Achievable

CMA PART 1 DUMP SHEET

Internal controls

Governance, risk & compliance

- **Corporate governance:** a system of rules and practices ensuring accountability, fairness, transparency; aligns management with shareholder interests
- **Agency theory:** tension between shareholders (principals) and management (agents); mitigated by independent committees, CEO/chair separation, performance pay, independent board oversight
- **Board of directors:** ultimate oversight; majority independent; approves strategy, appoints and evaluates the CEO, oversees risk
- **CFO:** financial planning, reporting, statement accuracy, regulator and auditor liaison
- **Audit committee:** oversees audits, internal controls, auditor independence, whistleblower complaints
  All members independent (SOX §301, Rule 10A-3); NYSE/Nasdaq add ≥ 3 members, 1 with financial expertise; SOX §407 only requires disclosing whether there is a financial expert
- **Documentary hierarchy:** articles of incorporation → bylaws → corporate policies → procedures and manuals

External audit & regulatory bodies

- **External audit:** an independent opinion on fairness and conformity with GAAP/IFRS; governed by the PCAOB (public companies) and SOX §404
- **Audit risk model:** $\mathrm{AR} = \mathrm{IR} \times \mathrm{CR} \times \mathrm{DR}$
  $\mathrm{RMM} = \mathrm{IR} \times \mathrm{CR}$, the risk of material misstatement; AR, IR, CR, DR = audit, inherent, control, detection risk
- **Opinions:** unqualified (clean), qualified, adverse, disclaimer

Internal control framework (COSO)

- **Objectives (3):** operations, reporting, compliance; controls give *reasonable*, not absolute, assurance
- **5 components**, in COSO's order (mnemonic CRIME: control activities, risk assessment, information & communication, monitoring, control environment):
  - Control environment (the foundation)
  - Risk assessment
  - Control activities: approvals, reconciliations, SoD
  - Information & communication
  - Monitoring activities
- **Limitations:** human error, collusion, management override, cost-benefit constraints, outdated controls
- **Control types:** preventive (stop before: SoD, access controls), detective (find after: reconciliations, audits), corrective/safeguarding
- **Segregation of duties (SoD):** separate authorization, recording, custody, and reconciliation; no one person completes a transaction end to end

Sarbanes-Oxley Act (SOX)

- **Purpose:** restore investor trust; applies to US public companies and their auditors; administered by the SEC and PCAOB
- **Titles:**
  - I: establishes the PCAOB
  - II: auditor independence (partner rotation, restricted non-audit services)
  - VIII: criminalizes record destruction; workpaper retention; whistleblower protection
- **Sections:**
  - §302: the CEO and CFO personally certify financial reports
  - §404: management and auditors report on internal-control effectiveness

System controls & security

- **General vs application controls:** general = the overall IT environment; application = transaction level
- **Application controls:** input (validation, batch/hash totals), processing (control totals, sequence checks), output (reconciliation, distribution controls)
- **System development:** follows the SDLC; management authorization + user-acceptance testing
- **Backup / BCP:** full, incremental, differential backups; DRP recovery sites: hot (immediate, costliest), warm (moderate), cold (slowest, cheapest)