INFOSECTRAIN

CISSP 45 Days Plan

	Chapter / subchapter name		Page	Target latest possible / actual completion date
Chapter difficulty	**Chapter 1 Security Governance Through Principles and Policies**		1	
1		Understand and Apply Concepts of Confidentiality, Integrity, and Availability	3	
		Confidentiality	4	
		Integrity	5	
		Availability	6	
		Other Security Concepts	8	
		Protection Mechanisms	12	
		Layering	12	
		Abstraction	12	
		Data Hiding	13	
		Encryption	13	
		Apply Security Governance Principles	13	
		Alignment of Security Function to Strategy, Goals, Mission, and Objectives	14	
		Organizational Processes	16	
		Security Roles and Responsibilities	22	
		Control Frameworks	23	
		Due Care and Due Diligence	24	
		Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines	25	
		Security Policies	25	
		Security Standards, Baselines, and Guidelines	26	
		Security Procedures	27	
		Understand and Apply Threat Modeling	28	
		Identifying Threats	30	
		Determining and Diagramming Potential Attacks	32	
		Performing Reduction Analysis	33	
		Prioritization and Response	34	
		Integrate Security Risk Considerations into Acquisition Strategy and Practice	35	
		Summary	36	
		Exam Essentials	38	
		Written Lab	41	
		Review Questions	42	
	Chapter 2 Personnel Security and Risk Management Concepts		47	
		Contribute to Personnel Security Policies	49	
		Employment Candidate Screening	52	
		Employment Agreements and Policies	53	
		Employment Termination Processes	54	
		Vendor, Consultant, and Contractor Controls	56	
		Compliance	57	
		Privacy	57	
		Security Governance	59	
		Understand and Apply Risk Management Concepts	60	
		Risk Terminology	61	
		Identify Threats and Vulnerabilities	63	
		Risk Assessment/Analysis	64	
		Risk Assignment/Acceptance	72	
		Countermeasure Selection and Assessment	73	
		Implementation	74	
		Types of Controls	75	
		Monitoring and Measurement	76	
		Asset Valuation	77	
		Continuous Improvement	78	
		Risk Frameworks	78	
		Establish and Manage Information Security Education, Training, and Awareness	81	
		Manage the Security Function	82	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Summary	83	
		Exam Essentials	84	
		Written Lab	88	
		Review Questions	89	
1		**Chapter 3 Business Continuity Planning**	93	
		Planning for Business Continuity	94	
		Project Scope and Planning	95	
		Business Organization Analysis	96	
		BCP Team Selection	96	
		Resource Requirements	98	
		Legal and Regulatory Requirements	100	
		Business Impact Assessment	101	
		Identify Priorities	101	
		Risk Identification	102	
		Likelihood Assessment	104	
		Impact Assessment	104	
		Resource Prioritization	106	
		Continuity Planning	107	
		Strategy Development	107	
		Provisions and Processes	108	
		Plan Approval	109	
		Plan Implementation	110	
		Training and Education	110	
		BCP Documentation	110	
		Continuity Planning Goals	111	
		Statement of Importance	111	
		Statement of Priorities	111	
		Statement of Organizational Responsibility	111	
		Statement of Urgency and Timing	112	
		Risk Assessment	112	
		Risk Acceptance/Mitigation	112	
		Vital Records Program	113	
		Emergency-Response Guidelines	113	
		Maintenance	114	
		Testing and Exercises	114	
		Summary	114	
		Exam Essentials	115	
		Written Lab	117	
		Review Questions	118	
1		**Chapter 4 Laws, Regulations, and Compliance**	123	
		Categories of Laws	124	
		Criminal Law	124	
		Civil Law	126	
		Administrative Law	126	
		Laws	127	
		Computer Crime	127	
		Intellectual Property	132	
		Licensing	138	
		Import/Export	139	
		Privacy	139	
		Compliance	146	
		Contracting and Procurement	147	
		Summary	148	
		Exam Essentials	149	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty	Chapter / subchapter name		Page	Target latest possible / actual completion date
		Written Lab	151	
		Review Questions	152	
1	**Chapter 5 Protecting Security of Assets**		157	
		Classifying and Labeling Assets	158	
		Defining Sensitive Data	158	
		Defining Classifications	160	
		Defining Data Security Requirements	163	
		Understanding Data States	164	
		Managing Sensitive Data	165	
		Protecting Confidentiality with Cryptography	172	
