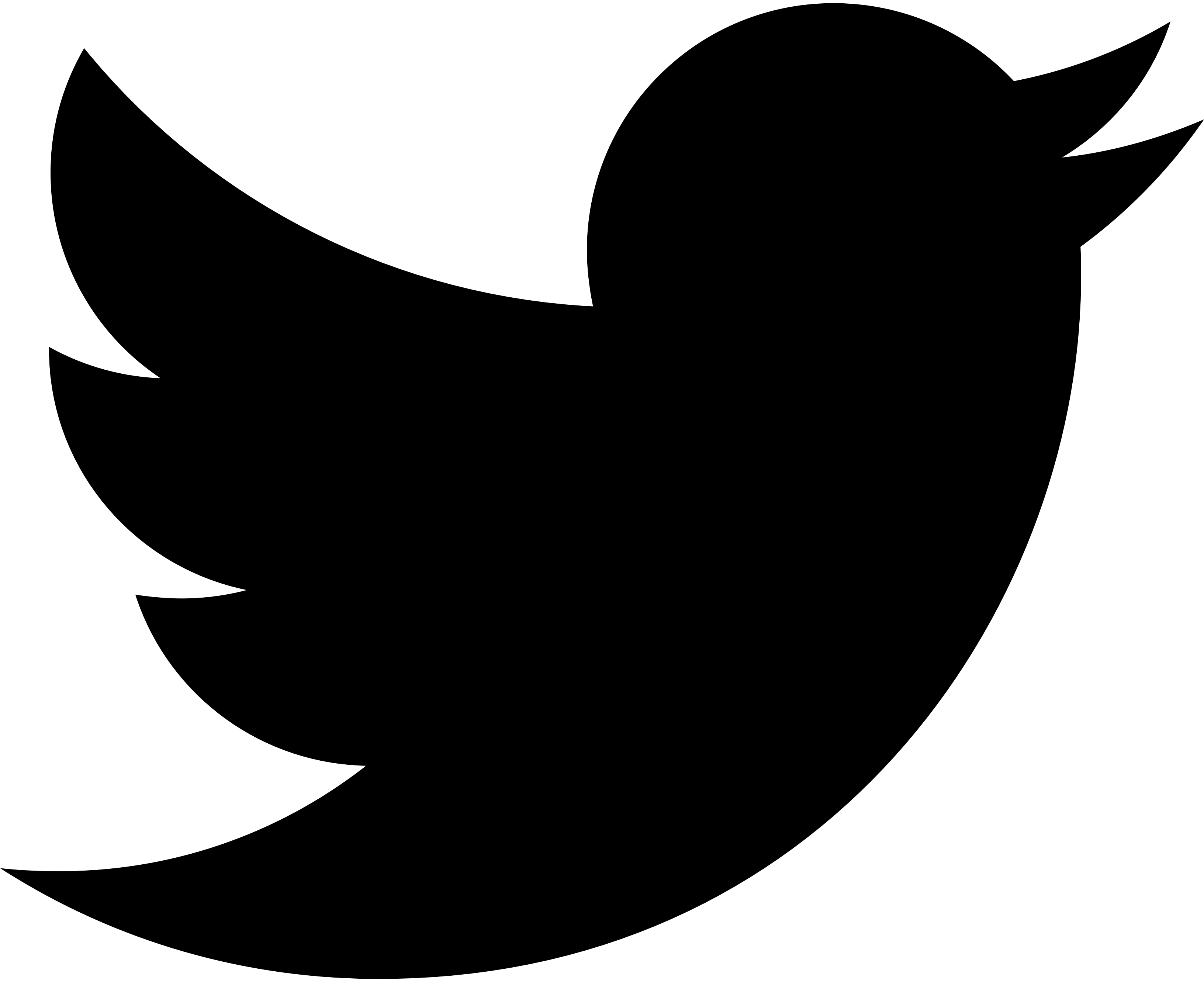
CISSP Cheat Sheet (Updated for Latest Exam)

February 14, 2023 / By Cassandra Lee



Listen to the article

You’ve made an intelligent choice to aim for CISSP as your next certification, but the sheer volume of CISSP study materials can be intimidating. CISSP study guides can also be overwhelming. Moreover, the CISSP exam is long, and you need a brief outline to help you remember how to tie all the exam concepts together.

The good news is, you’ve come to the right place: this CISSP cheat sheet is the brief outline you need. We’ve drawn a roadmap of top ideas to help you navigate this challenging certification. It highlights the concepts which are the foundations of the other concepts.

We hope this CISSP exam cheat sheet helps you prepare well for this examination wherever you are in your cyber security career. Download this cheat sheet **here**, and let's get started.

Search cheats here

What is the CISSP Certification?

