Governance, Control, and Enterprise Risk

Corporate Governance	5 Internal Control Components	8 Enterprise Risk Mgmt. Components
Compensation systems	Control Environment	Internal Environment
Board of Directors & Committees	Risk Assessment Process	Objective setting * Event Identification
External & Internal Auditors	Control Activities	Risk Assessment * Risk Response
Regulators * Lawyers * Creditors	Information & Communication	Control Activities
Internal Control systems	Monitoring	Information & Communication
Securities Analysts		Monitoring

Corporate Governance – Management = *Agents* for Shareholders * Must ensure that Mgmt *does not* act inappropriately

Articles of Incorporation => Secretary of State => *Purpose* & *Powers* of Corporation; plus Info & details on Corp. Stock
- **Amendments** need *at least* Majority Approval **&&** Dissenters can sell-out at FV *before* the amendment-vote

Bylaws => how officers & directors will be selected, their duties, how meetings are conducted, process for amending bylaws

Compensation Systems

***Bonuses* –** can be manipulated if *based* on *Accounting Profit* (e.g. timing of expenses or *deferred*)
Stock Options – *generally* good for Owners; ***but*** can focus on *Short-term* Profits **&&** if Price keep falling, *no more incentive*
Stock Grants – best if *Restricted* (holding requirements) * also can be based on *Performance* goals
Perquisites = Perks for Executives (e.g. retirement benefits, golden parachutes, loans, use of corporate jets)

Best Practices Compensation (ideal) => **mix** of *Fixed* & *Incentive* compensation based on *long-term* stock price

Balanced Scorecard **Performance bonuses =>** based in *composite* measures (e.g. Net Profit, R&D, Market Share, etc.)

Monitoring Management

Board of Directors = determine corporate *mission*, CEO, oversight, advising Mgmt., managing risk, and all major decisions
- ***Ordinary Care* & *Due Diligence*** * disclose any *Conflicts of Interest*
  * Business Judgment Rule = no liability for errors in judgment *if* in good faith, loyalty, and due care
- **Loyalty *Duty*** = put Best Interests of company *before* Personal Interests; *if Corp rejects opportunity, OK to then take it*
- *Majority* should be **Independent** *of management functions* **and** *not derive* other benefits *besides Director fees*
- *Entire* Board only can *bind corporation* * Decisions require Quorum *and* then ***majority*** approval

Nominating/Corporate Governance Committee = oversees Board *organization* * determines *qualifications* * *assignment* of committees * develops governance *principles* * oversees change in CEOs

Audit Committee = *all* must be Independent * oversees Accounting & Reporting Process + Audits * Whistle-blower system
* appoints & compensates external auditors * oversees disagreements between Mgmt. and Auditors
* *at least* 1 "Financial Expert" member (i.e. understand *company's* statements, GAAP, controls, audits *+ experience*)
* *Internal* Auditors *should* have *direct access* to the AudCom * *External* Auditors *must* report directly to AudCom

Compensation Committee = *all* must be Independent * reviews/approves of CEO compensation based on objectives
* advises Board on comp. plans * tries to *match* Executive *Incentives* with *Shareholder goals & risk appetite*

Executive *Officers* – limited *in authority* (as delegated to each by Board) ** *cannot bind* if acting *beyond* authority

Insider Directors = Officers, Employees, and *Major* Shareholders on the Board (i.e. *not independent outsiders*)

Dodd-Frank/Wall Street Reform *Requirements* – Disclose why CEO is ***or*** is *not* Board Chairman * ***Indy*** AudCom & CompCom
* must allow *non-binding* Shareholder Votes on *Executive Compensation* & *Golden Parachutes*

NYSE & NASDAQ *Independence* Requirements & *Other Rules* –> Board *Majority* must be Independent * *Indy* Coms
-> **NYSE *more strict* = 5 years * NASDAQ = 3 years** * must determine *Indy* according to each exchange's (*similar*) rules

* *cannot* have been an Employee or Affiliate within past X years * family member was an Officer within X yrs (Affiliates too)
* *substantial* compensation from other entities (or paid $120K as Director)

Internal Auditors – *includes* audits of IC, *Risk Mgmt. Activities* & *Governance Processes* * *also* required by NYSE
-> *should* communicate *directly* to AudCom ** IIA -> CIA designation -> 2 years' experience -> competent

