INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM

CA. CS. SIDHESHWAR BHALLA

PARTNER & LEADER, GOVERNANCE RISK RESILIENCE COMPLIANCE & SUSTAINABILITY
MAZARS IN INDIA

VICE PRESIDENT
THE INSTITUTE OF INTERNAL AUDITORS, INDIA

IMMEDIATE PAST PRESIDENT
THE INSTITUTE OF INTERNAL AUDITORS, INDIA (DELHI CHAPTER)

April 23, 2022

mazars

CORPORATE GOVERNANCE

CORPORATE GOVERNANCE

Corporate governance broadly refers to the ***mechanisms, processes*** by which corporations are controlled and directed.

The ***tone from top management*** is particularly important because it sets an example for all others in and around the organization!

A sound, ethical ***tone at the top*** permeates and inspires an organization. It must, however, be supported and enforced by ***checks and balances*** that, in times of temptation, would strengthen those inclined to stray!

Sidheshwar.Bhalla@Mazars.in

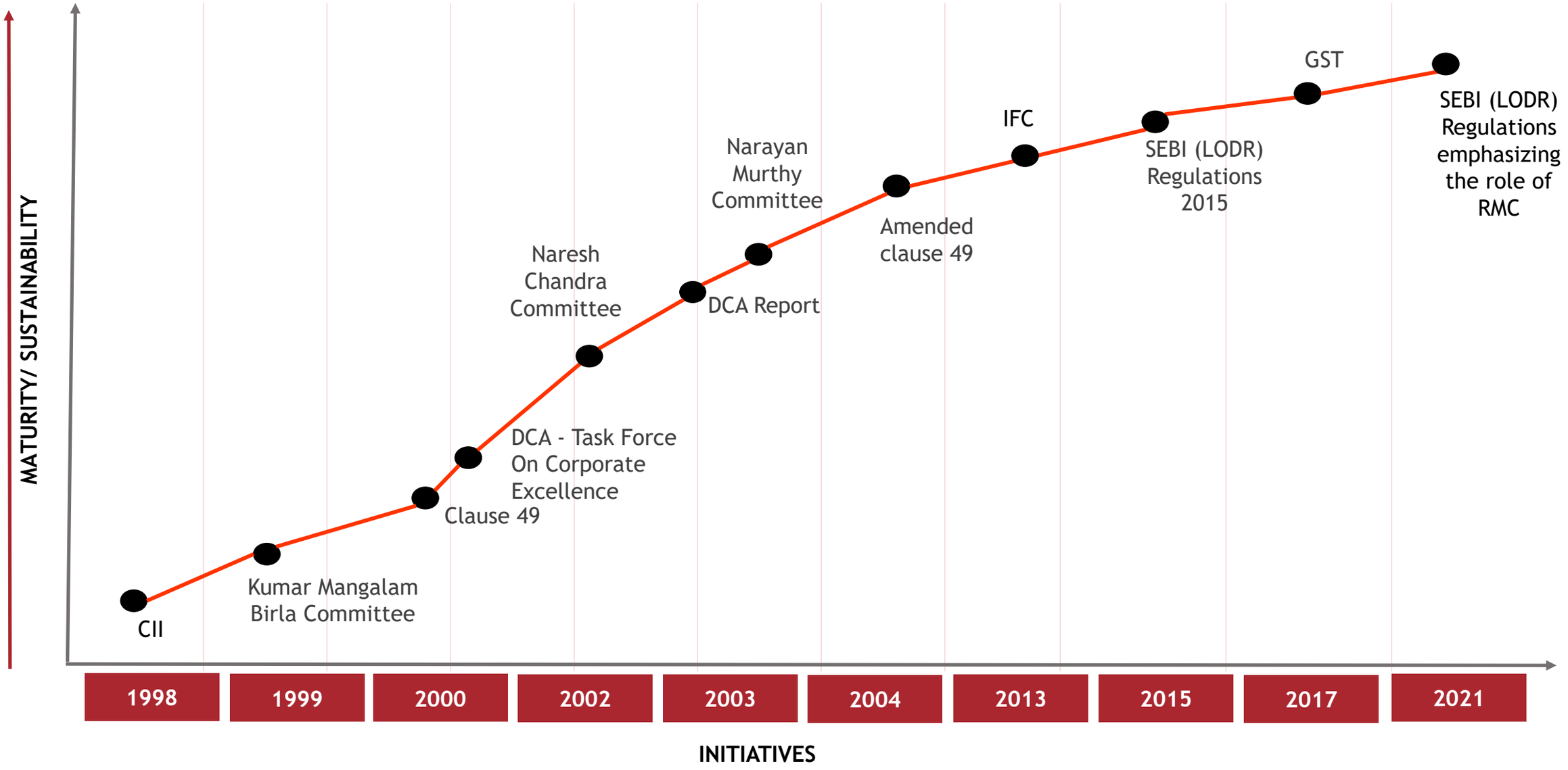
+91 98997 87786

CORNERSTONES OF CORPORATE GOVERNANCE

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

INDIA…ERA OF CORPORATE GOVERNANCE



Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

INTERNAL FINANCIAL CONTROLS

Companies Act, 2013

Directors responsibility statement

- Section 134(5)(e) - The directors, in the case of a **listed company**, had laid down **internal financial controls** to be followed by the company and that such internal financial controls are **adequate** and were **operating effectively**
- Section 134(5)(f) - The directors had devised proper systems to ensure **compliance with the provisions of all applicable laws** and that such systems were **adequate** and **operating effectively**
- Section 134(3)(q), sub-rule 8(5) - "In addition to the information and details specified in sub-rule (4), the report of the Board shall also contain: …"the details in respect of adequacy of **internal financial controls** with reference to the **financial statements**."
- Section 134(8) – contravention punishable with fine which shall not be less than Rs. 50,000 but which may extend to Rs. 2,500,000 and every officer of the company who is in default shall be punishable with imprisonment for a term which may extend to 3 years or with fine which shall not be less than Rs. 50,000 but which may extend to Rs. 500,000 or with both.

Explanation - For the purpose of this clause "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.

Internal financial controls reporting covers not just financial reporting aspects, but also the strategic and operational aspects of business and the efficiency with which those operations are carried out

Sidheshwar.Bhalla@Mazars.in # +91 98997 87786

INTERNAL FINANCIAL CONTROLS

Companies Act, 2013

Audit Committee

Section 177(4)(vii) - Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall inter alia, include ….., **evaluation of internal financial controls and risk management systems** ….

Section 177(5) - The Audit Committee may call for the comments of the auditors about internal control systems, the scope of audit, including the observations of the auditors and review of financial statement before their submission to the Board and may also discuss any related issues with the internal and statutory auditors and the management of the company.

Auditor's report

Section 143(3)(i) - Whether the company has **adequate internal financial controls system** in place and the **operating effectiveness** of such controls.

Whilst section 134(5) requires directors to state their responsibility on internal financial controls in case of listed companies, auditors are required to report on the adequacy and operating effectiveness of such controls in case of all companies.
Further, Rule 8(5)(viii) of the Companies (Accounts) Rules, 2014 requires the board report of all companies to state the details in respect of adequacy of internal financial controls with reference to the financial statements. IFC to be included as part of Directors Responsibility Statement from March 31, 2015 onwards and as part of Statutory Auditors Report from March 31, 2016 onwards

Sidheshwar.Bhalla@Mazars.in # +91 98997 87786

WHAT DOES THE LAW SAY?

mazars

Internal Financial Controls (IFC)

Internal Financial Controls (as per Companies Act of India)

Board of Directors (Section 134):

- Lay down adequate and effective IFCs and include it in Directors' Responsibility Statement
- Independent directors to satisfy themselves on the strength of financial controls.

Audit Committee (Section 177):

- Evaluate IFC systems
- Review Auditors' comments / observations with respect to controls before submission to the Board
- Discuss issues with Management or Internal / Statutory Auditors

Auditors (Section 143):

- Report on adequacy of IFCs system
- Report on operating effectiveness of such controls.

IFC to be included as part of Directors Responsibility Statement from March 31, 2015 onwards and as part of Statutory Auditors Report from March 31, 2016 onwards

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

INTERNAL FINANCIAL CONTROLS – WHAT TO DO?

