

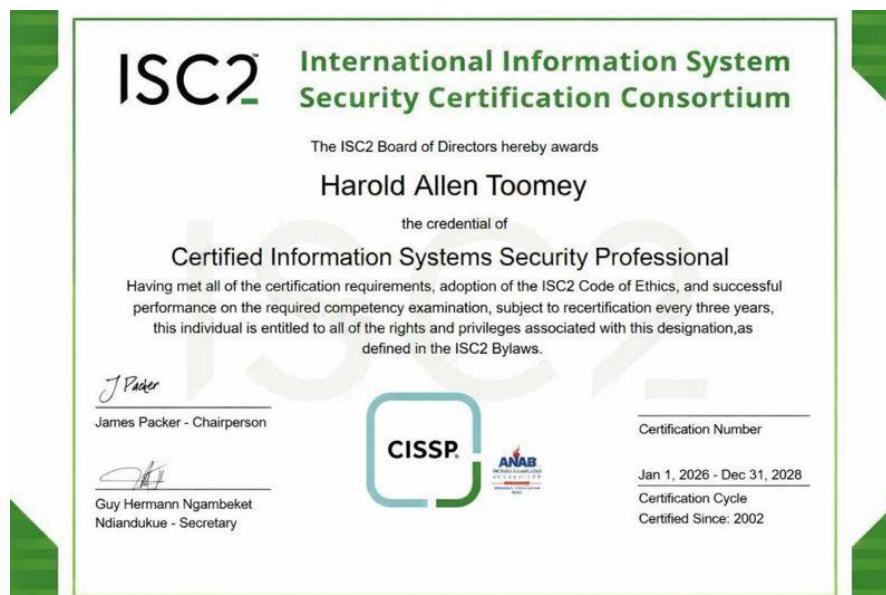
Harold's CISSP

Cheat Sheet

21 January 2026

Cybersecurity Certifications

Cert	Organization	Short Description
CISSP	ISC2	Broad, senior-level security credential covering governance, risk, architecture, operations, and security program leadership.
CISM	ISACA	Management-focused certification centered on information security governance, program development, and risk management leadership.
CEH	EC-Council	Ethical hacking overview covering common attack vectors, tools, and techniques used to assess security posture.
Security+	CompTIA	Entry-level, vendor-neutral baseline covering core security concepts, threats, risk management, and basic defensive practices.
CySA+	CompTIA	Defensive, analyst-focused credential emphasizing threat detection, monitoring, vulnerability management, and incident response.
PenTest+	CompTIA	Hands-on penetration testing fundamentals: planning/scoping, exploitation techniques, reporting, and remediation guidance.
CCSP	ISC2	Cloud security certification that is focused on cloud architecture, governance, risk, compliance, and security operations in cloud environments.
SSCP	ISC2	Practitioner-level systems security operations credential for implementing, monitoring, and administering security controls.
CISA	ISACA	Audit and assurance credential focusing on assessing controls, governance, and risk across information systems.
CRISC	ISACA	Risk-focused certification emphasizing enterprise IT risk identification, assessment, response, and control monitoring.



CISSP Overview

Aspect	Description
CISSP	Certified Information Systems Security Professional (CISSP) from ISC2
ISC2	International Information System Security Certification Consortium (ISC2) (Rebranded from (ISC) ² in 2023)
Description	CISSP is a globally recognized, senior-level, vendor-neutral cybersecurity certification focused on designing, managing, and governing an organization's overall security program. It's often treated as a benchmark credential for security leadership and experienced practitioners.
Target Audience	Best suited to people in roles like: <ul style="list-style-type: none"> • Security engineer / security architect • Security manager / security lead • GRC (governance, risk, compliance) • IT director / CISO-track professionals It's not an entry-level cert—most candidates already have several years in IT/security.
8 Domains (CBK)	CISSP spans broad security knowledge across eight areas (CBKs): <ol style="list-style-type: none"> 1. Security & Risk Management 2. Asset Security 3. Security Architecture & Engineering 4. Communication & Network Security 5. Identity & Access Management (IAM) 6. Security Assessment & Testing 7. Security Operations 8. Software Development Security
Experience Requirement	<ul style="list-style-type: none"> • To become fully certified, you typically need 5 years of paid work experience in 2 or more CISSP domains. • Some education/certs can reduce this requirement by 1 year. • If you pass the exam without the required experience, you can become an Associate of (ISC)² until you meet it.
The Exam	<ul style="list-style-type: none"> • Cost: \$599 • Retakes: <ul style="list-style-type: none"> ○ After 1st failed attempt: wait 30 days ○ After 2nd failed attempt: wait 60 days ○ After 3rd + failed attempts: wait 90 days • Computerized exam (English uses adaptive testing) • Mix of multiple-choice and advanced question formats • Tests both concepts and real-world judgment: risk tradeoffs, governance decisions, architecture thinking, etc.
Credibility	<ul style="list-style-type: none"> • The #1 most recognized cybersecurity certification • Signals broad security competency across the enterprise

