

Dear Sir/Madam,

**Sub: Inviting suggestions/ comments on draft “Value added business controls
- The right way to manage risk”**

The Committee for Members in Industry (CMII) is in the process to bring out publications on various topics relevant for the Members of The Institute of Chartered Accountants of India (ICAI) serving in industry. In response to our invite for Expression of Interest from members of the Institute and other experts, we have received a first draft on the topic “Value added business controls - The right way to manage risk”. This draft broadly covers the aspects related to risk management.

The Present Contents of the draft is as follow:

- Risks- Definition and Meaning
- Why assessment of risk is necessary
- Relationship between risks and control
- Sarbanes Oxley Act- Overview
- Corporate Governance- An introduction
- Corporate Governance in India
- Extracts of Sustainability audit report of M/s Infosys for FY2008-09
- Informational Technology risks
- Problem Solving and Quality Control – the 6 sigma way

We invite your valuable suggestions/comments on the first draft on the above mentioned topic. Please find below the complete draft for your ready reference.

You may send your suggestions at cmii@icai.org and for any query or clarification you may please contact Dr.T Paramasivan, Sr. Deputy Director at tparamasivan@ici.org .

We would be thankful if your views are furnished to us by **25th October, 2009**.

Committee for Members in Industry Secretariat

VALUE ADDED BUSINESS CONTROLS THE RIGHT WAY TO MANAGE RISKS

INDEX

Chapter	Description	Page No.
1	Risks- Definition and Meaning	4
2	Why assessment of risk is necessary	8
3	Relationship between risks and control	13
4	Sarbanes Oxley Act- Overview	25
5	Corporate Governance- An introduction	30
6	Corporate Governance in India	34
7	Extracts of Sustainability audit report of M/s Infosys for FY2008-09	40
8	Informational Technology risks	45
9	Problem Solving and Quality Control – the 6 sigma way	55

*“Anyone who stops learning is old, whether at twenty or eighty. Anyone who keeps learning stays young.
The greatest thing in life is to keep your mind young”.*

- Henry Ford

CHAPTER-1

Risks- Definition and meaning

Risk is easy to understand but difficult to define. In simple terms, Risk is the probability of happening of an unforeseen event leading to adverse impact on the entity.

Risk is-

*“The possibility of suffering harm or danger” or
“The possibility of bringing about misfortune or loss” or
“To expose to danger or loss”*

A more comprehensive definition of risks is as under:

“Probability or threat of ----- a damage, injury, liability, loss, or other negative occurrence -----, caused by external or internal vulnerabilities -----, and which may be neutralized through pre-mediated action -----”

The above definition can be divided into following elements.

Risk is

- a) Probability of occurrence
- b) Causing adverse impact- damage, injury, liability, loss or other negative occurrence
- c) Be caused by external or internal factors
- d) May be prevented or neutralized through pre-mediated action.

Let's discuss the above elements individually-

- a) **Probability** means likelihood of occurrence of an event and is expressed as a pct. or fraction of 1. On a scale of 0 to 1, the rarest chance of happening is 0 and the most certain chance of happening of the event is 1. Take an example; there are two balls in a pot, one red color and other white color. The probability that ball drawn is red is 0.5 or 50%. In other words, the risk that the ball drawn is not red is 0.5 or 50%.

What is the probability that the ball drawn is either red or white or the probability of the ball drawn is neither red nor white? The answer for former is 1 or 100% and the latter is 0 or 0%. *It needs to be understood from this example that there is no risk when the likelihood of occurrence is bound to happen or certain not to occur.* Continuing with same example, if you are betting on ball drawn to be white, then drawing a red ball is the risk and vice versa.

- b) **Adverse impact** relates to damage, injury and economic outflow of resources without corresponding flow of benefits or undesirable impact on reputation of the entity. Consider a case where the new government extends tax sops for entity operating in Software Technology Park or Export processing zone. Though this example satisfies the definition of probability as its likelihood of occurrence is somewhere between 0 to 1, but it has a favorable and not an adverse impact on profitability of the entities. Hence this is not a risk but an opportunity.
- c) **External or Internal factors** may lead to adverse impact on an entity. *External factors* are those that are not internal to the parties to the business and relate to:

- 1 Policies of government
- 2 Acts of nature like floods, earthquake, storm, cyclone etc
- 3 Acts of man- Riots, Quarrels, stoning etc.

- 4 Change in international laws and regulations.
- 5 Supplier or key customer bankruptcy etc

Internal factors are the ones that are caused internally in the company and relate to:

- 1 Employee unrest- strikes etc
- 2 Loss of key management personnel
- 3 Employee frauds
- 4 Incorrect decision of large capex
- 5 Failure of internal controls etc

d) **Prevention through pre-meditated means** require prior knowledge of the potential risk and developing plans and actions for mitigating the potential loss causable by such risk. Here it needs to be stressed that any risk can at the best be mitigated but in no circumstances it can be fully avoided. If a risk can be avoided then it no longer remains a risk since it loses its characteristic of adverse impact and risk of loss. Risk can be handled by following means:

- 1 **Transfer** - Risks can be transferred by way of insurance cover to insurance companies.
- 2 **Absorb** – It may be beneficial for the company to absorb the risk rather than bearing costs of mitigation in cases where the chances of occurrence are very remote and risks is not so very high.
- 3 **Prevent** – In this case the company forecasts the potential future uncertainty and change its current actions in such a manner that the uncertainty in future provide opportunity for the company. (e.g.): A plastic manufacturing company forecasts that the new government policy will ban the use of plastics bags. Based on this the company adds certain chemical to its existing raw material composition so as to manufacture bio-degradable plastic bags. In this manner, the company avoids the risk of shut down and also becomes eligible for government grant for promotion of the new invention.
- 4 **Defer** – Risk may be deferred in cases where the potential of loss is certain but timing and is not. Taking the case of ones life and death, the loss i.e. death can be postponed by various medical means but can never be avoided. We might have similar circumstances in business where, as managers and leaders, you may be required to take decision as to whether to bear the risk of loss now or do it later in anticipation that the amount of loss will come down in future.
- 5 **Terminate** – Eliminate the risk by avoiding the course of action or by stopping a particular activity. Assume a case where the Information Technology department of a MNC car manufacturing company has come out with new software available in the market that would integrate the entire production to delivery process and yield significant savings for the company. This project, if successful, would bring in lot of efficiencies in the process and help in reducing costs of inventory maintenance, order scheduling and maintenance, Warehouse fixed costs etc. Benefits are likely to be spread across a substantial period say over 10 years. But this will involve significant outflow of funds in current crunch situation. To avoid the risk of borrowings in light of

recessionary times, where loans from banks and financial institution are difficult to obtain, the company may decide to defer the project or terminate the proposal considering the long time lag of cash flow returns.

CHAPTER-2

Why assessment of risks is necessary?

In today's economy, a company that keeps itself abreast of various socio- economic factors is successful. There are umpteen cases where large sized companies suffer huge losses including close down of business because of not forecasting the risks and dangers caused to it through employee unrest, market loss due to competition, Change in governmental policies, Complicated contracts etc.

Catastrophes don't "just happen." From Enron to the space shuttle *Columbia* to 9/11, virtually every disaster is the result of a series of mistakes – each one easy to overlook, each one set in motion *because people simply refused to believe the evidence staring right at them.*

Let us look at few incidents with disastrous effects:

Enron - Living on the edge and loving it

Between 1985 and 2000, *Enron* transformed itself from a Houston-based natural gas distribution company into an internationally known giant that was the largest trader of electricity and natural gas, with operating entities in or planned in many of the developed and developing countries of the world. Enron was on a roll and believed they could expand their trading expertise to virtually every type of business and become the dominant middleman and market maker to the world.

A "we can do no wrong" culture had developed with Enron's impressive growth and success, but somewhere along the way it changed from legitimate pride in accomplishment in a competitive industry to arrogance and a feeling of invincibility. Enron quietly became a significant lobbying organization in a number of states and at the national level. They sought rule changes to reduce regulation on trading gas and electricity, lobbied states to deregulate their utility industries, and lobbied the Security Exchange Commission (SEC) to change revenue recognition rules that were favorable to their business.

Off- balance-sheet financing was not a new concept, but the sophistication and complexity of such deals evolved to a new level with the ever-inventive minds of investment bankers and consultants in the 1990s as special purpose entities (SPEs) became popular. Enron found a number of credible and willing investors, but over time their dreams got even bigger, requiring more capital. During 1990s Enron came to dominate the deregulated gas markets and then moved on to become the largest player in electricity trading. By 2000, Enron believed their "model" could be extended almost indefinitely.

Enron wanted to become a growth machine, and the only way they could do it was to do more and more deals. In fact, Enron CFO liked to give out dollar bills with his picture on them, in a western hat smoking a cigar, part of the persona he developed to convince insiders that he would find funding for their deals. Enron wanted to be seen by investors as a growth machine but with predictability. The reality was that they did this reasonably well in the early 1990s by taking advantage of changing market conditions. But their aspirations and arrogance, fed by earlier success, got the best of the team, and they set huge expectations, internally and externally.

Risk? Enron began to believe they could manage any risk created with financial engineering because they were not just smart but smarter than anyone else. Enron made a press release that announced a loss of \$618 million in income and made no mention of the fact that it had also written down shareholders' equity by \$1.2 billion. On Nov 8, 2001, Enron announced that it would restate earnings for the last 4 ¾ years because they had not followed generally accepted accounting principles (GAAP) in dealing with the off-balance sheet partnerships. Enron executives tried to arrange a last minute merger with Dynegy, a competitor in some similar businesses, to stabilize the financial situation, but Enron was in too much trouble for anyone to take risk. The end was scary, and on December 2 Enron filed for bankruptcy, unable to make multibillion dollar capital calls on its various deals plus debt downgrades that triggered covenants with lenders that it could not fund.

The technical cause of Enron's failure is straightforward- its executives took extraordinary risk by choosing to over leverage the company in an attempt to sustain high growth. These actions were blessed by accounting firm Arthur Anderson that was involved in a greater than average number of questionable audits and no longer exists. The bankruptcy led to layoffs, worthless pension plans, massive credit defaults and ripple effects wherever Enron did business, as shareholders saw virtually 100 pct of their equity wiped out and creditors lost an estimated 80 pct of their claims.

In related events, Arthur Anderson, Enron's accountants, implicated in the wrongdoing, put 10,000 or more employees out of work worldwide when they went under as a result of their Enron related activities.

Assessing the above case, we can derive the following cause of emergence and scary fall of Enron-

1. Desire for growth
2. Aggressive financial management
3. Unfailing belief in a new business model
4. Push boundaries to win
5. Lack of oversight

“Culture is powerful - What creates success may kill you”

Now let's read through a different episode of well known **Fast food company- the Hamburger Giant "McDonald"**.

