CHAPTER 5

CA AKHIL MITTAL

RISK ASSESMENT METHODOLOGIES AND APLLICATIONS

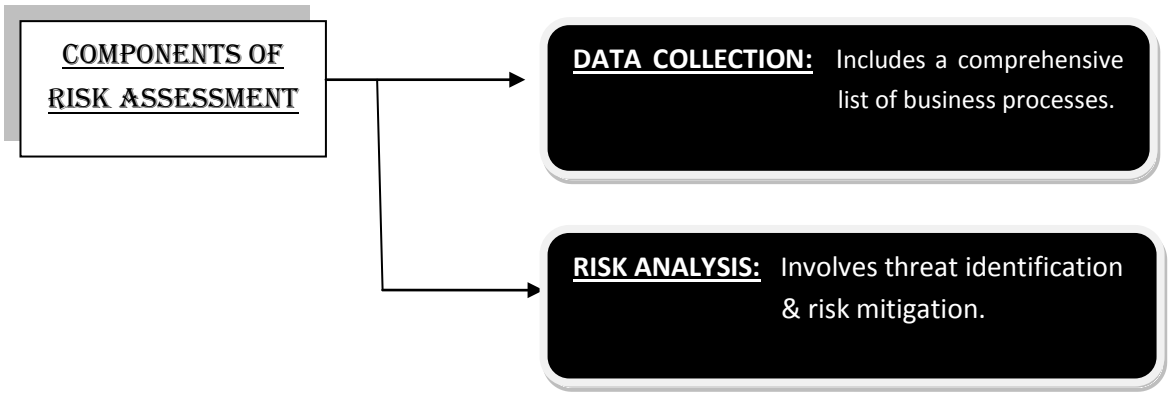
E-MAIL : caakhil24.srcc@gmail.com

CHAPTER 5

RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

A. RISK ASSESSMENT:

- Seeks to identify which business processes & resources are critical to business,
- What threats or exposure exists that can cause **unplanned interruption** of business processes.



B. RISK,THREATS, EXPOSURE & VULNERABILITY:

RISK:

-- It is **likelihood** that an organisation would face vulnerability becoming harmful.

-- These risk creates gap between **need to protect system & degree of protection** applied.

-- The gap is caused by:

CODE TO REMEMBER: **D.I.E.T.**

-> Devolution of management & control

-> Interconnectivity of systems

-> Elimination of distance, time and space as constraints

-> Technology usage is more

THREAT:

-- It is an action, event or condition **where there is compromise** in the **quality and ability** to harm the organisation.

-- It is a circumstance with the potential to cause harm to an **information system** of the organisation.

VULNERABILITY:

-- It is the **weakness** in the system safeguard that **exposes** system to **THREATS.**

-- For instance, **vulnerability** may be **poor access control system** allowing the personnel to alter/modify the records.

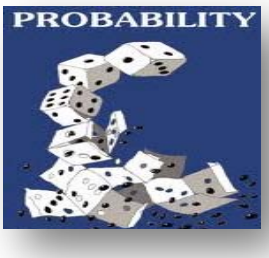
EXPOSURE:

-- It is the **extent of the loss** to the organisation when a **risk materialised (occurs).**

-- For instance, **loss of business, loss of reputation, violation of the privacy etc.**

LIKELIHOOD:

-- It is the **estimation** of **probability** that **threat will succeed** in **achieving** undesirable threat.



ATTACK:

-- It is the set of action **designed to** compromise **confidentiality, integrity & availability** of an information system.

-- **RESIDUAL RISK:** Any risk remaining after the **counter measures** are analysed & implemented.

C. THREATS TO THE COMPUTERISED ENVIRONMENT:

Any type of computerised environment depends upon the people. Threats are therefore likely to arise if there is dependency on **external agencies** for maintaining **IT assets.**

IT computing services depends on various vendors & service vendors. A few common threats to the computerised environment are:

FOR BETTER UNDERSTANDING I AM HERE BY DIVIDING THE THREATS INTO 3 CATEGORIES:

POINTS	EXPLANATION
TECHNOLOGICAL REASONS (C.M.-P.E.T.) [chief minister ka PET]	
Communication Failures	In case of communication failure, an organisation will not be able to transfer data. In case an enterprise **depends on PUBLIC communication lines, such** failure will have **direct** impact on their operations.
Malicious Code	Malicious code **i.e. computer viruses, worms** may affect the **organisation & business network.**
Power Failure	Power failure can cause **disruption of ENTIRE computer equipments as these depend on POWER SUPPLY.**
Errors	Errors may result from technical reason or negligence. For instance, **while communicating with outside network it might possible that certain parameters** to be **"DENIED"** but are **"ALLOW"** then organisation network is more prone to **attacks.**

