CompTIA SecurityX

CAS-005 Visual Cheat Sheet

25-Page Complete Reference | All Exam Domains

- Security Architecture
- Security Operations
- Security Engineering
- Governance, Risk & Compliance
- Cloud & Emerging Tech

90 min	90 Q	750/900	5 Domains	No Prereq
Exam Time	Questions	Pass Score	Coverage	Formal Req

Advanced-level certification | Requires strategic, architecture-level thinking

CAS-005 EXAM DOMAINS & WEIGHTINGS

1.0	Governance, Risk & Compliance	20%
2.0	Security Architecture	25%
3.0	Security Engineering	25%
4.0	Security Operations	20%
5.0	Security Program Mgmt & Oversight	10%

EXAM LOGISTICS AT A GLANCE

Duration	90 minutes (no extra time for non-native speakers)
Questions	90 questions – multiple choice + performance-based
Pass Score	750 / 900 (83.3%)
Delivery	Pearson VUE – online proctored or test centre
Validity	3 years; renew via CE or re-exam
Recommended	CASP+ / 10 yrs IT exp / 5 yrs hands-on security
Languages	English, Japanese, Portuguese, Simplified Chinese

ARCHITECT MINDSET – HOW TO THINK

1. **Read the SCENARIO first – understand business context**
2. **Identify the CONSTRAINT (budget, legacy, regulation)**
3. **Choose the MOST comprehensive control, not just technical**
4. **"Best" = most effective + proportionate to risk**
5. **Eliminate "always" / "never" – security is context-dependent**

DOMAIN MIND MAP

Governance, Risk & Compliance
- Risk Register & Treatment
- Compliance Frameworks
- BCP / DRP
- Privacy & Data Classification
- Third-Party / Supply Chain Risk

Security Architecture
- Zero Trust (NIST 800-207)
- Defense in Depth
- Cloud / Hybrid / Multi-cloud
- Microservices & Containers
- Secure Network Design

Security Engineering
- Cryptography & PKI
- TLS 1.3 / IPsec
- Identity & Access (IAM, PAM)
- Endpoint & Mobile Security
- Secure Coding / DevSecOps

Security Operations
- SOC Tiers & SIEM/SOAR
- Incident Response (NIST 800-61)
- Threat Intelligence & Hunting
- Vuln Mgmt & Pen Testing
- Forensics & eDiscovery

Prog Mgmt & Oversight
- Security Metrics & KPIs
- Security Awareness Training
- Policy & Standards Writing
- Vendor/Contract Security

EXAM STRATEGY
- Performance-based questions (PBQs) appear first – don't spend >4 min each
- Scenario questions test JUDGEMENT not just recall; re-read business context

PASS RATE INSIGHT
- CAS-005 replaced CAS-004 in 2023; heavier cloud/AI/supply chain content
- Focus: governance integration + architecture decisions, not tool names

ZERO TRUST CORE PRINCIPLE: "NEVER TRUST, ALWAYS VERIFY"

FIVE PILLARS OF ZERO TRUST

- **Identity** — Verify every user/service; MFA + risk-based auth
- **Device** — Posture checks; compliant before access granted
- **Network** — Micro-segmentation; no implicit internal trust
- **Application** — App-layer controls; ZTNA replaces VPN
- **Data** — Classify & protect; access based on sensitivity

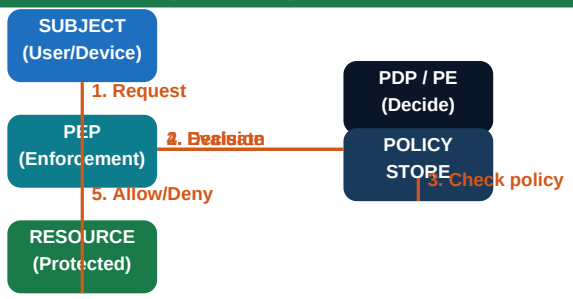
NIST SP 800-207 ZTA COMPONENTS

Policy Decision Point (PDP)	Evaluates access requests against policy
Policy Engine (PE)	Core logic: grant / deny / revoke
Policy Administrator (PA)	Issues credentials + configures enforcement
Policy Enforcement Point (PEP)	Gateway that allows/blocks traffic
Subject (User/Device)	Entity requesting access to resource
Resource (Enterprise Asset)	What is being protected / accessed
Control Plane	Policy evaluation & decision path
Data Plane	Actual resource access traffic path

ZTA DEPLOYMENT MODELS

- **Identity-Based** — IdP-driven (Okta, Azure AD) + SSO + MFA + device trust
- **Micro-Segmentation** — Workload-to-workload east-west controls via software-defined perimeter
- **ZTNA (Zero Trust Network Access)** — App-specific tunnels; replaces traditional VPN
- **SDP (Software Defined Perimeter)** — Dark cloud; resources invisible until authorised
- **SASE Model** — SD-WAN + ZTNA + CASB + FWaaS converged at edge

ZTA FLOW DIAGRAM (SIMPLIFIED)



COMMON ZTA MISTAKES TO AVOID

- ✗ Buying a "ZTA product" ≠ implementing Zero Trust
- ✗ Forgetting service accounts in identity policy scope
- ✗ No monitoring = ZT in name only (need SIEM/UEBA)
- ✗ Over-segmenting too fast = operational disruption
- ✗ Neglecting legacy apps that can't support modern auth
- ✗ Skipping user awareness – ZT still requires human compliance

ZTA vs TRADITIONAL PERIMETER

Factor	Perimeter Model	Zero Trust
Trust	Implicit inside network	Never implicit
Verification	Login once at border	Continuous per-request
Segmentation	Flat internal network	Micro-segments
Remote Access	VPN tunnel	ZTNA / SDP
Lateral Movement	Easy once inside	Blocked by policy
Visibility	Perimeter logs only	Full telemetry

■ EXAM INSIGHT

- NIST SP 800-207 is the ZTA reference architecture for CAS-005
- PEP + PDP + PA are the three enforcement components; know each role

■ MEMORY HOOK

- ZTA = "Verify explicitly, Use least privilege, Assume breach" (Microsoft 3 principles)
- SASE = ZTA + SD-WAN converged at cloud edge (Gartner term)

DEFENSE IN DEPTH – 7 LAYERS

Layer 7 – Policies & Procedures
Security policies, awareness training, governance

Layer 6 – Physical Security
Badge access, CCTV, mantraps, environmental controls

Layer 5 – Perimeter Security
Firewall, IPS, DMZ, WAF, DDoS mitigation

Layer 4 – Network Security
VLAN segmentation, NAC, zero trust micro-seg

Layer 3 – Host / Endpoint
EDR, AV, patch mgmt, host firewall, CIS benchmarks

Layer 2 – Application Security
Secure SDLC, SAST/DAST, WAF, input validation

Layer 1 – Data Security
Encryption, DLP, data classification, masking

SECURE DESIGN PRINCIPLES

Least Privilege	Grant minimum rights needed; JIT/JEA for admin
Fail Secure	On failure, default to deny/safe state, not open
Separation of Duties	No single person can complete high-risk task alone
Defence in Depth	Layered controls; compromise 1 ≠ compromise all
Economy of Mechanism	Simpler designs have smaller attack surface
Open Design	Security through obscurity alone is NOT security
Complete Mediation	Check every access request, every time (no cache)
Psychological Accept.	Controls must be usable or users bypass them
Weakest Link	System security = strength of weakest component
Attack Surface Reduction	Disable/remove unused services, ports, protocols

SECURITY CONTROL TYPES

Preventive
Stop incident before it occurs
Firewalls ■ MFA ■ Encryption ■ ACLs

Detective
Identify incident as/after it occurs
SIEM ■ IDS ■ Audit logs ■ UEBA

Corrective
Minimize damage; restore normal ops
Patches ■ Backups ■ IR procedures ■ EDR

Deterrent
Discourage attacks (psychological)
Warning banners ■ CCTV signs ■ Policies

Compensating
Alternative when primary unavailable
Monitoring in lieu of encryption ■ IDS/IPS

Recovery
Restore after incident
DR site ■ Backups ■ BCMS

CONTROL CATEGORIES

Technical / Logical	Software & hardware controls	Firewall, IDS, Encryption, MFA
Administrative	Policies, procedures, training	AUP, SETA, Background checks
Physical	Physical access, environmenta	Badge reader, Mantrap, CCTV, Locks
Operational	Day-to-day operational proced	Patch Tue, Change Mgmt, IR runbooks

EXAM – CONTROL SELECTION LOGIC

Q: Need to STOP an attack? → Preventive
Q: Need to DETECT compromise? → Detective
Q: Need to LIMIT damage after breach? → Corrective
Q: Primary control unavailable? → Compensating
Q: Need to RESTORE services? → Recovery
Q: Need to DISCOURAGE attackers? → Deterrent

■ EXAM INSIGHT

- "Fail secure" = locks door; "fail open" = unlocks door. Exam prefers fail secure.
- Compensating controls must provide equivalent protection to the replaced primary control

■ MEMORY HOOK

- Controls are: Preventive→Detect→Correct→Recover (lifecycle order of response)
- DiD = Swiss cheese model: many layers means holes don't align

SHARED RESPONSIBILITY MODEL

COMPONENT	IaaS	PaaS	SaaS
Data	Customer	Customer	Customer
Identity & Access	Customer	Customer	Customer
Application	Customer	Customer	Shared
Runtime / Middleware	Customer	Shared	CSP
OS	Customer	CSP	CSP
Virtualisation	CSP	CSP	CSP
Physical/Network	CSP	CSP	CSP