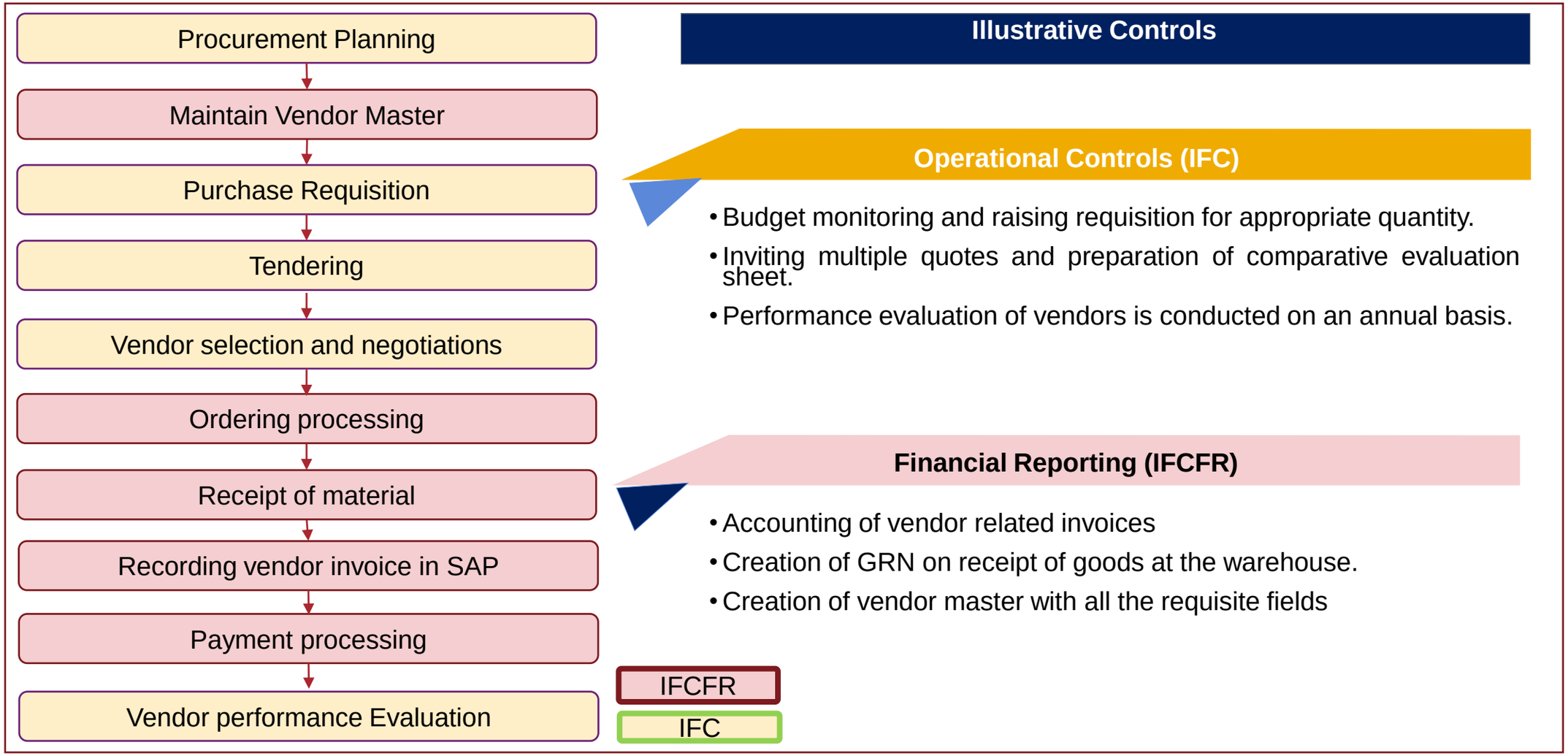
IFC Objective		IFC Requirements	What to do ?
Operations Objectives	Efficiency and effectiveness in Operations	• Defined **Policies and procedures** to ensure effective and efficient operations. • Effective **Delegation of Authority** and **Entity level controls**	• Define and ensure compliance to appropriate policies and procedures and Delegation of Authority • Define appropriate Entity level controls • Define and monitor operating effectiveness of appropriate controls over various activities. • Fraud Risk Management
	Prevention and detection of fraud and error	• Preventive controls to address **Fraud risk** • Mechanism for **timely detection** of fraud and errors	
	Safeguarding of assets	• Adequate control over **asset movement**, storage, loss or theft. • Risk identification and mitigation plan to reduce loss of asset	• Define appropriate asset movement controls • Effective asset verification program
Reporting Objectives	Accuracy and completeness of Accounting records	• Controls over **accurate and timely** update of accounting records • Control over **completeness** of accounting records	Defined effective controls and ensure operating effectiveness (ELC, PLC, ITGC and Fraud Risk)
	Reliability of Financial reporting	• **Timely** preparation of financial reports • Adequate **controls over preparation** of financial reports	• Defined appropriate controls over preparation of financial reports • Adequate review mechanism
Compliance Objectives	Compliance with applicable laws and regulations	• Adequate **framework** to ensure compliance to applicable laws and regulations • Adequate framework to **monitor** the compliance	Legal Compliance Framework

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

ILLUSTRATIVE COVERAGE IN IFCFR AND IFC

Illustrative comparison of activities covered in IFCFR framework and IFC framework for Procure to Pay process



Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

SEBI LISTING REQUIREMENTS - AN OVERVIEW

mazars

Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.

*Applicable to all existing listed entities having a paid up **share capital more than Rs. 10 crores** or **net worth more than Rs. 25 crores** as on the last day of the previous financial year.*

Regulation 4(f)(ii)(7) **Board of Directors**	Ensuring the integrity of the listed entity's accounting and **financial reporting systems**, including the independent audit, and that appropriate systems of control are in place, in particular, **systems for risk management, financial and operational control**, and compliance with the law.
Regulation 18 **Audit Committee**	Role of the audit committee and the information to be reviewed by the audit committee shall be as specified in Part C of Schedule II including • **evaluation of internal financial controls and risk management systems**; • reviewing, with the management, performance of statutory and internal auditors, **adequacy of the internal control systems**
Part B: Compliance Certificate **[Regulation 17(8)]**	**Compliance Certificate by Chief Executive Officer and Chief Financial Officer** to state: Responsibility for **establishing and maintaining internal controls for financial reporting** and that they have evaluated the **effectiveness of internal control systems** pertaining to financial reporting

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

THE CHANGING REGULATORY LANDSCAPE

IFC	LODR
Basel II	Contract Risk
IS Governance	Sarbanes-Oxley
C-SOX	J-SOX
OH&S	GDPR
Ind AS	IFRS
ESG	Fraud risk
Directors' responsibilities	Tax risk

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

THE FOUR PILLARS OF COMPLIANCE

mazars

1

Policies & Procedures

- Corporate Polices, code of ethics and conduct, Delegation of Authority, POSH etc.
- Functional Standard Operating Procedures/ Manuals
- Internal Company notifications, circulars

2

Statutory & Regulatory

- Corporate and Commercial Laws: Companies Act, SEBI Laws, PML etc.
- Financial Laws: GST, Direct Tax, FDI etc.
- HR, Labour, EHS: PF, Minimum Wages, Foreign Labor, E-waste, etc.
- Data Privacy Laws (GDPR).

3

Financial Reporting

- Internal Control over Financial Reporting (SOX, J-SOX, Clause 49, IFC)
- Indian Accounting Standards
- Generally Accepted Accounting Principles (US GAAP)
- International Financial Reporting Standards

4

Contractual Terms

- Compliance with contractual obligations (Commercial/ Financial/ Regulatory)
- Compliance to Service Level Agreement (SLA)

Landscape

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

mazars

Guiding Principles & Oversight of Internal Control System

KEY DRIVERS OF FRAMEWORK IN THE INTERNAL CONTROL VALUE CHAIN

mazars

Internal Control Environment

1 Governance

- Enhancements for effective risk governance
- Finalize lines of defense and aspects to be covered under each line of defense (Now 3 lines model)
- Suggest improvements in the framework
- Compliance as per various regulations (Companies Act Rules 2013 and SEBI Listing agreement.)

2 Operations

- Evaluate the control activities for each process
- Identify control redundancies
- Identify areas of improvement from design perspective
- Identify automation opportunities.