CISSP Study Tools

Tool	Cost	Strengths
Boson ExSim-Max for CISSP	\$99 (1 year)	Provides a full practice-exam simulator (multiple full-length exams). Provides detailed explanations, scoring, and reporting.
Quantum Exams	Free samples \$139.99 (1 year) \$199.99 (1 year) w/CAT	Offers a Computer Adaptive Test (CAT) with a 3-hour time limit and variable-length exam (100–150 questions). Gives detailed explanations.
Crucial Exams	Free demo \$19.99 (1 month) \$44.99 (3 months) \$119.99 (1 year) \$189.99 (lifetime pass)	Can generate timed, custom exams to simulate the real test. Study Mode provides detailed explanations. Runs on the website with a “practice test” flow and timer settings.
ISC2 Official App by LearnZapp	\$4.99 (1 week) \$16.99 (1 month) \$44.99 (3 months) \$79.99 (6 months) \$139.99 (1 year)	Designed for smartphones. Includes thousands of practice questions with detailed explanations.
Pocket Prep	Free to try \$20.99 (1 month) \$49.99 (3 months) \$124.99 (12 months)	Designed for smartphones. Provides detailed explanations.
Sybex/Wiley Official Study Guide (10th Ed.)	\$56.00 (eBook) \$70.00 (print)	Best core textbook. Updated for the 2024 CISSP exam. Includes 900+ practice questions with complete answer explanations.
ISC2 CISSP Official Practice Tests (Sybex), 4th Edition	\$34.00 (eBook) \$42.00 (print)	Best companion book (practice questions in book form). Official practice-test book aligned to the 2024 CISSP domains. Includes access to Sybex’s online test environment.
The Official ISC2 CISSP CBK Reference, 6th Edition	\$76.00 (eBook) \$95.00 (print)	Best “official reference” (deep lookup, not the easiest first read). ISC2’s comprehensive CBK reference (authoritative, but more “reference manual” than exam-prep narrative).

CISSP Common Body of Knowledge (CBK)