CLOUD SECURITY TOOLING

CASB	Cloud Access Security Broker	Visibility + control over SaaS/IaaS usage
CSPM	Cloud Security Posture Mgmt	Detect misconfigs (open S3, public RDS)
CWPP	Cloud Workload Protection	Runtime protection for VMs/containers
CNAPP	Cloud-Native App Protection	CSPM + CWPP + CIEM converged platform
CIEM	Cloud Infra Entitlement Mgmt	Identify over-privileged cloud identities
SSPM	SaaS Security Posture Mgmt	Misconfiguration in SaaS (M365, Salesforce)
WAF	Web Application Firewall	Layer 7 protection: SQLi, XSS, OWASP Top 10

CLOUD DEPLOYMENT MODELS

Public Cloud
AWS/Azure/GCP shared infra; CSP owns hardware; fastest innovation

Private Cloud
Dedicated infra; on-prem or hosted; full control; higher cost

Hybrid Cloud
Mix public + private; data gravity + burst capacity use cases

Multi-Cloud
Multiple CSPs; avoid lock-in; complex governance required

Community Cloud
Shared by orgs with common mission (Gov, Healthcare)

CLOUD SECURITY ARCHITECTURE PATTERNS

Hub & Spoke (VNet Peering)
- Central hub VNet: firewall, DNS, logging
- Spoke VNets connect only to hub (not each other)
- Centralised inspection + policy enforcement

Serverless / FaaS Security
- Function permissions = least-privilege IAM roles
- Secrets via vault (AWS Secrets Mgr / Azure Key Vault)
- Dependency scanning + SAST in CI/CD pipeline

Container & Kubernetes Security
- Image scanning: no root, no secrets in layers
- Admission controllers: OPA/Gatekeeper for policy
- Network policies: deny all → allow explicit

API Gateway Security
- OAuth 2.0 + JWT validation at gateway layer
- Rate limiting + throttling + IP allowlisting
- mTLS for service-to-service auth (zero trust)

TOP CLOUD MISCONFIGURATIONS (EXAM)

S3/Blob bucket PUBLIC read/write	→ Block public access + bucket policy
Security group 0.0.0.0/0 inbound	→ Restrict to known CIDRs + NAC
Root account used for daily ops	→ IAM roles + MFA on root; never use daily
No MFA on cloud console accounts	→ Enforce MFA via SCPs / Conditional Access
Secrets in environment variables	→ Use vault/secrets manager + rotation
Unencrypted EBS/RDS volumes	→ Enable encryption at creation; use CMK
CloudTrail / audit log disabled	→ Enable in all regions + immutable storage

■ EXAM INSIGHT
- CNAPP = most comprehensive cloud security platform (CSPM+CWPP+CIEM combined)
- IaaS = most customer responsibility; SaaS = least customer responsibility

■ MEMORY HOOK
- CASB: Visibility (Shadow IT) + Compliance + Data Security + Threat Protection
- "Cloud shift doesn't shift responsibility for data protection" – security stays yours

RISK FORMULAS

SLE	Single Loss Expectancy	Asset Value (AV) × Exposure Factor (EF)
ARO	Annual Rate of Occurrence	Expected # of incidents per year
ALE	Annual Loss Expectancy	SLE × ARO
TCO	Total Cost of Ownership	Acquisition + ops + maintenance costs
ROI	Return on Security Investme	(ALE_before – ALE_after) – Control_Cost
EF	Exposure Factor	% of asset value lost in single incident (0–1)

NIST RMF 7 STEPS (SP 800-37)

1. Prepare
Org-level risk management prep; establish context

2. Categorise
Classify information system impact (Low/Mod/High – FIPS 199)

3. Select
Choose baseline controls from SP 800-53

4. Implement
Apply controls; document implementation details

5. Assess
Evaluate control effectiveness (SP 800-53A)

6. Authorise
AO accepts residual risk; grants Authority to Operate (ATO)

7. Monitor
Ongoing assessment; respond to changes; automate

RISK TREATMENT OPTIONS

Avoid	Eliminate the activity causing the risk
Mitigate	Implement controls to reduce likelihood/impact
Transfer	Insurance, SLAs, contracts (cyber liability)
Accept	Acknowledge residual risk; document in risk register
Share	Distribute risk across partners/third parties
Reject	Ignore risk (negligent – NOT acceptable)

RISK REGISTER KEY FIELDS

Risk ID	Unique identifier (RK-0042)
Description	What could go wrong and how
Likelihood	1–5 scale (Rare → Almost Certain)
Impact	1–5 scale (Insignificant → Catastrophic)
Risk Score	Likelihood × Impact; heat map position
Owner	Business owner responsible for treatment
Treatment	Avoid / Mitigate / Transfer / Accept
Control Ref	Links to implemented controls (ISO/NIST)
Residual Risk	Remaining risk after controls applied
Review Date	When risk will be re-evaluated

QUALITATIVE vs QUANTITATIVE RISK

Factor	Qualitative	Quantitative
Method	Ratings (High/Med/Low)	Numbers ($ ALE)
Effort	Low – faster	High – needs data
Accuracy	Subjective	Objective
Best for	Unknown threats	Known, frequent risks
Output	Heat map / matrix	ROI / Cost-benefit

RISK ASSESSMENT METHODOLOGIES

NIST SP 800-30	Federal risk assessment guide; pairs with RMF
ISO/IEC 27005	ISMS risk management (pairs with 27001)
FAIR	Factor Analysis of Information Risk; quantitative
OCTAVE	Operationally Critical Threat/Asset/Vulnerability Eval
TARA	Threat Agent Risk Assessment; ties TTPs to assets
PASTA	Process for Attack Simulation & Threat Analysis

■ EXAM FORMULAS TO MEMORISE

- ALE = SLE × ARO; SLE = AV × EF; ROSI = (ALE_before – ALE_after) – Control_Cost
- Residual risk = Inherent risk – control effectiveness (always remains; accept or treat)

■ MEMORY HOOK

- NIST RMF steps: "Prepare Carefully, Select Implements, Allow Monitoring"
- Risk = Threat × Vulnerability × Impact (attack succeeds only if ALL three present)

MAJOR COMPLIANCE FRAMEWORKS

ISO/IEC 27001	ISMS certification; 93 controls (Annex A); PDCA cycle
ISO/IEC 27002	Best-practice guidance for 27001 controls
NIST CSF 2.0	Govern-Identify-Protect-Detect-Respond-Recover
NIST SP 800-53	Federal security controls catalogue; 20 control families
SOC 2 Type II	AICPA trust criteria: S-A-C-P-P over 6+ months
PCI-DSS v4.0	12 requirements; protects cardholder data; QSA audits
HIPAA Security	PHI protection; Admin+Physical+Technical safeguards
GDPR	EU data protection; 72h breach notify; right to erasure
CCPA/CPRA	California; right to know/delete/opt-out
FedRAMP	US federal cloud auth; Low/Moderate/High impact levels
CMMC 2.0	DoD supply chain; Level 1-3; maps to NIST 800-171
CIS Controls	18 controls; IG1/2/3 implementation groups; prioritised

POLICY HIERARCHY

Policy
High-level management intent & direction

Standard
Mandatory specific requirements to meet policy

Procedure
Step-by-step how to implement standards

Guideline
Recommended best practices (not mandatory)

Baseline
Minimum config for a specific system/platform

NIST CSF 2.0 FUNCTIONS

GOVERN
NEW in v2.0 – establish & monitor cybersecurity strategy

IDENTIFY
Asset mgmt, risk assessment, supply chain risk mgmt

PROTECT
Access controls, awareness training, data security

DETECT
Anomalies, continuous monitoring, detection processes

RESPOND
Incident management, communications, analysis, mitigation

RECOVER
Recovery planning, improvements, communications

PCI-DSS v4.0 – 12 REQUIREMENTS

1	Install & maintain network security controls
2	Apply secure configs to all system components
3	Protect stored cardholder data
4	Protect in-transit data with strong cryptography
5	Protect all systems against malware
6	Develop & maintain secure systems/software
7	Restrict access to system components / cardholder data
8	Identify users & authenticate access
9	Restrict physical access to cardholder data
10	Log & monitor all access to system components
11	Test security of systems & networks regularly
12	Support info security with org policies & programs

BREACH NOTIFICATION TIMELINES

GDPR	72 hours to supervisory authority
HIPAA	60 days to HHS + individuals
PCI-DSS	Immediately to card brands + acquirer
CCPA	45-day cure; no fixed notification
NY SHIELD	72 hours to AG (500+ affected)

■ EXAM INSIGHT
- NIST CSF v2.0 added GOVERN as the 6th function – exam will test on this change
- SOC 2 Type II = audit over time (6+ months); Type I = single point in time snapshot

■ MEMORY HOOK
- ISO 27001 = certification (can audit/certify); ISO 27002 = guidance only (no cert)
- NIST CSF = voluntary framework; NIST 800-53 = mandatory for US federal systems

KEY BCP/DR METRICS

RTO	Recovery Time Objective	Max acceptable downtime before service restored
RPO	Recovery Point Objective	Max acceptable data loss (time since last backup)
MTBF	Mean Time Between Failures	Avg operational time between failures (reliability)
MTTR	Mean Time to Repair/Recover	Avg time to restore system after failure
MTTF	Mean Time to Failure	Avg time until non-repairable component fails
SLA	Service Level Agreement	Contractual uptime/perf commitment from provider
MTO	Maximum Tolerable Outage	Absolute max before org suffers irreversible harm