3 Financial Reporting

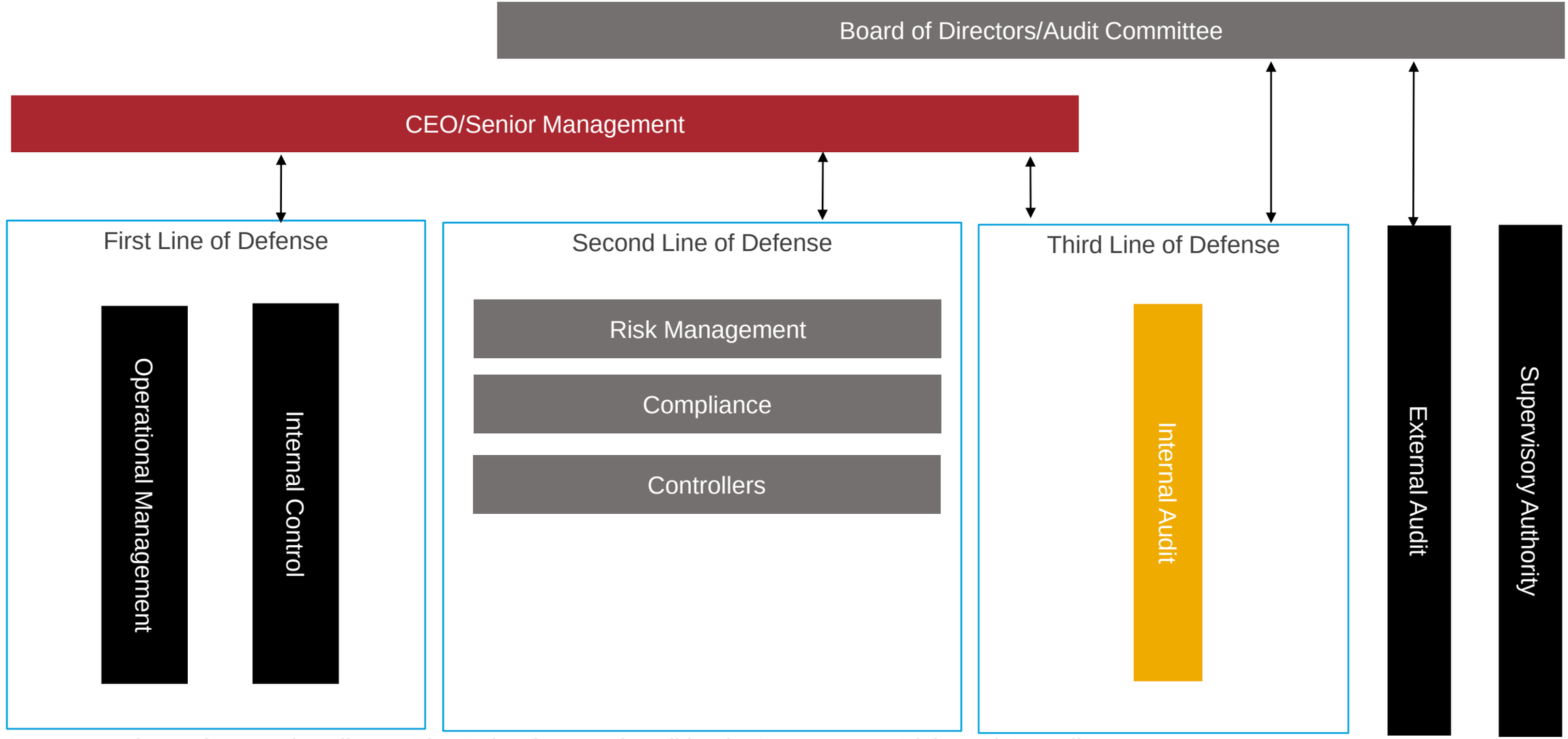
- Identify areas of improvement and reducing financial reporting risk
- Eliminate redundant controls
- Automate financial reporting related controls
- Segregation of Duty

Strengthening all lines within the value chain and ensure adequate and effective Entity Level Controls as well as Process Level Controls

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

THREE LINES OF DEFENSE

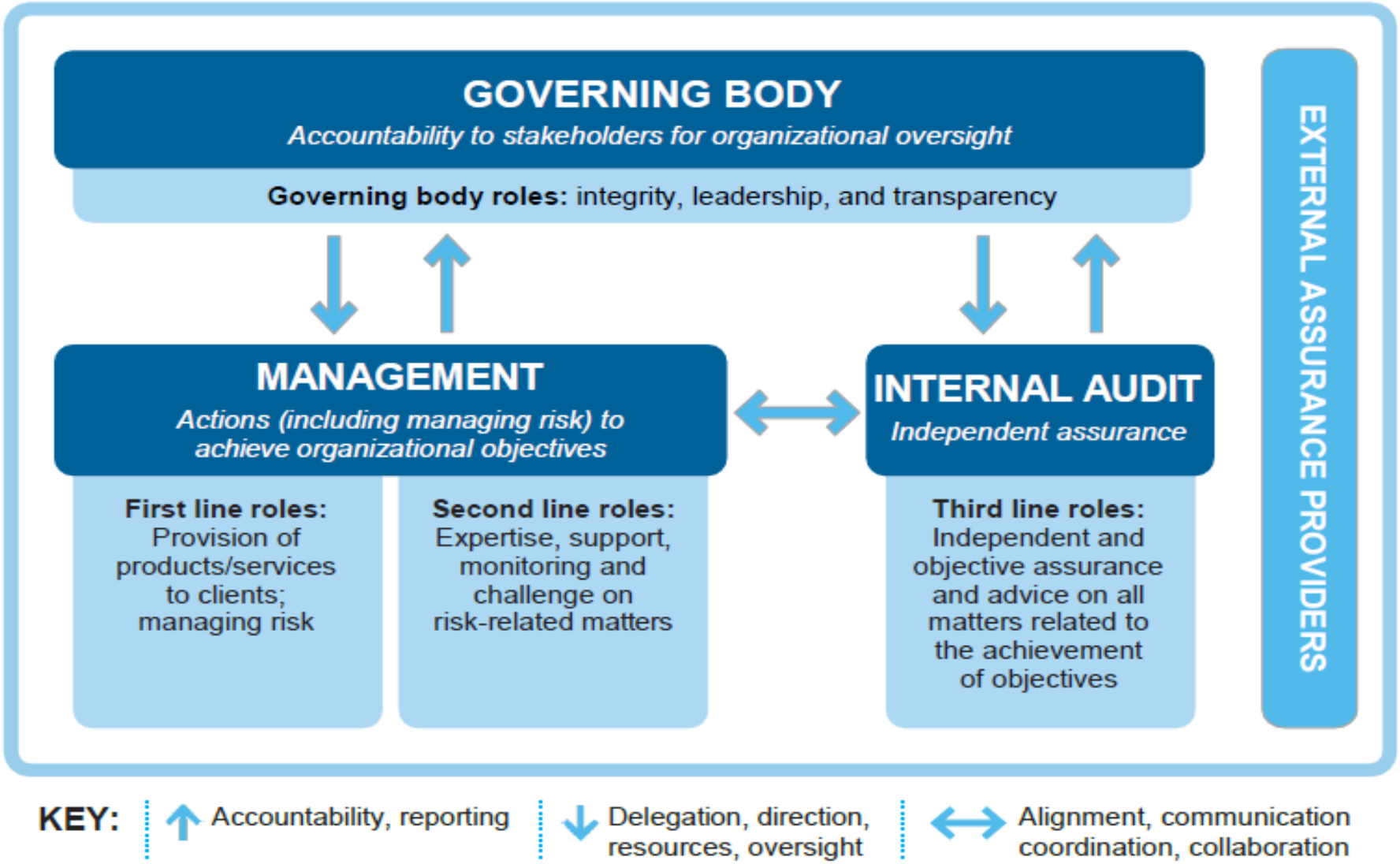


Source: Institute of Internal Auditors: The Role of Internal Auditing in Governance, Risk, and Compliance

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

THREE LINES OF MODEL



Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

UNDERSTANDING COSO

mazars

The Committee of Sponsoring Organisations of the Treadway Commission (**COSO)**

COSO is a joint initiative of five sponsoring organizations

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- Institute of Internal Auditors (IIA)

- Under COSO 2013 Internal Control Framework Update ("COSO 2013 Framework"), **17 "Principles of Control"** were established to provide clarity when designing and implementing effective systems of control

- These principles provide a **formal structure for the design and evaluation of the effectiveness of internal control** (i.e., considering whether each of the principles is present and functioning on the basis of the guidance provided for each principle)

- COSO 2013 Framework provides refreshed guidance within each of the components of internal control to reflect the significant changes to business and operating environments after the 1992 Framework was released (i.e. updated Framework focusses on **outsourced service providers** and **increased relevance of technology**)

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

COSO'S INTERNAL CONTROL FRAMEWORK PRINCIPLES

Components	Summarized Principles
Control Environment	1. Organization demonstrates commitment to integrity and ethical values 2. BOD exercise oversight over development of internal controls 3. Management establishes structure, authority and responsibility 4. Organization demonstrates commitment to competence 5. Individuals are accountable over internal control responsibilities
Risk Assessment	6. Organization specifies objectives with clarity to identify and assess risk 7. Organization identifies and analyzes risk for effective management 8. Organization considers potential for fraud in assessing risk 9. Identifies and analyzes significant change that impact internal control
Control Activities	10.Selects and develops control activities that mitigate risks 11.Selects and develops general controls over technology 12.Organization deploys control activities through policies and procedures
Information & Communication	13.Uses relevant and quality information to support internal control 14 & 15. Effective internal & external communication on matters affecting functioning of internal control
Monitoring	16.Conduct ongoing and/ or separate evaluations to ascertain functioning of internal controls 17.Organization evaluates and timely communicates of internal control deficiencies