1. Security & Risk Management

Topic	Diagrams and Lists

2. Asset Security

Topic	Diagrams and Lists

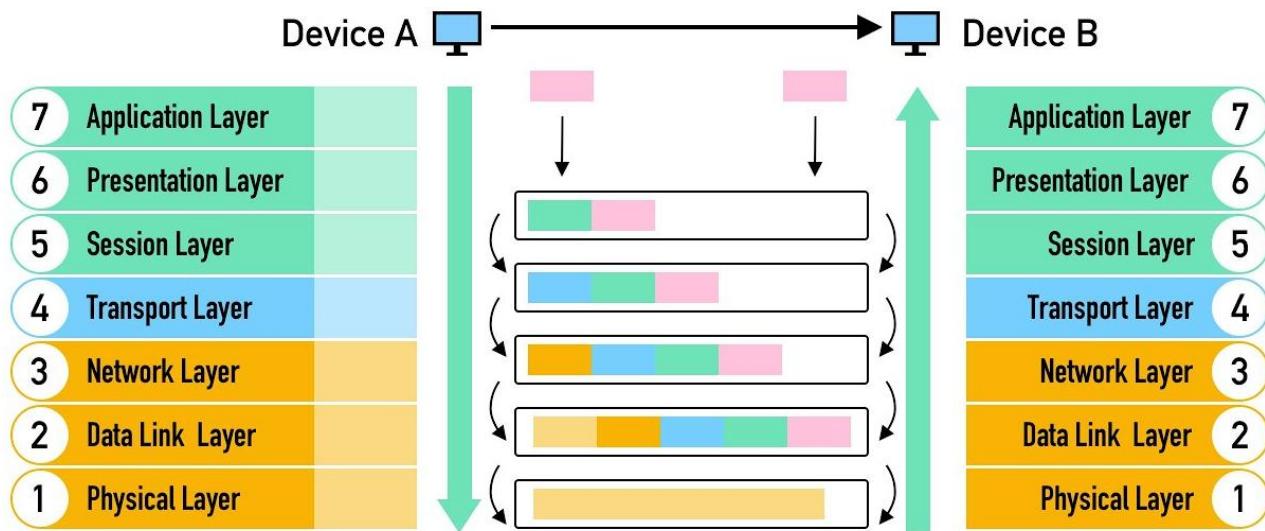
3. Security Architecture & Engineering

Topic	Diagrams and Lists

4. Communication & Network Security

Topic	Diagrams and Lists
OSI Model	ISO Open Source Interconnection 7-layer model
ASCII	American Standard Code for Information Interchange (ASCII)
Extended ASCII	ASCII extended by 128 characters for non-English languages
Unicode	Multi-byte character codes used internationally. Take more computer storage but offer unique characters for all of the world's languages + emojis.

ISO OSI Model



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the 'Translator' for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	Process
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R P A C K E T TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	Routers IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgement • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Can be used on all layers
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub Land Based Layers	Network

ASCII Table

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	Ø	96	60	~
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	\$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(72	48	H	104	68	h
9	09	Horizontal tab	41	29)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	:	91	5B	[123	7B	(
28	1C	File separator	60	3C	<	92	5C	\	124	7C	
29	1D	Group separator	61	3D	=	93	5D]	125	7D)
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Extended ASCII Table

Dec	Hex	Char									
128	80	ç	160	A0	á	192	C0	ł	224	E0	α
129	81	ü	161	A1	í	193	C1	ł	225	E1	ł
130	82	é	162	A2	ó	194	C2	ł	226	E2	ł
131	83	â	163	A3	ú	195	C3	ł	227	E3	ł
132	84	ä	164	A4	ñ	196	C4	ł	228	E4	ł
133	85	à	165	A5	Ñ	197	C5	ł	229	E5	ł
134	86	ã	166	A6	܂	198	C6	܂	230	E6	܂
135	87	܂	167	A7	܂	199	C7	܂	231	E7	܂
136	88	܂	168	A8	܂	200	C8	܂	232	E8	܂
137	89	܂	169	A9	܂	201	C9	܂	233	E9	܂
138	8A	܂	170	AA	܂	202	CA	܂	234	EA	܂
139	8B	܂	171	AB	܂	203	CB	܂	235	EB	܂
140	8C	܂	172	AC	܂	204	CC	܂	236	EC	܂
141	8D	܂	173	AD	܂	205	CD	܂	237	ED	܂
142	8E	܂	174	AE	܂	206	CE	܂	238	EE	܂
143	8F	܂	175	AF	܂	207	CF	܂	239	EF	܂
144	90	܂	176	B0	܂	208	D0	܂	240	F0	܂
145	91	܂	177	B1	܂	209	D1	܂	241	F1	܂
146	92	܂	178	B2	܂	210	D2	܂	242	F2	܂
147	93	܂	179	B3	܂	211	D3	܂	243	F3	܂
148	94	܂	180	B4	܂	212	D4	܂	244	F4	܂
149	95	܂	181	B5	܂	213	D5	܂	245	F5	܂
150	96	܂	182	B6	܂	214	D6	܂	246	F6	܂
151	97	܂	183	B7	܂	215	D7	܂	247	F7	܂
152	98	܂	184	B8	܂	216	D8	܂	248	F8	܂
153	99	܂	185	B9	܂	217	D9	܂	249	F9	܂
154	9A	܂	186	BA	܂	218	DA	܂	250	FA	܂
155	9B	܂	187	BB	܂	219	DB	܂	251	FB	܂
156	9C	܂	188	BC	܂	220	DC	܂	252	FC	܂
157	9D	܂	189	BD	܂	221	DD	܂	253	FD	܂
158	9E	܂	190	BE	܂	222	DE	܂	254	FE	܂
159	9F	܂	191	BF	܂	223	DF	܂	255	FF	܂