RECOVERY SITE TYPES

Hot Site (Highest cost)
Fully configured; mirrors production; RTO = minutes

Warm Site (Medium cost)
Hardware ready; data loaded periodically; RTO = hours

Cold Site (Lowest cost)
Facility only; no hardware/data; RTO = days/weeks

Mobile Site (Flexible)
Self-contained trailer; deployable anywhere rapidly

Cloud DR (Scalable)
DRaaS; elastic; pay-per-use; pilot light or warm standby

Reciprocal (Risk: capacity)
Agreement with another org to share facilities

DR TEST TYPES (LEAST → MOST DISRUPTIVE)

Tabletop Exercise
Discussion-based; no systems involved; find plan gaps

Walk-through / Checklist
Team reviews plan step-by-step; verify accuracy

Parallel Test
DR site activated; primary stays live; no failover

Full Interruption / Failover
Primary shut down; full cutover to DR site

Simulation
Realistic scenario (earthquake/breach); test full response

BCP LIFECYCLE (ISO 22301)

1. **Policy & Programme Mgmt** — Scope, objectives, leadership commitment
2. **Business Impact Analysis** — Identify critical processes; define RTO/RPO
3. **Risk Assessment** — Identify threats; assess likelihood/impact
4. **Strategy Selection** — Choose recovery options (hot/warm/cloud)
5. **Plan Development** — Document procedures, roles, comms plan
6. **Training & Awareness** — Train staff; run exercises
7. **Exercising & Testing** — Tabletop → full interruption; improve
8. **Maintenance & Improvement** — Annual review; update after incidents

BACKUP TYPES & STRATEGIES

Full Backup	All data; slowest to create; fastest to restore
Incremental	Only changes since LAST backup; fast backup; slow restore
Differential	Changes since LAST FULL; medium backup/restore
Snapshot	Point-in-time copy (VM/storage); near-instant
3-2-1 Rule	3 copies, 2 media types, 1 offsite
3-2-1-1-0	+1 offline/air-gapped, 0 errors verified
Immutable Backup	WORM storage; ransomware protection; S3 Object Lock

HA PATTERNS

Active-Active	Both nodes handle traffic; max performance
Active-Passive	Primary handles traffic; passive on standby
N+1 Redundancy	N working components + 1 spare
Geographic HA	Multi-region for disaster resilience
Load Balancing	Distribute traffic; health checks; auto failover

■ EXAM INSIGHT

- RTO < RPO is impossible – you can't recover faster than data allows
- Tabletop = lowest disruption; Full Interruption = highest risk/best validation

■ MEMORY HOOK

- RTO = how quickly; RPO = how much data loss is OK
- 3-2-1-1-0: 3 copies, 2 media, 1 offsite, 1 offline, 0 restore errors

SYMMETRIC ENCRYPTION

AES-128	Block 128b	GCM/CCM/CBC	Approved – minimum for new systems
AES-256	Block 128b	GCM/CCM	Preferred – CNSA/top-secret use
3DES	Block 64b	CBC	DEPRECATED (NIST 2023)
Blowfish	Block 64b	CBC	Avoid – 64b block birthday attacks
ChaCha20	Stream	+Poly1305 MAC	TLS 1.3 cipher suite; mobile-friendly
RC4	Stream	None (broken)	PROHIBITED – trivially crackable

ASYMMETRIC ENCRYPTION

RSA-2048	Encrypt + Sign	Minimum; 112-bit security; use 3072+ for new
RSA-3072	Encrypt + Sign	Recommended 128-bit equivalent; ≥2031
ECC P-256	ECDH + ECDSA	128-bit security at 256-bit key; efficient
ECC P-384	ECDH + ECDSA	192-bit security; Suite B / government
ED25519	Digital Sig	Fast; small key; Curve25519 basis
DH / DHE	Key Exchange	DHE = ephemeral; provides forward secrecy
ECDHE	Key Exchange	Elliptic DHE; TLS 1.3 standard; PFS

HASH FUNCTIONS

MD5	128b	BROKEN – collision attacks; never for security
SHA-1	160b	BROKEN – SHAttered attack; avoid completely
SHA-256	256b	APPROVED – TLS, code signing, general purpose
SHA-384	384b	Suite B; higher assurance; HMAC use
SHA-512	512b	Strongest SHA-2; password hashing base
SHA-3	256b+	Keccak basis; different structure; NIST approved
BLAKE3	256b	Fastest; secure; used in modern tools
bcrypt	192b	Password only; adaptive cost; salt built-in
Argon2id	var	PREFERRED password hashing; memory-hard; PHC winner

CIPHER MODES OF OPERATION

ECB	Electronic Code Book	BROKEN – identical blocks = identical ciphertext
CBC	Cipher Block Chaining	Padding oracle attacks (POODLE); needs IV
CTR	Counter Mode	Turns block cipher to stream; parallelizable
GCM	Galois/Counter Mode	Authenticated encryption (AEAD); preferred
CCM	Counter with CBC-MAC	AEAD; IoT/constrained devices (802.11i)
XTS	XEX-based tweaked codeb	Disk encryption (BitLocker, FileVault)
OCB	Offset Codebook	AEAD; single pass; patent issues (less used)

KEY MANAGEMENT LIFECYCLE

Generation	FIPS 140-2/3 validated RNG; HSM preferred
Distribution	KEK wraps DEK; TLS transport; key ceremony
Storage	HSM or KMS; never in application config files
Rotation	Scheduled + on compromise; document schedule
Revocation	CRL / OCSP; immediate on compromise/termination
Destruction	NIST 800-88 media sanitisation; cryptographic erase
Escrow	Key backup with trusted 3rd party; M-of-N control

POST-QUANTUM CRYPTOGRAPHY (NIST 2024)

ML-KEM (Kyber)	Key encapsulation; replaces RSA/ECDH
ML-DSA (Dilithium)	Digital signatures; replaces ECDSA/RSA
SLH-DSA (SPHINCS+)	Hash-based sigs; conservative option
Hybrid Mode	Classical + PQ in parallel during migration

CRYPTOGRAPHIC ATTACKS

Birthday	Find hash collision; P~50% at 2^(n/2) inputs
Brute Force	Try all keys; defeated by long key lengths
Rainbow Table	Pre-computed hash lookup; defeated by salting
Side-Channel	Power analysis, timing; bypass math entirely
Padding Oracle	CBC padding check leaks info; use AEAD instead
Downgrade	Force old cipher suite; use TLS_FALLBACK_SCSV
MITM	Intercept key exchange; use cert pinning or PKI

■ EXAM INSIGHT

- GCM = encryption + authentication in one pass (AEAD); preferred for new designs
- Argon2id = current best-practice password hashing; bcrypt = acceptable legacy

■ MEMORY HOOK

- AEAD = Authenticated Encryption with Associated Data = confidentiality + integrity
- Forward Secrecy (PFS) requires ephemeral keys (DHE/ECDHE) – not static RSA

PKI TRUST CHAIN COMPONENTS

Root CA	Self-signed; offline; ultimate trust anchor
Intermediate CA	Signed by Root; issues end-entity certs; online
End-Entity Cert	Issued to server/user; contains public key
CRL	Certificate Revocation List; periodic; can be stale
OCSP	Online Cert Status Protocol; real-time check
OCSP Stapling	Server caches OCSP resp; reduces privacy leak
CT Log	Certificate Transparency; public append-only log
HSM	Hardware Security Module; protects CA private key
RA	Registration Authority; verifies identity on behalf of CA

X.509 CERTIFICATE KEY FIELDS

Version	v3 (current standard, supports extensions)
Serial Number	Unique per CA; used in CRL entries
Issuer	DN of signing CA
Validity Period	Not Before + Not After dates
Subject	Who the cert belongs to (CN, O, C)
Public Key	Algorithm + public key value
Extensions	SAN, Key Usage, EKU, CRL Distribution Points
Signature	CA signature over the above fields (trust proof)

CERTIFICATE TYPES

DV (Domain Validation)	Validates domain ownership only; automated
OV (Org Validation)	Validates org identity; business info in cert
EV (Extended Validation)	Highest assurance; legal identity verified
Wildcard (*.domain.com)	One cert covers all subdomains one level deep
SAN/Multi-domain	Subject Alt Names; multiple FQDNs in one cert
Code Signing	Signs software; binds code to publisher identity
Client Auth	Authenticates user/device to server (mTLS)
S/MIME	Email signing + encryption; binds email to key

TLS 1.3 HANDSHAKE (SIMPLIFIED)

Client Hello	TLS 1.3 + cipher suites + key_share (ECDHE pubkey)
Server Hello	Chosen cipher + server key_share + Certificate
(Server Verify)	CertificateVerify: sig over handshake transcript
Finished	HMAC over transcript; derive session keys
Client Finished	Client HMAC; handshake complete; app data flows

TLS 1.3 improvements over TLS 1.2:
0-RTT optional (careful: replay risk) | No RSA key exchange | No CBC | Removed SHA-1/RC4

IPSEC MODES & PROTOCOLS

Transport Mode	Encrypt payload only; original IP header intact; host-to-host
Tunnel Mode	Encrypt entire packet; new IP header; gateway-to-gateway
AH (Auth Header)	Integrity + anti-replay; NO encryption; rarely used alone
ESP (Encap Sec Payload)	Confidentiality + integrity; most common mode
IKEv2	Key exchange; supports MOBIKE (mobile/multi-homing)
SA (Security Assoc.)	Simplex; unidirectional; defined by SPI+IP+protocol

CERTIFICATE VALIDATION METHODS

Path Validation	Verify chain from end-entity to trusted Root CA
Revocation Check	CRL download or OCSP query to confirm not revoked
DANE (TLSA)	DNS-based auth of named entities; tie cert to DNS
Certificate Pinning	App hardcodes expected cert/pubkey; HPKP for web
CAA Record	DNS record restricts which CAs can issue for domain

