Internal Controls & COSO Framework Master Cheat Sheet

The 5 COSO Components (CRIME), Segregation of Duties (CAR) & SOX 404 Audit Essentials

1. THE 5 COMPONENTS OF THE COSO FRAMEWORK (CRIME)

Component	Key Principles & Meaning	Audit Verification Examples
Control Environment (C)	Tone at the top, ethical values, board independence, organizational structure.	Code of conduct signed annually, whistleblower hotline in place.
Risk Assessment (R)	Identifying and analyzing organizational risks to financial reporting objectives.	Annual fraud risk assessments, cybersecurity penetration reviews.
Control Activities (I)	Policies and procedures established to mitigate risks (preventive vs. detective).	Dual approvals for wires > $25,000, mandatory passwords.
Information & Comm. (M)	Internal and external communication channels conveying operational responsibilities.	Timely monthly financial reporting packages sent to management.
Monitoring (E)	Ongoing evaluations assessing whether internal controls function effectively.	Internal audit testing of controls, periodic physical inventory counts.

2. SEGREGATION OF DUTIES: THE 'CAR' RULE

To prevent fraud and error, no single employee should handle more than one of the three critical functions: **Custody of Assets** (handling cash/checks), **Authorization of Transactions** (signing POs/checks), and **Recording Accounting Data** (general ledger entries).