Before we discuss the case, let's see some interesting facts:

- McDonald's corporation did not invent the hamburger. It only grew it into one of the most successful businesses of the planet.
- McDonald's had eight locations in southern California, was charging 15 cents for hamburgers, and happy customers were standing in the queue to be served.
- McDonald's advertised to let it franchise a store and sell franchises to others. Within 10 years, there were over 700 stores.
- McDonald's did not even invent the Big Mac and Egg McMuffin; they were invented by franchise operators. But McDonald's did develop and refine operational procedures, equipment, a *supply chain* and marketing that standardized it as the most effective and efficient global operation in the fast food business.

Now let's see what went wrong at the global food joint giant:

McDonald's experience was driven by culture and conscious objective of providing the customer with exactly similar product in taste and quality that he or she expected on every occasion. McDonald's was a pioneer in teaching the world the lesson on Standardization.

In mid 1950s, other food entrepreneurs saw opportunity to capture the post war interest in burgers, fries and shakes in efficient fashion and this gave rise to tough competitors to McDonald's in form of Burger King, Krystal, White castle and others. Call of that time was that any deviation from the standard would increase costs and complexity. While most customers were happy with the standard products that were on offer, some wanted different combinations of condiments. Most small stores actually accommodate a special request, but it took too much time because it disrupted the normal operating routine.

In an effort to differentiate itself, in 1974, Burger King came up with the "Have it Your Way" marketing campaign to offer customers some deviation from the standard McDonald's approach to its products. The McDonald's culture focused on standardization, and "we'll deviate for the customer, but only if we have to" served it well for decades. But as the 1990s drew to a close, consumer tastes were changing rapidly. People realized they were getting overweight and started looking for something more akin to a dining experience. Add to this a variety of diet craze from grape fruit to Atkins and McDonald's growth started to slow.

The cultural reaction was interesting. While Wendy's grew with a shift in menu by adding salads and Burger King added experimental sandwiches, McDonald's persistently stuck to their tried and true formula- standard products, rarely changed, and produced in a way that was efficient for the company. They also kept building new stores at a torrid pace, in the United States and abroad.

Sales slumped and franchisees became unhappy as owning a piece of the “Golden buck” was not as attractive as it had been. The stock, a growth stock for decades, declined as revenues and earnings turned down, declining from a peak of nearly \$50 per share (split adjusted) in late 1999 to \$12.50 in early 2003, when McDonald’s posted the first quarterly loss in its history. This was not a simple business downturn; the culture that served well for nearly 5 decades had somehow faltered. Double-digit growth through delivery of value based standard products delivered in standard settings, while adding as many new stores as possible each year, was at an end. The Board of Directors realized that McDonald’s had problems and acted or rather to say they reacted:

Revitalization plan began at McDonalds and following steps were undertaken:

- Closing underperforming stores
- Selling off some brands (such as Donatos Pizzeria) that were not central to the core business
- Focusing on basics: clean stores, friendly service, and hot food
- Pushing new products, including McGriddles and salads
- Stopping price wars
- Slowing expansion and last but not the least
- Appointed James Cantalupo as its new CEO, replacing Jack Greenberg, the predecessor.

McDonald’s went back to basics and found out their core competence is operations and marketing in a fairly narrow area, and expanding those competencies to similar but different product areas was more difficult than imagined. They refocused on the basics of a business that they had taught the world. This was something the organization knew to do well and the execution worked, with the performance turning around in a year.

The old saying “Don’t forget who brought you to the dance” sometimes applies to business as well.

One or more dramatic failures, in which many in an organization suddenly see the need to begin a change process. It is unfortunate that we need a disaster as a change agent, but in some cases, even those who see the need for change may need additional “evidence” to garner support from those with the power to initiate change or the broader group that wants to understand the need for change.

Exercise:

1. Large business is prone to larger risks. But the same may not be entirely applicable to a small or a medium enterprise. Assuming you want to venture into a restaurant business. List out potential risks that you may face and key points that you need to keep in mind when setting up the venture.

**“Nothing is particularly hard if you divide it into small jobs”
- Henry Ford**

CHAPTER-3

Relationship between Risk and Control

Let us consider a scenario and try to list out various considerations involved in a plan for expansion of business:

You are an established fast food joint in your city with branches set up at locations attracting young crowd. You are doing fairly well and your brand is fast spreading among juvenile class in the city. Now you want to venture out geographically and advertise the brand in different cities. You determine that a substantial funding would be required to fund marketing of your brand in other areas and for setting up branches. Your management evaluates several options of funding and ranks the alternatives against various criteria like dilution of control, cost of raising capital, difficulty of raising funds and so on and so forth.

While evaluating the option of expanding business into other areas, several considerations other than the financial consideration are to be included. A few of them are listed as under:

- Your existing success is attributable to Juvenile class. Setting up branches near jogging park for retired or Professional offices etc, need to be evaluated.
- Presence of stiff competition from established players in the area.
- Governmental restriction regarding use of specific products like plastics, chemicals used in your trade.
- Current informational infrastructure to support expansion.
- Costs of leasing or owning office space.
- Payback period for investment.
- Marketing methodologies in the area identified for expansion.
- Cash collection and treasury management.
- Level of delegation required.
- International currency risks and statutory filings in case of cross border expansion.
- And many others.

Now let us review the following statement:

“Risks cannot be eliminated but can only be mitigated or reduced”.

An opportunist will not agree to the above statement in sense that an opportunist finds an opportunity in everything? Let us see some scenarios and try to answer this.

Case 1: You are manufacturer of Plastic bag. Due to potential disaffects of use of non-degradable plastic and a related environmental risk, the Indian government is considering a ban on use of non-degradable plastics. If the law is passed, you may go out of business.

You pro actively recognize that an additional investment for modification of the Plant & Machinery and adding a new raw material would allow manufacture of bio-degradable plastics, other infrastructure remaining the same. The management of the company unanimously agrees to the proposal and capitalizes on the opportunity. The company is awarded incentive by way of tax waiver by the government for rewarding and encouraging the new initiative.

Hence an opportunist would look for various options to transform risk in to prosperous opportunity.

Case 2: You are a large corporate house into business of manufacture of Passenger cars. Your business caters to both at home in India and outside. Due to global financial meltdown, your key vendors supplying production parts are facing risks of bankruptcy and subsequent closure. Your company have had long term relationship with this supplier and been supported with prompt deliveries and service of high quality at all times. The vendor carries with it requisite technology and workmanship that is key to your business. The Vendor is critical to the introduction of new model by your company in the market. Management is worried about the situation and acclaims that it would be quite a task to replace the services of the vendor in question.

After lots of iterations, evaluation of available option and discussion with supplier's management following course of action is agreed:

Your company would give a lump sum production order to this vendor to cater to the production of the new model for next two years and agrees to pay 50% of the amount in advance. Terms of finance and other terms are mutually agreed between the two companies. Your company also acquires new equity in the vendors company.

Governments' globally taking account of the situation announces bailout and incentive plans to revive the economy. No problems are eternal. Positive actions reap benefits and economy revives sooner than expected.

Profitability of your company improves better than expected coupled with share of earnings from holdings in the vendor company. Relationship and control on the vendor company increases and afford higher confidence on future supply and pricing of the components.

This is another classic illustration of transforming risks into highly rewarding opportunity.

Summarize: But to assume that business face risks one at a time may not be true at all times. In fact, many a time the management is faced with situation of choosing one among various available options or prioritizing alternatives based on time. Management uses several available tools like Pay back period, Discounting method, Return on capital, Risks matrix and others to decide on which risks is to be eliminated, which one to be mitigated and the one to be absorbed. Hence, considering the complexity, size and volume of current businesses it would be fair to say that risks can only be mitigated and not eliminated.

Now let us understand the definition of control:

Definitions from the Business Dictionary:

Definition 1

Management process in which the (1) actual performance is compared with planned performance, (2) difference between the two is measured, (3) causes contributing to the difference are identified, and (4) corrective action is taken to eliminate or minimize the difference.

Definition 2

Device or mechanism installed or instituted to guide or regulate the activities or operation of an apparatus, machine, person, or system.

Elements of control are explained as under:

- 1. A management process:** Control is a management initiative. It is the responsibility of the top management to set up a tone at the top. This could be done by way of setting up of policies, procedures, rules & regulations, framework, organizational structure, Separation of Duties etc., and the organization down under holds the responsibility of supervising and executing them to ensure timely achievement of the overall objective. This concept of tone at the top is discussed more in detail later in this handbook.

Control is not a one time activity. It is a continuous process. Control is to be tried and tested at regular intervals and improvements made within. We will discuss about Control evaluation techniques and continuous improvement concept later in this handbook.

Following steps are involved in the management process for controls:

- a) Clear definition and communication of objective:** It is the primary responsibility of the management to lay down clear objectives of the business. The departmental and operational objectives should be SMART i.e. Specific, Measurable, Aligned to primary objective, Reasonable and Time bound.

Definition of objectives alone would not be effective unless these are communicated. In fact Employee communication is the most effective tool in gaining confidence of the staff and getting the team to work together towards achievement of common objective.

- b) Setting up of Policies, Procedures, Rules and Regulations:** Having defined and communicated the objectives, policies, procedures and rules are to be carefully thought over and informed at all levels. These policies and rules include but not limited to Human Resource, Purchasing, Treasury, Administration and Information Technology.

- c) Continuous evaluation of Objectives and underlying Policies and Rules:** New events and developments in Business necessitate continuous evaluation of policies and making changes as and when needed. Important factors to be considered include Growth of business, Governmental Policies, Competition, Employee reactions and other External and Internal considerations.

- 2. Comparison of actual and planned performance:** To ensure the rules, regulations are working as intended and that policies are being complied with, it is necessary to test actual performance. Any deviation from the planned performance would necessitate management attention on tightening of controls to ensure the achievement of the intended objectives. Periodicity of test of controls is a key decision to be made since any delay in identifying off track activities would cost the organization and would also place additional burden of rectifications of the incorrect actions. To ensure efficiency and effectiveness, it is important to compare costs of implementing process of periodic verification of controls against costs of rectification of the effects of incorrect actions and act accordingly.

There are various ways of evaluating the actual performance. Some of them are explained below:

- **Questionnaire:** The evaluator can prepare list of questions that needs to be answered while doing a walkthrough of the process. This method is useful for not so significant controls since it relies upon what is observed during the walkthrough process. To make it more useful, the timing and periodicity of the walkthrough is important and surprise element therein would add to utility of the tool.
- **Control Checklist:** This tool is similar to the Questionnaire tool but differ from it in a sense that the checklist is an enabler for the person actually performing the job. The checklist also serves as an audit log as evidence of work done in a manner it ought to be performed. Efficiency of the checklist depends on the utility and completeness of the control points mentioned therein. The checklist must be subjected to revision whenever there is change in the way the relevant activity is performed.
- **Adherence Testing:** This is a formal procedure of documentation of testing of existing controls. It contains various modules of end to end processes like Purchase to Pay, Order to Receivable, Warranty, Variable and Fixed Marketing, Safety and so on. Each module contains various control points and the risks associated with each such control. Testing may be done by self or by external auditors/evaluators. Sample guidelines are used to ensure sufficient representative samples are used in order to form appropriate opinion on working of controls. Entire testing is formally documented and serve as an audit log as evidence for test of controls.
- **Personal Interviews:** Personal interview with management would provide additional evidence of process of objective setting, process of review of policies, rules, handling of competition, compliance of laws etc. The interviews must be planned well and the questions to be asked must be well thought and deliberated in advance.