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

SIGNIFICANT ENHANCEMENTS TO THE COSO 1992

mazars

Risk Assessment	Outsources Service Providers	Information Technology
More detailed discussions about risk assessment concepts, including those related to inherent risk, risk tolerance, how risks may be managed, and linkage between risk assessment and control activities. Considering the potential for fraud risk when assessing risks to the achievement of an organization's objectives	Considerations related to OSPs are included throughout the framework, including 12 out of 17 principles Requires management to specifically consider how OSP's are monitored	Considerations related to IT are included in 14 of 17 principles Discussion of using IT to assist in continuous monitoring Requirements for ensuring quality of information (data integrity)

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

ENTITY LEVEL CONTROLS

Business Risk Management	Whether risk management policy and procedures are in place? Whether formal risk assessment has been carried out or not?
Business Ethics Framework	Whether whistle-blower policy and Code of conduct exists and implemented ?
Internal Audit and Financial Integrity	Whether internal audit function is independently reporting to Audit Committee? Whether roles and responsibilities of senior management is defined and documented? And Whether adequate segregation of duties exists?
Legal Compliance Framework	Whether legal compliance framework is documented and compliance health to checked on periodic basis?
Fraud Risk Management	Whether Fraud Risk Management policy exists, detailing structure of fraud deterrence, prevention and investigation, fraud incidence response guidelines. Whether Key controls to mitigate fraud risks are identified and monitored for compliance on regular basis.
Business and Operations Continuity	Whether Disaster Recovery Plan, Business continuity plan and crisis management policy defined and implemented?
Succession Planning	Whether formal process of succession planning defined and implemented?
Management Operational Review	Whether formal process management oversight and review mechanism exist and followed?

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

PROCESS LEVEL CONTROLS

PLC Component	Requirement
Design Effectiveness	**Significant policy and procedures are defined.** Process of assessing adequacy and appropriateness of policies and process to be developed
	Completeness of Risk and Controls Matrix (RCM) documented for all business cycles to be assessed. RCM's to include following: ▪ Review and update RCMs for all financial assertions. ▪ Controls description to be elaborated ▪ Fraud Risk to be highlighted ▪ Whether Policy/ Procedure exists or not to be documented ▪ Control Category specifying COSO control level ▪ Control Owner and responsibility for testing and reporting
Operating Effectiveness	**Policy of control testing and operating effectiveness**, containing the sampling criteria and strategy to be defined
	Standard documentation to be maintained in the forms of **test scripts** and support documents to evidence the operating effectiveness of the identified controls

Sidheshwar.Bhalla@Mazars.in # +91 98997 87786

IT CONTROL CONSIDERATIONS

The two broad groupings of Information System Control activities:

General Controls, which apply to all information systems and support secure and continuous operation. Examples of General Controls include:

- Application Systems Implementation and Maintenance
- Logical (Platform, Network and Database) and Physical Security

Application Controls, which apply to the business processes they support, and are designed within the application to prevent/ detect unauthorized transactions. When combined with manual controls, as necessary, application controls ensure completeness, accuracy, authorization and validity of processing transactions.

Application controls will be identified and tested at the business process level by the Operating Companies. Adequate General Controls increase the assurance that the Application Controls will continue to operate as intended.

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

ILLUSTRATIVE FRAMEWORK – INTERNAL CONTROLS

Risk Universe		
Business Cycle	Count	
	Total	Fraud
Record To Report (R2R)	24	12
Hire To Retire (H2R)	47	13
Procure to Pay (P2P)	19	6
Order To Cash (OTC)	18	9
Plan To Produce (P2P)	20	5
ITGC	112	40

Control mitigating fraud risk			
Count			
Preventive	Detective	Manual	Automated
20	3	18	5
12	8	20	-
7	1	6	2
25	5	30	-
15	6	21	-
39	1	24	16

Control Universe							
Business Cycle	Count						
	Total	Preventive	Detective	Manual	Automated	Key	Non - Key
Record To Report (R2R)	37	33	4	32	5	16	21
Hire To Retire (H2R)	63	39	24	59	4	22	41
Procure to Pay (P2P)	28	25	3	23	5	14	14
Order To Cash (OTC)	35	30	5	35	-	18	17
Plan To Produce (P2P)	35	27	8	33	2	13	22
ITGC	112	108	4	80	32	26	86
Total	**310**	**262**	**48**	**262**	**48**	**109**	**201**

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

KEY CONTROL (ILLUSTRATIVE DEFINITION)

mazars

1. **Key Control:**
    a. A key control is one that is required to provide reasonable assurance that fraud and material errors will be prevented or timely detected.
    b. It is the major control that covers a risk of material misstatement. If it fails, it is highly improbable that other control could detect the control absence.
    c. It is a control that covers more than one risk or support a whole process execution.
    d. It is usually part of entity-level controls (e.g. delegation of authority, segregation of duties, regulatory compliances etc.) or high-level analytic controls (inventory valuation, impairment assessment, debtor provisioning or write-offs etc.).
2. **Non Key Controls:** Controls other than key controls

Sidheshwar.Bhalla@Mazars.in # +91 98997 87786

mazars

Risk Management

RISK MANAGEMENT DEFINED

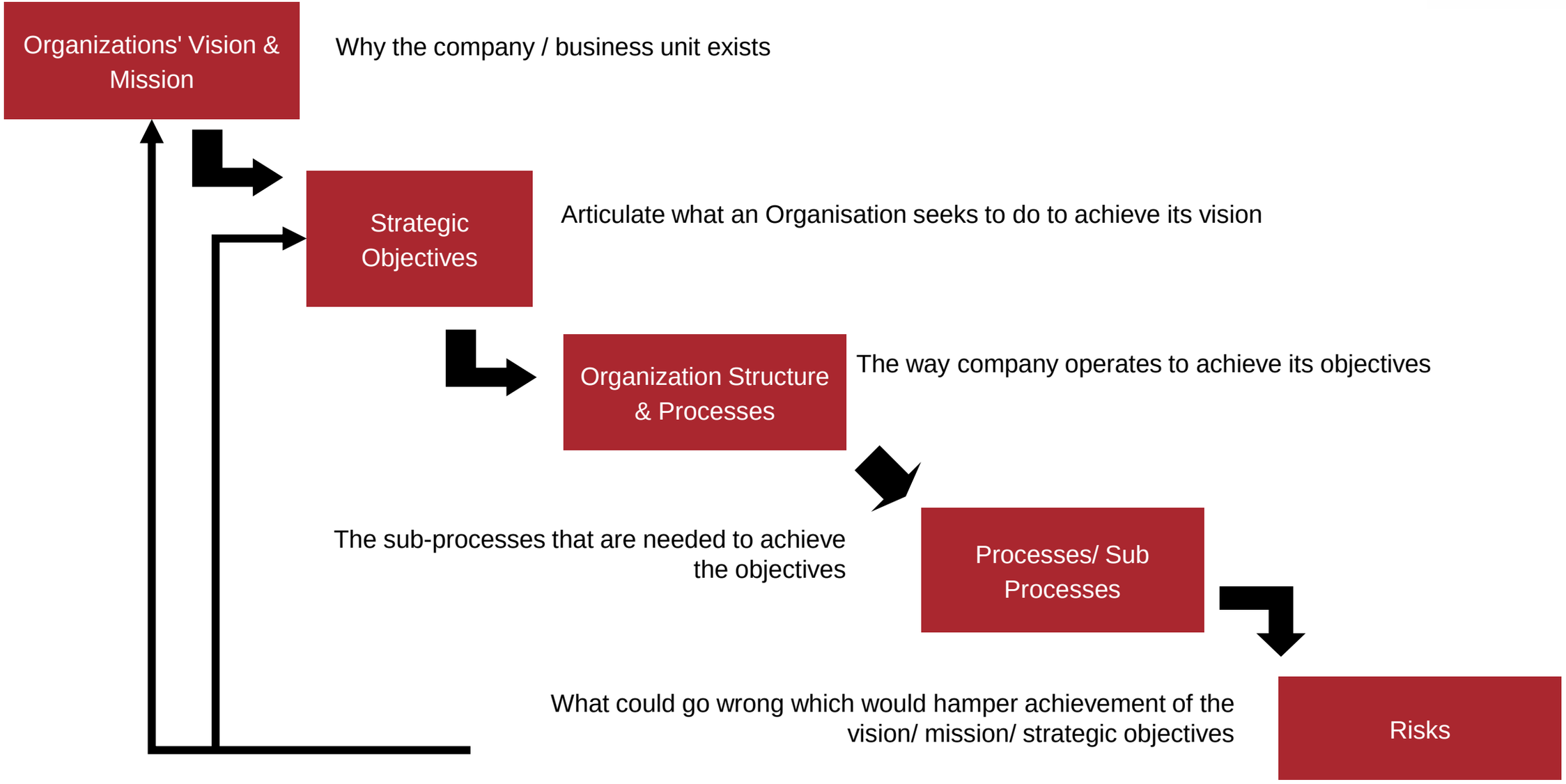
A structured, consistent and continuous process for identification and assessment of risks, undertaking control assessment and continuous monitoring of exposure of the risk

Risk Management is critical to value creation, offering shareholders improved stability and predictability

