> INFOSEC & NETWORKING

Certification Prep

CISSP · CEH · Networking Fundamentals

DOMAINS | FRAMEWORKS | CRYPTOGRAPHY | NETWORKING | THREATS

Course Overview & Objectives

01

CISSP Domains

8 knowledge domains — post & pre-2015

02

Frameworks & Compliance

NIST 800-53, FISMA, GRC, ISO 27001, Cloud/FedRAMP

03

Networking Fundamentals

OSI, TCP/IP, subnetting, routing

04

Firewalls & DPI

Rule sets, NGFWs, deep packet inspection

05

Cryptography

Hashing, encryption, PKI, Diffie-Hellman

06

CEH Attack Methodology

Recon, exploitation, evasion techniques

07

GRC

Governance, Risk & Compliance

08

POA&M Tracking

Remediation, milestones, ATO relationship

09

ISO 27001 / Cloud

ISMS, FedRAMP baselines, cloud security

10

Exam Strategy

CISSP mindset, time management, prep

01

CISSP Domains

Security knowledge framework — post & pre-2015

CISSP Domains — Post-2015 (Current)

D1 **Security & Risk Management** — EXAM 15%

Policies, ethics, compliance, risk frameworks

D2 **Asset Security** — EXAM 10%

Data classification, ownership, retention

D3 **Security Architecture & Engineering** — EXAM 13%

Security models, cryptography, vulnerabilities

D4 **Comm. & Network Security** — EXAM 13%

Network design, protocols, attack prevention

D5 **Identity & Access Management** — EXAM 13%

Authentication, authorization, SSO, biometrics

D6 **Security Assessment & Testing** — EXAM 12%

Audits, pen testing, log reviews

D7 **Security Operations** — EXAM 13%

Incident response, forensics, BCP/DR

D8 **Software Dev. Security** — EXAM 11%

SDLC, secure coding, DevSecOps

CISSP Domains — Pre-2015 (Legacy / Reference)

01 Access Control	Authentication types, SSO, biometrics, auditing
02 Telecom & Network Security	Network architecture, protocols, transmission security
03 Information Security Governance & Risk Mgmt	Policy, classification, risk treatment, training
04 Software Development Security	SDLC, change control, application security
05 Cryptography	Symmetric/asymmetric, PKI, digital signatures
06 Security Architecture & Design	Security models, OS protection, virtualization
07 Operations Security	Patch management, incident response, access controls
08 Business Continuity & Disaster Recovery	BIA, RTO, RPO, continuity planning
09 Legal, Regulations & Compliance	Computer crime law, forensics, evidence
10 Physical (Environment) Security	Facility design, perimeter, environmental controls

//

02

Frameworks & Compliance

NIST · FISMA · DIACAP · ISO 27001

SECTION

NIST SP 800-53 Rev 5 — Control Families

20 control families covering the full security and privacy lifecycle (NIST SP 800-53 Rev 5)

AC Access Control	**AT** Awareness & Training	**AU** Audit & Accountability	**CA** Assessment, Auth & Monitoring	**CM** Configuration Mgmt
CP Contingency Planning	**IA** Identification & Auth	**IR** Incident Response	**MA** Maintenance	**MP** Media Protection
PE Physical & Environmental	**PL** Planning	**PM** Program Management	**PS** Personnel Security	**PT** PII Processing & Transparency
RA Risk Assessment	**SA** System & Services Acquisition	**SC** System & Comm. Protection	**SI** System & Info. Integrity	**SR** Supply Chain Risk

NIST 800-53 — Security Control Baselines

Low · Moderate · High — control ranges per family

CONTROL FAMILY	LOW	MODERATE	HIGH
Access Control (AC)	AC-1 to AC-3	AC-1 to AC-17	AC-1 to AC-25
Audit & Accountability (AU)	AU-1 to AU-4	AU-1 to AU-12	AU-1 to AU-16
Config. Management (CM)	CM-1 to CM-4	CM-1 to CM-11	CM-1 to CM-14
Identification & Auth (IA)	IA-1 to IA-4	IA-1 to IA-10	IA-1 to IA-12
Incident Response (IR)	IR-1 to IR-4	IR-1 to IR-8	IR-1 to IR-10
Risk Assessment (RA)	RA-1 to RA-3	RA-1 to RA-7	RA-1 to RA-10
System & Comm. Protection (SC)	SC-1 to SC-5	SC-1 to SC-28	SC-1 to SC-51
System & Info. Integrity (SI)	SI-1 to SI-3	SI-1 to SI-12	SI-1 to SI-23

Higher impact systems require more controls with stricter implementation guidance.