Technological Failure	Information technology facilities might be unavailable due to technological failure. Due to such failure, the infrastructure may not be available for working. This **downtime** considerably affects the **critical business processes.**
TECHNOLOGICAL REASONS : P.A.D.	
Power Failure	Power failure can cause **disruption of ENTIRE computer equipments as these depend on POWER SUPPLY.**
Abuse of access privilege by employees	Company may provide **privileges** to its employees **to access & execute** applications. However it might be possible that they take **undue advantage**
Dissatisfied Employees	A dissatisfied customer may turn into threat for the organisation since it may have access to **critical/sensitive information.**

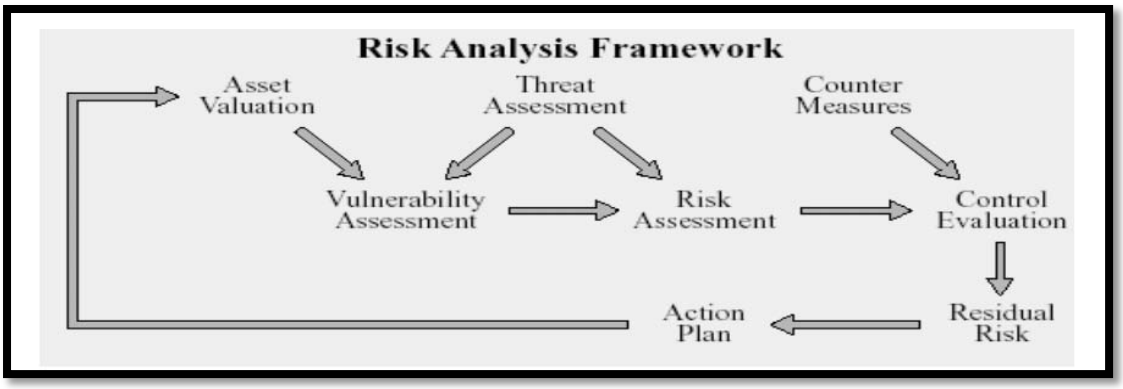
D. THREATS DUE TO CYBER CRIME:

POINTS	EXPLANATION
CODE TO REMEMBER : S.O.F.T. - D.E.V.	
Sabotage	It is deliberate **damage, alteration or modifications** of **electronic files, data, web pages and programs**
Other	This includes several reasons **i.e. intrusion, breaches, compromise of respondent's computer network.**
Fraud	It occurs when there is **intentional misrepresentation of information** in order to **deceive others.**
Theft	It refers to **illegal obtaining of :** **-- Designs, plan, blueprints** **-- codes, formulas, trade secrets etc.**
Denial of Services	There can be disruption of services **due to dependency of** EXTERNAL INFRASTRUCTURE. Denial of service is caused by **ping attacks, excessive incoming data etc.**
Embezzlement	It is **unlawful representation of money,** by the person to whom the same thing was entrusted.

Virus	A computer virus **is computer program that can copy itself & infect a computer without the** knowledge of the UESERS.

E. RISK ASSESSMENT:

- It serves as **FOUNDATION FOR AVOIDING OF DISASTERS.**
- Through **risk analysis,** it is possible to **identify, assess & mitigate** risk.
- Following is the **risk analysis framework**



Some more details on RISK ASSESSMENT:

¥ It is analysis of **THREATS** to resources & determining **amount of protection** needed to **adequately safeguard the RESOURCES.**

¥ Risk assessment is useful technique to **assess risk involved in :**

- Unavailability of information.
- Identify exposures & develop recovery procedures

¥ Areas to be focussed upon:

CODE TO REMEMBER: P.C. - I.R.I. - E.D.

Police **C**ome ----- **I R**un **I** ----- **E**xcise **D**uty

A. Prioritisation:

- All applications which are critical are to be identified.
- Each critical application is reviewed to assess IMPACT on organisation
- This helps in developing appropriate recovery plan.