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

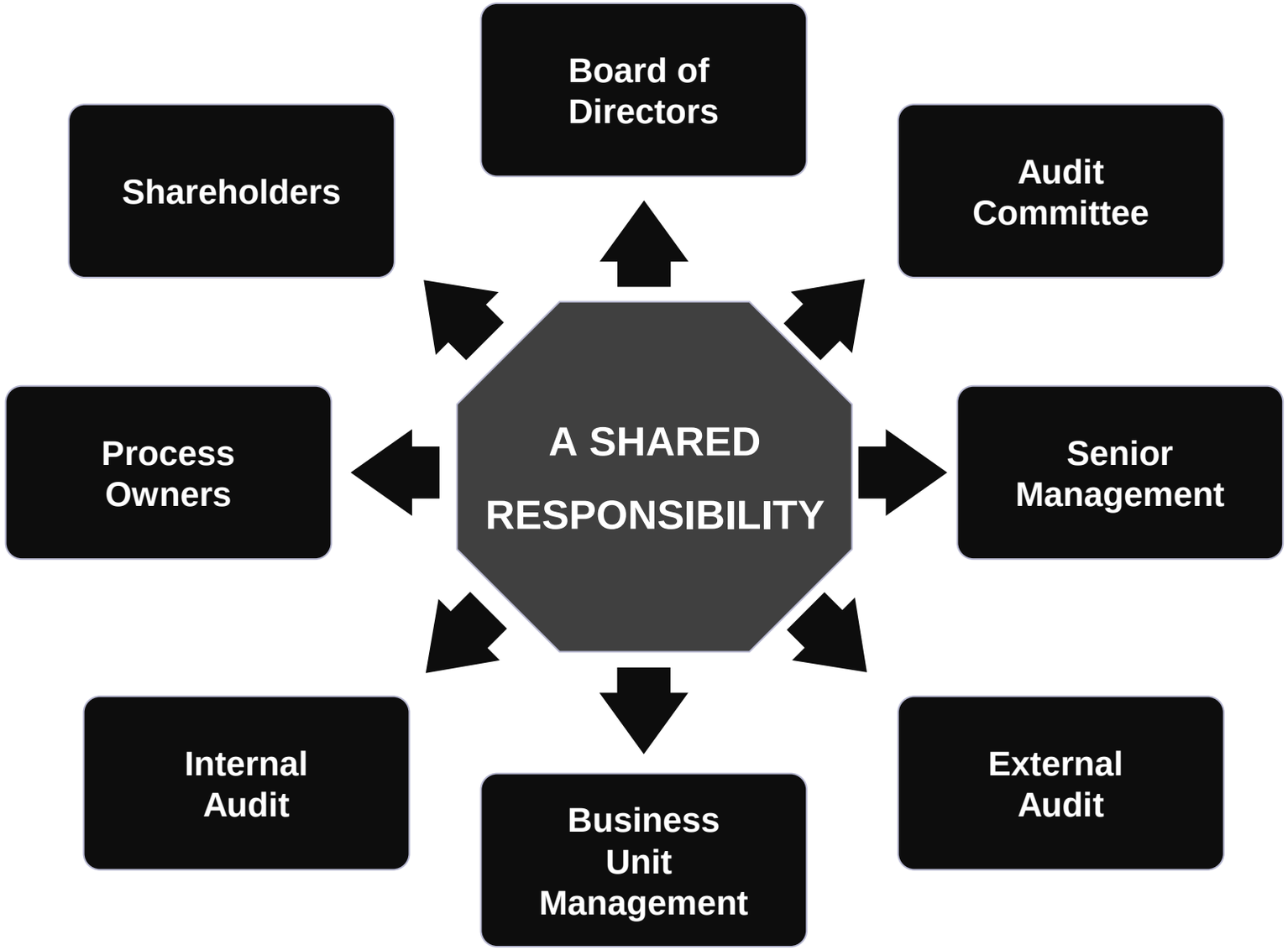
RISK MANAGEMENT – AN OVERVIEW



Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

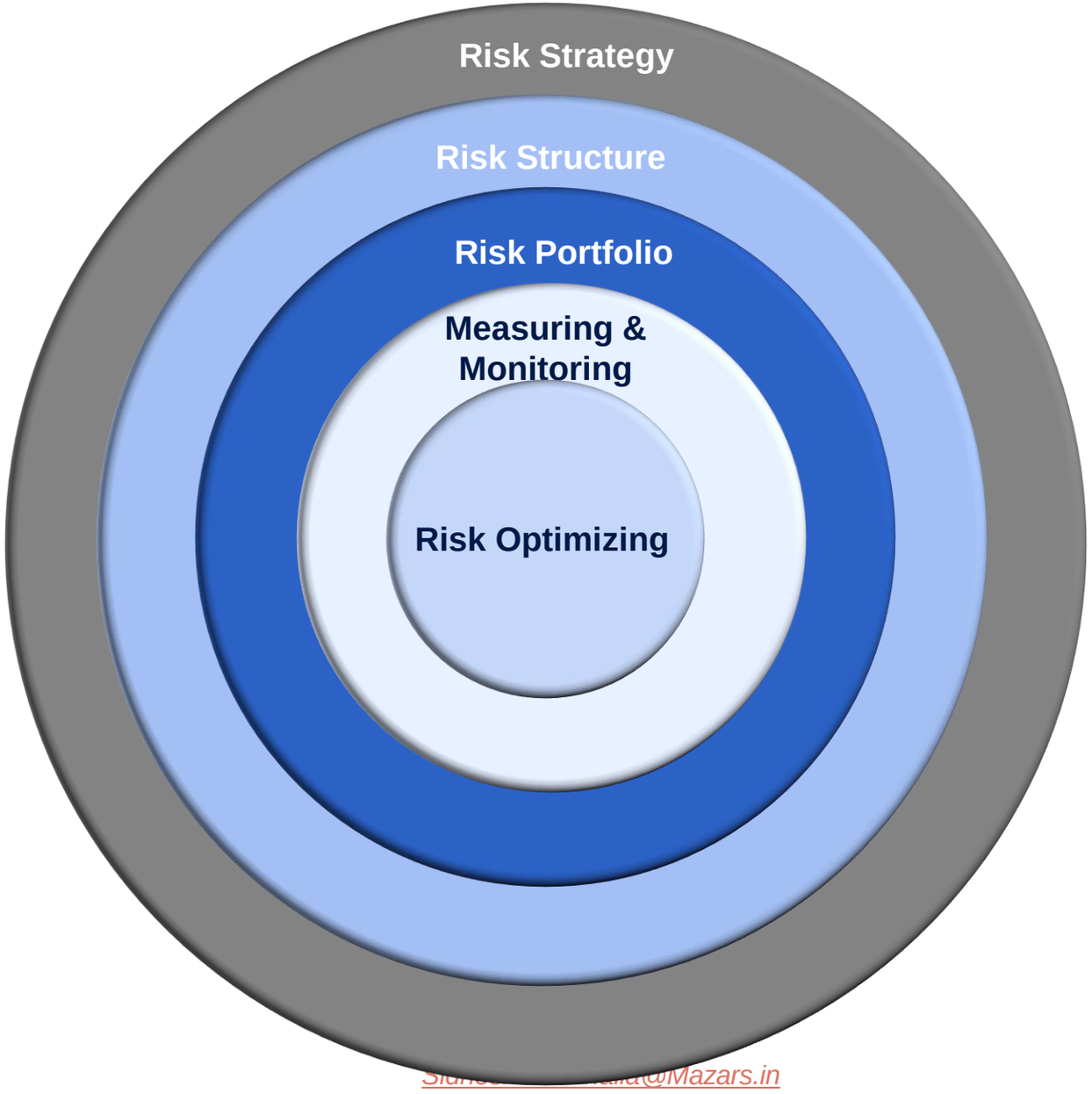
WHO IS RESPONSIBLE FOR RISK MANAGEMENT



Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

RISK MANAGEMENT FRAMEWORK COMPRISES OF...