NIST 800-53 — Impact Baselines (Low / Moderate / High)

CONTROL	LOW IMPACT	MODERATE	HIGH IMPACT
Access Control (AC)	3 controls	17 controls	25 controls
Audit & Accountability (AU)	4 controls	12 controls	16 controls
Config. Management (CM)	4 controls	11 controls	14 controls
Identification & Auth (IA)	4 controls	10 controls	12 controls
Incident Response (IR)	4 controls	8 controls	10 controls
Risk Assessment (RA)	3 controls	7 controls	10 controls
System & Comm. Protection (SC)	5 controls	28 controls	51 controls
System & Info. Integrity (SI)	3 controls	12 controls	23 controls

TOTAL (full baseline): Low ~ 125 controls | Moderate ~ 325 controls | High ~ 421 controls

FISMA 2014 — Federal Info Security Modernization Act

WHAT FISMA DOES

- Codifies DHS authority over federal civilian agency cybersecurity
- Requires all federal systems to adopt NIST 800-53 controls
- Mandates annual security reviews and C&A (ATO) process
- Clarifies OMB oversight over agency information security
- Requires OMB to revise A-130 to eliminate wasteful reporting
- Establishes continuous monitoring requirements (vs. point-in-time audits)

KEY ACTORS & ROLES

CISA (DHS)

Administers implementation, deploys security tech, provides assistance

OMB

Oversight authority; reviews agency practices and A-130 policy

NIST

Develops standards, guidelines (SP 800-series)

Agency CIO

Reports security status; owns ATO decisions

ISSO

Day-to-day security posture, POA&M management

NIST RMF — Risk Management Framework (7-Step Process)

NIST SP 800-37 Rev 2 — Structured process for integrating security and privacy into the system development lifecycle. Replaces DIACAP (DoDI 8510.01, 2014). Required for all federal systems under FISMA.

1

Step 1 — Prepare

Establish context, roles, and strategy. Define the risk management strategy; assign system owner, ISSO, and AO. Categorize mission needs.

2

Step 2 — Categorize

Classify system per FIPS 199 (Confidentiality, Integrity, Availability). Impact level = Low, Moderate, or High. Drives control baseline selection.

3

Step 3 — Select

Choose NIST 800-53 control baseline (Low/Moderate/High). Tailor controls, apply overlays, document in System Security Plan (SSP).

4

Step 4 — Implement

Deploy selected controls. Document implementation details in SSP. Apply compensating controls where required. Update POA&M as needed.

5

Steps 5-7 — Assess · Authorize · Monitor

Assess: Independent evaluator tests controls; produces SAR. Authorize: AO reviews SAR + POA&M; grants ATO, ATO w/Conditions, or DATO. Monitor: Continuous monitoring, ongoing POA&M, annual review cycle.

NOTE: DIACAP was superseded by the NIST RMF per DoDI 8510.01 (2014). RMF is now the authoritative framework for all federal and DoD systems. DIACAP may still appear on legacy exam versions — know both.

DoD 8570.01-M — IA Workforce Certifications

Three tracks: IAT (Technical) · IAM (Management) · IASAE (Architecture & Engineering). CE = Continuing Education edition required.

IAT — INFORMATION ASSURANCE TECHNICAL	*Operates & administers IA/CS systems*
IAT Level I	A+ CE, Network+ CE, SSCP, CCNA Security, CND, CySA+
IAT Level II	Security+ CE, CySA+, CCNA Security, GICSP, GSEC, SSCP
IAT Level III	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH

IAM — INFORMATION ASSURANCE MANAGEMENT	*Oversees IA programs, policy, and personnel*
IAM Level I	CAP, CND, Security+ CE, GSLC, HCISPP
IAM Level II	CAP, CASP+ CE, CISM, CISSP (or Associate), GSLC, CCISO
IAM Level III	CISM, CISSP (or Associate), GSLC, CCISO

IASAE — IA ARCHITECTURE & ENGINEERING	*Designs and engineers IA solutions*
IASAE Level I	CASP+ CE, CISSP (or Associate), CSSLP
IASAE Level II	CASP+ CE, CISSP (or Associate), CSSLP
IASAE Level III	CISSP-ISSEP, CISSP-ISSAP

DoD 8140.01 — Cyberspace Workforce Framework

Transition from DoD 8570.01-M

8570 Issued: 2005 → **8140 Signed: Nov 2015** → **8140.01 Manual: Feb 2023**

8570 formally retired — 8140 now governs all DoD cyberspace workforce roles

WHAT CHANGED IN 8140

NICE Framework aligned

Roles now map to NIST NICE Cybersecurity Workforce Framework (SP 800-181) — 7 categories, 33 specialty areas

Role-based vs. position-based

8570 tied certs to positions; 8140 ties them to work roles — finer granularity, more flexible assignment

Expanded role categories

Old: IAT/IAM/IASAE. New: Operate & Maintain, Protect & Defend, Analyze, Collect & Operate, Investigate, Oversee & Govern, Securely Provision

Qualification vs. certification only

8140 allows non-cert qualifications (degrees, training, experience) — not just vendor certs

