THE DEFINITIVE SECURITY CONTROLS MASTER GUIDE

A strategic breakdown of Categories, Functions, and Exam Arbitration Rules

PART 1: THE CATEGORIES (What is the mechanism?)

Managerial (Administrative)	*The Noun: High-level risk management & governance* Driven by executives, HR, or Legal to manage organizational liability and overall business posture.	• Policies (AUP, Data Retention) • Risk Assessments • Background Checks • Separation of Duties (SoD)
Operational	*The Verb: Tactical, human-driven daily processes* The day-to-day routine tasks performed by IT, SecOps, or physical security staff to maintain hygiene.	• Security Awareness Training • Manual Log Reviews • Threat Hunting • Media Sanitization
Technical (Logical)	*The Code: Automated solutions in silicon/software* Controls enforced by operating systems, network hardware, and applications.	• Firewalls / ACLs • Encryption (AES, RSA) • Multi-Factor Authentication (MFA) • Active Directory GPOs
Physical	*The Object: Tangible, real-world barriers* Environmental controls you can touch, install, or physically bypass.	• Fences, Mantraps, Bollards • Biometric Locks & Badges • HVAC & Fire Suppression • Server Racks & Cable Ramps

PART 2: THE FUNCTIONS (What is the primary intent?)

Preventive (Before / During)	Actively blocks the attack or violation from succeeding. The primary defense layer.	Firewall dropping a packet, OS locking an account after 3 fails, Mantrap stopping tailgating.
Detective (During / After)	Identifies and records an anomaly, but does not actively stop the execution.	CCTV cameras recording, SIEM dashboards, IDS logs, motion sensors.
Corrective (After)		

	Restores the system or environment to a known-good, secure state after damage is done.	Restoring data from a backup, re-imaging a compromised laptop, deploying a software patch.
Deterrent (Before)	Relies on human psychology and fear of consequence to discourage an attack.	"Guard Dog" signs, SSH warning banners, visible unarmed security guards.
Compensating (The Workaround)	The "duct tape" deployed when the ideal primary control is technically or financially impossible.	Putting an unpatchable legacy Windows XP system on an air-gapped, isolated VLAN.
Directive (The Mandate)	A strict rule, contract, or standard operating procedure that dictates human behavior.	Acceptable Use Policy (AUP), HIPAA compliance frameworks, signed employee contracts.

PART 3: THE EXAM ARBITRATION FRAMEWORK

1. The Noun vs. Verb Test (Directive vs. Operational)

Is the scenario about the *document* mandating the behavior? → **Directive** (e.g., The written AUP)

Is the scenario about the *human beings* actually doing the work? → **Operational** (e.g., Helpdesk running a phishing drill)

2. The Altitude of Risk Test (Managerial vs. Operational)

Is this mitigating high-level corporate/HR liability? → **Managerial** (e.g., HR background checks)

Is this a tactical SecOps/IT process to maintain daily hygiene? → **Operational** (e.g., Admin reviewing firewall logs)

3. The "Mindless Robot" Test (Preventive vs. Deterrent)

Imagine the attacker is an automated script that cannot feel fear or read warnings.

Does the control still physically/logically stop the script? → **Preventive** (e.g., Dropped IP, locked door)

Does the script ignore it and keep going? → **Deterrent** (e.g., Warning banner, fake camera)

4. The "State Change" Test (Detective vs. Corrective)

Does the control just make noise, flash a light, or write a log? → **Detective** (e.g., SIEM alert)

Does the control actively alter the environment to fix the broken thing? → **Corrective** (e.g., Re-imaging a drive)

5. The "Apology" Test (Compensating)

Is this the permanent, best-practice way to secure the system? → **Standard Function**

Are you apologizing to the auditor because you couldn't do it the right way? → **Compensating**