Use risk and control information to improve performance

Sidhes[illegible]ala@Mazars.in

+91 98997 87786

RISK MEASUREMENT – ILLUSTRATIVE RISK APPETITE CARD (IMPACT)

mazars

Impact Description	Impact Parameter	Impact Rating				
		5 Very High	4 High	3 Medium	2 Low	1 Insignificant
Financial Impact	Absolute impact on revenue	> INR 10 crores	INR 5 - 10 crores	INR 1 - 5 crores	INR 50 lacs - 1 crores	< INR 50 lacs
	Cost Increase	> INR 5 crores	INR 2 – 5 crores	INR 2 crores - 50 lakh	INR 50 – 25 lakh	< INR 25 lakh
	%age of average Profit of past 3 years	> 10% of NIBT	5% - 10% of NIBT	3% - 5% of NIBT	1% - 3% of NIBT	< 1% of NIBT
Business continuity	Criticality of data / designs / knowledge lost	Complete inability to deliver services for more than 15 days	Inability to deliver key services for 7 – 15 days.	-	-	-
	Unavailability of critical infrastructure, staff, utilities and/or IT services/funds	Widespread inability to deliver services.	Inability to deliver key services for up to 4 days. Consequent major disruption to services over multiple periods.	Unavailability between 1 & 3 days	Unavailability for less than 1 day	Inability to deliver non critical services during non-critical times of the year.
	Disruption of Business	Disruptions of more than 7 days	Disruption between 4 to 7 days	Disruption between 1 to 3 days	-	-
Loss of Talent	Attrition Rate	>9%	8% - 9%	6% - 8%	4% - 6%	<4%
	Separation of KMP and employees	Separation of key individuals at senior management level	Separation of skilled personnel effecting operations for long run	Separation of skilled personnel effecting operations for short term	Impacts operations but gaps can be filled with existing employees	Separation not impacting operations

Sidheshwar.Bhalla@Mazars.in # +91 98997 87786

RISK MEASUREMENT – ILLUSTRATIVE RISK APPETITE CARD (IMPACT)

mazars

Impact Description	Impact Parameter	Impact Rating				
		5 Very High	4 High	3 Medium	2 Low	1 Insignificant
Reputation	Brand Reputation	• Negative information impacting product & brand is continuously & widely published on international public media (print media, audio visual or social media) • Prolonged or wide-spread exposure or employee reaction • Global Government/ NGO involvement • Company's brand is legally used to release sensitive and political information that impacts the company's decision	• Negative information impacting product & brand is widely published on prestigious national public media (print media, audio visual or social media) • Strong or lengthy public exposure or employee reaction • Regional Government/ NGO involvement • Potential unauthorized use of company's brand and image for unlawful civil purpose	• Negative information impacting product & brand published on regional public media (newspaper or radio) • Considerable public exposure or employee reaction • Local or regional Government/ NGO involvement	• Negative information impacting product and branding is circulated on local media • Some or limited public exposure or employee reaction • Local or regional government/NGO/media involvement	• Negligible negative information company's brand and product • Isolated public (e.g., customer or shareholder) exposure; • Minimal employee reaction • No NGO/ media involvement

Sidheshwar.Bhalla@Mazars.in # +91 98997 87786

RISK MEASUREMENT – ILLUSTRATIVE RISK APPETITE CARD (IMPACT)

mazars

Impact Description	Impact Parameter	Impact Rating				
		5 Very High	4 High	3 Medium	2 Low	1 Insignificant
Health, Safety & Environment	**Accidents**	• Fatality or >2 major injuries (regulated by Ministry of Health) requiring >07 days of medical treatment	• More than 2 major injuries (regulated by Ministry of Health) that requires 03-07 day medical treatment	• 1 major injury that requires < 03-07 days of medical treatment	• 1 injury that requires < 03 days of medical treatment	• Minor injury that requires first aid only & causes no work disruption
	Environmental damage	• Environmental damage requiring >INR 5 lacs to correct. • Incident has environmental impact that exceeds Company-wide level & the incident is discovered & publicly reported	• Environmental damage requiring INR 1 to 5 lacs to correct • Incident has environmental impact that affects the whole factory & the incident is discovered & publicly reported at national level	• Environmental damage requiring INR 50k to 1 lac to correct • The incident has environmental impact within local community	• Environmental damage requiring less than INR 50k to correct • Single incident has minimum environment impact on an area/cluster	• Incident is considered as an environment incident but has no impact on interior area

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

RISK MEASUREMENT – LIKELIHOOD (ILLUSTRATIVE)

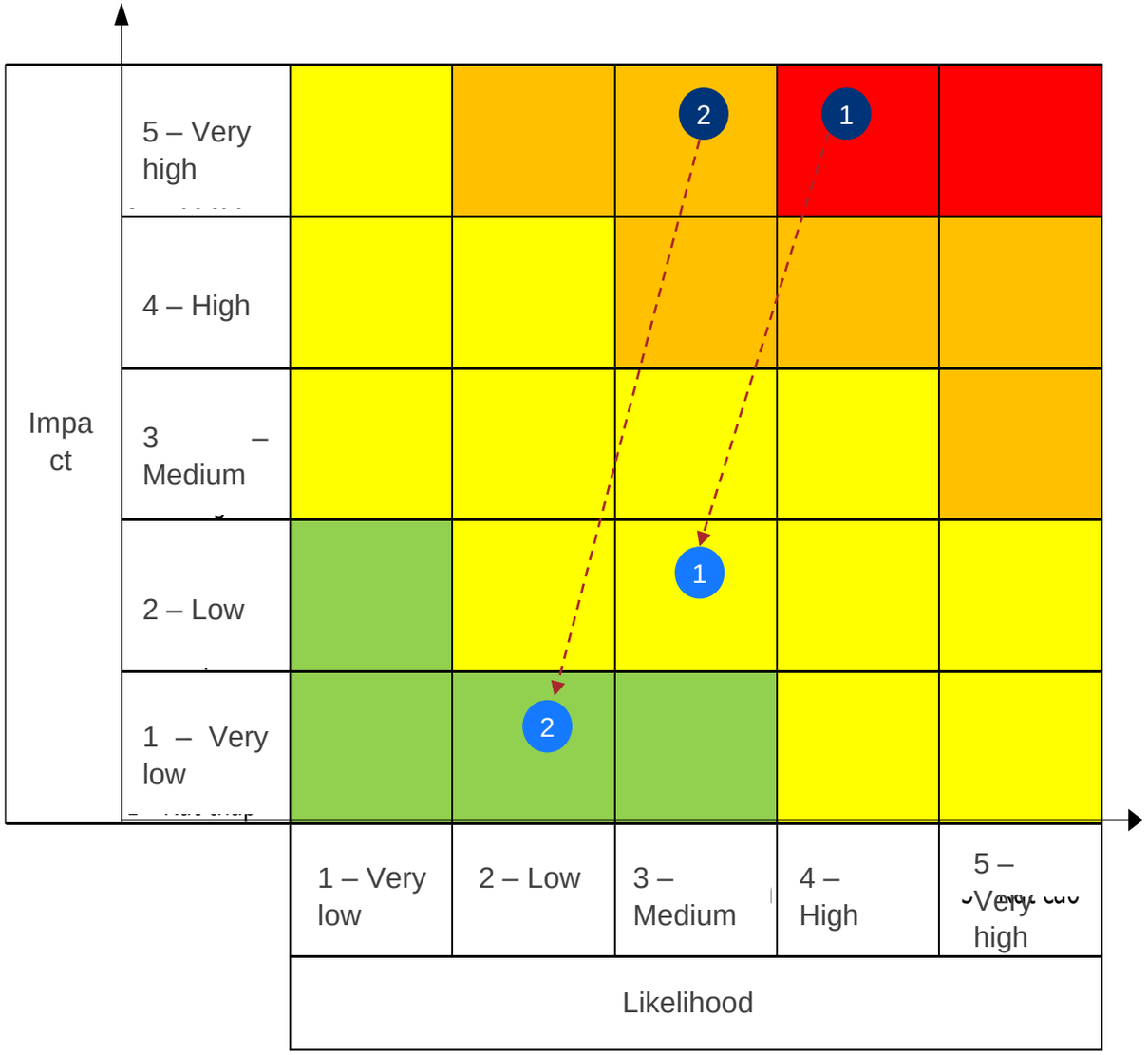
Scale	Criteria
5 – Very high	Probability of risk occurring is 90 - 100% or
	Risk exists
4 – High	Probability of risk occurring is 65 - 90% or
	Risk might occur weekly
3 – Medium	Probability of risk occurring is 35 – 65% or
	Risk might occur monthly
2 – Low	Probability of risk occurring is 10 – 30%
	Risk might occur once every year
1 – Very low	Probability of risk occurring is 0 -10% or
	Risk might only occur on particular circumstances