Continuous tracking required

eMASS and DCWMS used to track role assignments, cert status, and CPE compliance across DoD components

EXAM RELEVANCE

// **Still tested as '8570' —** CISSP, CEH, Security+ exams reference DoD 8570 by name — know the old framework cold

// **Know both frameworks —** 8140 questions are appearing on newer exam versions — expect mapping questions

// **IAT/IAM/IASAE still valid —** The three tracks persist under 8140 but are now sub-categories of broader work roles

// **CISSP = crown cert —** CISSP satisfies IAT III, IAM II/III, IASAE I/II — highest coverage of any single cert

// **CEH coverage —** CEH maps to IAT II and Protect & Defend / Analyze roles under 8140

// **CASP+ = DoD IASAE —** CompTIA CASP+ CE is the primary cert for IASAE I/II — required for architecture roles

POA&M Tracking

Plan of Action & Milestones — Remediation Management

What is a POA&M?

PURPOSE

A POA&M is a formal document that identifies security weaknesses, assigns responsibility, and tracks remediation activities with scheduled completion dates.

FISMA 2014

Requires POA&Ms for all federal information systems

NIST SP 800-53

CA-5 control mandates formal POA&M process

FedRAMP

Monthly POA&M submission required for CSPs

⚠ *POA&Ms are not optional — they are a contractual and regulatory deliverable. An ATO cannot be granted or maintained without an active, reviewed POA&M.*

POA&M Item Structure — Required Fields

Weakness ID

Unique identifier (e.g., POA&M-2024-001)

Weakness Name

Descriptive title of the finding

Point of Contact

Individual responsible for remediation

Resources Required

Budget, personnel, tooling needed

Scheduled Comp. Date

Target date for full remediation

Milestones

Interim steps with dates (min. quarterly)

Completion Date

Actual date when remediation was completed

Status

Open / In Progress / Completed / Risk Accepted / False Positive

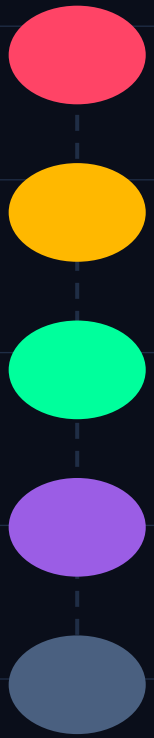
Source

Assessment, audit, scan, or self-identified

Control ID

Mapped NIST 800-53 control (e.g., AC-2, RA-5)

POA&M Lifecycle — Status Flow



OPEN

Weakness identified. POA&M item created and assigned.

IN PROGRESS

Remediation underway. Milestones being tracked. Monthly updates required.

COMPLETED

Control implemented. Evidence collected. Awaiting AO verification.

RISK ACCEPTED

AO formally accepts residual risk. Must be re-evaluated annually.

FALSE POSITIVE

Finding determined invalid after review. Documentation required to close.

Remediation Tracking & Milestones

MILESTONE REQUIREMENTS

Milestones must be **specific, measurable, and dated**. NIST requires at minimum **quarterly milestone updates** for open items. FedRAMP requires **monthly** status updates.

MILESTONE FIELDS

- Milestone #
- Milestone description
- Planned completion date
- Actual completion date
- Status

COMMON REMEDIATION TYPES

- Patch / software update
- Configuration change
- Policy / procedure update
- System redesign / replacement
- Compensating control implementation

RISK METRICS TO TRACK

- Days since opened (aging)
- Severity (Critical / High / Med / Low)
- CVSS score if applicable
- Overdue milestone count
- Residual risk level

Reporting to AO — ATO Decision Relationship

01

SYSTEM ASSESSED

Security Assessment Report (SAR) generated

02

POA&M REVIEWED

AO reviews open items, severity, and milestones

03

ATO DECISION

Grant ATO / Deny / Grant with Conditions

04

CONTINUOUS MON.

Ongoing POA&M updates required while ATO is active

WHAT THE AO EVALUATES

Severity distribution of open items · Realism of scheduled completion dates · Evidence of active remediation · Compensating controls for critical items

ATO GRANTED

Risk acceptable. All critical/high items remediated or have credible milestones.

ATO WITH CONDITIONS

Authorization granted with mandatory POA&M closure timeline imposed by AO.

ATO DENIED

Unacceptable residual risk. Critical findings without remediation plan.