■ EXAM INSIGHT

- TLS 1.3 only supports AEAD ciphers: AES-GCM, AES-CCM, ChaCha20-Poly1305
- OCSP Stapling = server attaches OCSP response to TLS handshake (performance+privacy)

■ MEMORY HOOK

- Root CA = offline vault; Intermediate CA = online signing factory
- HSM protects the CA private key – if CA key is compromised, entire PKI fails

SOC TIER MODEL

Tier 1 – Alert Triage
- Monitor SIEM dashboard; initial alert review
- Classify alerts: true/false positive
- Escalate to Tier 2 as needed
- Follow playbooks; close low-severity events

Tier 2 – Investigation
- Deep-dive incident analysis
- Threat hunting; correlate across sources
- Escalate APT/critical to Tier 3
- IOC extraction; SIEM rule tuning

Tier 3 – Threat Hunt / Expert
- Proactive hunting for unknown threats
- Malware reverse engineering
- Forensic analysis; IR leadership
- Detection engineering; red team collab

DETECTION & RESPONSE TOOLING

SIEM	Security Info & Event Mgmt	Log aggregation + correlation + alerting
SOAR	Security Orchestration/Automatic	Automate response playbooks + case mgmt
EDR	Endpoint Detection & Response	Agent-based; behavioural detection + rollback
XDR	Extended Detection & Response	EDR + network + cloud + identity unified
NDR	Network Detection & Response	Traffic analysis; east-west; ML anomaly
UEBA	User & Entity Behaviour Analytic	Baseline + anomaly scoring; insider threat
TIP	Threat Intelligence Platform	Aggregate, enrich, share IOCs/TTPs

SIEM USE CASES & DETECTION RULES
- Brute force: 5+ failed logins in 2 min same account
- Lateral movement: new admin login from unusual host
- Data exfil: large outbound transfer to new external IP
- Golden Ticket: Kerberos TGT lifetime > 600 min
- Privilege escalation: process runs as SYSTEM unexpectedly
- Impossible travel: login from two countries within 1hr
- Ransomware: mass file renames with crypto extensions
- C2 beacon: periodic HTTPS calls at fixed intervals

MITRE ATT&CK TACTICS (TA0001–TA0043)

Reconnaissance	Gather victim info pre-attack
Resource Development	Establish infra: C2, domains, certs
Initial Access	Phishing, exploits, supply chain
Execution	Run malicious code on target host
Persistence	Maintain foothold (reg keys, tasks)
Privilege Escalation	Gain higher permissions (UAC bypass)
Defence Evasion	Avoid detection (obfuscation, log clear)
Credential Access	Harvest creds (Mimikatz, LSASS dump)
Discovery	Enumerate env (net scan, AD query)
Lateral Movement	Move through network (PtH, PsExec)
Collection	Gather data of interest
C&C (C2)	Maintain comms with implants
Exfiltration	Steal data (DNS tunnelling, HTTPS)
Impact	Disruption: ransomware, wipe, DDoS

EXAM INSIGHT
- XDR = EDR + NDR + cloud + identity unified (broader than EDR alone)
- SOAR automates playbooks; SIEM detects; both needed for effective SOC

MEMORY HOOK
- ATT&CK Tactic = Why (goal); Technique = How; Sub-technique = specific method
- Detection = SIEM+EDR; Response = SOAR; Hunting = Tier 3 + TIP + ATT&CK

NIST SP 800-61 IR LIFECYCLE

1. Preparation
- IR policy + plan + playbooks
- Train team; run tabletop exercises
- Deploy SIEM, EDR, forensic tools
- Establish communication tree & contacts
- Baseline normal behaviour in environment

2. Detection & Analysis
- Monitor SIEM alerts + EDR telemetry
- Triage: severity classification (P1–P4)
- Correlate events; timeline construction
- Determine scope: blast radius assessment
- Declare incident; activate IR team

3. Containment, Eradication, Recovery
- Short-term: isolate affected systems
- Long-term: patch, rebuild, harden
- Eradicate malware; remove persistence
- Restore from clean backup; verify integrity
- Monitor closely post-recovery 30–90 days

4. Post-Incident Activity
- Lessons learned meeting (within 2 weeks)
- Update playbooks, detections, training
- Root cause analysis documentation
- Metrics: MTTD, MTTR, cost impact
- Regulatory reporting if required

ORDER OF VOLATILITY (MOST → LEAST)

1	**CPU Registers & Cache**	Lost on power cycle; ns-level lifespan
2	**RAM / Memory**	Running processes, passwords, keys
3	**Network Connections**	Active sessions, ARP cache, routing table
4	**Running Processes**	Process list, open file handles
5	**Temp Files / Swap**	Virtual memory; crash dumps
6	**Disk (Storage)**	Files, logs, installed programs
7	**Remote Logging**	SIEM, syslog, cloud trail – most durable
8	**Physical Config**	Network topology, hardware inventory
9	**Archival / Backups**	Backup tapes, cold storage – most stable

DIGITAL FORENSICS PRINCIPLES

Chain of Custody	Document who accessed evidence and when
Forensic Imaging	Bit-for-bit copy; verify with SHA-256 hash
Write Blockers	Hardware/software; prevent modifying source
Locard Principle	Every contact leaves a trace (Locard's Exchange)
Legal Hold	Preserve evidence for litigation; stop overwrites
eDiscovery	Legal process to collect/review electronic evidence
Steganography	Data hidden in files; detect with steganalysis tools

IR COMMUNICATION & REPORTING

Internal	Exec comms via secure out-of-band channel (if email compromised)
Legal	Engage counsel early; attorney-client privilege for IR docs
Regulatory	Breach notifications per GDPR/HIPAA/PCI timelines
Law Enforcement	FBI/CISA if nation-state or critical infra involved
Public	PR statement; honest, timely, no speculation
Vendor	Notify CSP/MSP if incident spans their infrastructure

■ EXAM INSIGHT
- NIST 800-61: Preparation is ongoing – not just a one-time phase before incidents
- Containment strategy depends on system criticality + incident type (don't always isolate)

■ MEMORY HOOK
- Volatility order: Registers > RAM > Network > Processes > Disk > Archive
- Chain of custody broken = evidence may be inadmissible in court

THREAT INTELLIGENCE LIFECYCLE

1. Direction
Define requirements: what threats matter to org?

2. Collection
Gather data: OSINT, dark web, ISACs, honeypots

3. Processing
Normalize, deduplicate, parse raw data

4. Analysis
Enrich, correlate, create actionable intelligence

5. Dissemination
Share to SIEM, SOAR, firewall, stakeholders

6. Feedback
Validate effectiveness; refine collection plan

IOC TYPES & EXAMPLES

IP Address	C2 servers, scanning IPs, known bad egress nodes
Domain / URL	Phishing domains, DGA-generated domains, malicious URLs
File Hash	MD5/SHA-256 of malware; detect exact file match
Email Header	Sender domain, X-Originating-IP, reply-to anomalies
Registry Key	HKCU\Run persistence keys; unusual autostart entries
Mutex	Malware-created mutexes to prevent re-infection
Yara Rule	Pattern matching rule for malware family detection
Network Pattern	Port/protocol combo; JA3/JA3S TLS fingerprints
Behaviour IOC	Process injection, LSASS access, shadow copy deletion

THREAT INTEL SHARING STANDARDS

STIX 2.1	Structured Threat Info eXpression; JSON format; objects+relationships
TAXII 2.1	Transport protocol for STIX; push/pull via HTTPS REST API
OpenIOC	Mandiant XML format; indicator logic with AND/OR operators
MISP	Open-source TI platform; event-based sharing; many orgs use
ISACs	Industry-specific sharing: FS-ISAC, H-ISAC, E-ISAC
MITRE ATT&CK	Adversary TTP knowledge base; tactics + techniques + mitigations

THREAT INTELLIGENCE TYPES

Strategic TI
High-level trends; for executives/board
Example: nation-state APT activity increasing

Operational TI
Specific campaigns/actors; for SOC managers
Example: APT29 targeting finance sector Q4

Tactical TI
TTPs of adversaries; for IR / detection teams
Example: Cobalt Strike beacon config patterns

Technical TI
Raw IOCs (IPs, hashes, domains); for tools
Example: 185.220.x.x Tor exit node list

THREAT HUNTING METHODOLOGY

Hypothesis	ATT&CK-based hypothesis: "Assume T1059 living-off-land"
Data Collection	Pull relevant logs: PowerShell, WMI, process telemetry
Investigation	Query SIEM/EDR; baseline vs anomaly analysis
Discovery	Find malicious artefacts or confirm all-clear
Inform/Improve	New detections; tune SIEM; update threat model

DIAMOND MODEL OF INTRUSION

Adversary	Who is conducting the intrusion?
Capability	What tools/malware/exploits are used?
Infrastructure	IPs, domains, C2 used by adversary
Victim	Target of the intrusion event
Meta-features	Timestamp, phase, result, direction, methodology

PYRAMID OF PAIN

Hash Values	Trivial – attacker recompiles to change
IP Addresses	Easy – change VPN/proxy/Tor exit node
Domain Names	Simple – register new domain in minutes
Network/Host Artefacts	Annoying – modify scripts/configs
Tools	Challenging – requires new malware
TTPs	HARD – must change entire methodology

■ EXAM INSIGHT

- STIX = what (data format); TAXII = how (transport); they work together
- Pyramid of Pain: targeting TTPs is most effective; hashes/IPs are easily changed

■ MEMORY HOOK

- Diamond Model: Adversary uses Capability over Infrastructure against Victim
- Threat hunting = proactive; IR = reactive – both needed in mature SOC