		Identifying Data Roles	174	
		Data Owners	174	
		System Owners	175	
		Business/Mission Owners	176	
		Data Processors	176	
		Administrators	177	
		Custodians	178	
		Users	178	
		Protecting Privacy	178	
		Using Security Baselines	179	
		Scoping and Tailoring	180	
		Selecting Standards	180	
		Summary	181	
		Exam Essentials	182	
		Written Lab	183	
		Review Questions	184	
2	**Chapter 6 Cryptography and Symmetric Key Algorithms**		189	
		Historical Milestones in Cryptography	190	
		Caesar Cipher	190	
		American Civil War	191	
		Ultra vs. Enigma	192	
		Cryptographic Basics	192	
		Goals of Cryptography	192	
		Cryptography Concepts	194	
		Cryptographic Mathematics	196	
		Ciphers	201	
		Modern Cryptography	208	
		Cryptographic Keys	208	
		Symmetric Key Algorithms	209	
		Asymmetric Key Algorithms	210	
		Hashing Algorithms	213	
		Symmetric Cryptography	214	
		Data Encryption Standard	214	
		Triple DES	216	
		International Data Encryption Algorithm	217	
		Blowfish	217	
		Skipjack	217	
		Advanced Encryption Standard	218	
		Symmetric Key Management	219	
		Cryptographic Life Cycle	222	
		Summary	222	
		Exam Essentials	223	
		Written Lab	225	
		Review Questions	226	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty	Chapter / subchapter name		Page	Target latest possible / actual completion date
2	**Chapter 7 PKI and Cryptographic Applications**		231	
		Asymmetric Cryptography	232	
		Public and Private Keys	232	
		RSA	233	
		El Gamal	235	
		Elliptic Curve	235	
		Hash Functions	236	
		SHA	237	
		MD2	238	
		MD4	238	
		MD5	239	
		Digital Signatures	240	
		HMAC	241	
		Digital Signature Standard	242	
		Public Key Infrastructure	242	
		Certificates	243	
		Certificate Authorities	243	
		Certificate Generation and Destruction	245	
		Asymmetric Key Management	246	
		Applied Cryptography	247	
		Portable Devices	247	
		Email	248	
		Web Applications	249	
		Digital Rights Management	252	
		Networking	255	
		Cryptographic Attacks	258	
		Summary	261	
		Exam Essentials	261	
		Written Lab	264	
		Review Questions	265	
1	**Chapter 8 Principles of Security Models, Design, and Capabilities**		269	
		Implement and Manage Engineering Processes Using Secure Design Principles	270	
		Objects and Subjects	271	
		Closed and Open Systems	271	
		Techniques for Ensuring Confidentiality, Integrity, and Availability	272	
		Controls	274	
		Trust and Assurance	274	
		Understand the Fundamental Concepts of Security Models	275	
		Trusted Computing Base	276	
		State Machine Model	278	
		Information Flow Model	279	
		Noninterference Model	279	
		Take-Grant Model	280	
		Access Control Matrix	280	
		Bell-LaPadula Model	282	
		Biba Model	284	
		Clark-Wilson Model	286	
		Brewer and Nash Model (aka Chinese Wall)	287	
		Goguen-Meseguer Model	288	
		Sutherland Model	288	
		Graham-Denning Model	288	
		Select Controls and Countermeasures Based on Systems Security Evaluation Models	289	
		Rainbow Series	290	
		ITSEC Classes and Required Assurance and Functionality	295	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Common Criteria	296	
		Industry and International Security Implementation Guidelines	299	
		Certification and Accreditation	300	
		Understand Security Capabilities of Information Systems	303	
		Memory Protection	303	
		Virtualization	303	
		Trusted Platform Module	303	
		Interfaces	304	
		Fault Tolerance	304	
		Summary	305	
		Exam Essentials	305	
		Written Lab	307	
		Review Questions	308	
2	**Chapter 9 Security Vulnerabilities, Threats, and Countermeasures**		313	
		Assess and Mitigate Security Vulnerabilities	314	
		Hardware	315	
		Input/Output Structures	335	
		Firmware	336	
		Client-Based	337	
		Applets	337	
		Local Caches	339	
		Server Based	341	
		Database Security	341	
		Aggregation	341	
		Inference	342	
		Data Mining and Data Warehousing	342	
		Data Analytics	343	
		Large-Scale Parallel Data Systems	344	
		Distributed Systems	344	
		Cloud Computing	346	
		Grid Computing	347	
		Peer to Peer	348	
		Industrial Control Systems	348	
		Assess and Mitigate Vulnerabilities in Web-Based Systems	349	
		Assess and Mitigate Vulnerabilities in Mobile Systems	350	
		Device Security	352	