POA&M in FISMA / RMF / FedRAMP

FISMA 2014

REQUIREMENT

Required for all federal information systems

FREQUENCY

Annual reporting to OMB / DHS

OWNER

ISSO / System Owner

NOTE

FISMA metrics include # of open POA&Ms, avg age, % overdue

NIST RMF

REQUIREMENT

Step 6 — Monitor; CA-5 control

FREQUENCY

Continuous; updated each assessment cycle

OWNER

ISSO with AO oversight

NOTE

RMF ties POA&M directly to ongoing authorization decisions

FedRAMP

REQUIREMENT

Required for all CSPs; reviewed by 3PAO

FREQUENCY

Monthly submission to JAB or Agency AO

OWNER

CSP (Cloud Service Provider)

NOTE

Template strictly defined; deviations cause rejection

POA&M Tools — eMASS, DCWMS & Manual Tracking

eMASS

Enterprise Mission Assurance Support Service

Authoritative system of record for DoD A&A. POA&M items tracked inside eMASS workflow; integrates with DIACAP and RMF.

- *Required for all DoD systems under RMF*

DCWMS

Defense Cybersecurity Workforce Mgmt System

Workforce qualification tracking; indirectly related — POA&M items for training gaps in 8570/8140 compliance tracked here.

- *Separate from technical POA&Ms; HR-focused*

XACTA / Archer

Commercial GRC Platforms

Used in civilian agency and commercial FedRAMP environments. Workflow-driven POA&M management with dashboard reporting.

- *FedRAMP-ready templates available*

Manual (Excel/SharePoint)

Agency-defined templates

OMB provides a standard POA&M template. Acceptable for smaller systems but lacks workflow automation and audit trails.

- *FedRAMP: spreadsheet submission accepted if template-compliant*

POA&M Metrics & Aging — What Auditors Look For

AGING THRESHOLDS (FISMA / OMB M-14-03)

< 30 days	30–90 days	90–180 days	> 180 days

% Open Critical / High

Target: 0 Critical unmitigated. High items must have active milestones.

POA&M Recurrence Rate

Items re-opened after closure indicate ineffective root cause correction.

Mean Time to Remediate

Average days from item creation to completion. Trending upward is a red flag.

Risk Accepted Volume

Excessive risk acceptances signal inability to remediate — auditors flag this.

Overdue Milestone Rate

items with missed milestone dates / total open. Should be near 0%.

//

04

Networking Fundamentals

OSI · TCP/IP · Subnetting · Routing

OSI Reference Model — 7 Layers

Mnemonic: Please Do Not Throw Sausage Pizza Away (Physical → Application)

7	APPLICATION	HTTP, FTP, SMTP, DNS, SNMP	*End-user applications*
6	PRESENTATION	SSL/TLS (L6), JPEG, ASCII, MPEG	*Encryption (SSL/TLS operates here), compression, formatting*
5	SESSION	NetBIOS, RPC, PPTP	*Session establishment & teardown*
4	TRANSPORT	TCP, UDP, SCTP	*Segment, flow control, reliability*
3	NETWORK	IP, ICMP, OSPF, BGP, ARP	*Routers, L3 switches*
2	DATA LINK	Ethernet, Wi-Fi (802.11), PPP, VLAN	*Switches, bridges, NICs*
1	PHYSICAL	Cables, fiber, radio, hubs	*Hubs, repeaters, cables, wireless AP*

TCP/IP Model vs OSI — Practical Mapping

TCP/IP MODEL

Application
Maps to OSI L5+L6+L7

Transport
Maps to OSI L4

Internet
Maps to OSI L3

Network Access
Maps to OSI L1+L2

IMPORTANT PORTS TO KNOW

PORT	SERVICE	DESCRIPTION	NOTES
20/21	FTP	File Transfer (data/control)	*Unencrypted — avoid in prod*
22	SSH	Secure Shell remote access	*Replaces Telnet*
23	Telnet	Unencrypted remote shell	*Legacy — never in prod*
25	SMTP	Email sending	*Use with TLS (587/465)*
53	DNS	Domain Name System	*UDP primarily; TCP for zone xfr*
80	HTTP	Unencrypted web traffic	*Redirect to HTTPS*
110	POP3	Email retrieval	*Superseded by IMAP*
123	NTP	Time synchronization	*Critical for Kerberos/logs*
443	HTTPS	TLS-encrypted web traffic	*Gold standard*
445	SMB	Windows file sharing	*Common attack vector*
1433	MS SQL	Microsoft SQL Server	*Restrict strictly*
3389	RDP	Remote Desktop Protocol	*High-value attack target*

IP Subnetting — CIDR & Subnet Masks

IPv4 Address Classes

Class A: 1.0.0.0–126.x.x.x | Class B: 128.0.0.0–191.255.x.x | Class C: 192.0.0.0–223.255.255.x | 127.x.x.x: Loopback

CIDR	SUBNET MASK	HOSTS/SUBNET	# SUBNETS (Class C)	USABLE RANGE EXAMPLE
/24	255.255.255.0	254	1	192.168.1.1 – 192.168.1.254
/25	255.255.255.128	126	2	192.168.1.1 – .126 / .129 – .254
/26	255.255.255.192	62	4	192.168.1.1 – .62 / .65 – .126…
/27	255.255.255.224	30	8	192.168.1.1 – .30 / .33 – .62…
/28	255.255.255.240	14	16	192.168.1.1 – .14 / .17 – .30…
/29	255.255.255.248	6	32	192.168.1.1 – .6 / .9 – .14…
/30	255.255.255.252	2	64	192.168.1.1 – .2 (point-to-point)
/16	255.255.0.0	65,534	N/A (Class B)	172.16.0.1 – 172.16.255.254
/8	255.0.0.0	16,777,214	N/A (Class A)	10.0.0.1 – 10.255.255.254

REMEMBER: Network address = first IP in range; Broadcast = last IP. Both are unusable.