LOCKHEED MARTIN CYBER KILL CHAIN

1. Reconnaissance
Gather target info (OSINT, LinkedIn, DNS)

2. Weaponisation
Create exploit + payload (trojan, macro)

3. Delivery
Phishing email, watering hole, USB drop

4. Exploitation
Trigger vulnerability on target system

5. Installation
Drop implant; establish persistence

6. C2 (C&C)
Beacon to attacker; await commands

7. Actions on Objectives
Data theft, lateral move, ransomware

APT CHARACTERISTICS & TTPS

Long Dwell Time	Avg 200+ days before detection; hide in noise
Living off the Land	Use legitimate tools (PowerShell, WMI, certutil)
Custom Malware	Purpose-built implants; evade AV signatures
Supply Chain	Compromise vendor software/hardware upstream
Spear Phishing	Targeted, researched emails; trust-based lures
Watering Hole	Compromise sites visited by target org
Zero-Day Exploits	Leverage unknown vulnerabilities; no patch
Credential Theft	Kerberoasting, pass-the-hash, DCSync attack

COMMON ATTACK TECHNIQUES (EXAM)

Pass-the-Hash	Replay NTLM hash without cracking; lateral movement
Pass-the-Ticket	Steal Kerberos TGT/TGS; impersonate user without creds
Kerberoasting	Request TGS for SPN; crack offline; get svc account creds
Golden Ticket	Forge TGT using krbtgt hash; unlimited Kerberos access
Silver Ticket	Forge TGS for specific service; no DC contact needed
DCSync	Mimic DC replication; extract password hashes
LLMNR Poisoning	Respond to multicast; capture NTLMv2 challenge-response
DLL Injection	Insert malicious DLL into legitimate process memory

RED / BLUE / PURPLE TEAM

Red Team

- Simulate real adversary TTPs
- Persistent multi-phase engagement
- Goal: test people, process, technology
- Uses: social eng, phishing, exploits
- Reports: detection gaps + attack paths

Blue Team

- Defend, detect, respond to attacks
- Tune SIEM; manage vulnerabilities
- Hardening + patching + IR
- Provides: threat hunting, detection rules
- Reports: MTTD, MTTR, coverage gaps

Purple Team

- Red + Blue working together
- Red executes TTP; Blue tests detection
- Immediate feedback loop; tune detections
- Most effective for maturing SOC
- Not a separate team; a collaboration mode

PENETRATION TESTING PHASES (PTES)

Pre-Engagement	Scope, rules of engagement, legal agreement
Reconnaissance	Passive (OSINT) + active (scan) information gathering
Threat Modelling	Map attack vectors; prioritise high-value targets
Vulnerability ID	Scan + enumerate vulnerabilities in scope
Exploitation	Attempt to exploit; demonstrate business impact
Post-Exploitation	Pivot, escalate, persist; show blast radius
Reporting	Executive summary + technical findings + remediation
Remediation Test	Verify fixes; retest vulnerabilities that were patched

■ EXAM INSIGHT

- Golden Ticket = krbtgt hash compromise; Silver Ticket = service account hash
- Kill Chain disruption: block at Delivery/Exploitation phases for best ROI

■ MEMORY HOOK

- Red = attack; Blue = defend; Purple = collaborate to improve detections
- Kerberoasting targets SERVICE accounts (SPN); doesn't need elevated privileges

CVSS v3.1 SCORING (BASE METRICS)

Exploitability Metrics

Attack Vector (AV)	Network(N)=3.9 / Adjacent(A) / Local(L) / Physical(P)=0.85
Attack Complexity (AC)	Low(L)=0.77 / High(H)=0.44 – how hard to repeat
Privileges Required (PR)	None(N)=0.85 / Low(L)=0.62 / High(H)=0.27
User Interaction (UI)	None(N)=0.85 / Required(R)=0.62

Impact Metrics

Confidentiality (C)	None/Low/High impact on CIA triad confidentiality
Integrity (I)	None/Low/High impact on data accuracy/trust
Availability (A)	None/Low/High impact on system/service uptime

Scope (S)

Unchanged (U)	Vulnerable component only affected
Changed (C)	Other components beyond vulnerable one affected

CVSS SCORE RANGES & SEVERITY

0.0	None	No action required
0.1–3.9	Low	Patch in next maintenance windo
4.0–6.9	Medium	Patch within 30–90 days
7.0–8.9	High	Patch within 7–30 days
9.0–10.0	Critical	Emergency patch – immediate act

VULNERABILITY MANAGEMENT LIFECYCLE

1. **Asset Discovery**
   Know what you have – network scan, CMDB, cloud inventory
2. **Vulnerability Scan**
   Authenticated scans (Nessus/Qualys/Rapid7); full coverage
3. **Risk Prioritisation**
   CVSS + threat intel + asset criticality = priority score
4. **Remediation**
   Patch > mitigate > accept; track in ticketing system
5. **Verification**
   Rescan after patching; verify closure
6. **Reporting**
   Metrics: mean-time-to-patch, open critical count, SLA compliance

VULNERABILITY SCANNING TYPES

Credentialed / Authenticated	Logs into host; deeper findings; fewer false positives
Non-Credentialed / External	No login; attacker perspective; more false positives
Agent-Based	Agent on endpoint; continuous; offline scanning
Passive / Network Tap	Monitor traffic; no intrusion; detect running vulns
Cloud API-Based	Query CSP APIs (AWS Inspector, Azure Defender)
Container Image Scanning	Scan before deploy; Trivy, Clair, Snyk

PATCH PRIORITISATION STRATEGY

Tier 1 – Critical + Exploited	CISA KEV listed; CVSS 9+; patch in 24–72 hrs
Tier 2 – Critical, not exploited	CVSS 9+; patch within 7 days if possible
Tier 3 – High Severity	CVSS 7–8.9; patch within 14–30 days
Tier 4 – Medium	CVSS 4–6.9; patch in next change window
Tier 5 – Low	CVSS <4; track; address in quarterly cycles

■ EXAM INSIGHT
- CVSS alone is insufficient – augment with EPSS (Exploit Prediction Scoring System)
- CISA KEV (Known Exploited Vulnerabilities) = top priority for immediate patching

■ MEMORY HOOK
- Credentialed scan = internal view; unauthenticated = attacker view – use BOTH
- Vulnerability = weakness; Threat = potential exploit; Risk = likelihood × impact

DEVSECOPS CI/CD PIPELINE SECURITY

Plan
Threat model; security requirements; SBOM tracking

Code
IDE plugins (Semgrep); pre-commit hooks; secrets scan

Build
SAST (Checkmarx/Fortify); SCA (Snyk/OWASP Dep-Check)

Test
DAST (OWASP ZAP/Burp); IAST; container image scanning

Release
Security gate: fail build on critical vuln; approvals

Deploy
IaC scan (Checkov/Terrascan); signed artefacts only

Operate
RASP; WAF; runtime monitoring; CSPM alerts

Monitor
SIEM ingestion; anomaly detection; SBOM updates

SOFTWARE SUPPLY CHAIN SECURITY

SBOM (Software BOM)	Inventory of all components + versions + licences
Code Signing	Sign releases; verify integrity; EV code signing cert
Dependency Pinning	Lock exact versions; prevent dependency confusion attack
Dependency Confusion	Attacker uploads malicious public pkg with private name
SLSA Framework	Supply chain Levels for SW Artefacts; L1–L4 assurance
Signed Commits	GPG-sign git commits; verify author identity in pipeline
Artefact Registry	Internal registry; no direct pull from internet in prod

AI / ML SECURITY RISKS

Prompt Injection	Malicious input overrides AI system instructions
Data Poisoning	Corrupt training data to bias model behaviour
Model Inversion	Extract training data from model outputs
Adversarial Examples	Perturb input to cause model misclassification
Model Theft	Query API repeatedly to reconstruct model
Hallucination	Confident but factually wrong output; trust risk
LLM Plugin Abuse	Chained LLM actions bypass access controls
Shadow AI	Employees use unapproved AI tools; data exfil risk

SECURE AI ARCHITECTURE CONTROLS

- ■ Input validation + prompt sanitisation (LLM firewall)
- ■ Output filtering + PII redaction before display
- ■ Least-privilege API keys; rate limiting on AI calls
- ■ Audit logging of all AI interactions + queries
- ■ Data classification before feeding to external AI
- ■ Human-in-the-loop for high-risk AI decisions
- ■ Red team AI systems (adversarial testing)
- ■ Vendor risk assessment for AI API providers

CONTAINER & KUBERNETES SECURITY

Image Hardening	No root; minimal base image; no secrets in layers
Admission Control	OPA/Gatekeeper; Kyverno; block policy violations
Network Policies	Default-deny; explicit allow east-west traffic
RBAC	Least-privilege; no cluster-admin for workloads
Secrets Management	External vault; never env vars or ConfigMaps
Node Hardening	CIS Benchmark; container runtime (containerd)
Pod Security Std	Restricted > Baseline > Privileged profile
Image Signing	Cosign/Notary; only signed images in prod

■ EXAM INSIGHT

- SBOM = inventory list of all software components; mandatory for federal software (EO 14028)
- Dependency confusion: attacker publishes malicious package with same name as internal one

■ MEMORY HOOK

- Shift-left = move security earlier in SDLC (design/code) not just testing/deploy phase
- SLSA Level 3+ = tamper-proof build pipeline; most supply chain attacks prevented