3. Identification of causes of deviation: Upon evaluation of controls, the deviations are identified. The deviations are brainstormed among the stakeholders that include the operational team, the supervisors and the managers and impact is ascertained. The high impact deviations are filtered and causes are determined. Other deviations are set right as these are low hanging fruits. Techniques like 5 W 1 H are used. This technique involves the “why” and the “how” questioning repeatedly till the fundamental cause of the deviation is determined. More often than not, the cause that seems apparent is not the actual root cause and the errors/deviations continue to occur even after rectification of the cause. Hence the technique 5 Why and How works well in most of situations.

(e.g.): Why? - The battery is dead. (First why) Why? - The alternator is not functioning. (Second why) Why? - The alternator belt has broken. (Third why) Why? - The alternator belt was well beyond its useful service life and has never been replaced. (Fourth why) Why? - I have not been maintaining my car according to the recommended service schedule. (Fifth why, root cause)

Following are various other methods that are used for preemptive identification of failures:

- **Root Cause Analysis:** Root cause analysis (RCA) is a class of problem solving methods aimed at identifying the root causes of problems or events. The practice of RCA is predicated on the belief that problems are best solved by attempting to correct or eliminate root causes, as opposed to merely addressing the immediately obvious symptoms. By directing corrective measures at root causes, it is hoped that the likelihood of problem recurrence will be minimized. However, it is recognized that complete prevention of recurrence by a single intervention is not always possible. Thus, RCA is often considered to be an iterative process, and is frequently viewed as a tool of continuous improvement.

RCA initially is a reactive method of problem detection and solving. This means that the analysis is done after an event has occurred. By gaining expertise in RCA it becomes a pro-active method. This means that RCA is able to forecast the possibility of an event even before it could occur.

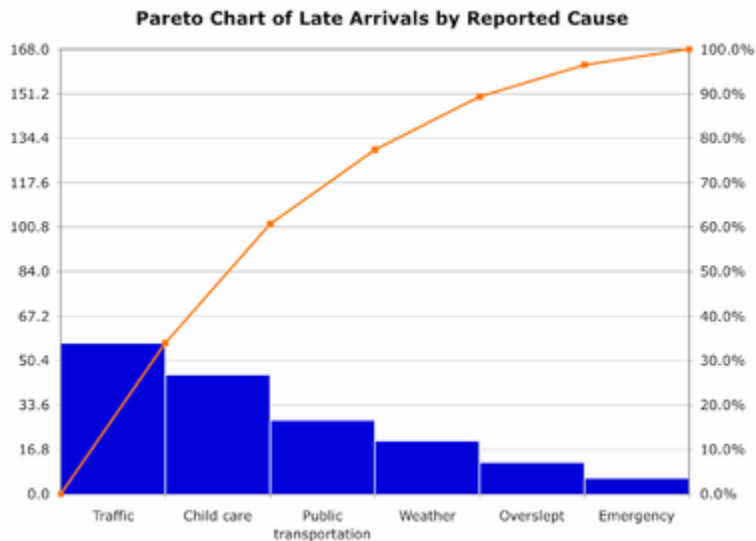
General process for performing and documenting an RCA-based Corrective Action:

- i. Define the problem.
- ii. Gather data/evidence.
- iii. Ask why and identify the causal relationships associated with the defined problem.
- iv. Identify which causes if removed or changed will prevent recurrence.
- v. Identify effective solutions that prevent recurrence, are within your control, meet your goals and objectives and do not cause other problems.
- vi. Implement the recommendations.
- vii. Observe the recommended solutions to ensure effectiveness.
- viii. Variability Reduction methodology for problem solving and problem avoidance.

The 5 W 1 H techniques is a form of RCA only. Some other RCA tools are as under:

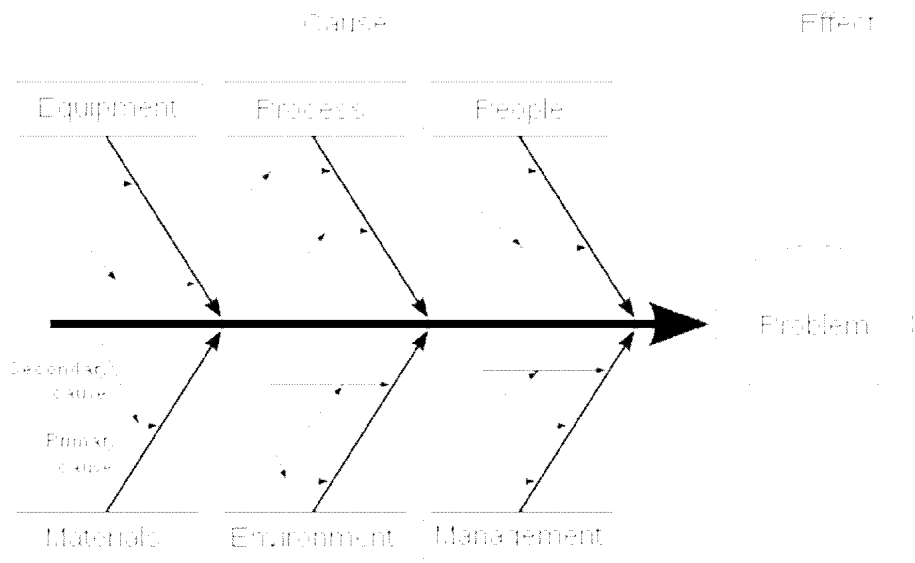
- a) **Pareto Analysis:** Pareto analysis is a statistical technique in decision making that is used for selection of a limited number of tasks that produce significant overall effect. It uses the Pareto principle - the idea that by doing 20% of work you can generate 80% of the advantage of doing the entire job. Or in terms of quality improvement, a large majority of problems (80%) are produced by a few key causes (20%).

Pareto analysis is a formal technique useful where many possible courses of action are competing for your attention. In essence, the problem-solver estimates the benefit delivered by each action, then selects a number of the most effective actions that deliver a total benefit reasonably close to the maximal possible one.



Above Pareto diagram is a simple example of a Pareto chart using hypothetical data showing the relative frequency of reasons for arriving late at work.

- b) **Ishikawa Diagram:** Also famously called a Fishbone or a Cause and Effect Diagram, it is a diagrammatic representation of cause and effect. Causes in a typical diagram are the 4 M's i.e. Machine, Methods, Material and Man. In case of service industries, the typical causes of problems can be divided into 4 P's i.e. People, Process, Policies and Procedures.



Above is an Ishikawa diagram, in fishbone shape, showing factors of Equipment, Process, People, Materials, Environment and Management, all affecting the overall problem. Smaller arrows connect the sub-causes to major causes.

Apart from above, there are other graphical quality control tools like Histogram, Check sheet, Flowchart, Scatter Diagram and others.

Now let us understand the 4th and final element of Control:

- 4. Corrective actions:** Having identified the key root cause for the problem, the same needs to be corrected. Here it is important to understand the difference between Correction and Corrective action. A Correction fixes the symptom of an existing problem whereas a corrective action stops its further recurrence. Lets understand this better with help of an simple example.

Assuming Mr. A is allergic to dust and he catches cold and gets fever upon exposure during stock audit of a Dealer of Tyres. Here the problem is Cold and fever. Mr. A takes a medicine and gets well. This is called correction of the problem. Presuming Mr. A consults a homeopathy practice and undergoes a course to not to be affected by dust allergy. After a long course, Mr. A develops resistance to dust. This is called a corrective action. Presuming Mr. A avoids going to places prone to dust, then he is exercising a preventive control.

Corrective action is a process and not an isolated activity. Following are the steps in a Corrective action process.

- i. Identify the required performance level:** The first and foremost step in the corrective action process is the defining of the performance level. It may be defined in various ways like service level agreements, industry benchmarks, self developed performance level, audited work procedures and others. A service level agreement states the voice of customer and is an excellent tool to identify deviation from expected performance. Similarly, industry benchmarks form the basis of objectives development and assessment standards for a company. Work procedures should be developed after considering the framework in which the process operates and related legal and compliance requirements.

(e.g.): M/s KMG provides accounting and shared services to customers globally. Service levels of the company are defined in its agreements with its clients. If the service level agreement (SLA) requires processing of invoices within 48 hours from the day of receipt, then the minimum objective or performance level cannot be more than 48 hours. Nevertheless, M/s KMG can internally have a stretch target of processing of invoices with 24 hours from receipt.

- ii. Measure actual performance:** An entity must have an inbuilt mechanism of measuring its performance in quantifiable terms. It is also important to ensure that there is continuity and consistency in measurement. In terms of Quality and Six Sigma methodology, the process of gauging the measurement system capability is called *Measurement system analysis* and abbreviated as MSA. Measurement capability analyses are critical to the success of every measurement and ensure that future measurements will be representative of the characteristic being measured. MSA is performed by use of various mathematical & statistical tools.

Once the actual performance is measured, it must be compared to the performance level as defined in step one. Any difference between the two is termed as variation. The very objective of control is to reduce variation in the process.

- iii. **Classify deficiency:** Performance deficiency may be classified in the following types depending upon the impact that it could have on ultimate achievement of objectives.
- **Level III - Major deficiency:** These are the deficiencies of highest order requiring immediate attention of the decision making authority and quick resolution. It may be related to Health and Safety, Going concern assumption or any other deficiency impacting the well being of the company's reputation among its clients. In such cases, the corrective action is usually necessitated within 24 hours.
 - **Level II – Significant Deficiency:** These are deficiencies that do not pose imminent danger to client relationship but jeopardizes the long term well being of the company and its financials. In such cases, the corrective action is usually necessitated in 10 to 30 days.
 - **Level I – Minor Deficiency:** These are deficiencies that are relatively insignificant in nature and that do not impact well being of the company or jeopardize its relationship with its clients. Corrective action in such cases can be planned over 3 to 6 months.
- iv. **Developing Corrective action plan:** Once the deficiency/deviations are identified, a corrective action plan must be developed to eliminate or mitigate the deficiency. Problem solving techniques must be used and various option and alternative solution must be evaluated for pros and cons and the best implementable alternate must be implemented. The costs of implementation and corresponding benefit must be compared more so in case of Level 1 deficiencies. In such case management has the option to absorb the risk arising out of it considering the high implementation costs.
- v. **Evaluate the success of corrective action:** It is important to measure the success of the implemented action at key times. This is called tollgate reviews. These reviews are required at the time of implementation of the corrective action so that any deviation from the expected performance level can be rectified before it causes irreparable damage. Plan 2 or supplementary plan must be prepared and agreed before hands to ensure it is implemented upon failure of Plan 1 without any waste of time.