Int'l Internal Auditing Stds. – **(1)** ***Assurance*** services <u>*checks-up*</u> on Organization * **(2)** ***Consulting*** <u>*improves*</u> Org's processes
* <u>Attribute standards</u> = *characteristics* of internal audit activities * <u>Performance standards</u> =*quality* of IA activities

-Corporate *IA Charter* to formally define purpose & responsibility of IA, including adherence to Int'l *Code of Ethics*
-*Organizational* Independence & Objectivity by IA Dept. * no influence from Mgmt. or ability to so
-Disclose Impairment * IA Individuals => unbiased attitude & avoid conflicts of interest * Cooling-off period if prior worker
-Chief Audit Executive => prioritize audits *by risk* * monitor Mgmt's use of audit results

External Auditors – *major* governance monitoring device
* *Large* Corporations (accelerated filers) -> SOX requires that Auditors also *attest to Mgmt's IC Report* (<u>not req'd if Small</u>)
* Disclosures to AudCom: *Significant Findings* (auditor's views, difficulties encountered, disagreements, non-corrections)
* Material *corrected* MS; significant issues discussed with Mgmt. ; Mgmt. consulting other accountants; Sig. Defi. & MW

Analysts & Investment Banks – both function as External Monitoring Devices
-Banks/Underwriters need Due Diligence *before* getting involved with a new IPO/company
-Analysts use *multiple sources* of info for recommendations ** Conflicts of Interest *Risks* * SEC rules to mitigate conflicts

Creditors – External Monitoring => regularly *check* Corp's financial condition & compliance with debt terms
* *Risk*: reliance on Mgmt-supplied information ***but*** mitigated by use of External Auditors

Ratings Agencies – External – ***Bonds*** mostly * *Slow process* of Downgrading * Conflicts of Interest & Transparency

Corp Counsel/Attorneys – External – review Securities filings & legal compliance/violations (which Corp may disclose)

SEC – protect Investors * maintain efficient markets * facilitate capital formation * 5 commissioners appointed by President
* *Corporate Finance* division = reviews corporate *filings* for compliance with disclosure rules (and *quality* of disclosures)
* *Enforcement* division = recommends which cases investigate, take to court, and whether to prosecute via SEC
* *Chief Accountant* = advises SEC on accounting & auditing; *approves PCAOB proposals * oversees GAAP development

SOX – makes prosecuting Securities Fraud much easier

IRS – External device – due to requirements of *accounting (book)* information included on tax returns

Threat **of Corporate Takeovers** – supposedly *should* deter Mgmt. from being lazy/inefficient, otherwise a buyer will
*** Poison Pill** => *option* for owners to buy *at a discount* (prevents from buying a controlling interest)

Shareholders – also vote on *whether* to Dissolve Corp * *fundamental* changes * only one class of *voting stock* possible
* *Cumulative Voting Rights* – allows owners to vote *all* shares at once instead of dividing between choices
* *Books Inspection right* – need good faith & valid purpose to request
* *Derivative Suits* – sue on *behalf* on Corp because Mgmt. won't do so * any proceeds go to company (*not* stockholders)

Internal Control Framework – *process* to provide *reasonable assurance* of achieving *objectives* of Reliable Fin. Reporting
* Effective & Efficient *Operations* * Legal & Regulatory *Compliance*

1. Control Environment – "tone" of an organization that creates the foundation for internal control (*or lack of*)
-**Integrity & Ethical Values** => set by Mgmt. & *communicated* (conducts codes, official policies)
-**Commitment to Competence** => ensuring personnel have adequate skills, training, knowledge to perform duties correctly
-**Directors (and AudCom)** => IC improved when Board *structure* is effective & also competent/independent
-**Mgmt's Philosophy & Operating style** => *how* Mgmt. *runs* the company influences the Env. & informs employee behaviors
-**Org.** ***Structure*** => effective design *and* implementation necessary for planning, directing, and controlling operations
-***Communicating*** **Assignment of Authority & Responsibility** => charts/manuals; so personnel know their functions & *limits*
-**HR Policies & Procedures** => ensure excellent personnel via hiring, training, evaluation, promotions, and compensation

