&sr=8-1

Read an official study guide minimum two times after listening the online classes (I preferred Simplilearn SAAZ RAI classes). Online classes helped me to take notes on important topics and to identify important concepts that helped me to avoid unnecessary things in book. After each end of chapter there are topics of exam essentials, please go to accordingly and understand in depth of topics of those topics particularly.

This Official study guide consists of 8 domains, divided into 21 chapters. Weightage

Domain 1, Chapters 1, 2, 3, and 4: Security and Risk Management 15%

Domain 2, Chapter 5: Asset Security 10%

Domain 3, Chapters 6, 7, 8, 9, and 10: Security Architecture and Engineering 13%

Domain 4, Chapters 11 and 12: Communication and Network Security 14%

Domain 5, Chapters 13 and 14: Identity and Access Management (IAM) 13%

Domain 6, Chapters 15: Security Assessment and Testing 12%

Domain 7, Chapters 16, 17, 18, and 19: Security Operations 13%

Domain 8, Chapters 20 and 21: Software Development Security 10%

Practise Papers are necessary to apply our concepts in attempting the question. There are 8 domains in practise book, there are 100 questions for each domain. Attempt these 100 questions. For the wrong attempt refer the solution provided end of the book and learn to understand the concept. That helps us to attempt any twisted question.

It also provided with two tests of each 250 questions. Solve these two model papers too.

(Important topics that helped me is written below).

Follow one book Sybex eighth edition Official study guide and practise papers (Link provided). Don't try to refer more books, it creates confusion. Always refer one book to understand the concepts.

2. BOSON simulation tests:

Use coupon available in special offer in boson website

https://www.boson.com/practice-exam/cissp-isc2-practice-exam

After completion of online classes, book reading and attempting practice papers. I have attempted the 5 Simulation tests of boson to know my knowledge levels and concepts that I have understood. If you're good enough to score 80% in Boson tests, I can say we are capable of attempting the main exam. Don't be tremble, if you score 50 – 60 % in BOSON test papers in first attempt.

BOSON tests papers are good and they make you prepare well and such that they refer sybex official study guide which we read as main source of information. Each question has four multiple choice questions. Try to understand and know all four options mean. By this, we can eliminate the distractor.

It helps gives us to refer the answer, why it is correct. CISSP is the exam which we should know " **why".**

3. Simplilearn online classes:

https://www.simplilearn.com/cyber-security/cissp-certification-training

Listen to SAAZ RAI classes, his classes are clear and precise. Help us to understand the concepts for attempting any question. Register his classes before reading. It will be easy to acquire the concepts try to attend his classes.

He will be prompting us to take notes of important topics, it will help us to revise afterwards.

Concepts to read and tips:

Be prepared in mind, that we are going to attempt exam in 3-4 months and register the exam and start preparing. I can suggest team preparation, group discussions will certainly help us to clear the concepts. I prepared alone, took three months dedicated preparation.

First, I have attended simplilearn SAAZ RAI (Tutor name) classes. I have joined weekdays batch. starts evening 8 pm to 11 pm. He will complete the classes in 10 days from Monday to Friday continuously in two weeks. Batch consists mix of aspirants from all over the world with batch size of 20 -30 members. It is done through CISCO webex meetings and it is good tool for online learners. We can raise doubts and clarify the concepts.

You can register multiple batches to his classes till we understand the concepts.

Important topics are:

Domain 1, Chapters 1, 2, 3, and 4: Security and Risk Management 15%

As said above domain 1 gets the highest weightage, easy to understand.