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

RISK SCALE

USED TO MEASURE A SPECIFIC RISK EVENT AT COMPANY-LEVEL



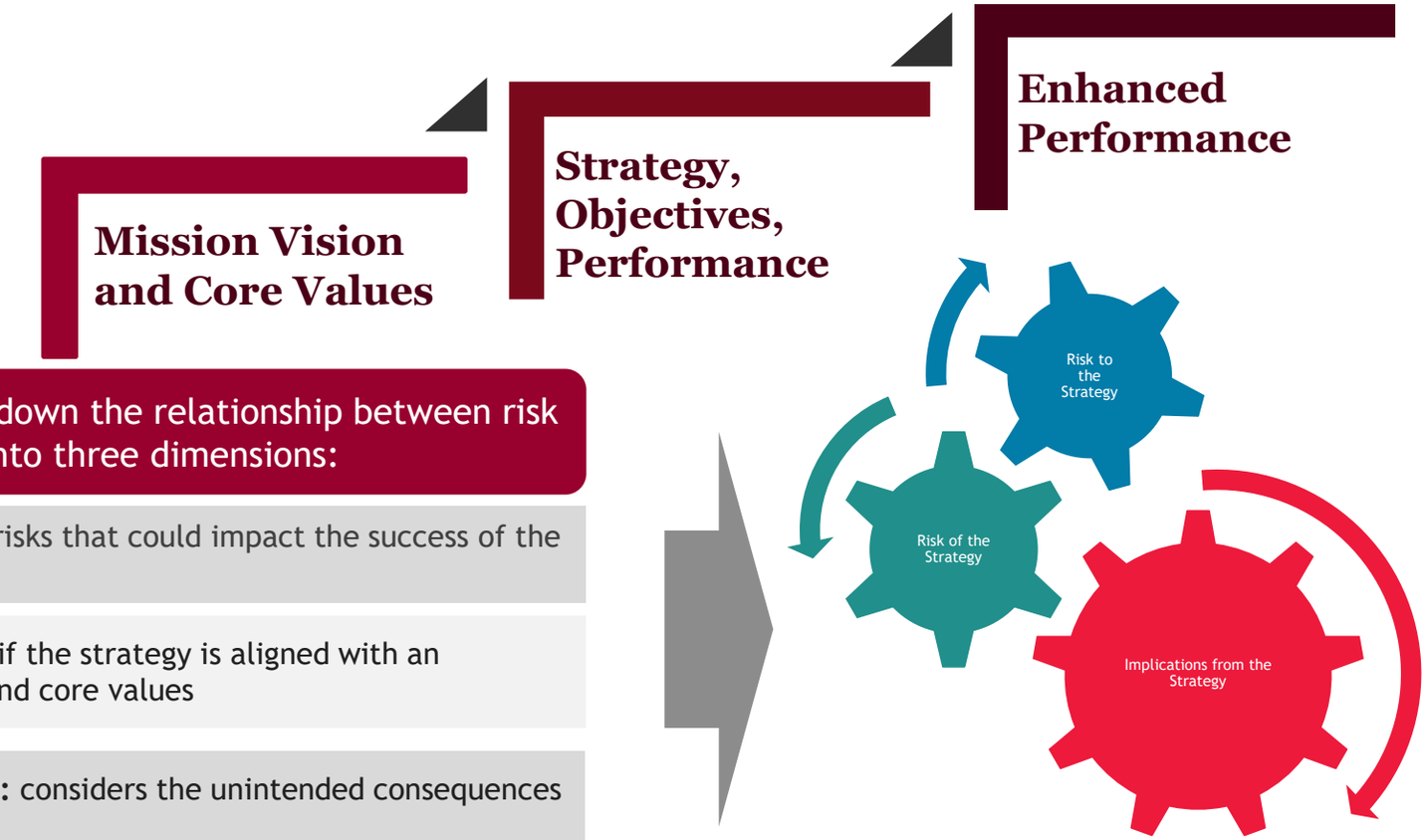
	VERY HIGH ▪ Required to immediately execute risk management action plans at related departments ▪ Escalate issues to Chairman and CEO for instruction
	HIGH ▪ Risk management action plans must be ready for execution and can be immediately executed in case risk occurs ▪ Escalate issue to CEO for instruction
	MEDIUM ▪ Add to watchlist ▪ Risk control/ response plans are executed and supervised by department head. 2nd line off defence functions strengthens their indirect supervisory roles
	LOW ▪ Pose no significant threat and is monitored by control in the process ▪ 1st line and 2nd line of defence functions consider adding self-assessment of control and risk at functions, and 2nd line's supervision over 1st line to action plan ▪ Add to watchlist

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

COSO 2017-ERM FRAMEWORK

The ERM framework emphasizes the importance of aligning business objectives and strategy with an organization's mission, vision, and core values. Organizations need to identify, assess, prioritize, and manage risks. Companies that can do this are better able to achieve business objectives, execute strategies and improve their performance.



The new framework breaks down the relationship between risk and strategy into three dimensions:

Risk to the strategy: considers risks that could impact the success of the selected strategy;

Risk of the strategy: evaluates if the strategy is aligned with an organization's mission, vision, and core values

Implications from the strategy: considers the unintended consequences of the selected strategy.

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

mazars

Why Frauds Happen?

FRAUD ~ SECTION 447 OF COMPANIES ACT 2013

Definition:

Fraud in relation to affairs of a company or any corporate body includes ***any act, omission, concealment of any fact or abuse of position*** committed by any person or any other person ***with the connivance*** in any manner, with ***intent to deceive***, to ***gain undue advantage*** from, or to ***injure the interests*** of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

Role of Audit Committee:

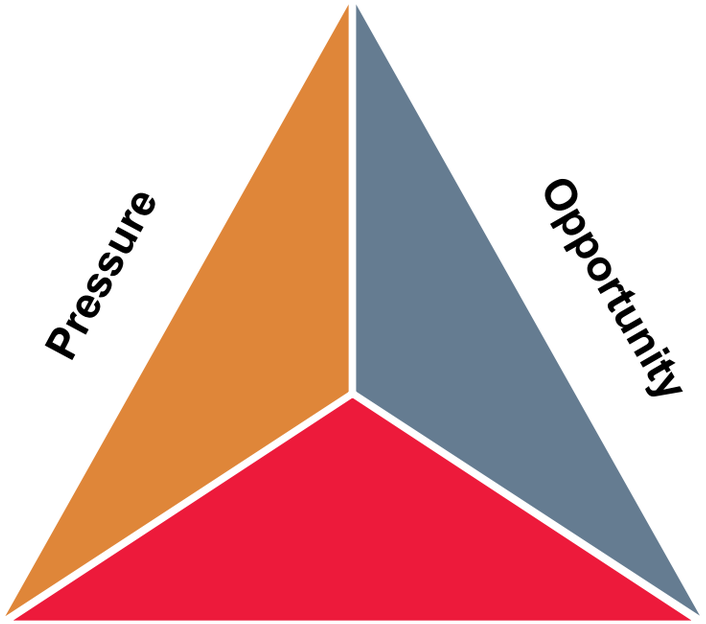
Audit committee is required to monitor that every listed company shall ***establish a vigil mechanism*** for directors and employees to report genuine concerns. It shall make provision for ***direct access to the Audit Committee Chair*** in appropriate cases.

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

CRESSEY'S FRAUD TRIANGLE – WHY FRAUDS HAPPEN?

- "Results, results, results!"
- Credit crunch
- Revenge
- Addiction – drink, drugs, gambling
- Coercion or blackmail
- Illness
- Debts
- Family pressure
- "I need the money"



- Poor governance
- Poor controls
- Exploiting errors
- Inadequate segregation of duties
- Abuse of authority
- Lack of effective oversight
- Complex transactions

Rationalization

- "They do not pay me enough"
- "Rules are meant to be broken"
- "Who cares?"
- "Its only a small amount"
- "It's a victimless crime"
- "It is a cost of doing business"
- "I'll never get caught"
- "They can afford it"
- "I am in charge"
- "Everyone else does it"

