

Scan to drill
this sheet

Preventive, Detective & Corrective Controls

Every control has a **type** — how it is implemented — and a **function** — what it does. Here is the full 3 × 3 with 51 worked examples.

	Preventive Stop it happening	Detective Notice it happening	Corrective Fix it afterwards
Physical Doors, walls, hardware — the built environment.	Door locks & key cards Security guards Fences & barriers Biometric scanners Mantrap doors	CCTV cameras Motion sensors Badge reader logs Glass break detectors Visitor management systems	Emergency response procedures Backup power (UPS / generators) Fire suppression systems Evacuation plans Physical asset recovery
Technical Enforced by systems and software.	Firewalls Antivirus software Multi-factor authentication Data encryption Input validation Access control lists	Intrusion detection systems (IDS) SIEM systems Log monitoring File integrity monitoring Network traffic analysis Vulnerability scanners	Intrusion prevention systems (IPS) Automated patch management System backups & recovery Quarantine systems Failover systems Incident response tools
Administrative People, policy and process.	Security awareness training Background checks Separation of duties Acceptable use policies Password policies Security procedures	Security audits Log reviews Performance monitoring Compliance assessments Peer reviews Whistleblower programs	Incident response teams Business continuity plans Disciplinary actions Policy updates Lessons-learned programs Process improvements

Beyond the 3 × 3 Security+ lists six functions, not three — compensating controls turn up most often in exam questions.

Deterrent

Discourages an attempt without physically stopping it.

e.g. warning signage, visible cameras, login banners stating monitoring is in effect.

Compensating

A stand-in giving comparable protection when the primary control is not feasible.

e.g. a legacy server that cannot take MFA, isolated on its own VLAN with session logging.

Directive

Instructs people what to do; relies on compliance, not enforcement.

e.g. an acceptable use policy, a documented procedure, mandatory onboarding training.

TYPE × FUNCTION A **firewall** is Technical + Preventive

CCTV is Physical + Detective

An **IR team** is Administrative + Corrective

Reading a matrix won't stick — turn it into instinct.

Drill type-vs-function questions until the answer is automatic. Ten minutes a day, free forever, no card.

cyberquizzier.com/go/controls-sheet