- Confidentiality, Integrity, availability, identification-user id, authentication-password, authorisation, auditing, accountability, non-repudiation.
- Protection mechanism-layering, Abstraction, data hiding, encryption.
- Strategic plan, tactical plan and operational plan
- Data classification, data owner, data custodian, data steward-----**

- Government data classification—top secret, secret, confidential, sensitive but unclassified, unclassified—*
- Commercial classification-confidential, private, sensitive and public-important topic
- Understand the difference between two terms due care and due diligence-*
- Difference between Policy, standard, guideline and procedure
- Threat modeling- STRIDE and DREAD models
- Separation of duties, job rotation, NDA and NCA, privacy, compliance,
- Risk terminology like threat, vulnerability, exposure, risk, asset value, safeguard/control, breach
- Risk assessment- Quantitative and qualitative risk analysis-**
- Simple maths formula in calculating quantitative risk analysis are
- Single loss expectancy SLE: Asset value * exposure factor
- Annual loss expectancy ALE: SLE*ARO
- Risk response methods
- Detective controls, preventative controls, deterrent controls, administrative controls, logical controls/technical controls, directive controls, corrective controls
- Difference between training, education, awareness
- Business continuity plan and disaster recovery plan
- Civil law/tort law, administrative law, criminal law
- IPR topics copyright, trademark, patent and trade secret*
- US security law like COPPA, DMCA, FOURTH AMENDMENT, GLBA, GDPR (important), HIPPA

Domain 2, Chapter 5: Asset Security 10%

- Asset classification and data classification
- Data states- data in motion, transit, in use and its protection methods in rest-encryption, in motion TLS 1.2/1.3, in use – encryption/decryption by application
- Marking/labelling of assets
- Destroying sensitive data i.e., eliminating data remanence -like purging, clearing, degaussing, and physical destruction***
- Removing data remanence in SSD and Hard disk important. SSD uses electric circuits. Hard disk uses magnetic stripes.
- Pseudonymisation/tokenisation, anonymisation
- Baselines, scoping, tailoring

Domain 3, Chapters 6, 7, 8, 9, and 10: Security Architecture and Engineering 13%

- Terms to know XOR Boolean function, key size and block size
- Nonce, zero knowledge proof, split knowledge, substitution and transposition ciphers
- Difference between confusion and diffusion
- Symmetric key algorithms—DES, 3DES, DES 5 types of block encryption Electronic code book, cipher block chaining, cipher feedback mode, output feedback mode, counter mode
- IDEA, FLOWFISH, SKIPJACK, TWO FISH, AES
- Public key cryptography, RSA, EL GAMAL, ECC
- HASH functions MD2, MD5 , SHA, SHA 256, HAVAL, HMAC
- Digital signature
- Public key infrastructure CA, RA, CRL, CPS
- Trusted platform module**, Pretty good privacy, steganography, Digital rights management, IP SEC
- Cryptographic attacks
- Terms like confinement, bounds, objects, subjects, trusted computing base, security parameter,
- Security models

- bell la padula-confidentiality
- biba – integrity
- clark Wilson - segregation of duties
- Chinese wall/brewar nash - conflict of interest
- TCSEC, ITSEC and its classification
- Common criteria, Evaluation assurance levels
- Certification and accreditation
- Protection rings, security modes **
- Data base security mechanisms-aggregation, inference
- Virtualization and hypervisor
- Cloud models and IOT
- SQL injection, cross site scripting, XSRF**
- XML, LDAP, HTML
- Covert channel attacks like timing and storage
- Emanation and tempest
- Physical security design order
- Deterrence 2. Denial 3. Detection 4. Delay
- MTBF, MTTR
- Emanation security, Faraday cage
- HVAC controls
- Static electricity- low humidity, corrosion -High Humdity
- Know terms like sag, spike, brownout, black out, fault, surge**
- Fire extinguisher classes like A, B, C, D
- Water suppression systems
- Fences, gates, turnstiles, mantraps

Domain 4, Chapters 11 and 12: Communication and Network Security 14%

- OSI model and TCP/IP model -**********
- TCP three-way handshake
- Private ip ranges
- IPV4 and IPV6
- Important TCP port numbers
- ARP, DNS, Content delivery networks, wireless networks, wpa 2
- Switches, routers, firewalls, proxies
- Co-axial cables, cat 6, fibre optics
- Network topology
- Secure communication protocols
- Authentication protocols
- VPNs, VLANS, NAT, Switching technogies, WAN technologies
- DOS, DDOS attacks, DNS poisoning, replay attacks