Certified Information Systems Security Professional (**CISSP**) is a highly sought-after information security certification developed by (ISC)^2, an abbreviation for the nonprofit "International Information System Security Certification Consortium."

To become CISSP-certified, you need to:

1. Pass the CISSP examination to become an Associate;
2. Submit the required documentation showing you have cumulative paid full-time work experience of five years, or four years plus proof of having gained a four-year tertiary degree or (ISC)^2-approved credential; and
3. Get **endorsed by a member of (ISC)^2**.

Find the details on **CISSP work experience requirements here**.

The following diagram illustrates the eight domains of the CISSP Common Body of Knowledge (CBK).

Here is an overview of the two **CISSP exam** formats available:

EXAM FORMAT	DYNAMIC; **COMPUTERIZED ADAPTIVE TESTING (CAT)**	LINEAR; FIXED-FORM
Language(s) available	✓ English	✓ French ✓ German ✓ Brazilian ✓ Portuguese ✓ Spanish

EXAM FORMAT	DYNAMIC; **COMPUTERIZED ADAPTIVE TESTING (CAT)**	LINEAR; FIXED-FORM
		(Modern) ✓ Japanese ✓ Simplified Chinese ✓ Korean
Length (hours)	3–4	6
Number of questions	125–175	250
Can I change answers to earlier questions?	No	Yes

The passing mark is 700 out of 1000, and you can only take the examination on a computer via Pearson VUE. The exam consists of multiple-choice (four options, one correct answer) and scenario-based questions. As CISSP is a long examination, candidates may take breaks but won't get compensation in the form of extra exam time.
Remember to pick up (ISC)^2's **CISSP Ultimate Guide** and **Exam Action Plan**.

Domains

We've broken down the concepts and terms of the CBKs below. You may find **the latest updates on the exam here**. Remember to check out our **Security+ cheat sheet**, as both syllabi have overlapping concepts.

Security and Risk Management

This domain is the basis for all other domains, covering fundamental risk mitigation, legal and regulatory issues, professional ethics, and security concepts in an organizational context.

CONCEPT	ELABORATION
CIA	Confidentiality, Integrity, Availability
DAD	Disclosure, Alteration, Destruction
IAAA	Identification and Authentication, Authorization and Accountability

CONCEPT	ELABORATION
Least privilege	Minimum necessary access
Need to know	Just enough data to do your job
Non-repudiation	One cannot deny having done something
PCI-DSS	Payment Card Industry Data Security Standard
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
FRAP	Facilitated Risk Analysis Process
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations
ITIL	Information Technology Infrastructure Library
ISMS	Information security management system
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISO/IEC 27000 series	International standards on how to develop and maintain an ISMS developed by ISO and IEC
Defense in Depth/Layered Defense/Onion Defense	Multiple overlapping security controls to protect assets
Liability	Who is held accountable; C-level executives (senior leadership/management) are **ultimately liable**
Due care	Implementing security practices and patches Memory aid: **Do Correct**
Due diligence	Checking for vulnerabilities Memory aid: **Do Detect**
Negligence	Opposite of due care, without which you may become liable

CONCEPT	ELABORATION
GDPR	General Data Protection Regulation
Court-admissible evidence	• Relevant • Complete • Sufficient/believable • Reliable/accurate
HIPAA	Health Insurance Portability and Accountability Act
ECPA	Electronic Communications Privacy Act
USA PATRIOT ACT	**2001 legislation expanding law enforcement electronic monitoring**
CFAA	Computer Fraud and Abuse Act—Title 18 Section 1030 for prosecuting computer crimes
GLBA	Gramm-Leach-Bliley Act
SOX	Sarbanes-Oxley Act (2002)
Red team, blue team, purple team, etc.	(Refer to graphic below)

Check out our articles on **cyber security rules and regulations here**.

What do terms like “red team” and “blue team” mean in penetration testing?

The primary colors red, blue, and yellow refer to attackers, defenders, and builders of a system respectively. The secondary colors are combinations of these roles. For example, purple team members

Asset Security

Key concepts involving data and information are here.

CONCEPT	ELABORATION
Data at rest	On computer storage
Data in use/processing	In RAM being accessed

CONCEPT	ELABORATION
Data in transit/motion	Traveling along cables or broadcasting wirelessly
DRM	Digital Rights Management
CASB	Cloud Access Security Broker
DLP	Data Loss Prevention
Soft destruction	Preserve storage hardware
Full physical destruction	Destroy storage hardware

Security Architecture and Engineering

Here we focus on the most important methods to protect our assets.

Secure architecture and design

A well-designed computer system/network can deter many attacks.