Subnetting Quick-Math — Exam Technique

THE MAGIC NUMBER METHOD

1. Find the interesting octet (where mask ≠ 0 or 255)

2. Magic Number = 256 − subnet_mask_octet
   Example: mask 224 → 256−224 = 32

3. Subnets start at multiples of the magic number:
   0, 32, 64, 96, 128, 160, 192, 224

4. Broadcast = next subnet start − 1
   Example: subnet .32 → broadcast .63

5. Hosts = magic_number − 2
   Example: 32−2 = 30 usable hosts

WORKED EXAMPLE

Given: 192.168.10.0 /27
Subnet mask: 255.255.255.224

Magic #:
256 − 224 = 32

Subnets:
.0 .32 .64 .96 .128 .160 .192 .224

Hosts/subnet:
32 − 2 = 30 usable

Subnet .64:
Net: .64 | BC: .95 | Hosts: .65–.94

Subnet .96:
Net: .96 | BC: .127 | Hosts: .97–.126

Routing Protocols & Network Devices

PROTOCOL	TYPE	METRIC	AD	USE CASE
RIP v2	Distance Vector	Hop count (max 15)	120	Small/flat networks; legacy; study reference
OSPF	Link State	Cost (bandwidth)	110	Enterprise interior routing; most common IGP
EIGRP	Hybrid	Bandwidth+Delay+Load	90	Cisco proprietary; fast convergence
BGP	Path Vector	AS Path + attributes	20/200	Internet inter-AS routing; ISP backbone
IS-IS	Link State	Cost	115	ISP core networks; competes with OSPF

NETWORK DEVICES — OSI LAYER REFERENCE

Hub (L1)

Broadcasts to all ports; no intelligence; collision domain

Switch (L2)

Forwards based on MAC address; separates collision domains

Router (L3)

Forwards based on IP; separates broadcast domains

Firewall (L3-L7)

Filters traffic by rule set; stateful inspection; DPI at L7

Load Balancer (L4-L7)

Distributes traffic across backend servers; VIP concept

//

05

Firewalls & Deep Packet Inspection

Rule sets · NGFW · Stateful inspection

Firewall Generations & Inspection Types

Gen 1 Packet Filter	Inspects headers only (src/dst IP, port, protocol)	PRO: Fast; low overhead	CON: No state tracking; blind to session context
Gen 2 Stateful	Tracks connection state table; validates packet belongs to established flow	PRO: Context-aware; blocks unsolicited inbound	CON: Still no payload inspection
Gen 3 App-Layer / Proxy	Proxies connections; inspects up to L7 payload	PRO: Stops app-layer attacks; protocol anomaly detection	CON: Higher latency; complexity
Gen 4 NGFW	Stateful + DPI + IPS + App-ID + User-ID + TLS inspection	PRO: Full visibility; threat prevention; granular policy	CON: CPU-intensive; TLS inspection introduces latency

Firewall Rule Sets — Multi-Site Scenario

Scenario: Branch (192.22.22.0/24) · Main (129.88.0.0/16) · Euro (194.50.20.0/24) | Stance: Default Deny / Stateful

BRANCH OFFICE FIREWALL

#	IFACE	SOURCE	DEST	PORT	ACTION	NOTE
1	eth1	192.22.22.2	ANY	ANY	PERMIT	Workstation to Internet
2	eth1	192.22.22.2	129.88.0.0/16	ANY	PERMIT	Branch to Main
3	eth1	192.22.22.2	194.50.20.0/24	ANY	PERMIT	Branch to Euro
4	eth0	ANY	192.22.22.2	ANY	BLOCK	Block Internet-initiated
5	ANY	ANY	ANY	ANY	DENY	Default deny

MAIN OFFICE FIREWALL

#	IFACE	SOURCE	DEST	PORT	ACTION	NOTE
1	eth1	129.88.0.0/16	ANY	ANY	PERMIT	Main to Internet
2	eth0	ANY	129.88.1.11	80,443	PERMIT	Internet to Web Server
3	eth0	192.22.22.2	129.88.1.11	8080,8443	PERMIT	Branch to Web Server
4	eth0	194.50.20.0/24	129.88.1.11	8080,8443	PERMIT	Euro to Web Server
5	ANY	ANY	ANY	ANY	DENY	Default deny

//

06

Cryptography

Hashing · Symmetric · Asymmetric · PKI

SECTION

Cryptographic Fundamentals — CIA Triad Application

Confidentiality

`Encryption (AES, RSA)`

Prevent unauthorized disclosure. Symmetric for bulk data; asymmetric for key exchange.