Domain 5, Chapters 13 and 14: Identity and Access Management (IAM) 13%

- Types of access controls
- Type 1, type 2, and type 3 authentication
- Synchronous and asynchronous tokens
- Biometrics—FRR, FAR, ERR
- Retina and IRIS can
- Single sign on -Kerberos, SAML, O AUTH 2.0, Federated identity management system, Open ID,
- Authentication protocols RADIUS, DIAMETER, TACACS +
- Managing identity and provision life cycle
- Understanding terms like rights, permissions and privileges

- Access control mechanisms like Role based, rule based, discretionary based , attribute and mandatory access controls***
- Social engineering attacks vishing, phishing and whaling

Domain 6, Chapters 15: Security Assessment and Testing 12%

- Security testing, assessments and auditing
- Internal, external and third-party audits
- VA scan and its tools
- Port scanning and tools
- Network vulnerability and application vulnerability scans and its tools
- Penetration testing and its process/phases and types of PTs
- Code review, Fagan inspection, static, dynamic, fuzz testing, test coverage analysis
- Interface testing
- Website testing
- Least privilege, need to know, transitive trust
- Change management, patch management, configuration management, vulnerability management

Domain 7, Chapters 16, 17, 18, and 19: Security Operations 13%

- Incident management
- Attacks like botnets, smurf, fraggle, tear drop, ping of death, land, ping flood and zero day
- IDS and its types-promiscuous mode
- IPS -in line mode
- HIDS and NIDS
- Honeynets, honey pots, whitelisting and blacklisting
- SIEM, log types, clipping level
- DLPs
- Disaster recovery tests and types of tests like walkthrough, tabletop, simulation, parallel run and full interruption*
- RAID and types of RAID*
- Recovery sites like hot site, cold site, warm site, mobile sites, reciprocal agreements /MAA
- Backup strategies like Full, incremental and differential, remote vaulting, mirroring, electronic journaling
- Source code escrow agreements
- Investigation types, understanding terms like ethics and law, type of evidences, imp: hearsay evidence, chain of custody
- Four canons of ISC2----by heart them

Domain 8, Chapters 20 and 21: Software Development Security 10%

- Understanding executable and interpreter languages, SDLC models like waterfall, agile, spiral models
- CMMI levels* , gantt charts, pert, DevOps, APIs
- Database models, ACID principle, Database security mechanisms like polyinstantiation
- Aggregation and inference data leakage in database, dirty reads, lost updates
- Expert systems, neural networks and artificial intelligence
- Virus types, virus attacks, password attacks like dictionary attacks, rainbow table attacks, application attacks like buffer overflow, TOC/TOU, back door/maintenance hook, cross site scripting, XSRF*, SQL injection attacks, man in the middle

Exam day tips:

Divide the exam into three parts of 50 questions each, take a break after 50 questions have water, use restroom. Give 2 -3 minutes break to relax mind. As exam may happen or may not happen at 100th question. I feel to utilise maximum time for first 100 questions. I kept 40 mins grace for attempting the last 50 questions if I would move to 101 to 150 questions.

English makes little bit confusion, read twice a question and answers and choose the suitable best answer. Try to eliminate two distractors and choose a better one from the remaining two options.

There will be 6 to 8 drag and drop questions, it will be simple which can do as we are doing the same in our day to day job like e.g.: step by step change management process.

As there is no recheck of the attempted question, please careful while choosing the answer. Once we submit the answer, we cannot re-edit the attempted question. Based on the previous question and its answer given by you, the computer will throw the next question. Suppose, if u made previous question with the wrong answer, computer may throw the next question simpler.

Be confident, be normal its inch depth exam only and not a technical exam.

All the best wish you good luck……. ☺

*important