B. Critical application identification:

- Amongst the applications, critical applications identified.
- Further analysis is done to point out CRITICAL specific jobs

C. Impact assessing:

- Business continuity plan must also focus on the other functions together with the business disruption.
- Areas to be considered:
  - A. Legal liabilities
  - B. Interruption of customer services
  - C. Possible Losses
  - D. Likelihood of fraud/ recovery procedures.

D. Recovery time determination:

- Critical Recovery time = Time in which business processing must resumed.
- This critical time depends upon NATURE OF OPERATIONS.
- Involves involvement of END USERS to determine critical functions & their recovery time period.

E. Insurance coverage:

- Information system policy must be MULTI-PERIL policy,
- i.e. must provide various types of coverage.
- List is as follows:

Hardware

The equipments should be covered adequately. Provision to be made for the replacement of the equipments.

Errors & Omission

This covers **liability arising out of ERROR & OMISSION** committed by **System analyst, programmers & other personnel.**

 **Software Reconstruction**	 **Fidelity Insurance**
It includes **programming cost** for **recreating the software** is to be covered.	This covers **act of the employees,** in case where own computers are used to provide service to **clients.**
 **Extra Expense**	**Media Transport**
This cost **includes COST FOR continuing the OPERTIONS** till **original** facility is **restored.**	Potential **damage to MEDIA** while bring **transported to OFF SITE** storage premises.
 **Business Interruption**	 **Valuable papers & records**
This applies to entity performing OUTSOURCED JOBS OF CLIENTS.	The **actual cost of VALUABLE PAPERS & RECORDS** stored in insured premises.

F. Exposure identification:

- It is not possible to precisely estimate the occurrence of DISASTER,
- So it needs some estimation of occurrence.

G. Development of recovery plan:

- The plan should be designed to provide for RECOVERY from total destruction.

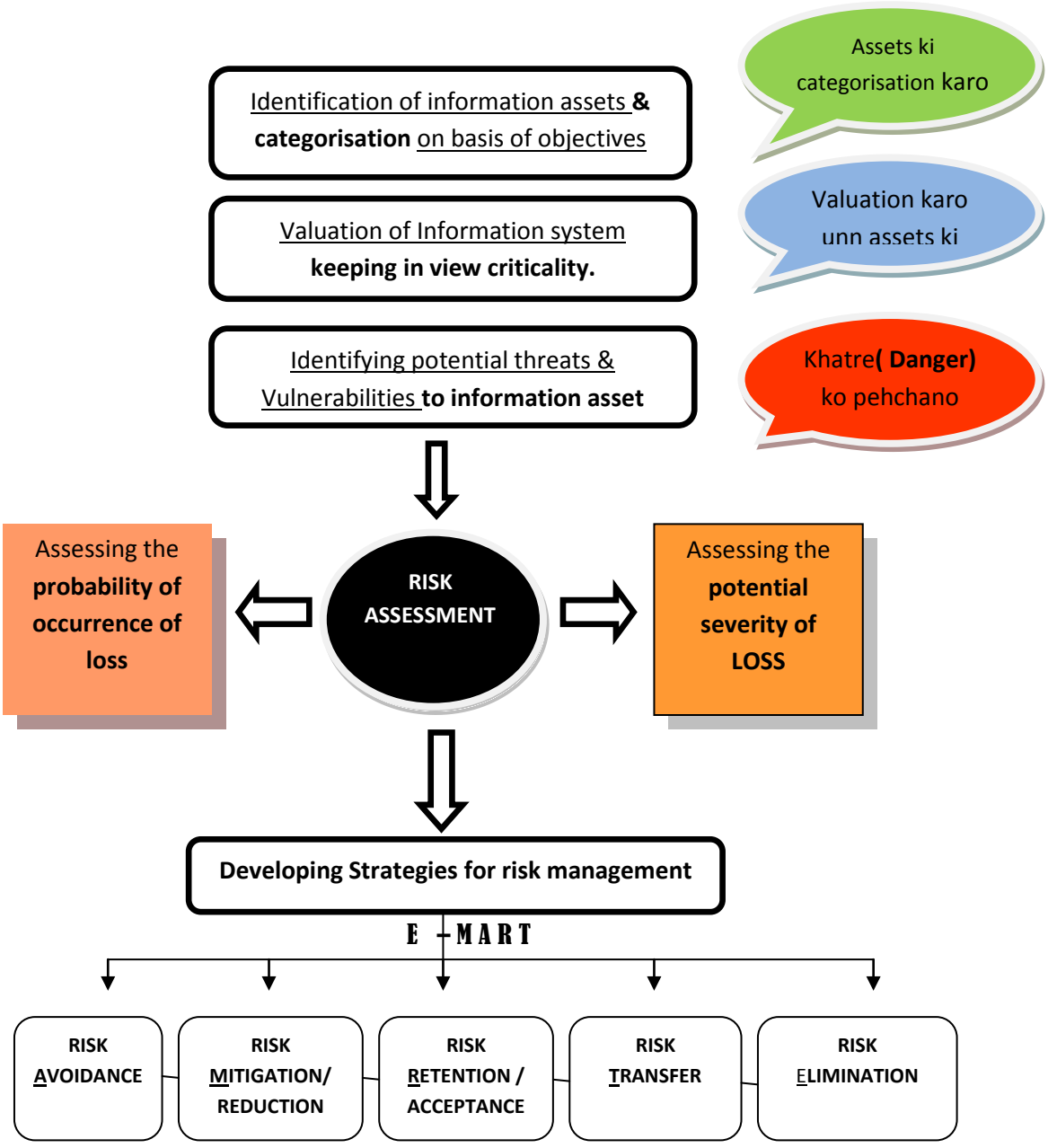
F. RISK MANAGEMENT:

CLASSIFICATION OF RISK = SYSTEMATIC RISK + UNSYSTEMATIC RISK

I AM HEREBY EXPALINING THE DIFFERENCE BETWEEN THE SYSTEMATIC & UNSYSTEMATIC RISK

Basis Of Difference	Systematic Risk	Unsystematic Risk
Definition	These are un**avoidable risk.**	These are **avoidable risk.**
Example	Probability of power cut is not dependant on type of industry.	One can use computer system with automatic mirroring to reduce exposure of data.
Effect of Technology	Systematic risks would remain **same** no matter what the **technology** is.	This risk can be mitigated by **using an advanced technology or system.**

G. RISK MANAGEMENT PROCESS:

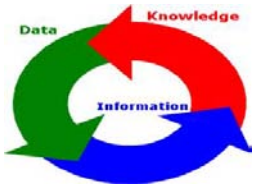


Now explaining each step in detail as follows:

STEP 1: IDENTIFIACTION OF INFORMATION ASSETS

- First step is to identify **information assets** supporting **critical business operations** that need to be protected.
- The asset could fall in the following categories:

CONCEPTUAL/INTANGIBLE ASSETS



Business & related information **contained in various STORAGE devices** must be protected from **unauthorised access, theft, damage etc.**

Application & system software are **prone to intentional/ unintentional** modifications by **person**

PHYSICAL/TANGIBLE ASSETS

PEOPLE

Skilled users, analyst, programmers

Hardware, microcomputers printers, storage media etc

HARDWARE

Documentation

Printed forms, manuals, system & data base documentation

Communication lines, hubs, switches etc

Networking Devices

STEP 2: VALUATION OF INFORMATION ASSETS

- Not all data of the organisation has **same value.**
- Data which is used for making **strategic decisions because** it aids them in making **long/short term decisions.**

- Loss of such information **effects the organisation badly.**
- Information can be classified into following:

A. TOP SECRET:

- This indicates **highest classification,**
- Wherein any compromise with this information **can endanger existence of the organisation.**

B. SECRET:

- Information in this category is **STRATEGIC** to the survival of the organisation.
- Unauthorised disclosure may cause **damage to stakeholders & organisation.**

C. CONFIDENTIAL:

- Information in this category needs **high level of protection.**
- Unauthorised disclosure may cause **significant damage.**
- Such information is highly **sensitive & to be protected.**

D. SENSITIVE:

- Information requires **higher protection** than others.
- Disclosure **may cause serious impact on organisation.**

E. UNCLASSIFIED:

- Contains information that doesn't fall in other class.
- Unauthorised access of such information would not cause **any adverse impact on the organisation.**

STEP 3: IDENTIFYING POTENTIAL THREATS

THREATS = **It is the event that contributes to the INTERRUPTION** of any service, product or process. Common classes of threats:

ERRORS

MALICIOUS DAMAGE

FRAUD

THEFT

EQUIPMENT FAILURE

VULNRABILITIES= **It is characteristic of information resources** that can be exploited **by a threat to cause harm.** Examples of vulnerabilities:

-- **Lack of user knowledge** -- **Poor choice of password**

-- **Lack of security functionality** -- **Untested Technology**

Computer systems are prone to threats & vulnerabilities. These can cause damage to computer database. These threats affect confidentiality, integrity & availability of the system information.