Integrity

`Hashing (SHA-256, HMAC)`

Detect unauthorized modification. Hash produces fixed-length digest. HMAC adds shared secret.

Non-Repudiation

`Digital Signatures (RSA, ECDSA)`

Prove origin. Sender signs with private key; receiver verifies with public key.

HASH FUNCTION COMPARISON

ALGORITHM	OUTPUT	STATUS	USE CASE
MD5	128-bit	Broken	Legacy only — do not use
SHA-1	160-bit	Mand. Retirement 2030	Mandatory retirement by 2030 (NIST 2022); collision found 2017; do not use for new systems
SHA-256	256-bit	Strong	NIST recommended; TLS 1.3, code signing
SHA-512	512-bit	Stronger	Higher collision resistance; server-side
BLAKE2	256/512-bit	Strong	Faster than SHA-2; used in password hashing
bcrypt	variable	Strong (adaptive)	Password storage; deliberately slow
PBKDF2	variable	Strong (KDF)	Key derivation; RFC 2898; FIPS 140-2

Encryption Schemes — Symmetric vs Asymmetric

SYMMETRIC ENCRYPTION

One shared key — same key encrypts and decrypts.
Fast; used for bulk data encryption.

AES-128/256 — Block
US Gov standard; mandatory for classified (256-bit)

3DES (TDEA) — Block
Legacy; 112-bit effective strength; being phased out

ChaCha20 — Stream
TLS 1.3 alternative to AES; mobile-friendly

Blowfish — Block
64-bit block; replaced by Twofish; legacy

RC4 — Stream
Broken — prohibited in TLS; do not use

ASYMMETRIC ENCRYPTION

Public/private key pair — encrypt with public, decrypt with private.
Slow; used for key exchange and signatures.

RSA-2048/4096
De facto standard; key exchange + signatures. 2048 min.

ECDSA / ECDH
Elliptic curve variant; shorter keys, same strength. TLS 1.3.

Diffie-Hellman
Key AGREEMENT — not encryption. Establishes shared secret.

ElGamal
Encryption + signatures; based on discrete logarithm

DSA
Signatures only; FIPS 186-4; being superseded by ECDSA

PKI & Diffie-Hellman Key Exchange

PUBLIC KEY INFRASTRUCTURE (PKI)

CA (Certificate Authority)

Issues and signs digital certificates; root of trust

RA (Registration Authority)

Verifies identity before CA issues certificate

CRL (Cert Revocation List)

List of revoked certs; checked before trusting

OCSP

Online real-time revocation check; replaces CRL polling

X.509 Certificate

Standard format: subject, issuer, public key, validity, sig

Certificate Chain

Root CA → Intermediate CA → End-Entity cert

DIFFIE-HELLMAN KEY EXCHANGE

Allows two parties to derive a shared secret over an insecure channel WITHOUT transmitting the secret.

Both:	Agree on public prime p and base g
Alice:	Picks secret a; sends A = g^a mod p to Bob
Bob:	Picks secret b; sends B = g^b mod p to Alice
Alice:	Computes shared = B^a mod p
Bob:	Computes shared = A^b mod p
Result:	Both have same shared secret — never transmitted

DHKE variants: DHE (ephemeral), ECDHE (elliptic curve ephemeral) — used in TLS 1.3 for Perfect Forward Secrecy

Governance Risk & Compliance

How frameworks, controls, and accountability connect

GRC — Governance, Risk & Compliance

GOVERNANCE

The system by which an organization directs and controls its information security activities.

- Policies, standards, procedures
- Roles & accountability (CISO, Board)
- Strategic alignment with business goals
- COBIT 2019 is the primary governance framework

RISK

The identification, assessment, and prioritization of threats — and the decisions made in response.

- Risk identification & analysis
- NIST 800-30 risk assessment process
- Risk treatment: accept, mitigate, transfer, avoid
- Residual risk & risk appetite

COMPLIANCE

Adherence to laws, regulations, standards, and internal policies applicable to the organization.

- Regulatory: FISMA, HIPAA, PCI-DSS
- Standards: ISO 27001, NIST 800-53
- Audit & evidence: SOC reports, assessments
- Non-compliance consequences: fines, loss of ATO

GRC Framework Landscape — What Lives Where

No single framework covers all of GRC. Students are expected to know which framework applies to which problem — and how they relate to each other.