		Application Security	355	
		BYOD Concerns	357	
		Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems	360	
		Examples of Embedded and Static Systems	360	
		Methods of Securing	362	
		Essential Security Protection Mechanisms	364	
		Technical Mechanisms	364	
		Security Policy and Computer Architecture	367	
		Policy Mechanisms	367	
		Common Architecture Flaws and Security Issues	369	
		Covert Channels	369	
		Attacks Based on Design or Coding Flaws and Security Issues	370	
		Programming	373	
		Timing, State Changes, and Communication Disconnects	373	
		Technology and Process Integration	374	
		Electromagnetic Radiation	374	
		Summary	375	
		Exam Essentials	376	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty	Chapter / subchapter name	Page	Target latest possible / actual completion date
	Written Lab	379	
	Review Questions	380	
1	**Chapter 10 Physical Security Requirements**	385	
	Apply Secure Principles to Site and Facility Design	386	
	Secure Facility Plan	387	
	Site Selection	387	
	Visibility	388	
	Natural Disasters	388	
	Facility Design	388	
	Design and Implement Physical Security	389	
	Equipment Failure	390	
	Wiring Closets	391	
	Server Rooms	393	
	Media Storage Facilities	394	
	Evidence Storage	395	
	Restricted and Work Area Security (e.g., Operations Centers)	395	
	Datacenter Security	396	
	Utilities and HVAC Considerations	399	
	Water Issues (e.g., Leakage, Flooding)	402	
	Fire Prevention, Detection, and Suppression	402	
	Implement and Manage Physical Security	407	
	Perimeter (e.g., Access Control and Monitoring)	407	
	Internal Security (e.g., Escort Requirements/Visitor Control, Keys, and Locks)	409	
	Summary	415	
	Exam Essentials	416	
	Written Lab	420	
	Review Questions	421	
3	**Chapter 11 Secure Network Architecture and Securing Network Components**	425	
	OSI Model	426	
	History of the OSI Model	427	
	OSI Functionality	427	
	Encapsulation/Deencapsulation	428	
	OSI Layers	429	
	TCP/IP Model	437	
	TCP/IP Protocol Suite Overview	438	
	Converged Protocols	452	
	Content Distribution Networks	453	
	Wireless Networks	454	
	Securing Wireless Access Points	454	
	Securing the SSID	456	
	Conducting a Site Survey	457	
	Using Secure Encryption Protocols	458	
	Determining Antenna Placement	461	
	Antenna Types	461	
	Adjusting Power Level Controls	461	
	Using Captive Portals	462	
	General Wi-Fi Security Procedure	462	
	Secure Network Components	463	
	Network Access Control	464	
	Firewalls	465	
	Endpoint Security	469	
	Other Network Devices	469	
	Cabling, Wireless, Topology, and Communications Technology	473	
	Network Cabling	473	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Network Topologies	477	
		Wireless Communications and Security	480	
		LAN Technologies	485	
		Summary	490	
		Exam Essentials	490	
		Written Lab	494	
		Review Questions	495	
3		**Chapter 12 Secure Communications and Network Attacks**	499	
		Network and Protocol Security Mechanisms	500	
		Secure Communications Protocols	501	
		Authentication Protocols	502	
		Secure Voice Communications	503	
		Voice over Internet Protocol (VoIP)	503	
		Social Engineering	504	
		Fraud and Abuse	505	
		Multimedia Collaboration	507	
		Remote Meeting	508	
		Instant Messaging	508	
		Manage Email Security	508	
		Email Security Goals	509	
		Understand Email Security Issues	510	
		Email Security Solutions	511	
		Remote Access Security Management	513	
		Plan Remote Access Security	515	
		Dial-Up Protocols	516	
		Centralized Remote Authentication Services	517	
		Virtual Private Network	517	
		Tunneling	518	
		How VPNs Work	519	
		Common VPN Protocols	520	
		Virtual LAN	522	
		Virtualization	523	
		Virtual Software	523	
		Virtual Networking	524	
		Network Address Translation	525	
		Private IP Addresses	526	
		Stateful NAT	527	
		Static and Dynamic NAT	528	
		Automatic Private IP Addressing	528	
		Switching Technologies	530	
		Circuit Switching	530	
		Packet Switching	531	
		Virtual Circuits	532	
		WAN Technologies	532	
		WAN Connection Technologies	534	
		Dial-Up Encapsulation Protocols	536	
		Miscellaneous Security Control Characteristics	537	
		Transparency	537	