It also needs to be ensured that the corrective action plan is approved at appropriate level of management and key stakeholders participation is ensured.

“Coming together is a beginning; keeping together is progress; working together is success”

Henry Ford

Risks and controls- Relationship

Risks and controls are directly related to each other though they may not be exactly proportional. Higher the risk, higher is the requirement for control and vice versa. This relationship is very important to understand to ensure redundant controls are avoided and high risks processes are not left to operate with inadequate controls. Management recognizes the risks and control relationship at various times like when trying to prioritize investment options, implementing controls, Lease versus buy decisions, expansion projects, New supplier or market, diversification of products and so on. Similarly, an auditor uses ABC principle or the 80:20 rule to perform his testing in order to gain reasonable confidence of the true and fair view of financial and existence and effective operation of the internal control system within the organization. Selection between Substantive procedures and Adherence testing is a step in this direction only.

Let us see the below diagram and understand this relationship better:

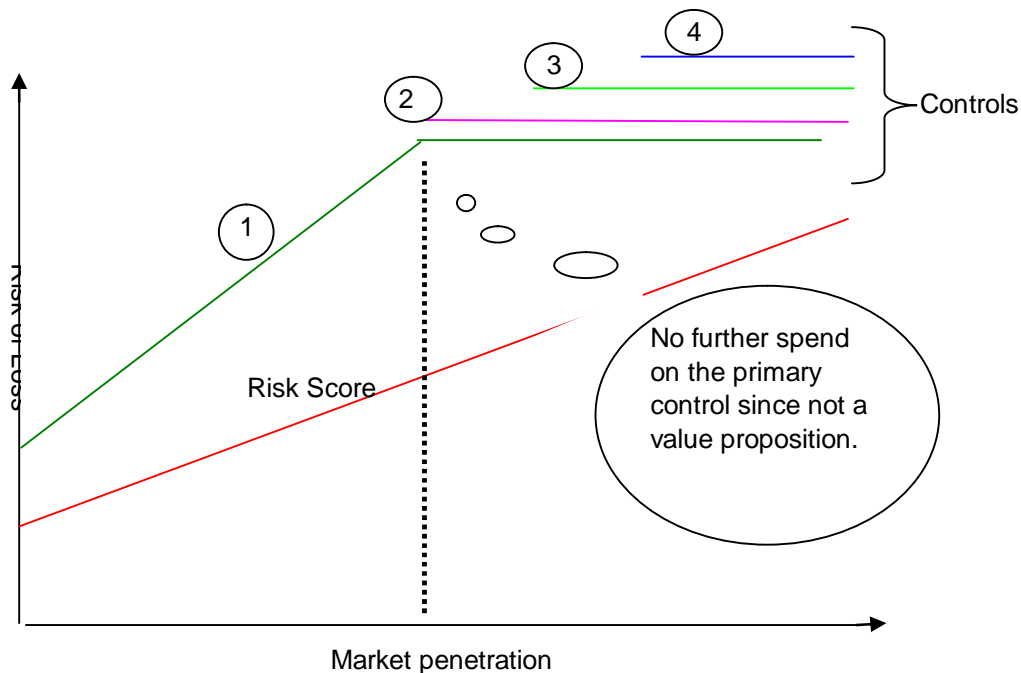


Figure showing the relationship of Risks and Controls

Below are the interpretations:

1. The X Axis is the level of market penetration by the company. More the diversification in business more is the risks. Hence we could see direct relationship between Market penetration and Risk of loss represented by the Risk Score.
2. During initial phase, controls are set up and with experience and maturity; the company attains higher control score. The primary control is represented by Line 1. The dotted line depicts that stage in controls where further investment in the primary control is not cost beneficial.

3. Since primary controls cannot be further strengthened, additional supplementary controls are introduced to ensure controlled process performance.

Consider the following example:

M/s Axis Enterprises is operating departmental store at Greenwich Road in Chennai. Its low margin products attract lots of customer from the vicinity. Local residents prefer purchasing ambience at the stores and the store is a hit in a short time span. The management is encouraged with the potential of the store and decides to expand its product line into larger variety of departmental products. Hence the supplier base of the firm increases.

The firm exercised closer control on the stock delivery and payment to suppliers. Each invoice accompanied by delivery challan is verified and authorized by store keeper and before it reaches accounts payable department for payment. As the volume of business increases, the number of vendor transaction rise and the firm adds more supplementary controls to its purchase and pay process. It implements additional controls in form of authorization of invoices above Rs.25, 000/- by the store manager, Weekly stock verification of high value stocks against monthly stock check done earlier, Periodic Supplier statement review and reconciliation and so on. The firm adds supplementary controls to back up the primary control to ensure significant deviation/deficiencies are identified before it leads to incorrect payments.

“Most people spend more time and energy going around problems than in trying to solve them”.

- Henry Ford

CHAPTER-4

Sarbanes Oxley Act- An overview

Investors in U.S. really saw the bad phase in the financial market with the collapse of big companies like Enron & WorldCom.

What went wrong in Enron and WorldCom?

Enron abused of Accounting and disclosure rules to inflate profits. From 1998-2000, Enron's revenue shot from \$31 billion to more than \$100 billion. It was reported that the high rank officials of the company used certain complex structures, hidden payment and secret loans to create appearance that certain entities funded and controlled were independent of Enron, whereas these must have been consolidated into its financial statements. The officials exploited the notion that these entities were independent of Enron so as to misappropriate millions of dollars representing undisclosed fees and illegal profits.

WorldCom, the second largest telecom company in U.S. then was abused of accounting inadequacies. The Accounting scandal was uncovered by the Internal Auditor of the company in June 2002. It discovered that revenue expenses were being treated as capital expenses and deferred over a period of time, while they had to be booked in that quarter itself. During 1999-2001 and the first quarter of 2002, the company counted as capital expenditure \$7 billion that it spent on everyday expenses. The Auditor's of WorldCom, Arthur Anderson L.L.P, confirms that the company complied with all Accounting Standards.

Hailed as the most significant change to securities laws since the 1934 Securities Exchange Act, a new penal law, an act commonly known as the Sarbanes-Oxley Act of 2002 (SOX), was signed into law by George W. Bush and became effective on July 30, 2002. The Act contains sweeping reforms for issuers of publicly traded securities, auditors, corporate board members, and lawyers. It adopts tough new provisions intended to deter and punish corporate and accounting fraud and corruption, threatening severe penalties for wrongdoers, and protecting the interests of workers and shareholders.

What are implications of Non-Compliance of SOX?

The dire consequences of SOX are directly on CEO/CFOs. Under the Corporate Responsibility for financial reporting, any certification and willful certification would entail a fine of \$ 1 million or imprisonment up to 10 years or both and a fine of \$ 5 million or imprisonment up to 20 years or both respectively.

Review Reports and facts under SOX:

Pursuant to **section 302**, CEOs and CFOs have to certify that all Quarterly and Annual filings with the security Exchange Commission are error free and such statements do not contain any untrue statements of material information and do not skip any material information, CEOs and CFOs are also required to confirm that all necessary information required for preparation of financial condition (i.e. Balance Sheet), results of operation (Profit and Loss statement) are duly incorporated. In order to enable the CEOs/CFOs to certify and confirm, the company should have strong design and operation of internal control in place, based on which the opinion could be formed.

The controls must be designed so as to ensure that all material information of the company and its subsidiary are duly reported effectively. Moreover, the responsibility of evaluation of controls also lies with them. The evaluation should be made within 3 months prior to the date of their report.

Section 404 requires management to provide a report annually on internal controls over financial reporting (called as Internal Control report) stating following:

- Responsibility of management for establishing and maintaining an adequate internal control structures and procedures for financial reporting.
- Also containing an assessment on the effectiveness on internal control structures and procedures for financial reporting.

Pursuant to **section 404**, the auditor of the company is also required to attest the assertion made by the management on the effectiveness on internal control structures and procedures for financial reporting.

CEOs /CFOs are required to disclose following to auditor and the audit committee:

- All significant deficiencies in the design or operation of internal control which can adversely affect the financial reporting.
- Any fraud identified whether material or not involving management and employee.

After setting the internal controls for each and every relevant process and transaction in the company, the management has to assess them with the International benchmarks. Following questions can be put forth at this junction.

- i. Are all significant processes in the company defined?
- ii. What are the key and non-key controls in the company?
- iii. Whether what can go wrong analysis done for significant process?
- iv. Is Risk Assessment of all necessary controls done?
- v. Are ways to mitigated, avoid, ignore and transfer risks identified?
- vi. Is there a process of regular assessment and reviews of process controls?
- vii. Is there a process of identification and corrective action for gaps identified in internal control?
- viii. How are material weaknesses and significant deficiencies handled?
- ix. Is there a proper information and communication mechanism for timely update?

In order to assess an organization's internal control, one must first identify the criterion against which the assessment will be made. Therefore, it is important to appropriately define internal control early in the evaluation process. Necessary internal control framework is required to assess the controls prevailing and established by the company. COSO is one such standard that is highly recommended and has a wide use in numerous companies.

According to COSO, Internal Control is defined as a process effected by an entity's board of directors, management and other personnel to provide reasonable assurance regarding the achievement of objectives in following three categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting and
- Compliance of laws and regulations.

According to COSO, there are five interrelated components of effective internal control:-

- 1) **Control Environment** – A Control Environment creates the foundation for effective internal control and establishes the “*tone at the top*” and represents the apex of the corporate governance structure. Control environment in an organization refers to intangibles as integrity, ethical values, People competency, management philosophy and operating style. It can be observed in an organization through its various policies like Environment Policy, Human Resource Policy, Policy for general society, Employee welfare Policy etc. It has a top to bottom influence in the company. Healthy control environment helps to curb the fraud by creating strong anti – debacle mechanism. The control environment in a company influences the rest of the component discussed below.
- 2) **Risk Assessment** – Risks assessment involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form basis of determining control activities.

Management assessment of risk should include the following:

- Wrong financial reporting
- Tampering with documents, mail communications
- Misappropriation of assets
- Influencing Auditors on reporting and presenting incorrect facts and figure
- Tax evasion

In Risks Assessment, the possibility of frauds and failures are considered.

- 3) **Control Activities** – Control activities are the policies, procedures, instructions and practices that are put into place to ensure achievement of objectives and risks mitigation.

Following are some examples of Control Activity and the type of control:

<u>Sl.</u>	<u>Control Activity</u>	<u>Type of Control</u>
1	Reconciliation of Bank statement	Detective
2	Physical verification of Assets	Preventive
3	Authorization of Expenses	Preventive
4	Job Rotation	Preventive
5	Separation of Duties	Preventive
6	Surprise visits	Detective
7	Budget authorization	Preventive
8	Budget review	Detective
9	Training of Personnel	Preventive & Corrective
10	Periodic meetings	Preventive, Detective & Corrective (based on purpose of the meeting).