SASE ARCHITECTURE COMPONENTS

SD-WAN	Software-defined WAN; path selection; cloud breakout
ZTNA	Zero-trust network access; replaces VPN; app-specific
CASB	SaaS visibility + compliance + DLP + threat protection
FWaaS	Firewall-as-a-Service; Layer 7 inspection at cloud edge
SWG	Secure Web Gateway; URL filtering; SSL inspection; DLP
DNS Security	Block malicious domains; detect DGA; DNS over HTTPS
UEBA	User/entity baseline; insider threat; account takeover

IDENTITY & ACCESS MANAGEMENT (IAM)

MFA Types	Type 1=Know, Type 2=Have, Type 3=Are; FIDO2=gold std
SSO	One credential for all apps; SAML/OIDC; reduce password fatigue
PAM	Privileged Access Management; vault creds; JIT admin access
JIT Access	Just-In-Time: grant privileged access only when needed
Conditional Access	Risk-based; device compliance + location + user risk score
Lifecycle Mgmt	Joiner-Mover-Leaver process; auto-deprovision on HR event
Directory Sync	HR system → Azure AD/LDAP; authoritative source of identity
Entitlement Review	Quarterly access certification; remove excess permissions

IOT / OT / SCADA / ICS SECURITY

Purdue Model	5-level ICS model; Level 0=field device to Level 5=enterprise
Air Gap	Physical isolation of OT from IT; strict if safety-critical
Data Diode	One-way data transfer: OT→IT only; no return path
OT-Specific IDS	Claroty, Dragos, Nozomi – understand industrial protocols
Protocol Risks	Modbus, DNP3, BACnet, PROFINET – legacy, no auth built-in
Firmware Sec	Secure boot; signed firmware; patch lifecycle for devices
Network Seg	Separate OT VLAN; strict firewalls; DMZ between IT/OT

NETWORK SECURITY CONTROLS

NGFW	App-aware; IPS; SSL inspection; user identity-based rules
WAF	L7 HTTP/HTTPS; OWASP Top 10; rate limiting; bot management
IDS/IPS	Signature + anomaly; IPS can block; IDS alerts only
NAC (802.1X)	Endpoint posture check before network access granted
Micro-Segmentatio	East-west control; workload isolation; SDN-based
VPN / ZTNA	IPsec/SSL VPN = network-level; ZTNA = app-level; prefer ZTNA
DDoS Mitigation	Rate limit; anycast scrubbing; CDN + cloud protection
DNS Security	DNSSEC integrity; RPZ block; split-horizon; DoH/DoT

EMAIL SECURITY CONTROLS

SPF	Authorised senders for domain; TXT DNS record; reject spoofed
DKIM	Digital signature in email header; verify sender integrity
DMARC	Policy: none/quarantine/reject based on SPF+DKIM alignment
DMARC repor	Aggregate + forensic reports; visibility into abuse
BIMI	Brand logos in email; requires DMARC enforcement + VMC
S/MIME	End-to-end signing + encryption; cert-based; enterprise use
Email Gatewa	Spam filter; malware scan; DLP; outbound filtering

MOBILE DEVICE SECURITY

MDM	Mobile Device Management; full device control; remote wipe
MAM	Mobile App Management; app-level control; BYOD-friendly
EMM	Enterprise Mobility Mgmt; MDM+MAM+MCM combined platform
UEM	Unified Endpoint Mgmt; extends to laptops, IoT, desktops
Conditional A	Require compliant/managed device for corp data
Container	Corporate data in encrypted container; separate personal

■ EXAM INSIGHT

- ZTNA replaces VPN; provides per-app access vs network-level exposure
- DMARC requires both SPF AND DKIM aligned to enforcement policy to be effective

■ MEMORY HOOK

- Purdue Model levels: 0=sensor, 1=PLC, 2=SCADA, 3=site ops, 4/5=enterprise/IT
- MDM=device control; MAM=app control; EMM=both; UEM=all endpoints unified

CRITICAL FORMULAS CHEAT SHEET

SLE = AV × EF
Single Loss Expectancy: asset value × exposure factor

ALE = SLE × ARO
Annual Loss Expectancy: per event × events per year

ROSI = (ALE_b – ALE_a) – CC
ROI of security: before minus after minus control cost

Risk = T × V × I
Threat × Vulnerability × Impact

MTD > RTO > RPO
Max tolerable downtime must exceed recovery time

Availability = MTBF / (MTBF + MTTR)
System reliability metric

IF YOU SEE → THINK (EXAM TRIGGER TABLE)

Insider threat + behaviour anomalies	→ UEBA (User Entity Behaviour Analytics)
Cloud SaaS misconfiguration	→ CASB + SSPM
Container runtime threat protection	→ CWPP
API security at scale	→ API Gateway + OAuth 2.0 + WAF
Legacy OT network protection	→ Purdue Model + data diode + IDS
Employee exits / access	→ Joiner-Mover-Leaver + IAM lifecycle
Privileged account abuse	→ PAM + JIT + session recording
Ransomware prevention	→ 3-2-1-1-0 backup + immutable storage + EDR
Third-party vendor security	→ Third-party risk assessment + contractual SLA
Regulatory audit evidence	→ Centralised logging + SIEM + access reviews
Secret exposure in code	→ SAST + secrets scanning + vault
Phishing mitigation	→ DMARC + email gateway + security awareness
DDoS defence	→ Anycast scrubbing + CDN + rate limiting
Wireless rogue device	→ NAC (802.1X) + WIDS + port security

ACRONYM MASTER LIST

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AICPA	American Institute of CPAs (SOC reports)
ALE	Annual Loss Expectancy
APT	Advanced Persistent Threat
ARO	Annual Rate of Occurrence
ATO	Authority to Operate (NIST)
AV	Asset Value (risk formula)
BYOD	Bring Your Own Device
CA	Certificate Authority
CASB	Cloud Access Security Broker
CIA	Confidentiality, Integrity, Availability
CIEM	Cloud Infrastructure Entitlement Mgmt
CISA	Cybersecurity & Infrastructure Security Agency
CMK	Customer Managed Key (cloud)
CMDB	Configuration Management Database
CNAPP	Cloud-Native App Protection Platform
CSPM	Cloud Security Posture Management
CTI	Cyber Threat Intelligence
CVSS	Common Vulnerability Scoring System
CWPP	Cloud Workload Protection Platform
DCO	Defensive Cyber Operations
DKIM	DomainKeys Identified Mail
DMARC	Domain Message Auth Reporting & Conformance
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoH	DNS over HTTPS
DPoP	Demonstration of Proof of Possession
DR	Disaster Recovery

■ EXAM STRATEGY

- Read ALL answer options before selecting; eliminate wrong answers first
- Look for "most comprehensive", "BEST practice" or "architect-level" language

■ RAPID RECALL MNEMONICS

- DiD = Defense in Depth = Swiss cheese layers
- CIA = Confidentiality Integrity Availability

ACRONYM MASTER LIST (E–P)

EAP	Extensible Authentication Protocol
EDR	Endpoint Detection & Response
EF	Exposure Factor (CVSS / risk calc)
EMM	Enterprise Mobility Management
EPSS	Exploit Prediction Scoring System
FDE	Full Disk Encryption
FIDO2	Fast Identity Online v2 (WebAuthn)
GDPR	General Data Protection Regulation
HA	High Availability
HIPAA	Health Insurance Portability & Accountability Act
HSM	Hardware Security Module
HTTPS	HTTP Secure (HTTP over TLS)
IAM	Identity & Access Management
ICS	Industrial Control System
IDS	Intrusion Detection System
IKE	Internet Key Exchange (IPsec)
IPS	Intrusion Prevention System
ISMS	Information Security Management System
JIT	Just-In-Time (access provisioning)
KEK	Key Encryption Key
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MISP	Malware Info Sharing Platform
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTD	Mean Time to Detect

ACRONYM MASTER LIST (M–Z)

MTTR	Mean Time to Repair / Recover
NAC	Network Access Control
NDR	Network Detection & Response
NGFW	Next-Generation Firewall
OCSP	Online Certificate Status Protocol
PAM	Privileged Access Management
PCI	Payment Card Industry
PDP	Policy Decision Point (ZTA)
PEP	Policy Enforcement Point (ZTA)
PFS	Perfect / Forward Secrecy
PHI	Protected Health Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PKCE	Proof Key for Code Exchange
RASP	Runtime App Self-Protection
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SASE	Secure Access Service Edge
SBOM	Software Bill of Materials
SIEM	Security Info & Event Management
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SOAR	Security Orchestration, Auto & Response
SOC	Security Operations Centre
SSPM	SaaS Security Posture Management
STIX	Structured Threat Info eXpression
TAXII	Trusted Automated eXchange of Indicator Info
TDE	Transparent Data Encryption
TTP	Tactics, Techniques & Procedures
UEBA	User & Entity Behaviour Analytics

SECURITY MNEMONICS

CIA:
Confidentiality → Integrity → Availability

STRIDE:
Spoof Tamper Repudiate Info-disclose DoS Elevate

AAA:
Authenticate → Authorise → Account (log)

NIST RMF:
"Prepare Cats, Select IAM" (Prepare Categorise Select Implement Assess Authorise Monitor)

DiD:
People Process Technology – 3 pillars first

3-2-1:
3 copies, 2 media types, 1 offsite location

PKI chain:
Root → Intermediate → End-Entity (R-I-E)

IR Phases:
Prepare, Detect, Contain/Eradicate, Recover, Review (PDCRR)

■ EXAM INSIGHT

- UEM > EMM > MDM/MAM – UEM is most comprehensive endpoint management
- FIDO2 / passkey = strongest phishing-resistant MFA (replaces TOTP in exam scenarios)

■ LAST EXAM TIPS

- "Best" answer = most comprehensive + business-aligned + risk-proportionate
- When in doubt between two answers: choose the one that preserves availability last