		Verify Integrity	537	
		Transmission Mechanisms	538	
		Security Boundaries	539	
		Prevent or Mitigate Network Attacks	539	
		DoS and DDoS	540	
		Eavesdropping	541	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Impersonation/Masquerading	542	
		Replay Attacks	542	
		Modification Attacks	542	
		Address Resolution Protocol Spoofing	542	
		DNS Poisoning, Spoofing, and Hijacking	543	
		Hyperlink Spoofing	544	
		Summary	545	
		Exam Essentials	546	
		Written Lab	549	
		Review Questions	550	
1	**Chapter 13 Managing Identity and Authentication**		555	
		Controlling Access to Assets	556	
		Comparing Subjects and Objects	557	
		Types of Access Control	557	
		The CIA Triad	560	
		Comparing Identification and Authentication	560	
		Registration and Proofing of Identity	561	
		Authorization and Accountability	561	
		Authentication Factors	563	
		Passwords	564	
		Smartcards and Tokens	566	
		Biometrics	568	
		Multifactor Authentication	572	
		Device Authentication	572	
		Implementing Identity Management	573	
		Single Sign-On	573	
		Credential Management Systems	578	
		Integrating Identity Services	579	
		Managing Sessions	579	
		AAA Protocols	580	
		Managing the Identity and Access Provisioning Life Cycle	582	
		Provisioning	582	
		Account Review	583	
		Account Revocation	584	
		Summary	585	
		Exam Essentials	586	
		Written Lab	588	
		Review Questions	589	
1	**Chapter 14 Controlling and Monitoring Access**		593	
		Comparing Access Control Models	594	
		Comparing Permissions, Rights, and Privileges	594	
		Understanding Authorization Mechanisms	595	
		Defining Requirements with a Security Policy	596	
		Implementing Defense in Depth	597	
		Discretionary Access Controls	598	
		Nondiscretionary Access Controls	598	
		Understanding Access Control Attacks	604	
		Risk Elements	605	
		Identifying Assets	605	
		Identifying Threats	607	
		Identifying Vulnerabilities	609	
		Common Access Control Attacks	610	
		Summary of Protection Methods	619	
		Summary	621	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Exam Essentials	622	
		Written Lab	624	
		Review Questions	625	
1		**Chapter 15 Security Assessment and Testing**	629	
		Building a Security Assessment and Testing Program	630	
		Security Testing	630	
		Security Assessments	631	
		Security Audits	632	
		Performing Vulnerability Assessments	634	
		Vulnerability Scans	634	
		Penetration Testing	642	
		Testing Your Software	643	
		Code Review and Testing	644	
		Interface Testing	646	
		Misuse Case Testing	648	
		Test Coverage Analysis	648	
		Implementing Security Management Processes	649	
		Log Reviews	649	
		Account Management	649	
		Backup Verification	650	
		Key Performance and Risk Indicators	650	
		Summary	650	
		Exam Essentials	651	
		Written Lab	653	
		Review Questions	654	
1		**Chapter 16 Managing Security Operations**	659	
		Applying Security Operations Concepts	661	
		Need to Know and Least Privilege	661	
		Separation of Duties and Responsibilities	663	
		Job Rotation	666	
		Mandatory Vacations	666	
		Monitor Special Privileges	667	
		Managing the Information Life Cycle	668	
		Service Level Agreements	669	
		Addressing Personnel Safety	670	
		Provisioning and Managing Resources	670	
		Managing Hardware and Software Assets	671	
		Protecting Physical Assets	672	
		Managing Virtual Assets	672	
		Managing Cloud-based Assets	673	
		Media Management	675	
		Managing Configuration	678	
		Baselining	678	
		Using Images for Baselining	678	
		Managing Change	680	
		Security Impact Analysis	682	
		Versioning	683	
		Configuration Documentation	683	
		Managing Patches and Reducing Vulnerabilities	684	
		Patch Management	684	
		Vulnerability Management	685	
		Common Vulnerabilities and Exposures	688	
		Summary	688	
		Exam Essentials	689	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Written Lab	691	
		Review Questions	692	
1		**Chapter 17 Preventing and Responding to Incidents**	697	
		Managing Incident Response	698	
		Defining an Incident	698	
		Incident Response Steps	699	
		Implementing Preventive Measures	704	
		Basic Preventive Measures	705	
		Understanding Attacks	705	