C.I.A.

CONFIDENTIALITY:

It involves **protection of organisation's sensitive information** from disclosure to unauthorised access.

Given the type of exposure that may damage the confidentiality of the information:

- **Improper application controls in application software** e.g. **payroll personnel may get access to confidential data about salary of people of management.**
- **Unauthorised disclosure of data because of access of confidential data.**

INTEGRITY:

Requires that the business **information & related processes** should not suffer any **unauthorised access.**

Integrity of information may be affected due **to system errors** i.e. **power failure, virus** etc. A few examples of threats are here as under:

- **Computer virus may disrupt the DATA/PROGRAM.**
- **Bank employee tampering the data files by changing application controls.**

AVAILABILITY:

Refers to **whether the INFORMATION** and **information technology** processes are available to **unauthorised** business users when required.

Availability requires **safeguarding** the information system. A few example of exposure given below:

- **Improper functioning of power system can lead to de-functionality of system.**
- **Improper capacity availability such as** low computer resources, bandwidth etc.

STEP 4: INFROMATION RISK ASSESSMENT

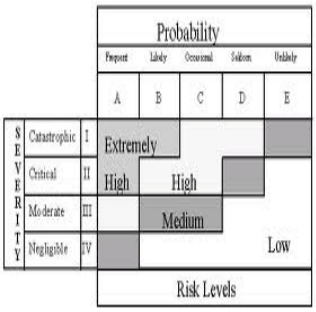
Once the assets & its corresponding threats are identified, **now weaknesses in the** system are reviewed.

Following type of assessment can be performed. The same is as follow:

VULNERABILITY ASSESSMENT:

- It is weakness in the safeguards, technical or physical controls,
- That can be exploited by the threats.
- For example: **Hackers may find out a loophole in architecture of firewall of an organisation.**

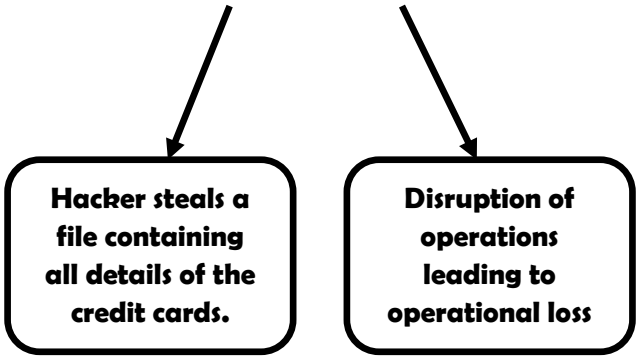
PROBABILITY OR LIKELIHOOD ASSESSMENT:



- It is the estimation of **frequency, or chance of threat happens.**
- **LIKELIHOOD ASSESSMENT: Consider presence, strength of threats etc.**
- Some threats affect **data especially** threats to physical assets.
- Nature & value of information assets **affects likelihood of occurrence of a threat.**
- Likelihood of occurrence of a threat needs to be reassessed **due to change in structure, direction & environment** of the organisation.

IMPACT ANAYSIS:

- Threat that is successful in causing harm, **results in an IMPACT.**
- **IMAPCT =** Monetary + Non Monetary



STEP 5: DEVELOPING STRATEGIES FOR INFORMATION RISK NAMAGEMENT

Once risks are assessed, next step is to make **appropriate corrections.** Proper process is to be undertaken to recognise these risks.

CODE TO REMEMBER: M.A.R.T.

A. Risk **M**itigation:

-- It involves implementing **controls to protect IT infrastructure.**

-- To reduce the severity of losses. For e.g. **Anti-virus to protect from virus.**

B. Risk **A**voidance:

-- It means **not doing an activity that involves RISK.**

-- It involves **losing gain** if the activity involving **risk** is accepted.

-- For example using **standalone computers** instead of using **intranet.**

C. Risk **R**etention:

--It means **formally acknowledging that RISK exists &** monitoring it.

--Risk management **aims at identifying, selecting & implementing** controls to reduce the **residual exposure** (Risk that retains by default after all controls are implemented)

D. Risk **T**ransfer:

-- It involves causing **another party to ACCEPT the risk.**

-- It means **sharing risk with partners, insurance coverage** etc.

H. UNDERSTANDING RELATION BETWEEN IT RISK & CONTROLS:

If the IT controls are weak & not appropriate, then **risk may prove to be a GREAT THREAT** to information system.