4) Information and Communication – Information is required at all levels of the organization in order to effectively run the business and achieve the objectives. Information Technology play a very important part in sharing of the information to various users when required and within the time frame in order to allow them to carry out their duties and achieve the control objectives. The IT department may also assist in implementing mechanisms to identify and communicate significant events, such as e-mail systems or executive decision support systems. To be effective, it is very important to ensure that the information is Appropriate, Timely, Current, Accurate and Accessible. Communication can be at the company level and/or at the department level. There can be top down communication i.e. Superior to Subordinate, Down-top i.e. Subordinate to Superior and Peer to Peer communication.

5) Monitoring – Process of monitoring covers the oversight of internal control by management through continuous and point-in-time assessment process. Monitoring can be done in many ways:

- Supervision and reporting
- Monitoring through use of Information technology
- Use of metrics reporting techniques
- Exceptional reporting etc.

Metrics provides a track and assess mechanism for analyzing trends of actual results against plan and forms the basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability.

Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, can ensure a reduction of the unavailability of key systems. Large transaction base and size of corporate has made information technology an integral part of SOX implementation program. Hence general IT application controls must be documented and evaluated to ensure appropriate change control and that the application renders the output expected from it.

To simply put, IT governance forms an essential element and base for better financial governance. The very nature of IT governance and IT Control is to prevent a fraud at its genesis. In addition it can also support on detecting and again controlling fraud by enabling necessary check and controls in place.

For setting the right pitch through the organization, tone is to be set right at the top by the senior management and the board. This is done by way of framing policy and related procedures and setting a process to ensure compliance throughout.

At this point, let us introduce the concept of Corporate Governance:

CHAPTER-5

Corporate Governance- An introduction

Let us study the below case of Mr. Natwarlal, who has just set up a new business with money invested out of his own inherited funds and some borrowed from family and friends.

Mr. Natwarlal son of Late Mr. Bhawarlal, a renowned businessman has decided to venture into business of trading in women cosmetics. He has managed to fund his capital requirement partly out of his accumulated funds and rest from external borrowings. He has been successful in maintaining decent profits from his business and pays back the interest costs to the creditors. After experiencing the high margin from the business, he decides to expand into costlier cosmetic items and gains support from the existing and new creditors based on his track of prompt payments done earlier. To enjoy further high margins, he opts for cash purchase of stock and gets larger discount on the deal. Since the product is fast moving in the market, he is successful in increasing profitability and continues to satisfy the creditors by prompt payments.

But business is not all about profits and good times. Risk is inbuilt in any business. The product that Mr. Natwarlal trades in is banned by the Department of cosmetology for containing harmful chemicals affecting the skin and causing cancer. In no time, the news spreads among the affluent community and the sales dip almost to being negligible. At this moment of time, Mr. Natwarlal has in his stock huge quantities of the cosmetic. In couple of months, the creditors start demanding settlement of their loan being fully aware of the sudden dip in the business of Mr. Natwarlal.

Natwarlal, unable to pacify the creditors for long, decides to take an alternate route. He falsifies the existing banned product by rebranding it to another competitive product and begins to sell the same. Customers are back to their old shop well known earlier and sales begin to boom again. In no time, Natwarlal gets back to profits. An official from the Department of Cosmetology, upon being tipped, raids Natwarlal shop and identifies the forgery. Natwarlal, in order to avoid legal consequences, bribe the official and is let off.

Natwarlal is now completely conscious of the false means of trade. After some years he goes public for further expanding his business. He continues the short cut ways of making profits and reaches big heights. He is now the promoter of M/s Lal industries Ltd, manufacturer and distributor of various varieties of women cosmetics. He has also acquired few foreign companies in similar endeavor. In few years the share prices of Lal Industries goes sky rocketing. Natwarlal is hand in hand with the speculators in the stock market and the company's stock is now trader's favorite.

But as believed by all and also portrayed in our super Bollywood films that evil is short lived. The authorities find out the fabrication, misrepresentation and fraud done by Natwarlal and clutch all his businesses. Stock prices plunge and retail and institutional investors look to sell off their holdings. Lal industry is now the talk of much business news in India and abroad and an educational case study in business schools. Economist and Business men start promoting Business wisdom, transparency, discipline, fairness and social responsibility. Government is questioned on the governance process and several committees are formed to study and evolve a governance policy for corporate houses to ensure investor safety. In short, Corporate Governance begins to evolve in the country.

Corporate governance denotes the process, structure and relationship for overseeing the action of the management and directing and controlling them.

“Corporate Governance is concerned with holding a balance between economic and social goals and between individual and communal goals..... The aim is to align as nearly as possible, the interest of individual, corporations and society”.

Corporate Governance is all about promoting corporate fairness, transparency and accountability. The basic premise of having Corporate Governance in place is to build up a trustful environment among stakeholders. Further, it is required to enhance shareholder value and perfect the interest by enhancing the corporate performance and accountability. Senior management/Board of Directors of the company play a vital role in the intrinsic growth of the company in terms of connecting it with capital market, gaining investors confidence, ensuring and evaluating companies performance and assuring the desired corporate returns, and also boosting up the confidence level of overseas investors so as to attract the fund flow from abroad. Thus, a responsibility on the senior management relating to best corporate governance practice is on the higher side.

Seven characteristics were pointed out by the King Committee report for South Africa in 2002, the period when Corporate Governance gained huge popularity. These characteristics are detailed as under:

1. **Discipline:** Corporate discipline is a commitment by a company’s senior management to adhere to behavior that is universally recognized and accepted to be correct and proper. This encompasses a company’s awareness of, and commitment to, the underlying principles of good governance, particularly at senior management level.

“All involved parties will have a commitment to adhere to procedures, processes, and authority structures established by the organization.”

2. **Transparency:** Transparency is the ease with which an outsider is able to make meaningful analysis of a company’s actions, its economic fundamentals and the non-financial aspects pertinent to that business. This is a measure of how good management is at making necessary information available in a candid, accurate and timely manner – not only the audit data but also general reports and press releases. It reflects whether or not investors obtain a true picture of what is happening inside the company.

“All actions implemented and their decision support will be available for inspection by authorized organization and provider parties.”

3. **Independence:** Independence is the extent to which mechanisms have been put in place to minimize or avoid potential conflicts of interest that may exist, such as dominance by a strong chief executive or large share owner. These mechanisms range from the composition of the board, to appointments to committees of the board, and external parties such as the auditors. The decisions made, and internal processes established, should be objective and not allow for undue influences.

“All processes, decision-making, and mechanisms used will be established so as to minimize or avoid potential conflicts of interest.”

4. **Accountability:** Individuals or groups in a company, who make decisions and take actions on specific issues, need to be accountable for their decisions and actions. Mechanisms must exist and be effective to allow for accountability. These provide investors with the means to query and assess the actions of the board and its committees.

“Identifiable groups within the organization - e.g., governance boards who take actions or make decisions - are authorized and accountable for their actions.”

5. **Responsibility:** With regard to management, responsibility pertains to behavior that allows for corrective action and for penalizing mismanagement. Responsible management would, when necessary, put in place what it would take to set the company on the right path. While the board is accountable to the company, it must act responsively to and with responsibility towards all stakeholders of the company.

“Each contracted party is required to act responsibly to the organization and its stakeholders.”

6. **Fairness:** The systems that exist within the company must be balanced in taking into account all those that have an interest in the company and its future. The rights of various groups have to be acknowledged and respected. For example, minority share owner interests must receive equal consideration to those of the dominant share owner(s).

“All decisions taken, processes used, and their implementation will not be allowed to create unfair advantage to any one particular party.”

7. **Social responsibility:** A well-managed company will be aware of, and respond to, social issues, placing a high priority on ethical standards. A good corporate citizen is increasingly seen as one that is non-discriminatory, non-exploitative, and responsible with regard to environmental and human rights issues. A company is likely to experience indirect economic benefits such as improved productivity and corporate reputation by taking those factors into consideration.

With the emergence of the concept of liberalization, privatization and globalization, an effort is made to design and develop a unique code of corporate governance, worldwide. Further it must be recognized that corporate governance goes far off the boundaries of company law. The quality, quantity and frequency of financial and managerial disclosures, the extent to which the board of directors enforce responsibilities, the quantum of disclosures to shareholders and the methodology to run the business for profit and wealth maximization cannot be tabulated or legislated at any extent of completeness.

Corporate governance is the mechanism required to be followed by the management of the company, which governs the unchallengeable rights of the shareholders as the implicit owners of the corporation and of their own as trustees on the behalf of the shareholder owners.

“There is most intimate connection between decency and good business”.

- Henry Ford

CHAPTER-6

Corporate Governance in India

In India, the eventual purposes of bringing Corporate Governance initiatives are –

- To bring transparency in decision making
- To bring accountability among board members and the top management to safeguard the interest of the stakeholders
- To bring responsibility for good governance.

In India, substantial amount of efforts have been made to bring out the technical and standard corporate governance practice code. Taskforce were set up by Confederation of Indian Industry (CII) in 1996 and final code 'Desirable Corporate Governance Code' was released. Subsequent to this, various commission were formed under the leadership of renowned businessmen like –

- SEBI commission under the chairmanship of Mr. K.M Birla
- MCA (Ministry of Company Affairs) commission headed by Mr. Naresh Chandra
- SEBI committee under the chairmanship of Infosys mentor Mr. Narayana Murthy
- National task force under leadership of Mr. Rahul Bajaj

Above commission, committees and task force made various mandatory and recommendatory recommendations, many of which are being implemented in stages. We try to select a few of them and reproduce as under:

- i. Board of Directors:** There should be an optimum combination of executive and non-executive directors on the board so as to run the business of the company with more transparency and with varied experience. The requirement of keeping more number of non-executive directors on the board is great on road. There must be a limit to which a person should hold directorship in different companies to ensure he afford justice in terms of his time and energy spent on each.

For non-executive directors to play a material role in corporate decision making and maximizing shareholder value, they need to –

- Become active participants on board and not passive advisors
- Have clearly defined responsibilities within the board such as the audit committee
- Financially knowledgeable as to read the balance, profit and loss and the cash flow statement and have some knowledge on company law. But there can be other directors who are from other technical field like engineering, science, technology etc.

For securing best efforts of non-executive directors, companies should:

- Pay commission over and above the sitting fees for use of their professional service.
- Offer stock options, so as to relate rewards to performance. An appropriate mix of commission and stock option can align a non-executive director towards keeping an eye on short term profits as well as a long term value from shareholding.

Discipline from directors must be appropriately ensured. While re-appointing directors on the board, their attendance to the board meetings must be put on record. If a director is absent from majority of the meetings then his re-appointment must be put on hold unless justifiable reasons for the absenteeism are quoted.

There are varied recommendations on appointment of nominee directors. Some said that the nominee director must have same responsibility as other directors, while other questioned their current appointment process itself. According to them, the nominee director must be appointed by the shareholder.