2. Risk Assessment by Mgmt – *process* of Identifying, Analyzing, and Responding to Risks
(1) Internal Risk Factors = changes in personnel * new information/accounting systems * new products * etc.
(2) External Risks = economic conditions * competition * industry technological changes

3. Control Activities – helps tackle IC risks & determining if Management's orders are carried out
-Physical Controls - Segregation of Duties
-Performance Reviews => check *Actual results* **vs.** Budgets, Forecasts, Prior Period, etc.
-Information Processing controls => checks on Accuracy and Completeness of data + proper Authorization of transactions
* General Controls: *widespread* areas like Data Center ops., System software maintenance, Access Security, etc.
* Application Controls: for *specific* areas, like Payroll, Sales Orders, etc.
(1) *Input Controls* (incl. authorization) (2) *Processing Controls* (accuracy) (3) *Output* (distribution/accuracy)

4. Information & Communication – capture, process, summarize, and report relevant information *accurately & timely*
* Identify & record *all valid* transactions * Describe transactions on a timely basis * properly measure *values*
* record in proper time period * properly present & disclose transactions * communicate responsibilities

5. Monitoring (**of controls**) – assesses the *quality* of Internal Control *Performance* over time* *Ongoing* **or** *Separate Evals*
-*Ongoing* = *regular* Supervisory & Mgmt. Activities, like monitoring of customer complaints, reasonableness tests
-*Separate Evaluations* = non-routine; e.g. periodic internal audits
!* *ongoing* generally more effective => can quickly detect & correct deficiencies

Evaluators = Individuals that *monitor* controls * should be *Competent* to evaluate & *Objective* to detect all deficiencies

Reasons for Control System Failures - improperly designed/implemented
-proper design/implement BUT *Environment* changes have made Controls *ineffective* -**OR-** change in *Operation* of controls

Baseline Understanding of Controls' Effectiveness => *starting point* for monitoring * helps in designing such procedures
1) Control Baseline = starting point of an *existing* internal control system *that has been understood*
2) Change Identification = i.e. specific control changes needed *due to* changes in Operating Environment
3) Change Management = establish a *new* baseline *after* Evaluating any change in control design/implementation
-must fully study & evaluate any changes to properly understand & for establishing a new baseline
-*thoroughly test* changes *before* implementation, because *many other* areas are affected & employees need *re-training*
4) Control Updates (Re-Validation) = periodic check-ups on *operations of controls* when no *known* changes have occurred

-*Other* methods of discovering changes in controls & environment *besides* monitoring (e.g. risk evals, complaints, etc.)
-*Enhanced* Monitoring by *supplementing* with results from *IC Risk Assessments*, especially *Key Controls*
-***Key Controls*** are *essential* to IC objectives & potentially *material*

Direct Evidence – obtained from *Observing* and *Re-performing* controls
Indirect Evidence – anything that *indicates* Control changes or failures (e.g. operating measures, risk indicators, etc.)

Limits of Control – Human Failure, Errors, and Judgment * Collusion * Management Override * Cost Constraints

Additional Specific Controls
* Inventory Standard Cost systems * Payrolls segregations: Time-keeping, Preparation, Personnel (HR), Check Distr.
* Payroll reconcile Job Time Tickets to Clock Cards * Treasurer signs paychecks * *Unclaimed* stored by non-payroll
* PPE transactions via Capital Budgeting * Approvals for Asset Retirements * Periodic PPE inspections

Enterprise Risk Management – via COSO framework => Process designed to *Identify* potential Events (good *and* bad) that may affect entity **and** *Manage* Risk *to be within* appetite ***to provide*** *Reasonable assurance* of achieving Entity Objectives

* *Matches* Risk Appetite with organization's Strategy * Enhances Risk Response Decisions * Reduces Operational *Surprises*
* Also works for *Cross-enterprise* Risks * *Integrates* Risk Responses * Helps to *Seize Opportunities* * Improves Capital *Plans*

!* *Every member* affects ERM => Control Environment & *Risk Culture* essential => Internal Control *part of* ERM

ERM *Process* = Identify Risks -- Assess Risks -- Prioritize Risks -- Determine Responses -- Monitor Risk Responses

Types of Events – (1) *Negative Impacts* = Risks **(2) *Positive*** = Opportunities and/or may offset Negative impacts (i.e. risks)

<u>8 Components of ERM</u> – interrelated

1. Internal Environment – *foundational* Structure and "Tone" of company affecting Risks, Appetite, Ethics, etc.
-Board of Directors = oversee Mgmt's implementation of ERM & check on effectiveness
-Management *sets the Tone* affecting lower workers: e.g. focus on short-term with incentives might result in bad behavior
-Org. Structure, Assignments of Responsibility & Authority, effective HR, *Quality* of Personnel, etc.