FRAMEWORK	DOMAIN	USED FOR	TESTED ON
NIST CSF	Cybersecurity	Risk-based security program structure	CISSP, Sec+
NIST 800-53	Federal controls	Control selection & implementation	CISSP, CISA
NIST 800-30	Risk assessment	Threat/vulnerability risk analysis	CISSP, CISA
NIST RMF	Authorization	A&A lifecycle for federal systems	CISSP, CISA
ISO 27001	ISMS	International security mgmt certification	CISSP, CISA
ISO 31000	Enterprise risk	Organization-wide risk management	CISSP, CISA
COBIT 2019	IT governance	Governance of enterprise IT	CISA primary
FISMA / FedRAMP	Federal compliance	Legal compliance + cloud authorization	CISSP, CISA

GRC in Practice — How the Pieces Connect

IN A FEDERAL AGENCY

- Governance: agency policy + NIST 800-53 controls
- Risk: RMF process, POA&M tracking
- Compliance: FISMA reporting, ATO maintenance
- Audited by: IG, GAO, or third-party assessor

IN A COMMERCIAL ENTERPRISE

- Governance: COBIT 2019, board-level oversight
- Risk: ISO 31000 or NIST CSF risk tiers
- Compliance: SOC 2, ISO 27001 certification
- Audited by: external CPA firm or certification body

ON THE CERT EXAM

- CISSP: governance concepts in Domain 1; risk in Domain 2
- CISA: all 5 domains are GRC-centric
- Security+: risk management, compliance concepts
- Key: know which framework answers which question

EXAM PATTERN

GRC questions test judgment, not memorization. The correct answer is usually the one that addresses governance or risk first — before jumping to a technical control. When in doubt: policy before technology, risk-based before compliance-based.

//

08

CEH
Attack Methodology

Ethical hacking lifecycle · Attack types · Detection

CEH — Hacking Methodology (5-Phase Model)

1 Reconnaissance (Footprinting)

- Passive: OSINT, WHOIS, DNS, job postings, Shodan
- Active: social engineering, direct probing
- Google dorking: site:, filetype:, inurl:
- Tools: Maltego, theHarvester, Recon-ng

2 Scanning & Enumeration

- Port scanning: TCP SYN, FIN, XMAS, NULL scans
- Service/version detection: Nmap -sV
- OS fingerprinting: Nmap -O, p0f
- Enumeration: NetBIOS, SNMP, LDAP, NFS shares

3 Gaining Access & Exploitation

- Vulnerability exploitation: Metasploit, manual CVE
- Password attacks: brute force, credential stuffing
- Social engineering: phishing, vishing, pretexting
- Web attacks: SQLi, XSS, CSRF, LFI/RFI

4 Maintaining Access

- Persistence: cron jobs, registry run keys, WMI subscriptions
- Backdoors: Netcat, Meterpreter reverse shells
- Rootkits: kernel-level or userland; hide processes/files
- Lateral movement: pass-the-hash, Kerberoasting

5 Clearing Tracks

- Log manipulation: Windows Event Log, syslog tampering
- Disable audit policies temporarily
- Steganography to hide exfiltrated data
- Anti-forensics: timestomping, slack space injection

IDS/IPS — Detection Methods & Evasion Techniques

DETECTION METHODS

Signature-Based	Known attack patterns matched against database of signatures	✓ Low false positives; fast ✗ Blind to zero-days; requires constant updates
Behavioral / Anomaly	Baseline normal traffic; flag statistically significant deviations	✓ Detects novel attacks ✗ High false positives; baselining required
Protocol Anomaly	RFC compliance checking; flags non-standard protocol behavior	✓ Catches protocol-level exploits ✗ May block valid edge-case traffic
Heuristic / AI	ML models trained on attack patterns and benign traffic	✓ Adaptive; reduces zero-day exposure ✗ Model training costs; adversarial evasion possible

COMMON IDS EVASION TECHNIQUES

> Fragmentation — split payload across IP fragments below inspection threshold
> Encoding — URL encoding, Unicode, base64 to obfuscate payload
> TTL manipulation — craft packets that die before reaching IDS but reach target
> Session splicing — split TCP segments so no single segment triggers signature
> Slow scanning — rate below threshold triggers; blend in with normal traffic

//

09

ISO 27001, Cloud Security and Risk Management

Framework, Cloud Focused and Understanding Risk

SECTION

ISO/IEC 27001 — Information Security Mgmt System (ISMS)

ISO 27001 vs 27002

ISO 27001

The SPECIFICATION. Defines ISMS requirements. The only standard against which organizations achieve certification.

ISO 27002

The GUIDANCE document. Best-practice guidance on applying Annex A controls. Read alongside 27001.

ISO 27008

Guidance for auditors reviewing information security controls.

ISO 9001

Quality Management System. Often implemented alongside 27001 for integrated management.