Revised clause 49 of the Sebi listing agreement requires companies to maintain a combination of executive and non-executive directors, in which there must be not less than 50 pct. of the board of directors comprising of non-executive directors. Thus it is clear that focus have been shifted towards independence principle, in governing the policies and procedures of the company.

- ii. **Code of Conduct:** There should be laid down code of conduct for all the board members and senior management of the company. Further, the code of conduct must be properly disseminated to the top management of the organization so that they are made aware of such policy and requirement and thus compliance is assured. The top management must set an example for others to follow at middle and lower level organization. The conduct must prescribe high level of ethical behavior and impart highest punishment for deviation including termination of job.

Companies must promote employees to bring out fearlessly any unethical behavior in the organization including those done by the highest level of management. Such a tool is termed as “Whistle Blower Policy”. It is a tool and an approach for employees to report any discrepancy and fraud about the company’s code of conduct or ethics policy. This mechanism also provide for adequate safeguards for employees against their escalation to the top management and paves direct access to the chairman of the investigation committee or the incident coordinating committee or in some case the audit committee also. Once established, it is important to communicate the mechanism to all levels of the organization. Employees may report a local incident through the system tracking, by use of a toll free number or by approaching the escalation point.

- iii. **Audit Committee:** An independent audit committee plays a vital role in supervising the company’s financial reporting and disclosure process. An audit committee works closely with the management of the company in the accounting and audit related functions. Again, the audit committee must comprise of independent and financial learned persons so that they can oversight the company’s financial performance. The audit committee keeps track of the internal control weaknesses of the company. Further, they regularly interact with the auditors to know the pitfalls in the system.

The taskforce under the chairmanship of Mr. Rahul Bajaj recommended the following in respect of audit committee in Indian companies:

- Listed Companies with either a turnover of Rs.100 crores or a paid - up capital of Rs. 20 crores should set up an audit committee within two years.
- Audit committees should consist of at least 3 members, all drawn from the company’s non-executive directors, who should have adequate knowledge of finance, accounts and basic elements of company law.
- To be effective, the audit committee should have clearly defined Terms of Reference to spend more time on the company’s work vis-à-vis other non-executive directors.

- Audit committees should assist the board in fulfilling its functions relating to corporate accounting and reporting practices, financial and accounting controls and financial statements. The committees should also assist the board on proposals that accompany the public issue of securities and thus provide effective supervision of the financial reporting process.
- Audit committee should periodically interact with the statutory and the internal auditors to ascertain the quality and veracity of company's accounts as well as the capability of the auditors itself.
- For audit committees to discharge their fiduciary responsibilities with due diligence, it must be incumbent upon management to ensure that members of the committee have full access to financial data of the company, its subsidiary and associated companies including data on contingent liability, debt exposure, current liabilities, loans and investments.

Other recommendation by other commissions includes but not limited to the following:

- Majority of the members of the audit committee should be independent directors.
- Chairman of the committee should be an independent director.
- The chairman of the committee should be present at the Annual General Meetings to answer the queries of the shareholders.
- The Company Secretary should also act as the secretary of the committee.
- The committee should meet at least thrice a year. One meeting must be held before finalization of accounts and one necessarily every six months.
- The audit committee should have minimum of following powers:
 - To investigate any activity within its terms of reference
 - To seek information from any employee
 - To obtain outside legal or professional advice
 - To secure attendance of outsiders with relevant expertise, if it is considered necessary.
- A board is responsible for implementing the recommendations of the committee or that it provides justification for non-implementation that is acceptable to the committee.
- The committee must look into the reason for substantial defaults in the payments to the depositors, debenture holders and creditors.
- The committee must review the company's financial and risk management policy.
- The committee must review any findings of any internal investigations by the internal auditors into matters where there is suspected fraud or irregularity or a failure of internal control systems of a material nature and reporting the matter to the board.

- iv. Disclosure and Reporting process:** It must be ensured that change in accounting policies and effectiveness of the internal control systems of the company is reported to the shareholders. The board should disclose all significant events and transactions in their report. Further, in connection to the internal audit function, it is the audit committee that must keep an eye on the recurring instances of deviations and cases of misfeasance as brought to the notice by internal auditor and the same can be taken to the shareholders of the company, if it material and large.

Again, it is the duty of the statutory auditors to make sure that sufficient amount of disclosures have been made and the financial statement depict the '*true and fair view*' of the company's state of affairs.

SEBI committee under the chairmanship of Mr. K.M Birla recommended the following disclosures in the corporate governance section of the annual report:

- All elements of remuneration package of all the directors i.e. salary, benefits, bonuses, stock options, pensions etc.
- Details of fixed component and performance linked incentives, along with the performance criteria.
- Service contracts, notice period, severance fees.
- Stock option details, if any – and whether issued at a discount as well as the period over which accrued and over which exercisable.

Task force formed under Mr. Rahul Bajaj's chairmanship recommended the following compliance certificate to be signed by the CEO/CFO clearly stating that:

- The management is responsible for the preparation, integrity and fair presentation of the financial statements and other information in the annual report, and which also suggest that the company will continue in business in the course of the following year.
- The accounting policies and procedures conform to standard practice and where they do not, full disclosure must be made of any material departures.
- The board has overseen the company's system of accounting and administrative control through its audit committee (for companies with turnover of over Rs. 100 crores or paid up capital more than Rs. 20 crores).

Naresh Chandra's committee report on corporate governance recommended responsibilities on auditors of the company as under:

- Auditors must ensure that the contingent liabilities of the company be disclosed in such a way that investors and shareholders get a clear idea of the significant risk factors that could adversely affect the entity's future health. The committee recommended that management should provide a clear description in plain English of each material liability and its risk, which should be followed by the auditor's clearly worded comments on the management view. This section should be highlighted in the management notes on accounts as well as auditor's report wherever necessary.

- The auditor must ensure that qualification of accounts, if any, must form a distinct, and adequately highlighted section in the auditor's report to the shareholders.
- It is also recommended that the auditor reads out the qualification of the report to the shareholders in the annual general meeting.
- It was proposed to make it mandatory for the audit firm to separately send a copy of the qualified report to the ROC, the SEBI and the principle stock exchange (for listed companies), about the qualifications, with a copy of this letter being sent to the management of the company.

The committee also proposed specific provision in relation to subsidiary.

- It was proposed to have at least one independent director of the Board of Directors of holding company on the board of materially non-listed subsidiary. The word materially non-listed subsidiary is also defined specifically in the report.

CHAPTER-7

Now let us read through the excerpts from sustainability audit report of M/s Infosys Limited for the year 2008-09.

Below is the chairman's message to the shareholders.

The primary purpose of corporate leadership is to create wealth legally and ethically. This translates to bringing a high level of satisfaction to five constituencies - customers, employees, investors, vendors and the society-at-large. The raison d'être of every corporate body is to ensure predictability, sustainability and profitability of revenues year after year.

- N. R. Narayana Murthy
Chairman of the Board and Chief Mentor

Corporate Governance Policies

Corporate governance is a reflection of our culture, policies, our relationship with stakeholders, and our commitment to values. Infosys has been a pioneer in benchmarking its corporate governance practices with the best in the world. The company's policies on corporate governance relate to:

- Board composition
- Board Meetings
- Board committees
- Code of ethics for principal executive & senior financial officers
- Management review and responsibility
- Shareholders
- Code of Business conduct and Ethics

Corporate Governance Report

"Directors and managements must take upon themselves to improve accountability by setting a "tone at the top", honoring the responsibilities that arise from the trust placed in them by investors. All directors and managements should implement their own best practices for corporate governance that promote integrity, transparency and accountability."

Elisse B. Walter, Commissioner, U.S. Securities and Exchange Commission, remarks before the Practicing Law Institute, New York, February 18, 2009

Corporate governance is about commitment to values and ethical business conduct. It is a set of laws, regulations, processes and customs affecting the way a company is directed, administered, controlled or managed. This includes its corporate and other structures, culture, policies and the manner in which it deals with various stakeholders. Some of the important best practices of corporate governance framework are timely and accurate disclosure of information regarding the financial situation, performance, ownership and governance of the Company.

Corporate governance guidelines and best practices have evolved over a period of time. The Cadbury Report on the financial aspects of corporate governance, published in the United Kingdom in 1992, was

a landmark. Over the past decade, various countries have issued recommendations for corporate governance. Compliance with these are generally not mandated by law, although codes that are linked to stock exchanges sometimes have mandatory provisions. The Sarbanes-Oxley Act of 2002 brought about sweeping changes in financial reporting. In India, the Confederation of Indian Industry (CII) took the lead in framing a desirable code of corporate governance in April 1998. This was followed by the recommendations of the Kumar Mangalam Birla Committee on Corporate Governance. The recommendations of the Kumar Mangalam Birla Committee were incorporated as Clause 49 of the Listing Agreement.

Securities and Exchange Board of India (SEBI) instituted a committee under the chairmanship of N. R. Narayana Murthy which recommended enhancements in corporate governance. SEBI incorporated the recommendations made by the Narayana Murthy Committee on Corporate Governance in Clause 49 of the Listing Agreement. The revised Clause 49 has been made effective from January 1, 2006.

Following the recent financial upheaval, the National Association of Software and Service Companies (NASSCOM) is set to focus on good corporate governance and ethics among its member companies. NASSCOM has constituted a Corporate Governance and Ethics Committee headed by N. R. Narayana Murthy.

The objectives of the committee are to strengthen the existing appropriate code of ethics, values and corporate code of conduct for the industry; emphasizing existing regulations and practices on corporate governance and re-drafting and re-affirming appropriate code of ethics, values and corporate code of conduct for the industry. The committee will work with authorities, policy makers and regulators in the areas of corporate governance and transparency.

We believe that sound corporate governance is critical to enhance and retain investor trust. Accordingly, we always seek to ensure that we attain our performance rules with integrity. Our Board exercises its fiduciary responsibilities in the widest sense of the term. Our disclosures always seek to attain the best practices in international corporate governance. We also endeavor to enhance long-term shareholder value and respect minority rights in all our business decisions.

Our corporate governance philosophy is based on the following principles:

1. Satisfy the spirit of the law and not just the letter of the law. Corporate governance standards should go beyond the law
2. Be transparent and maintain a high degree of disclosure levels. When in doubt, disclose
3. Make a clear distinction between personal conveniences and corporate resources
4. Communicate externally, in a truthful manner, about how the Company is run internally
5. Comply with the laws in all the countries in which we operate
6. Have a simple and transparent corporate structure driven solely by business needs
7. Management is the trustee of the shareholders' capital and not the owner.

The Board of Directors is at the core of our corporate governance practice and oversees how the Management serves and protects the long-term interests of all our stakeholders. We believe that an active, well-informed and independent Board is necessary to ensure highest standards of corporate governance.

The majority of our Board, 8 out of 15, are independent members. Further, we have audit, compensation, investor grievance, nominations, and risk management committees, which comprise only independent directors.