		Intrusion Detection and Prevention Systems	715	
		Specific Preventive Measures	721	
		Logging, Monitoring, and Auditing	731	
		Logging and Monitoring	731	
		Egress Monitoring	740	
		Auditing to Assess Effectiveness	742	
		Security Audits and Reviews	745	
		Reporting Audit Results	746	
		Summary	748	
		Exam Essentials	750	
		Written Lab	754	
		Review Questions	755	
1		**Chapter 18 Disaster Recovery Planning**	759	
		The Nature of Disaster	760	
		Natural Disasters	761	
		Man-made Disasters	765	
		Understand System Resilience and Fault Tolerance	770	
		Protecting Hard Drives	771	
		Protecting Servers	772	
		Protecting Power Sources	773	
		Trusted Recovery	773	
		Quality of Service	775	
		Recovery Strategy	775	
		Business Unit and Functional Priorities	776	
		Crisis Management	777	
		Emergency Communications	777	
		Workgroup Recovery	778	
		Alternate Processing Sites	778	
		Mutual Assistance Agreements	782	
		Database Recovery	783	
		Recovery Plan Development	784	
		Emergency Response	785	
		Personnel and Communications	786	
		Assessment	787	
		Backups and Offsite Storage	787	
		Software Escrow Arrangements	790	
		External Communications	791	
		Utilities	791	
		Logistics and Supplies	791	
		Recovery vs. Restoration	791	
		Training, Awareness, and Documentation	792	
		Testing and Maintenance	793	
		Read-Through Test	793	
		Structured Walk-Through	794	
		Simulation Test	794	

INFOSECTRAIN

CISSP 45 Days Plan

Chapter difficulty		Chapter / subchapter name	Page	Target latest possible / actual completion date
		Parallel Test	794	
		Full-Interruption Test	794	
		Maintenance	794	
		Summary	795	
		Exam Essentials	795	
		Written Lab	797	
		Review Questions	798	
1		**Chapter 19 Incidents and Ethics**	803	
		Investigations	804	
		Investigation Types	804	
		Evidence	806	
		Investigation Process	810	
		Major Categories of Computer Crime	812	
		Military and Intelligence Attacks	813	
		Business Attacks	814	
		Financial Attacks	814	
		Terrorist Attacks	815	
		Grudge Attacks	815	
		Thrill Attacks	817	
		Incident Handling	817	
		Common Types of Incidents	818	
		Response Teams	820	
		Incident Response Process	821	
		Interviewing Individuals	824	
		Incident Data Integrity and Retention	825	
		Reporting and Documenting Incidents	825	
		Ethics	826	
		(ISC) 2 Code of Ethics	827	
		Ethics and the Internet	828	
		Summary	829	
		Exam Essentials	830	
		Written Lab	832	
		Review Questions	833	
2		**Chapter 20 Software Development Security**	837	
		Introducing Systems Development Controls	838	
		Software Development	838	
		Systems Development Life Cycle	844	
		Life Cycle Models	847	
		Gantt Charts and PERT	853	
		Change and Configuration Management	853	
		The DevOps Approach	855	
		Application Programming Interfaces	856	
		Software Testing	857	
		Code Repositories	858	
		Service-Level Agreements	859	
		Software Acquisition	860	
		Establishing Databases and Data Warehousing	860	
		Database Management System Architecture	861	
		Database Transactions	864	
		Security for Multilevel Databases	866	
		ODBC	868	
		Storing Data and Information	869	
		Types of Storage	869	
		Storage Threats	870	

CISSP 45 Days Plan

		Understanding Knowledge-based Systems		
		Expert Systems		870
		Neural Networks		
		Decision Support Systems		
		Security Applications		
		Summary		
		Exam Essentials		
		Written Lab		
		Review Questions		
1.5		**Chapter 21 Malicious Code and Application Attacks**		
		Malicious Code		
		Sources of Malicious Code		
		Viruses		
		Logic Bombs		
		Trojan Horses		
		Worms		
		Spyware and Adware		
		Countermeasures		
		Password Attacks		
		Password Guessing		
		Dictionary Attacks		
		Social Engineering		
		Countermeasures		
		Application Attacks		
		Buffer Overflows		
		Time of Check to Time of Use		
		Back Doors		
		Escalation of Privilege and Rootkits		
		Web Application Security		
		Cross-Site Scripting (XSS)		
		SQL Injection		
		Reconnaissance Attacks		
		IP Probes		
		Port Scans		
		Vulnerability Scans		
		Dumpster Diving		
		Masquerading Attacks		
		IP Spoofing		
		Session Hijacking		
		Summary		
		Exam Essentials		
		Written Lab		
		Review Questions		
		Full practice tests		