ISMS Key Concepts

// ISMS must align with organizational goals and business objectives

// Management must champion and commit — resource allocation mandatory

// Charter Document defines Scope, SoA, and policy hierarchy

// Statement of Applicability (SoA) lists which of 114 controls apply/exclude

// Risk-based approach: identify assets → threats → vulnerabilities → treatment

// Continuous improvement cycle (Plan-Do-Check-Act / PDCA)

// Internal audits + certification audits + surveillance audits

// Incident response, root cause analysis, after-action debriefs

ISO 27001 — Annex A Control Sets (114 Controls / 14 Sets)

A.5 — **Information Security Policies**
Top-down direction; communicate to all staff

A.6 — **Organization of Information Security**
Management framework; on-site & remote

A.7 — **Human Resource Security**
Pre/during/post-employment responsibilities

A.8 — **Asset Management**
Classify and protect physical and info assets

A.9 — **Access Control**
Least privilege; user responsibility for credentials

A.10 — **Cryptography**
Key management policies; confidentiality/integrity

A.11 — **Physical & Environmental Security**
Prevent unauthorized physical access

A.12 — **Operations Security**
Malware protection; data loss prevention

A.13 — **Communications Security**
Network and data-in-transit protection

A.14 — **System Acquisition, Dev & Maintenance**
Security across full system lifecycle

A.15 — **Supplier Relationships**
Third-party due diligence; supply chain risk

A.16 — **Incident Management**
Consistent, effective incident handling

A.17 — **Business Continuity**
Embed InfoSec in BCP/DR practices

A.18 — **Compliance**
Legal, regulatory, and contractual obligations

Cloud Security — Service Models & Compliance

IaaS

Infrastructure as a Service

AWS EC2, Azure VM, GCP Compute

You own OS, apps, data. Provider secures hardware/hypervisor.

PaaS

Platform as a Service

Heroku, Azure App Service, GCP App Engine

Provider owns OS/runtime. You secure app code and data.

SaaS

Software as a Service

M365, Salesforce, Google Workspace

Provider owns nearly everything. You manage access and data governance.

FedRAMP — Federal Risk and Authorization Management Program

// Standardizes security assessment, authorization, and monitoring for cloud products used by US federal agencies

// Based on NIST SP 800-53 controls — Low, Moderate, and High baselines

// CSP (Cloud Service Provider) must achieve ATO via sponsoring agency or JAB (Joint Authorization Board)

// Major providers: AWS GovCloud, Azure Government, Google Cloud Gov, Oracle Government, IBM Cloud

// Defense in Depth model must be applied to all cloud architectures — no single control point

Risk Management Frameworks & Methodologies

NIST SP 800-30
US Government

Threat-likelihood matrix; identifies threats, vulnerabilities, impact on mission

ISO 27005
International Standard

Risk-based ISMS input; asset-centric; aligns with ISO 31000

OCTAVE
Asset-Centric

Operationally Critical Threat, Asset and Vulnerability Evaluation; org-led

MEHARI
French Standard

Multi-dimensional risk analysis; quantitative and qualitative scoring

CRAMM
UK Government

CCTA Risk Analysis & Mgmt Method; full lifecycle risk process

Microsoft SDL
Vendor Method

Threat modeling (STRIDE) built into development process

RISK TREATMENT OPTIONS

Modification (Mitigation)

Implement controls to reduce likelihood or impact. Most common option.

Avoidance

Eliminate the risk by not performing the activity. Highest risk reduction.

Retention (Acceptance)

Accept the risk; budget for loss. For low-likelihood or low-impact risks.

Sharing (Transfer)

Shift financial impact via insurance or contractual obligation.

Exam Strategy & Key Reminders

10

CISSP MINDSET

- MANAGER vs. TECHNICIAN: Answer as a senior security MANAGER setting policy — not the technician implementing it. Ask: what would the CISO recommend?
- RISK-BASED THINKING: Best practices and vendor-neutral solutions always win. If one answer fixes the immediate problem and another fixes the underlying risk — choose the risk.
- POLICY OVER TECHNOLOGY: When two answers look correct, choose the one that addresses GOVERNANCE or POLICY first — technology is always secondary. Controls flow from policy, not the reverse.
- Read ALL four options before selecting — CISSP loves 'most correct' answers

CEH MINDSET

- Know the SEQUENCE: Recon → Scan → Gain Access → Maintain → Cover Tracks
- Know attack types by signature: SYN flood, fragmentation, pass-the-hash
- Understand tools conceptually — what each does, not just its name
- Understand both offensive technique AND the defensive countermeasure

NETWORKING QUICK HITS

- OSI 7 layers — know protocols AND device types per layer
- Default deny is always the secure stance for firewalls
- Subnetting: practice the magic number method until it's automatic
- Stateful > stateless; NGFW > traditional; DPI catches payload-level threats

END OF MODULE

Continue Learning

Practice exams · Lab environments · Peer study groups

CISSP | CEH | CCNA | CompTIA Sec+ | CISM