Corporate Social Responsibility

At Infosys, the distribution of wealth is as important as its legal and ethical creation. A strong sense of social responsibility is therefore an integral part of our value system.

Infosys Foundation

We are committed to contributing to the society and established Infosys Foundation in 1996 as a not-for-profit trust to support our social initiatives. The Foundation supports programs and organizations devoted to the cause of the destitute, the rural poor, the mentally challenged, and the economically disadvantaged sections of the society.

The Foundation also helps preserve certain cultural forms and dying arts of India. Grants to the Foundation aggregated Rs. 19 crore during the fiscal year 2007, as compared to Rs. 13 crore in the previous year.

Community service

Through our Computers@Classrooms initiative launched in January 1999, we donated 2,567 computers to various institutions across India. Additionally, we have applied to the relevant authorities for permission to donate computers to educational institutions on an ongoing basis in the future. Microsoft Corporation continues to participate in this initiative by donating relevant software. We would like to place on record our appreciation for their continued support.

Social commitment in education

Infosys' Education & Research group has the pride of anchoring the Infosys Extension Program (IEP), which consists of the Infosys Fellowship Program, Rural Reach program, Catch Them Young and Train the Trainer.

End of Infosys sustainability report

Conclusion: To conclude, it can be conceived that corporate governance is a global concept; it is applicable to all countries and to all corporate working in the globe. Even after several attempts to device a unique corporate governance practice, it is found that the governance is majorly dependant upon the

background of the management personnel, their past tracks, integrity of other top officials of the company, level of internal control compliance, independence of auditors and their competency and various other factors.

“Governance is as effective as its management”

CHAPTER-8

Information Technology risks

As information technology (IT) increasingly falls within the scope of corporate governance, management must increasingly focus on the management of risk to the achievement of its business objectives. In current scenario, companies businesses are wide spread across continents with customers and vendors hugely distributed. Thus investment in information technology is inevitable. In fact, large business houses have developed their own IT division to cater to their business needs.

Managing Risk in Information Technology

IT systems usually represent significant investments of financial and executive resources. The manner in which they are planned, managed and measured should therefore be a key management accountability, in the way similar to which risks associated with information assets themselves are managed. Clearly, well managed information technology is a business enabler. Every deployment of information technology brings with it immediate risks to the organization and, therefore, every director or executive who deploys, or manager who makes any use of, information technology needs to understand these risks and the steps that should be taken to counter them. Risks in Information Technology can be broadly divided into the following:

- 1) **Hardware Acquisition Risk:** There are five main phases in hardware acquisition process viz. Planning, Acquisition, Implementation, Selection, Operation and Maintenance and Disposal. These have been discussed below:
 - i. **Planning Phase:** This phase consists of identification of a demand or requirement, specification formulation to match the requirement, overview of the resources and the budget that could be allocated to purchase hardware, cost – benefit analysis and issue of purchase requisition.
 - ii. **Acquisition and requirement analysis:** This phase includes the requirement analysis, analysis of alternatives, invitation to tender, receipt and comparative analysis of proposals, selection of the vendor and placement of the order. Requirement analysis involves consideration regarding hardware component specification, criticality of the hardware including its cost, reliability of the equipment and availability of use in terms of system downtime and maintenance.
 - iii. **Hardware selection** involves consideration regarding price, performance, network instruction per second, delivery schedules, hardware upgradeability, environmental requirements, Hardware compatibility, maintenance agreement with vendor, configuration flexibility, availability of user documentation, availability of repair facility etc.
 - iv. **Implementation** phase begins after awarding the contract a vendor and includes all procedures such as inspection, installation, trial run, interface testing and resultant fully operational system. Process should be established by the organization to document vendor response time, equipment downtime and vendor performance.
 - v. **Operation and maintenance** phase consists of tasks to keep the hardware functional and to maintain an optimum uptime. This phase commences once the installation is complete. Proper procedures and schedules have to be maintained by the organization documenting the causes of equipment failures, downtime, repair details and frequency of negative responses.

- vi. **Disposal of equipment:** This phase starts at the end of life of the hardware and consists of all step required to dispose off the equipment that is no longer required for its original purpose. It is important to ensure that all equipment containing sensitive information in storage media are checked prior to disposal. Also to ensure effectiveness, risk assessment must be performed on the damaged equipment to determine if it should be destroyed, repaired or discarded. The process of destruction and discarding must be defined.
- 2) **Hardware Security Risk:** The main aim of hardware security is to prevent loss, damage and compromise of information assets as well as to prevent interruption to business activities. Equipment should be physically security threats and environmental hazards. Equipment should be sited and protected to reduce the risk from environmental threats and hazards and opportunities for unauthorized access. Following key issues may be noted:
- i. Equipment should be sited to minimize unnecessary access into work area.
 - ii. Information processing and storage facility handling sensitive data should be positioned to reduce risk of over-looking during their use.
 - iii. Items requiring special protection should be isolated to reduce the general level of protection required.
 - iv. Controls should be adopted to minimize the risk of potential threats including theft, fire, explosives, smoke, water, dust, vibrations, chemical effects, electrical supply interference and electromagnetic radiations.
 - v. Eating, drinking and smoking near information processing facilities should be prohibited.
 - vi. Environmental conditions should be monitored for conditions which could adversely impact the information processing function.
 - vii. The impact of disaster happening in the nearby premises, e.g. a fire in the neighboring building, water leakage from the floor above, etc. should be considered.

Following guidelines are to be considered in regards to management of removal media:

- i. No media should be used without authorization.
- ii. Erase previous contents of any re-usable media if it is no longer required.
- iii. Authorization should be required for all media removed from the organization and a record of all such removals should be maintained as an audit trail.
- iv. All media should be stored in a safe and secure environment.
- v. Disposal of sensitive items should be logged.
- vi. Back-ups should be carried to an off – site secured place.
- vii. System document should be stored securely and access to it should be restricted and logged.

3) **Software Security Risk:** The proliferation of increasingly complex, sophisticated and global threats to information security, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is driving organizations to take a more strategic view of information security. Software security may be managed through five major controls as described below:-

- i. **Access Control:** In regards to access control following aspects must be taken care of :-
 - a) **User access management** – Formal procedures should be in place to control the allocation of access rights to information assets. Entire life - cycle of user access from registration to de-registration must be formalized.
 - b) **Privilege management** – The allocation and use of privileges should be restricted and controlled. Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process.
 - c) **User password management** – Passwords are the most common means of identification and authentication to system resources. Password must be policy driven to ensure there is restriction on sharing, periodic change, storage etc. Other techniques like biometric identification, hardware tokens etc should be considered if appropriate, in addition to or in lieu of password based access.
 - d) **Network access control** – Persons having access to network must be sensitized on compromise of the security of these network services. Appropriate controls must be in place wherever there are interfaces between internal and external networks. Wherever deemed appropriate equipment identification may be enforced in addition to user identification.
 - e) **Operating system access control** – This control is used to restrict access to computer resources. These controls should be capable of recognizing and verifying identity of users and identity of terminal or location. It should also have capability of recording failed system access attempts, providing appropriate means of authentication in case password management system is used, ensuring quality passwords and where appropriate restrict connection time of users.
 - f) **Terminal log-on procedures** – Access to information services should be attainable through a secure log-on process that minimizes the opportunity for unauthorized access. The log-on procedure should disclose minimum of information about the system and authentication procedure, in order to avoid providing unauthorized user with unnecessary assistance.
 - g) **User identification and authentication** – All users, irrespective of functions performed, should have a unique identifier (user id) for their sole use so that accountability for transactions can be established.
 - h) **Use of system utilities** – Most computer installations have one or more system utility programs capable of overriding system and application controls. It is imperative that their use is restricted and tightly controlled.

- i) **Terminal time out** – Inactive terminal, especially those in high risk locations and application outside the organization's security management should be designed to shut down after a defined period of inactivity. The time out facility should clear the terminal screen and close both application and network sessions after a defined period of inactivity. This reduces the window of opportunity for unauthorized access.
 - j) **Application access control:** Access to application must be restricted to authorized users only. This can be ensured by controlling user access in line with policy, access based on need to know basis, complying with separation of duties (SOD) matrix, additional controls wherever resources are shared with other systems.
 - k) **Sensitive system isolation:** Sensitive system may require a dedicated and isolated computing environment, depending on sensitivity of the function or information. Sensitive application may even run on a dedicated system and may share resources only with trusted application.
- ii. **Operational controls:** These are mainly integrated within the domain of application control. The controls and techniques that are often used include the following:
- a) **Computer matching** – Computer matching can be effective as a control for accuracy of the input and processing for only those elements that are matched by the program.
 - b) **Batch totals** – Under this control, agreement of manually established batch totals can ensure the accuracy of input, processing and output.
 - c) **Checking of detailed reports** – This control involves checking of data with original input documents.
 - d) **Reasonableness check** – These are checks to verify whether the input falls within the predetermined parameters.
 - e) **Dependency checks** – This control checks if two or more data elements bear the correct logical relationship. This will help to ensuring correct processing.
 - f) **Existence checks** – This input control checks whether data codes entered agrees with valid codes used by the system.
 - g) **Format checks** – This control checks the format of the input against that defined in the application (only numeric / alpha numeric etc)
 - h) **Range checks** – This input and output control checks if the value falls within the predefined range.
 - i) **Audit Trail** – This is a sub-system that includes the origin, contents and timing of data and instructions entered into the application system. It also helps fix accountability on the users by providing the log in information include unsuccessful attempts.
 - j) **Exception Reports** – This control involves the computer system examining data on both master and transaction file to report items that appear incorrect or out-of-date. This includes both input and access controls.

- iii. **Protection against malicious software:** Organization must ensure the following controls in respect to software:-
 - a) Formal policy for compliance with software licenses and prohibiting use of any unauthorized software.
 - b) Formal policy to protect against risk associated with obtaining files and software from or via external networks, magnetic media or on any other medium, indicating what protective measures should be taken.
 - c) Installation, regular updation and use of anti-virus software.
 - d) Conducting regular reviews to identify presence of any unapproved software on user desktops.
 - e) Management procedures and responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks.
 - f) Appropriate business continuity plan for recovering from virus attacks, including recovery of data, software and system.
 - g) Procedure to update users about new malicious software and steps to be taken to prevent them.

- iv. **Information Back up:** Adequate back-up facilities must be in place to ensure that all essential business information, software and system can be recovered following a disaster or media failure. Ideally three generations or cycles of back-up information should be retained and back-up media should have appropriate level of physical and environmental protection. The restoration procedure must be regularly checked and tested to ensure that they can be completed within the time allotted in the operational procedures for recovery. Retention period for business information and requirement for archiving should be identified.

- v. **Operator log:** Operational staff should maintain a log of their activities. The log must generally include-
 - a) System starting and finishing time
 - b) System errors and corrective actions taken
 - c) Confirmation of the correct handling of data files and computer output.
 - d) The name of the person making the log entry.