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

mazars

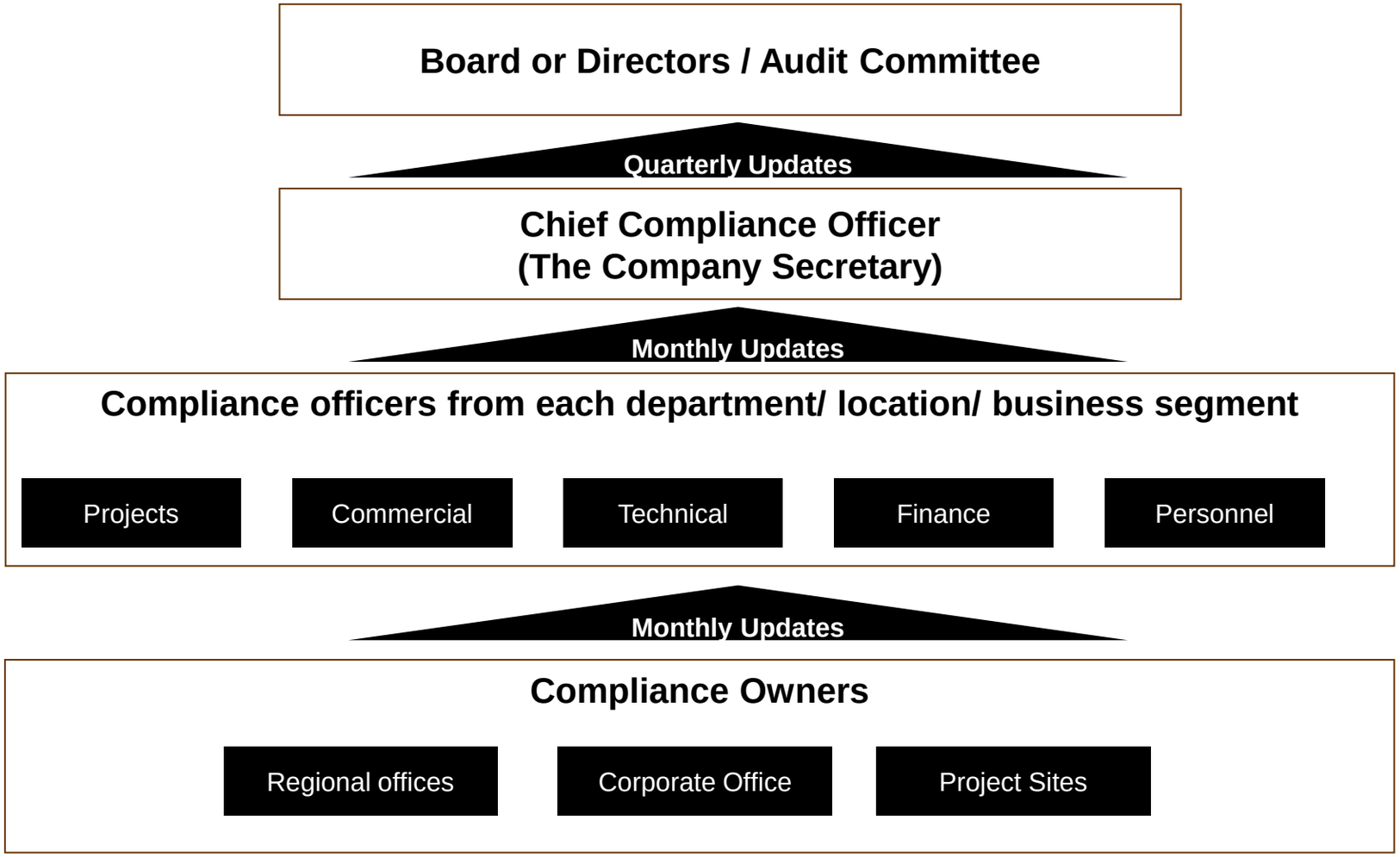
Legal and Regulatory Compliance

LEGAL COMPLIANCE STRUCTURE

Typical Legal Compliance Structure

•The Legal compliance structure should be supported by a legal compliance database maintained by a database administrator.

•The database should provide periodic alerts and should be used to input compliance information.

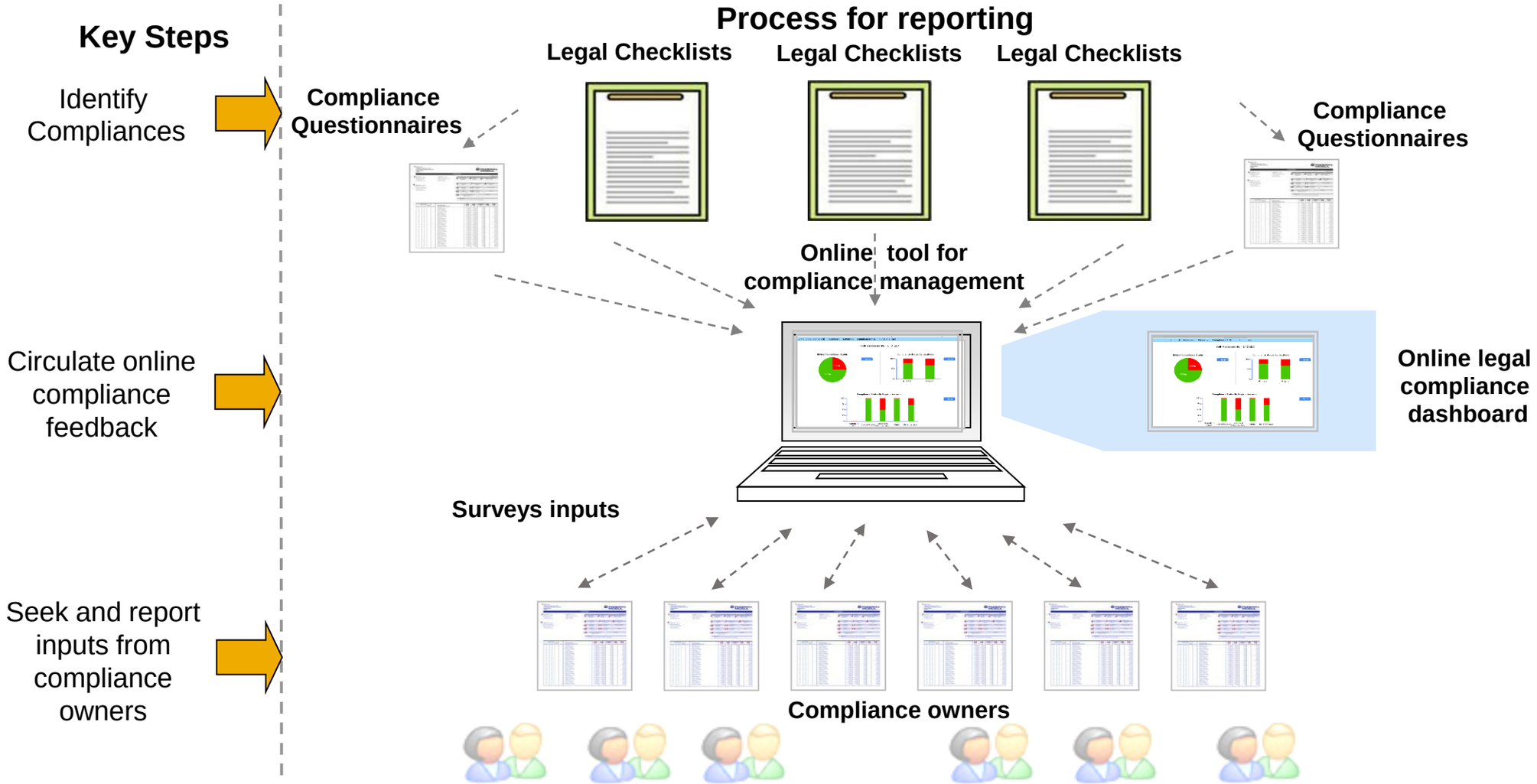


Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

ONLINE LEGAL COMPLIANCE REPORTING – THE FRAMEWORK

mazars



Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

INTERNAL AUDIT

mazars

What is Internal Audit?

As per the Institute of Internal Auditors 'Internal auditing is an **independent, objective** assurance and consulting activity that **adds value** to and improves an organization's operations. Internal Audit helps an organization **accomplish** its objectives by bringing a systematic, disciplined approach to **evaluate and improve** the effectiveness of **risk** management, **control**, and **governance** processes'

IA may involve topics such as efficacy of operations, reliability of financial reporting, highlighting red flags, safeguarding assets, and compliance with policies, procedures, applicable laws

Requirement of IA under Companies Act 2013

As per Section 138 of Companies Act 2013, following class of companies shall be required to appoint an internal auditor or a firm of internal auditors:

Amount in Rs

	Listed Company	Unlisted public company	Private company
Turnover	Always applicable	200 crores	200 crores
Loan	Always applicable	100 crores	100 crores
Capital	Always applicable	50 crores	NA
Deposit	Always applicable	25 crores	NA

Who Can Perform Internal Audit?

Chartered Accountant | **Cost Accountant** | **'Other Professionals' as may be decided by Board of Directors**

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

SMART – DIA (DIGITAL, INTELLIGENT AND ANALYTICAL) INTERNAL AUDIT PROGRAM

mazars

Smart DIA, IT

For sharper, efficient and greater coverage

Advanced data analytics tool to provide exceptional reporting for effective internal auditing

Risk & Resilience

To make business more resilient against the uncertainties

To cover risks at an enterprise level, review the effectiveness of the mitigation plans and integrating the same with Internal Audit

Eye of Forensic

Focus on anti fraud controls

Applying knowledge and repository of fraud risks to focus on anti-fraud controls

Statutory Compliance

To align business with regulatory compliance

To cover the risk of legal and financial exposure to the Company due to legal and statutory non compliances

Internal Financial Controls (IFC) Incl. IT & Cybersecurity

- *Internal financial controls*
- *IT & Cybersecurity controls*
- *ERP application controls*
- *Operating effectiveness of the identified controls*

Operational Auditing

To be able to do a deeper audit

- *Health & Safety*
- *Volatility in prices*
- *Identification and recommending process automation*
- *Sector Insights & Multidisciplinary and SME*

Sidheshwar.Bhalla@Mazars.in

+91 98997 87786

QUESTIONS...COMMENTS...CONCERNS…

CA. CS. SIDHESHWAR BHALLA

Partner & Leader, Governance Risk Resilience Compliance & Sustainability
Mazars in India

Vice President
The Institute of Internal Auditors, India

Immediate Past President
The Institute of Internal Auditors, India (Delhi Chapter)

E-mail: Sidheshwar.Bhalla@Mazars.in
Mobile: +91 98997 87786

…THANK YOU !!!