CONCEPT	ELABORATION
Zachman framework	• What/data, How/function, Where/network, Who/people, When/time, and Why/motivation • Planner, Owner, Designer, Builder, Implementer, and Worker
TOGAF	The Open Group Architecture Framework
MODAF	Ministry of Defence Architecture Framework
SABSA	Sherwood Applied Business Security Architecture
The Red Book	Trusted Network Interpretation (TNI); part of a Rainbow Series
The Orange Book	The Trusted Computer System Evaluation Criteria (TCSEC); part of a Rainbow Series
Type 1 hypervisor	Bare or native metal
Type 2 hypervisor	App-like virtual machine on the operating system

00:00 00:00 1

CONCEPT	ELABORATION
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service

Cryptography

“A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.”—Auguste Kerckhoffs, cryptographer

CONCEPT	ELABORATION
Symmetric cipher	Streaming: • RC4 Block: • DES • Blowfish • 3DES Considerations: • key length • block size • number of rounds
	Examples: • Elliptic-curve cryptography
Hashing	One-way, deterministic process of transforming a string of characters into another
Salting	Characters appended to a string (e.g., password) before hashing
Steganography	Hide data inside other data
Quantum	Exploit quantum mechanics
Post-quantum	Secure against cryptanalysis by quantum computer

CONCEPT	ELABORATION
Brute-force attack	Trying character combinations Variant: spraying (trying the same password across different accounts)
Dictionary attack	Using lists of probable passwords
Rainbow tables	Using pre-calculated password hashes
Key stretching	Method that strengthens weak passwords

Physical security

A given physical security measure can fall into one or more categories below.

CONTROL TYPE	ELABORATION
Preventative	For preventing attacks, e.g., tall fences, locked doors, bollards
Detective	For detecting attacks, e.g., CCTV, alarms
Deterrent	For obstructing an attack, e.g., fences, security guards, dogs, lights, warning signs.
Compensating	To compensate for other controls, e.g., locks, alarms, sensors, shock absorbers in data center
Administrative	Compliance, policies, procedures, staff training, etc.

Communication and Network Security

CONCEPT	ELABORATION
Simplex	One-way communication
Half-duplex	Send/receive one at a time only
Full-duplex	Send/receive simultaneously

CONCEPT	ELABORATION
Baseband	One channel, send one signal at a time Example: Ethernet
Broadband	Multiple channels, send/receive many signals at a time
OSI model	Open Systems Interconnect: 1. Physical 2. Data Link 3. Network 4. Transport 5. Session 6. Presentation 7. Application Memory aid: **Please Do Not Throw Sausage Pizza Away**
ARP	Address Resolution Protocol
NAT	Network Address Translation
PAT	Port Address Translation
DHCP	Dynamic Host Configuration Protocol
PANA	Protocol for Carrying Authentication for Network Access
SLIP	Serial Line Internet Protocol
DMZ	• External network • External router • Perimeter network • Internal router • Internal network

00:00 00:00 1 ✕

Learn more about ports and protocols with our **Common Ports Cheat Sheet** here.

Identity and Access Management (IAM)

Logical and physical controls, identity-related services, and access control attacks comprise this domain.

CONCEPT	ELABORATION
2FA	Two-factor authentication
FRR	False rejection rate
FAR	False acceptance rate
CER/EER	Crossover error rate/equal error rate
IDaaS	Identity as a Service
Kerberos	Ticketing-based authentication protocol
SESAME	Secure European System for Applications in a Multi-vendor Environment
RADIUS	Remote Authentication Dial-In User Service
TACACS	Terminal Access Controller Access Control System
XTACACS	TACACS with separate authentication, authorization, and auditing processes
TACACS+	XTACACS plus 2FA
Diameter	Like RADIUS and TACACS+ with more flexibility
PAP	Password Authentication Protocol
CHAP	Challenge-Handshake Authentication Protocol

▶ 00:00 00:00 1⚡ ✕

Identity and Access Provisioning Lifecycle

Security Assessment and Testing

Penetration testing (pentesting) falls under this domain, which, being much more expansive, encompasses technical stress tests and reporting of vulnerabilities to non-technical members of the organization.

CONCEPT	ELABORATION
Static testing	Passively test code but not run it
Dynamic testing	Test code during execution
Fuzzing (Fuzz testing)	Input random characters and expect spurious results
Penetration testing (pentesting)	Actively exploit vulnerabilities
Black/gray/white box	Zero/Partial/extensive-knowledge pentesting
SOC	Service Organization Controls: 1, 2, and 3

Security Operations

This domain emphasizes the aspects of information security on management, prevention, recovery, and digital forensics.