Intel x86 CPU Opcodes

ADD Eb Gb 00	ADD Ev Gv 01	ADD Gb Eb 02	ADD Gv Ev 03	ADD AL Ib 04	ADD eAX Iv 05	PUSH ES 06	POP ES 07	OR Eb Gb 08	OR Ev Gv 09	OR Gb Eb 0A	OR Gv Ev 0B	OR AL Ib 0C	OR eAX Iv 0D	PUSH CS 0E	TWOBYTE 0F
ADC Eb Gb 10	ADC Ev Gv 11	ADC Gb Eb 12	ADC Gv Ev 13	ADC AL Ib 14	ADC eAX Iv 15	PUSH SS 16	POP SS 17	SBB Eb Gb 18	SBB Ev Gv 19	SBB Gb Eb 1A	SBB Gv Ev 1B	SBB AL Ib 1C	SBB eAX Iv 1D	PUSH DS 1E	POP DS 1F
AND Eb Gb 20	AND Ev Gv 21	AND Gb Eb 22	AND Gv Ev 23	AND AL Ib 24	AND eAX Iv 25	ES: 26	DAA 27	SUB Eb Gb 28	SUB Ev Gv 29	SUB Gb Eb 2A	SUB Gv Ev 2B	SUB AL Ib 2C	SUB eAX Iv 2D	CS: 2E	DAS 2F
XOR Eb Gb 30	XOR Ev Gv 31	XOR Gb Eb 32	XOR Gv Ev 33	XOR AL Ib 34	XOR eAX Iv 35	SS: 36	AAA 37	CMP Eb Gb 38	CMP Ev Gv 39	CMP Gb Eb 3A	CMP Gv Ev 3B	CMP AL Ib 3C	CMP eAX Iv 3D	DS: 3E	AAS 3F
INC eAX 40	INC ecX 41	INC eDX 42	INC eBX 43	INC eSP 44	INC eBP 45	INC eSI 46	INC eDI 47	DEC eAX 48	DEC eCX 49	DEC eDX 4A	DEC eBX 4B	DEC eSP 4C	DEC eBP 4D	DEC eSI 4E	DEC eDI 4F
PUSH eAX 50	PUSH eCX 51	PUSH eDX 52	PUSH eBX 53	PUSH eSP 54	PUSH eBP 55	PUSH eSI 56	PUSH eDI 57	POP eAX 58	POP eCX 59	POP eDX 5A	POP eBX 5B	POP eSP 5C	POP eBP 5D	POP eSI 5E	POP eDI 5F
PUSHA 60	POPA 61	BOUND Gv Ma 62	ARPL Ew Gw 63	FS: 64	GS: 65	OPSIZE: 66	ADSIZE: 67	PUSH Iv 68	IMUL Gv Ev Iv 69	PUSH Ib 6A	IMUL Gv Ev Ib 6B	INSB Yb DX 6C	INSW Yz DX 6D	OUTSB DX Xb 6E	OUTSW DX Xv 6F
JO Jb 70	JNO Jb 71	JB Jb 72	JNB Jb 73	JZ Jb 74	JNZ Jb 75	JBE Jb 76	JA Jb 77	JS Jb 78	JNS Jb 79	JP Jb 7A	JNP Jb 7B	JL Jb 7C	JNL Jb 7D	JLE Jb 7E	JNLE Jb 7F
ADD Eb Ib 80	ADD Ev Iv 81	SUB Eb Ib 82	SUB Ev Ib 83	TEST Eb Gb 84	TEST Ev Gv 85	XCHG Eb Gb 86	XCHG Ev Gv 87	MOV Eb Gb 88	MOV Ev Gv 89	MOV Gb Eb 8A	MOV Gv Ev 8B	MOV Ew Sw 8C	LEA Gv M 8D	MOV Sw Ew 8E	POP Ev 8F
NOP 90	XCHG eAX eCX 91	XCHG eAX eDX 92	XCHG eAX eBX 93	XCHG eAX eSP 94	XCHG eAX eBP 95	XCHG eAX eSI 96	XCHG eAX eDI 97	CBW 98	CWD 99	CALL Ap 9A	WAIT 9B	PUSHF Fv 9C	POPF Fv 9D	SAHF 9E	LAHF 9F

5. Identity & Access Management (IAM)

Topic	Diagrams and Lists

6. Security Assessment & Testing

Topic	Diagrams and Lists

7. Security Operations

Topic	Diagrams and Lists

8. Software Development Security

Topic	Diagrams and Lists

TBD

Topic	Diagrams and Lists

Sources

- <Author> (year). <Title>. <Link>

TBD

TBD