-*Risk Appetite* = amount of risk company is *willing to accept to achieve its goals* => *result* of entity's Culture & Strategies

-**Risk Tolerance** = acceptable variation from defined objectives/goals (e.g. Goal: 55% Mkt. Share; but 51% also OK)

2. Objective Setting – need to know company objectives *before* identifying events that might affect their achievement
-> process by which Mgmt. sets *specific* goals *consistent* with the company's *mission, overall strategy,* & *risk appetite*

- 3 types of objectives -- <u>*Operational*</u> – <u>*Reporting*</u> (internal & external) -- <u>*Compliance*</u> (legal)

3. Event Identification – potential to *affect* Strategy implementation ***or*** Objectives Achievement -- *Internal* **or** *External*
-*must respond* to Risks (negative impacts) -Opportunities: up to Mgmt. whether to ignore, integrate, seize, etc.

-External = economic, environmental, political, social, outside technological factors

-Internal = *own* infrastructure, personnel, processes, etc.

ID Methods -- Event "Inventories" (make a list) -- Internal Analysis (diy info) -- Escalation/Threshold Triggers (to investigate)
- "Facilitated" Workshops or Interviews (solicit info from personnel) -- Process Flow Analysis (weak links in ERM process)
- Leading Event Indicators (correlated predictors) -- Analyses on data from *prior* Events resulting in *losses*

4. Risk Assessment: consider *Likelihood* -- *Impact* -- Inherent Risk -- *Residual* Risk (if event could still occur *after response*)
- Qualitative & Quantitative => Probability & *Non*-probability Models to *quantify* risk
- Non-probabilistic Models = use assumptions to estimate *impact* of events *without likelihood* factor
  * e.g. Stress Tests, Scenario Analyses, and Sensitivity Measures

Black Swan Analysis = post-occurrence evaluation of Negative Impact Events that were Unanticipated or seen as Unlikely

5. Risk Responses – should be *consistent* with entity's risk appetite **&** within Cost-Benefits
-Avoidance = stopping/exiting the activity that creates an identified risk
-Reduction = minimize a specific Risk's *Likelihood*, *Impact, **or** both* at same time (e.g. add extra controls; *manage* the risk)
-Sharing *or* Transferring risk = insurance, hedging, outsourcing
-Acceptance = Retention = do nothing because consistent with risk appetite

6. Control Activities – policies & procedures to ensure that Risk Responses are *carried out effectively*

7. Information & Communication – need *relevant* info for personnel to effectively carry out their ERM responsibilities
-> supports all of the above identification, analyses, decision-making, etc. -- without proper info, ERM would fail

8. Monitoring – *entire* ERM process, so that any *necessary* ERM modifications can be implemented
-> via Ongoing Mgmt. Activities -- Separate Evaluations by internal auditors

Limits of ERM – *Future Uncertainty* -- Only for Info on *Risks related to* Achieving Objectives (can't *assure* achievement)
- never Absolute Assurance ** same exact limits as Internal Control **

41 – Information Systems – process data & transactions to provide users with needed/desired information
-Even computerized Accounting systems still have *Manual portions* (so not *entirely* digital)

General IT Systems – Transaction Processing *and* Management Reporting
-Transaction Processing = *daily processing* of transactions (e.g. payroll, cash receipts & disbursements, etc.)

-Mgmt. Reporting = help with *decision-making*
- ***Mgmt. Information systems*** – for planning, organizing, and controlling an entity's *Operations*
- ***Decision-support systems –*** combine data & models to solve *non-structured* problems with user involvement
- ***Expert systems*** – apply *reasoning methods* to data in a specific, structured area to provide advice/recommendations
- ***Executive Information systems*** – specially designed to support the work of Executives