CONCEPT	ELABORATION
BCP	Business continuity plan
BIA	Business impact analysis
COOP	Continuity of operations
DRP	Disaster Recovery Plan
MTBF	Mean time between failures
MTTR	Mean time to repair
RTO	Recovery time objective
RPO	Recovery point objective
SIEM	Security information and event management
NDA	Non-Disclosure Agreement

00:00 00:00 1 ⚡ ×

CONCEPT	ELABORATION
PAM	Privileged Account/Access Management
UEBA	User and Entity Behavior Analytics
Database Shadowing	Exact real-time copies of database/files to another location
Electronic Vaulting (E-vaulting)	Make remote backups at certain intervals or when files change
Remote Journaling	Sends transaction log files to a remote location, not the files themselves
Ways to minimize insider threats	• Least privilege • Need to know • Separation of duties • Job rotation • Mandatory vacations
Digital forensics	Process: • Identification • Preservation • Collection • Examination • Analysis • Presentation in Court • Court decision • Real evidence • Evidence integrity ○ When did they handle it? ○ What did they do with it? ○ Where did they handle it?
Disk-based forensic data	• Allocated space • Unallocated space • Slack space • Bad blocks/clusters/sectors

00:00 00:00 1

* This step is for real-world job settings only. It’s outside the CISSP exam syllabus, but in practice, the more thoroughly an organization equips its team for security incidents, the better it handles problems

00:00 00:00 1

Software Development Security

Building security controls into software applications is a new best practice in cyber security, and a CISSP needs to know how to secure software during its development.

CONCEPT	ELABORATION
SDS	Software-Defined Security
EULA	End-User License Agreement

CONCEPT	ELABORATION
SDLC	Software development life cycle: • Planning • Defining • Designing • Building • Testing • Deployment
CI/CD	Continuous Integration/Continuous [Delivery/Deployment/Development]
DevOps	Cooperation between development, operations, and quality assurance
DevSecOps	DevOps plus security
Software Development Methodologies	• Waterfall • Sashimi • Agile • Scrum • Extreme Programming (XP) • Spiral • Rapid Application Development (RAD) • Prototyping
ACID model	Atomicity, Consistency, Isolation, and Durability
OWASP	Open Web Application Security Project; identifies top vulnerabilities
CSRF/XSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting
TOC/TOU	Time-of-check/time-of-use

00:00 00:00 1

CONCEPT	ELABORATION
SOAR	Security Orchestration, Automation, and Response
Expert System	Computer system that emulates humanlike decision-making ability
ANN	Artificial Neural Networks
GP	Genetic Programming

Conclusion

We hope this CISSP exam cheat sheet provides a bird's-eye view of the CISSP syllabus, accelerates your cyber security journey, and helps you realize your career ambitions.

Find our **CISSP course offerings here** and check out **our other articles on CISSP**. We wish you all the best in your CISSP exam and beyond.

Frequently Asked Questions

⊖ Can I pass the CISSP exam in three months?

Yes, depending on your level of expertise. If you're new to (ISC)^2 certifications, expect your preparation to span three months or longer. If you have hands-on experience, that can affect the time you need. If you're a seasoned (10+ years) IT security professional, you're more likely to pass it with less study time.

⊕ Is the CISSP exam hard?

⊕ Why do people fail CISSP?

⊕ Can a beginner take CISSP?

⊕ Does CISSP increase salary?

⊕ How many times can you fail CISSP?

⊕ Is CISSP like a Master's degree?

Grow your Cyber Security Skills

CYBER SECURITY
Nathan House - Instructor
1. Welcome and Introduction to the Instructor Preview

FIND OUT MORE

00:00

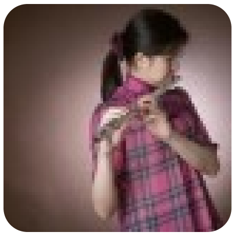
00:00

1

CATEGORIES

CERTIFICATIONS

CHEAT SHEETS



Cassandra Lee

I make connections across disciplines: cyber security, writing/journalism, art/design, music, mathematics, technology, education, psychology, and more. I've been advocating for girls and women in STEM since the 2010s, having written for Huffington Post, International Mathematical Olympiad 2016, and Ada Lovelace Day, and I'm honored to join StationX. You can find me on **LinkedIn** and **Linktree**.

Related Articles

Nmap Cheat Sheet 2023: All the Commands, Flags & Switches

Read More »

Linux Command Line Cheat Sheet: All the Commands You Need

Read More »

00:00 00:00 1

Read More »

Read More »

INFO

Affiliates

Legal Notices

Privacy Policy

Site Map

SECURITY ASSESSMENT

Penetration Testing

Vulnerability Scanning

Build Reviews

Source Code Review

Social Engineering

CONSULTING

Audit & Compliance

Incident Response

Security Architecture

Risk Assessment

Security Training

00:00 00:00 1