Control is a **check on a system which is designed to enhance its security.** Controls are implemented to do the following:

I am hereby trying to link all the points together

KOSHISH KARI KI THREAT NO HO

- Reducing a threat.
- Reducing vulnerability to a threat.

THREAT NE SYSTEM KO AFFECT KAR DIYA, SO

- Reduce the impact of the threat.
- Detect impact.

THREAT KA IMAPCT HO GYA, SO

- Recovery from the impact.

Some points on risks & IT controls:

MANAGEMENT DUTY IN RESPECT OF REDUCING RISK

→Objective of IT controls is to **prevent the threats** from -- **exploiting** vulnerabilities **(weakness in the system)** – of the assets.

→ If controls are enable to prevent threats from being happen, **then controls must ensure TIMELY DETECTION,** so correction action van be taken.

AUDITOR DUTY IN RESPECT OF REDUCING RISK

→IS must understand relationship between **RISK & IT CONTROL.** He must be thorough with the process & procedures of evaluating the controls.

→ IS auditor must evaluate whether the controls are **adequate & appropriate.**

→ In case of any weaknesses found in the controls, **auditor must report to the management** along with **appropriate recommendations.**

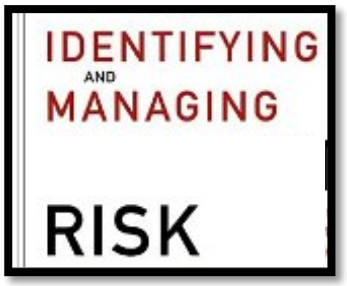
→ Auditor must also do **COST BENEFIT** analysis of the controls. Following principle must be followed in determining the **use of new controls:**

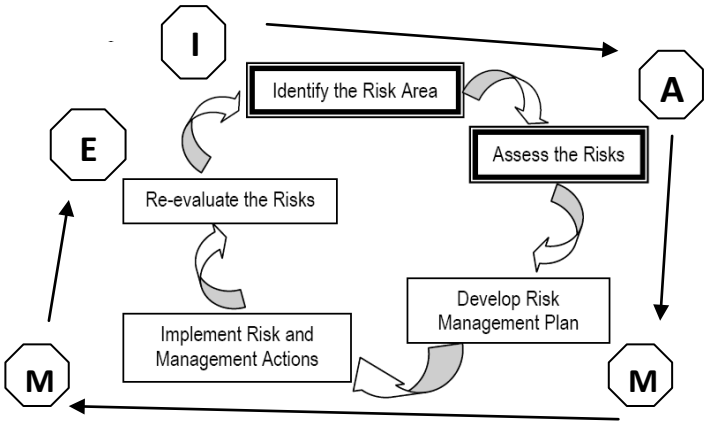
EFFECT OF CONTROLS ON RISK MITIGATION	ALTERNATIVE THAT CAN BE USED
CONTROL REDUCES RISK MORE THAN NEEDED	Find out some **LESS EXPENSIVE alternative.**
CONTROL COST > RISK REDUCTION	**Find something else**
CONTROL DON'T REDUCES RISK SUFFICIENTLY	**Look for different control**
CONTROL = **Risk Reduction + Cost Effective**	**Use it.**

I. RISK MANAGEMENT CYCLE:

Involves the following steps:

CODE TO REMEMBER: I-A.M.-M.E.





RISK IDENTIFICATION --------- (I)

I am hereby categorising the topics in this phase in the following manner

1. PURPOSE: Purpose of risk evaluation is to **identify** inherent risk of performing various business functions.

-- **Identify the probabilities of threat & failures** (Determine **danger)**

-- Calculate the EXPOSURE i.e. **damage to the assets.**

-- Making RECOMMENDATIONS keeping cost benefit analysis.

2. ACTIVITIES INVOLVED IN RISK IDENTIFICATION:

Following questions can be put up for identifying the risk

VULNERABILITIES & ASSETS
What assets need protection?
Whether we have liquid assets with alternate uses
What are the vulnerabilities?

ACTIVITIES/ OPERATIONS & OBJECTIVES
How operation is disrupted by anyone?
How we know that we are achieving our objectives
What activities are – COMPLEX Which activities are – REGULATED

INFORMATION
On what information do we rely?
What decision requires most judgement?

3. QUESTIONS TO BE CONSIDERED IN RISIK IDENTIFICATION:

- PROBABILITY: What is the probability that things can go wrong?
- EXPOSURE: What is the cost if what can go wrong goes wrong?