WI-FI SECURITY STANDARDS

WEP	RC4 stream (broken)	PROHIBITED – crack in minutes
WPA	TKIP (RC4-based)	DEPRECATED – TKIP crackable
WPA2-P	AES-CCMP + PSK	Vulnerable to PMKID offline attack
WPA2-E	AES-CCMP + 802.1X	Enterprise; RADIUS auth; much stronger
WPA3-P	SAE (Dragonfly)	Resistant to dictionary attacks; PFS
WPA3-E	192-bit Suite B crypto	CNSA-compliant; government/enterprise

WIRELESS ATTACK TECHNIQUES

Evil Twin AP	Rogue AP mimics legit SSID; intercept tr	WPA3-E + 802.1X + cert pinning
Deauth Flood	802.11 mgmt frames unauthenticated; di	WPA3 PMF (802.11w)
KRACK	Key Reinstall Attack on WPA2 4-way ha	Patch all devices; WPA3 immune
PMKID Attack	Offline PSK crack from single captured f	Strong random PSK (20+ chars)
Rogue RADIUS	Fake RADIUS harvests EAP credentials	Validate server cert in EAP config
Bluetooth BLESA	BLE Spoofing on reconnection events	Require re-authentication on reconne
NFC Relay Attack	Relay contactless card to fraudulent rea	Distance bounding; shielded wallet

SHORT-RANGE WIRELESS REFERENCE

Bluetooth 5.x	~100m	BLE: IoT/sensors; Classic: audio/file transfer
NFC	~4cm	Contactless pay, badge tap, device pairing
Zigbee	~100m	IoT mesh; 2.4 GHz; low power; smart home
Z-Wave	~30m	Home automation; sub-GHz; less interference
RFID LF/HF	<1m	Asset tracking, proximity access cards
UWB	~10m	Precise location (Apple AirTag, car key)

PHYSICAL SECURITY LAYERS

Perimeter Controls
- Fencing + bollards + vehicle barriers
- Security lighting (motion-activated)
- CCTV + video analytics
- Warning signs / deterrent signage

Facility Entry Controls
- Mantrap / airlock – prevents tailgating
- Badge + PIN + biometric (multi-factor)
- Visitor log + escort policy
- Guard station at entry points

Interior Controls
- Cipher locks on server rooms
- Faraday cage for RF-sensitive areas
- Cable locks; equipment anchors
- Clean desk + screen lock policy

Environmental Controls
- HVAC: 68-77F / 45-55% humidity
- FM-200 or clean agent fire suppression
- UPS + generator for power redundancy
- Water/flood sensors under raised floors

■ EXAM INSIGHT
- WPA3-Personal = SAE (Simultaneous Auth of Equals) – no more 4-way handshake attack
- PMF (Protected Mgmt Frames) = 802.11w – required in WPA3; stops deauth/disassoc attacks

■ MEMORY HOOK
- Tailgating = unauthorised person follows authorised; mantrap = two-door airlock solution
- NFC max range ~4cm; RFID LF/HF up to 1m; both vulnerable to relay/skimming attacks

OAUTH 2.0 GRANT FLOWS

Authorization Code + PKCE

1. App → Auth Server: code_challenge (S256)
2. User authenticates + consents
3. Auth Server → App: authorization_code
4. App + code_verifier → Token Endpoint
5. App receives access_token + refresh_token

→ **Recommended for ALL clients: SPA, mobile, server**

Client Credentials

1. App → Token Endpoint: client_id + secret
2. Token Endpoint → App: access_token

(No user involved – machine-to-machine)

→ **M2M / service accounts / microservice APIs**

Implicit (DEPRECATED)

Token returned in URL fragment – insecure

Replaced by Auth Code + PKCE for SPAs

→ **DO NOT USE – token leaks in browser history**

OAUTH 2.0 KEY CONCEPTS

Access Token	Short-lived (15min); JWT or opaque; used for API calls
Refresh Token	Long-lived; exchange for new access token; store securely
Scope	Limit permissions: read:email, write:files, admin
PKCE	Proof Key for Code Exchange – stops auth code interception
Bearer Token	No proof of possession; protect in transit (TLS required)
DPoP Token	Binds token to client key; prevents bearer token theft

SAML 2.0 SSO FLOW

1. User	Accesses Service Provider (SP) resource
2. SP	Redirects to IdP with AuthnRequest (Base64 XML)
3. User	Authenticates at IdP (MFA if configured)
4. IdP	Issues signed XML SAML Assertion to browser
5. Browser	HTTP-POST SAML Response to SP ACS URL
6. SP	Validates signature; extracts attributes; allows access

SAML vs OIDC vs OAUTH 2.0

Factor	SAML 2.0	OIDC	OAuth 2.0
Format	XML	JSON/JWT	JSON token
Transport	HTTP POST/Redir	REST/HTTP	REST/HTTP
Use Case	Enterprise SSO	Consumer SSO	Delegated Auth
Token	Assertion (XML)	ID Token (JWT)	Access Token
Mobile	Poor support	Excellent	Native

FEDERATION & DIRECTORY PROTOCOLS

LDAP / AD	TCP 389 (plaintext) / LDAPS 636 (TLS). Directory access protocol.
Kerberos	Ticket-based auth; KDC issues TGT → TGS → Service ticket; port 88
RADIUS	UDP 1812/1813; centralized AAA; NAS forwards auth to RADIUS server
TACACS+	TCP 49; Cisco; separates AAA; encrypts full payload (vs RADIUS partial)
SAML	XML SSO federation; IdP + SP trust relationship; metadata exchange
SCIM	System for Cross-domain Identity Management; auto-provision accounts

■ EXAM INSIGHT

- SAML = XML enterprise SSO (legacy); OIDC = OAuth 2.0 + identity layer (modern)
- Always use Auth Code + PKCE – never Implicit flow for any new application

■ MEMORY HOOK

- OAuth = authorization ("can I use your car?"); OIDC = authentication ("who are you?")
- RADIUS = UDP, AAA combined; TACACS+ = TCP, AAA separated – Cisco prefers TACACS+

OWASP TOP 10 (2021) + MITIGATIONS

A01	Broken Access Control	IDOR, path traversal, privilege esc	RBAC + deny-by-default + logging
A02	Cryptographic Failures	Weak ciphers, hardcoded keys, H	TLS 1.3, AES-256, key rotation
A03	Injection	SQLi, XSS, CMDi – untrusted to ir	Parameterized queries, WAF, valida
A04	Insecure Design	No threat model, missing security	STRIDE, threat model, security sto
A05	Security Misconfiguration	Default creds, verbose errors, ope	CIS benchmarks, CSPM, IaC scan
A06	Vulnerable Components	Outdated libs, unpatched depende	SCA scanning, SBOM, patch pipelin
A07	Auth & Session Failures	Weak passwords, no MFA, sessio	MFA, session expiry, secure cookie
A08	SW Integrity Failures	CI/CD compromise, no code signi	SBOM, code signing, supply chain
A09	Logging & Monitoring Fail	No audit trail, undetected breache	Centralised logs, SIEM, alerts
A10	SSRF	Server-Side Request Forgery via u	Allowlist outbound, disable URL sc

TESTING TYPES COMPARISON

SAST	White-box; analyze SOURCE CODE without exec
DAST	Black-box; test RUNNING app from outside
IAST	Gray-box; agent inside running app; hybrid
SCA	Scan 3rd-party libs; find CVEs; SBOM generation
RASP	Runtime; app protects itself from within; blocks att
BAS	Breach & Attack Simulation; continuous automated

THREAT MODELING – STRIDE

S	Spoofing	Impersonate user/system → Authentication controls
T	Tampering	Modify data in transit/at rest → Integrity checks, HMAC
R	Repudiation	Deny performing action → Audit logs, digital sigs
I	Info Disclosure	Expose data to unauthorised party → Encryption, access ctrl
D	Denial of Service	Make resource unavailable → Rate limit, redundancy
E	Elevation of Priv	Gain higher privileges → Least privilege, RBAC

SECURE SDLC ACTIVITIES BY PHASE

Requirements	Security user stories; abuse cases; privacy requirements
Design	Threat modeling (STRIDE/PASTA); architecture review
Development	Secure coding standards; IDE security plugins; peer review
Testing	SAST + DAST + SCA; security test cases; fuzzing
Deployment	IaC scanning; signed artefacts; hardened config
Operations	Vulnerability scanning; patching; RASP; SIEM monitoring
Decommission	Secure data disposal; certificate revocation; NIST 800-88

COMMON WEB ATTACK TECHNIQUES

SQL Injection	Untrusted data in SQL query; extract/destroy DB
XSS (Stored)	Malicious script persisted in DB; runs for all users
XSS (Reflected)	Script in URL; victim must click crafted link
CSRF	Victim's browser makes unintended authenticated request
Path Traversal	../../../etc/passwd; escape web root; read files
XML/XXE Injection	External entities in XML parser; SSRF / file read

■ EXAM INSIGHT
- STRIDE threat modeling pairs with data flow diagrams – exam standard approach
- A01 Broken Access Control = #1 OWASP risk since 2021; heavily tested on SecurityX

■ MEMORY HOOK
- SAST = white-box (code visible); DAST = black-box (runtime); IAST = gray-box (agent)
- SSRF: Server makes outbound requests to internal resources on attacker's behalf

DATA CLASSIFICATION TIERS

TOP SECRET / RESTRICTED
Nation-state secrets, M&A targets, nuclear codes
→ Air-gapped systems, full-disk encrypt, cleared personnel only

CONFIDENTIAL / SECRET
PII, PHI, financial records, trade secrets, source code
→ Encryption at rest+transit, strict ACLs, NDA required