- 4) **Business Disruption Risk:** IT must be managed systematically to support the organization in achieving its business objectives, or it will disrupt business processes and undermine business activity. IT management, of course, has its own processes - and many of these processes are common across organizations of all sizes and in many sectors. Processes deployed to manage the IT organizations itself need both to be effective and to ensure that the IT organization delivers against business needs. The Business Continuity and Disaster Recovery process in an organization may be divided over four broad sections:

The Business Continuity and Disaster Recovery process in an organization may be divided into four broad sections:

- i. **Business Impact Analysis:** It is the process of identifying the critical business functions and the losses and effects if these functions are not available. The key questions to be answered for assessment of impact and varied requirements of recovery are:-

Impact assessment

- a) How vital the function is to the overall business strategy?
- b) How long the function could be inoperative without any impact or losses?
- c) What is the operational impact on other activities of the business?
- d) What is the revenue loss due to the outage and what is the cost of quickest resumption?
- e) Whether the outage of the activity results in non-compliance of any statutory / legal requirement or violation of service level agreement or any other contractual / legal impact?
- f) Whether there is any effect on customer satisfaction?
- g) Whether it affects in industry ranking – loss of competitive edge?
- h) Whether there is any loss of future sales – opportunity loss?
- i) What is the length of the maximum permissible outage?

Recovery requirements

- a) What the resource and records requirement would be to continue the function?
- b) What is the bare minimum resource requirement?
- c) What is the source of the resource requirement and how many of it is external?
- d) What are the dependant functions and what is the level of dependency?
- e) What the backup needs would be?
- f) What is the lag time involved to recreate the data from the back-ups?
- g) What verifications are needed for recovering without a test environment?

ii. **Incident analysis:** An incident is an attack against a system that poses a clear threat to continuation of the organization's activity. Incidents will be generally, though not universally, recognized by presence of some indicators. The classification may include, but are not limited to the following:

a) Possible indicators of incidents:

- Presence of unfamiliar files
- Unknown programs or processes
- Unusual consumption of resources
- Unusual power failure

b) Probable indicators of incidents:

- Activities at unexpected times
- Presence of new accounts
- Reported attacks
- Repeated tripping of power line

c) Definite indicators of incidents:

- Use of Dormant accounts
- Changes to logs
- Presence of hacker tools
- Cracks in premises walls

d) Predefined situations that signal an automatic incident:

- Loss of availability
- Loss of integrity
- Loss of confidentiality
- Violation of policy
- Violation of law

iii. **Disaster Recovery Plan:** Disaster recovery is the ability to respond to an interruption in services by implementing a plan to restore an organization's critical business functions. The disaster recovery plan must cover the following areas:-

- a) Define the conditions for activating the plans which describe the process to be followed before each plan is activated.
- b) Emergency procedures which describe the actions to be taken following an incident which jeopardizes business operation and/or human life.
- c) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations and to bring business process back into operation in the required time scale.

- d) Resumption procedures which describe the actions to be taken to return to normal business operations.
- e) A maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan.
- f) Awareness and education activities which are designed to create an understanding of the business continuity process and ensure business continues to be effective.
- g) The responsibilities of individuals describing who is responsible for executing which component of the plan.
- h) Detailed description of the purpose and scope of the plan.
- i) Contingency plan testing and recovery procedure.
- j) List of vendors of the company and their contact numbers for emergency purpose.
- k) Inventory taking checklist and updating the contingency plan on a regular basis.
- l) Medical procedure to be followed in case of injury.
- m) Employee contact list in case of emergency.
- n) Insurance papers and claim forms.
- o) Primary computer center hardware, software, peripheral equipment and software configuration.
- p) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- q) Alternate manual procedures to be followed.
- r) Details of airlines, hotels and transport arrangements.

iv. **Business Continuity Plan:** The strategy on Business Continuity Plan should include the following:

- a) **Prevention** aims at reducing the chances of occurrence of disaster.
- b) **Response** is the reaction when the event occurs. It must curtail further damage, assess the extent of damage, salvage the business entity's reputation by providing appropriate communication to the external world and indicate a possible recovery timeframe.

- c) **Resumption** involves resuming only the time sensitive business processes, either immediately after the interruption or after the soon thereafter. All operation may not be fully recovered at this stage.
 - d) **Recovery** addresses the start-up of less sensitive processes. The time duration of this naturally depends upon the time taken for the time sensitive functions. It can also be proposed to start these activities at an alternate location.
 - e) **Restoration** is the process of repairing and restoring the primary site. At the end of this, the business operations are resumed in totality from the original site or a completely new site, in case of catastrophic disaster.
- 5) **Regulatory and Compliance Risk:** All organizations are subject to a range of information-related national and international legislation and regulatory requirements. These range from broad corporate governance guidelines to the detailed requirements of specific regulations. Those organizations with US operations may also be subject to US regulations such as [Sarbanes Oxley](#) and SEC regulations, as well as sectoral regulation such as HIPAA, USA Patriot Act etc. Most organizations are possibly also subject to US state laws that appear to have wider applicability. Compliance depends as much on information security as on IT processes and services.

In India the “Information Technology Act, 2000” provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “Electronic Commerce”.

The above IT Act, 2000 recognizes the following offences:

- a) Tampering with computer source documents
- b) Hacking with computer system
- c) Punishment for sending offensive messages
- d) Dishonestly receiving stolen computer resource or communication device
- e) Identity theft
- f) Personating
- g) Violation of privacy rights
- h) Cyber Terrorism
- i) Publishing of information which is obscene in electronic form
- j) Publishing of material containing sexually explicit act

CHAPTER-9

Problem Solving and Quality Control – the 6 sigma way

Six Sigma was formalized in the mid- 1980s at Motorola. New theories and ideas were combined with basic principles and statistical methods that had existed in quality engineering circles for decades. The result was a staggering increase in the levels of quality for several Motorola products. Many other corporations replicated Motorola Six Sigma strategy to reap huge benefits and growth in their businesses.

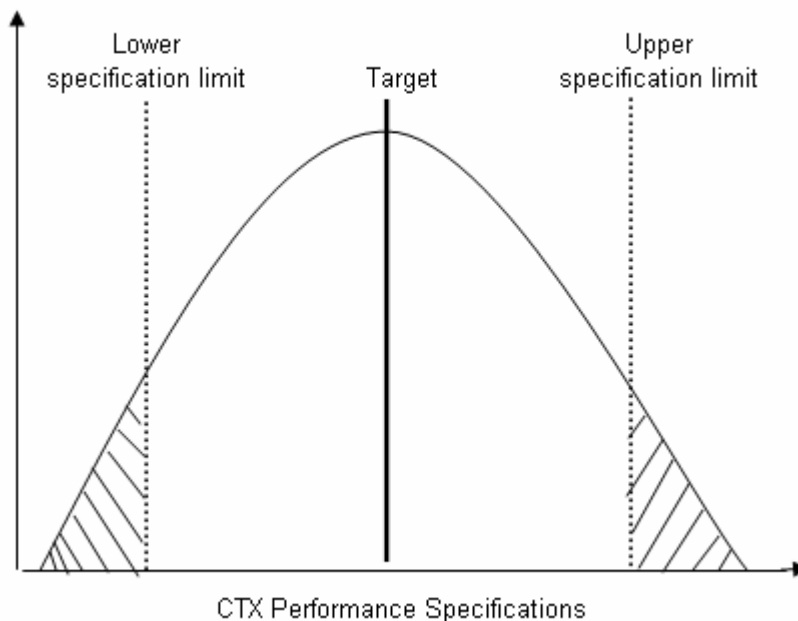
Six - Sigma became the global standard of quality business practice, embraced by the American Society for Quality. Six Sigma strategy works under the basic fundamental assumption of Cause and effect relationship and is represented by following simple equation –
 $Y = f(x)$

Where, Y represents the effect that is a function of several causes represented by the x.

In Six Sigma, important characteristics are referred to as CTX's, where C stands for 'Critical' and X's stands for key characteristics viz. Quality, Cost, Time and Satisfaction and so on. Implementation of Six Sigma methodology leads towards reduction of variation in the process. This ensures achievement of objectives of maximization profit at least costs.

Henry Ford knew about variation nearly a decade ago when he was mass producing his model T cars. He acclaimed that there is variation in everything we do, and all the car parts would vary in their CTX dimensions. He incorporated specifications and standards into his business in order to reduce these variations. By doing so, he could accept the inevitable presence of variations while not ignoring its tendency to create defects and cause business loss.

Variation is represented graphically as under:



Assume following example:

Pizza shop asks its employees to apply 7 to 9 ounces of cheese on each pizza. Its goal is 8 ounce. Applying cheese below 7 ounces will lead to an unsatisfied customer and over 9 ounces would be a bad profit proposition.

Six Sigma is driven by data. One of the commonly used methodologies in Six Sigma is DMAIC – Define, Measure, Analyze, Improve and Control. DMAIC is a formalized problem solving process. The DMAIC can improve any type of process in any organization to improve its efficiency and effectiveness.

Define phase set the context and objective for the project.

Measure phase sets the baseline performance and capability of the process or system being improved.

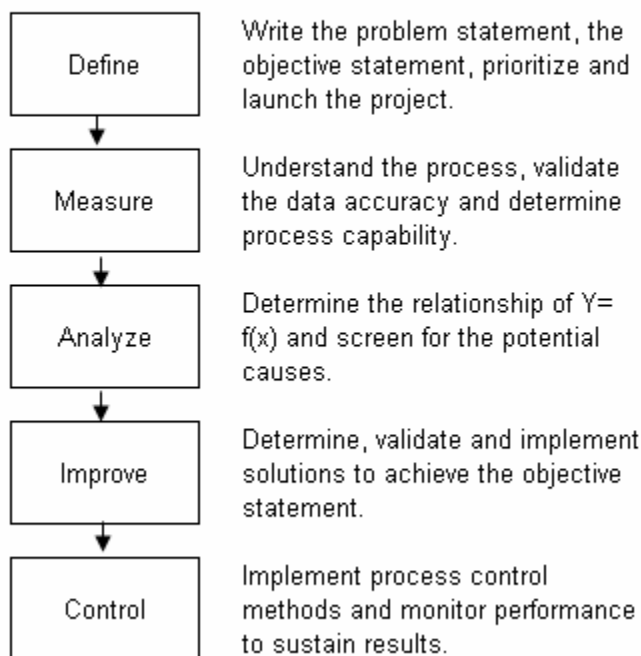
Analyze phase uses data and tools to understand the cause and effect relationship in the process or system.

Improve phase develops the modifications that lead to a validated improvement in the process or system.

Control phase establishes plans and procedures to ensure that the improvements are sustained.

In DMAIC, business processes are improved by following a structured method with set steps, or tollgates. Only as one step is complete, the next can be started.

DMAIC improvement methodology



Conclusion:

Six Sigma is a collection of several mathematical, statistical and quality tools to improve performance of a process. Being driven by data, this is a very dynamic and largely adopted tool for problem solving.