4. TECHNIQUES OF RISIK EVALUATION:

CODE TO REMEMBER: Q^2. -J.D.S.

A. Quantitative Techniques:

- Involves **calculating ANNUAL LOSS EXPOSURE VALUE,**
- Based on the probability of the event & exposure in terms of costs.

B. Qualitative Techniques

- Most likely approach to **RISK ANAYSIS.**
- Qualitative risk analysis methodologies make use of these elements:
  - -- **THREATS**
  - -- **VUNERABILITIES**
  - -- **CONTROLS:** There are 4 controls (Countermeasures)
    - ❖ **DETERRENT CONTROLS:** Reduces likelihood of an **ATTACK.**
    - ❖ **PREVENTATIVE CONTROLS:** Protect vulnerabilities, reduce threat impact
    - ❖ **CORRECTIVE CONTROLS:** Reduces effect of an **EFFECT.**
    - ❖ **DETECTIVE CONTROSL:** Discover attacks & trigger controls.

C. Judgement & Intuition:

- This technique is used by the **AUDITORS** for risk assessment.
- It depends upon **PERSONAL & PROFESSIONAL** experience of auditors.

D. Delphi Technique:

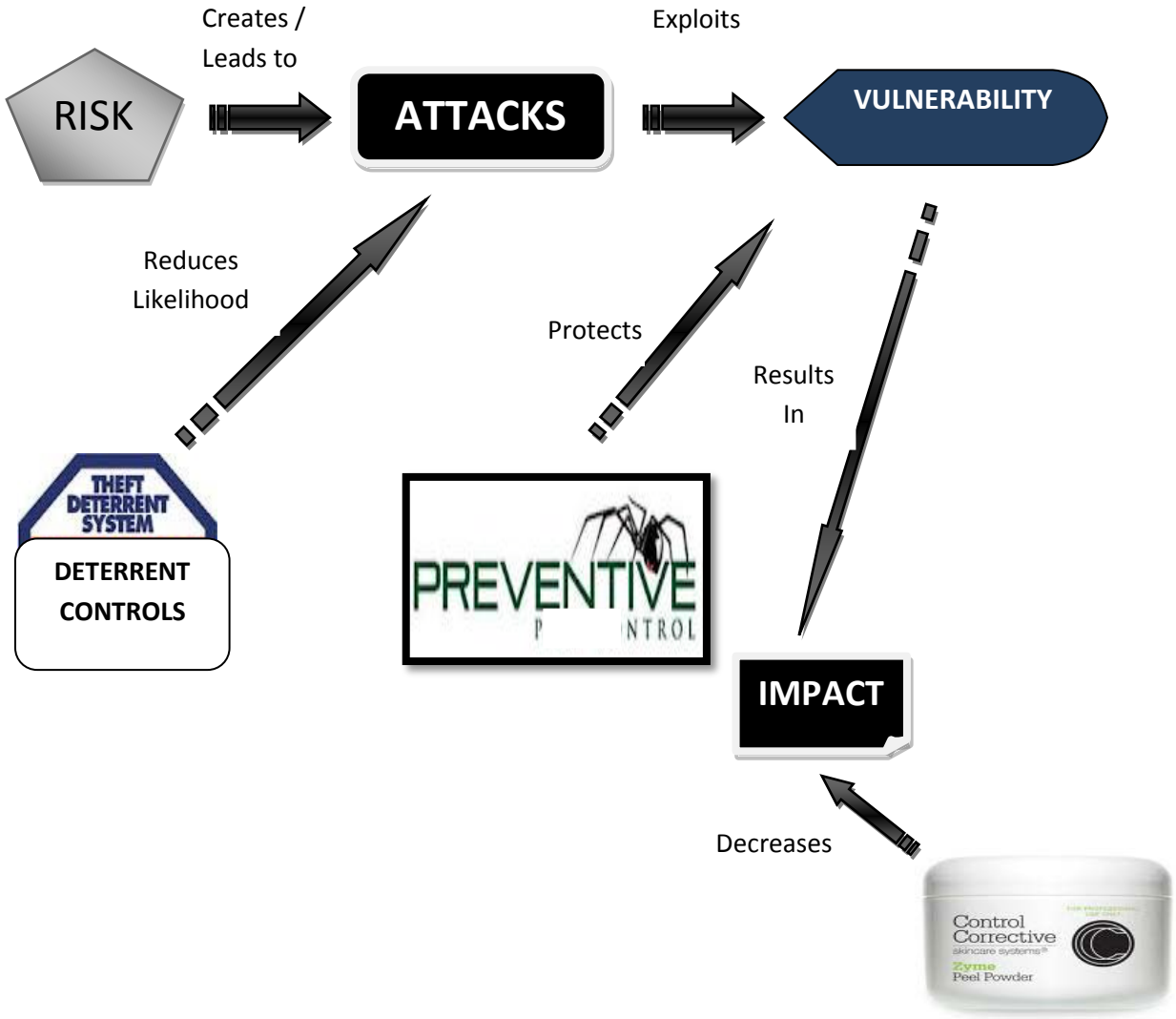
- In this approach **PANEL OF EXPERTS** is appointed.
- Each expert gives his opinion in writing & independent manner.
- They enlist the **COST & BENEFITS** that why a system to be chosen. Their estimates are **COMPLILED** thereon.
- The estimates within a **range are ACCEPTED.**