INTERNAL / SENSITIVE
Employee data, internal policies, project plans
→ Access controls, encrypted email, need-to-know basis

PUBLIC / UNCLASSIFIED
Marketing materials, press releases, open-source code
→ Minimal controls; integrity verification only

DATA STATES & PROTECTION METHODS

Data at Rest Disk, DB, backup tapes	AES-256-GCM, FDE, TDE, encrypted backups
Data in Transit Network, API, sync	TLS 1.3, IPsec, SFTP, encrypted tunnels
Data in Use RAM, CPU, active processing	Confidential Computing (Intel SGX, AMD SEV)
Data in Archive Long-term, retention	WORM, immutable S3, key escrow

DLP CONTROL TYPES

Network DLP	Inspect perimeter traffic; block sensitive data egress
Endpoint DLP	Agent on workstation; control USB, print, clipboard, upload
Cloud DLP	CASB + cloud-native DLP (Google, Microsoft Purview)
Email DLP	Scan outbound mail for PII, financial data, code
Storage DLP	Discover + classify sensitive data at rest across repos

PRIVACY BY DESIGN (7 PRINCIPLES)

1. Proactive, Not Reactive	Prevent risks before they occur
2. Privacy as Default	Max privacy without user action
3. Privacy Embedded	Built into design; not bolted on
4. Full Functionality	Win-win: privacy AND full features
5. End-to-End Security	From collection through to destruction
6. Visibility & Transparency	Open about policies; user trust
7. Respect for Users	Consent, accuracy, access rights

GDPR KEY REQUIREMENTS

- Lawful basis required for all processing
- Data Subject Rights: access, erasure (right to be forgotten), portability
- DPIA mandatory for high-risk processing activities
- 72-hour breach notification to supervisory authority
- DPO required for public bodies + large-scale special processing
- Data minimisation: collect only what is necessary
- Storage limitation: delete when purpose is fulfilled
- Privacy notices at point of collection (transparent)

PRIVACY TECH CONTROLS

Tokenisation	Replace sensitive data with non-sensitive token (PCI use)
Anonymisation	Irreversible removal of PII; GDPR: no longer personal data
Pseudonymisation	Reversible with key; still personal data under GDPR
Data Masking	Substitute real data in non-prod environments
k-Anonymity	Each record indistinguishable from k-1 others
Differential Privacy	Add calibrated noise; used by Apple, Google, US Census

■ EXAM INSIGHT

- Data in Use (confidential computing) = most complex to protect; emerging exam topic
- DPIA = mandatory for GDPR high-risk processing; maps to NIST Privacy Impact Assessment

■ MEMORY HOOK

- Anonymisation = GDPR no longer applies; Pseudonymisation = GDPR still applies
- Tokenisation used in PCI-DSS to protect PANs; vault holds token↔PAN mapping

SECURITY METRICS & KPIs

Mean Time to Detect (MTTD)	Avg time from incident start to detection
Mean Time to Respond (MTTR)	Avg time from detection to containment
Mean Time to Patch (MTTP)	Avg time from vuln disclosure to patch deploy
Patch SLA Compliance %	% of vulns patched within SLA by severity tier
Phishing Click Rate	% of employees clicking simulated phishing
Open Critical Vulns	Number of unpatched CVSS 9+ vulnerabilities
Security Training Completion	% of staff completing annual SETA program
Incident Rate	Number of confirmed security incidents per period
Cost per Incident	Total incident response cost / incident count
Risk Register Open Items	Count of accepted vs mitigated vs overdue risks

SECURITY AWARENESS (SETA) PROGRAMME

Annual Training	Policy acknowledgement + compliance training required
Phishing Simulations	Automated campaigns; track click/report rate over time
Role-Based Training	Devs get OWASP; IR team gets forensics; exec get strategy
Tabletop Exercises	Test response process; identify plan gaps without impact
Posters & Comms	Visual reminders; intranet updates; monthly security tips
New Hire Onboarding	Security intro Day 1; policy sign-off before system access
Metrics & Reporting	Measure awareness change; report to CISO/board annually

THIRD-PARTY / VENDOR RISK MANAGEMENT

Risk Tiering	Classify vendors: Critical/High/Med/Low by data access
Security Questionnaire	SIG Lite, CAIQ (CSA), custom questionnaires
Contractual Controls	DPA, NDA, right-to-audit, SLA, breach notification
SOC 2 / ISO 27001	Require vendor to provide annual audit reports
4th Party Risk	Vendor's vendors also in scope; review supply chain
Offboarding	Revoke access; data return/deletion; close credentials
Ongoing Monitoring	Annual reassessment; CVE monitoring; news feeds

SECURITY GOVERNANCE STRUCTURE

Board / Audit Committee
Oversee risk; approve strategy; review metrics quarterly

CISO / CSO
Own security strategy; accountability for programme

Security Steering Cmte
Cross-functional; approve policies; resolve conflicts

Risk Management
Risk register; treatment decisions; risk appetite

Compliance
Regulatory mapping; audit coordination; remediation

Security Architecture
Design standards; review + approve new systems

SOC / Operations
Day-to-day detection/response; incident management

EXAM DOMAIN 5 – PROGRAMME OVERSIGHT

Security Roadmap	Multi-year plan aligned to business strategy
Maturity Models	CMMC, C2M2, BSIMM – measure and improve capability
Security Budget	Align spend to risk; justify ROSI to board
Legal & Regulatory	GDPR, HIPAA, PCI – ensure ongoing compliance
Privacy Programme	Privacy by design; DPIA; data governance
Merger & Acquisition	Due diligence: security assessment before deal closes
Security SLAs	Define service levels for SOC, patch, IR response

COMMON POLICY TYPES

AUP	Acceptable Use Policy – governs system/network use
ISP	Information Security Policy – top-level security intent
BCP	Business Continuity Policy – resilience commitments
IRP	Incident Response Policy – escalation + obligations
DRP	Disaster Recovery Policy – recovery targets
BYOD Policy	Rules for personal devices accessing corp data
Clean Desk	Ensure sensitive data not left visible unattended
Password Policy	Complexity, length, MFA, password manager usage

■ EXAM INSIGHT

- Domain 5 (10%) tests on strategy + governance + maturity; not just technical controls
- M&A security due diligence: assess target's risk posture before deal closes

■ MEMORY HOOK

- CISO reports to CEO or Board; NOT to CIO (avoid conflict of interest in most frameworks)
- Right-to-audit clause = contractual right to inspect vendor security; negotiate upfront

KEY PORT NUMBERS

20/21	FTP data/control
22	SSH/SFTP/SCP
25	SMTP (unencrypted)
53	DNS (UDP+TCP)
67/68	DHCP
80	HTTP
88	Kerberos KDC
110	POP3
143	IMAP
161/162	SNMP v3
389	LDAP
443	HTTPS (TLS)
445	SMB/CIFS
465	SMTPS
500	IKE/IPsec
514	Syslog UDP
587	SMTP/TLS submit
636	LDAPS
993	IMAPS
1433	MS SQL Server
1521	Oracle DB
3306	MySQL
3389	RDP
5432	PostgreSQL
8080	HTTP Alt
8443	HTTPS Alt

ALGORITHM STRENGTH MATRIX

PURPOSE	ALGORITHM	MINIMUM
Symmetric	AES-128/256-GCM	128-bit key
Asymmetric	RSA-3072+	3072-bit
Elliptic Curve	ECC P-256/384	256-bit
Key Exchange	ECDHE/DHE-3072	PFS req
Hash	SHA-256/SHA-3	256-bit
Pwd Hash	Argon2id/bcrypt	cost>=12
HMAC	HMAC-SHA256	256-bit
Dig. Sig	ECDSA/RSA-3072	256-bit EC
PQ KEM	ML-KEM (Kyber)	ML-KEM-768
PQ Sign	ML-DSA (Dilithium)	ML-DSA-44
CSPRNG	CTR_DRBG (AES)	NIST 800-90A

BREACH NOTIFICATION TIMELINES

GDPR	72 hrs to supervisory authority
HIPAA	60 days to HHS + individuals
PCI-DSS	Immediately to card brands
NY SHIELD	72 hrs to AG (500+ affected)
CCPA	45-day cure; no fixed timeline
PIPEDA (CA)	ASAP; no fixed timeline

EXAM TRIGGER → ANSWER MAP

Forward secrecy	→ ECDHE/DHE key exchange
Encrypt+auth combo	→ AES-GCM (AEAD mode)
Prevent replay	→ Nonces + timestamps + seq#
SQL injection fix	→ Parameterized queries
Third-party risk	→ Vendor assessment + BAA
Audit trail	→ Non-repudiation + dig. sig
Cloud key control	→ BYOK (Bring Own Key)
Code signing	→ EV code signing + HSM
Detect data exfil	→ DLP + UEBA + egress mon.
Container security	→ Image scan + CWPP + RBAC
API protection	→ OAuth 2.0 + rate limit + WAF
Privileged accounts	→ PAM + JIT + session record
BYOD security	→ MDM/MAM + conditional access
Email authentication	→ SPF + DKIM + DMARC
Rogue device detect	→ NAC 802.1X + port security
OT network attack	→ Air-gap + Purdue + IDS
Ransomware response	→ Isolate + backup + wipe
Shadow IT detection	→ CASB + DNS monitoring

LAST-MINUTE MANTRAS

"Business context > technical perfection"
"Architect for the threat, not the tool"
"Least privilege everywhere, always"
"Assume breach; design for resilience"
"Controls proportionate to risk"
"Log everything; alert on anomalies"
"Compliance is the floor, not ceiling"
"Supply chain is your attack surface"