E. Scoring:

- In this risk in the system & their respective exposures are listed
- **WEIGHT** assigned = to the risk & exposure depending **on severity, impact & cost.**
- **RISK** X **WEIGHTS** = **WEIGHTED SCORE**
- **EXPOSURE** X **WEIGHTS** = **WEIGHTED SCORE**

Sum of this score & rank is given on same basis

THESE ELEMENTS IS SHOWN IN A DIAGRAMMATIC MANNER



RISK RANKING

A. Organisation must rank risk according to their severity & impact.

B. Organisations have to device **their own ranking methods.**

C. For instance:

RISK RANGE	MEANING
0	No impact in operations
1	Impact for up to **8 hours**
2	Damage to equipments, impact **8-48 hours**
3	Major damage, interruption more than **48 hours.** Office must be **relocated**

D. PERFORMING RISK ASSESSMENT:

- To measure potential risk, **WEIGHTED POINT SYSTEM** to follow. Each probability to be assigned POINTS:

PROBABLITY	POINTS
High	10
Medium	5
Low	1

E. CONSIDERATIONS IN ANALYSING RISK:

CODE TO REMEMBER: F - .P.W.D.

- ¥ Investing the **F**requency of the disaster.
- ¥ Determining the degree of **P**rediction.
- ¥ Determining amount of **W**arning associated with disaster.
- ¥ Estimating **D**uration of the disaster.

Disaster Hone se pehle

IMPACT OF THE DISASTER

- ¥ Vital records **are destroyed.**
- ¥ Vital records are **not destroyed.**

Disaster Ho gya then what was its impact on records

CONSEQUENCESOF THE DISASTER

- PERSONNEL AVAILABILITY
- PERSONNEL INJURIES

- LOSS OF OPERATING CAPABLITY
- LOSS OF ASSETS
- FACILITY DAMAGE

Disaster hone par kya impact hua on the entity

ACCOMODATING THE CRITICAL SYSTEM

- ¥ Hardware
- ¥ Information
- ¥ Communication
- ¥ Information
- ¥ Services

ESTIMATING POTENTIAL LOSS

TANGIBLE LOSS	INTANGIBLE LOSS
Code: I – F.C.A.	Code: C – M.C.G.
LOSS OF:	LOSS OF:
-- **Income**	-- **Competitive Edge**
-- **Financial management Capability**	-- **Positive Media Coverage**
-- **Assets**	-- **Stakeholder Confidence**
INCREASED:	-- **Goodwill**
-- **Operating Cost**	

RISK MITIGATION

- Analysis helps the organisation to take appropriate actions to control & manage risks.
- Knowing**" WHAT CAUSES WHAT"**gives an ability to implement necessary controls.
- Cause model helps in implementation of **risk mitigation measures.**
- Some of the **risk mitigation measures are:**

CODE TO REMEMBER: - S.I.R.-C.O.L.D. - R

SIR Ko COLD ho gya so Risk hai--- Mitigate Karo

A. **S**elf assessment.

B. **I**nsurance.

C. **R**isk management department to be set up.

D. **C**reating culture supportive of risk mitigation.

E. **O**utsourcing operations with strict service level agreements.

F. **L**imit of operational risk to be set up.

G. **D**isaster Recovery Plan & backup system to be established

H. **R**eserves calculating & capital requirements.

Common risk mitigation techniques:

INSURANCE:

- Entity takes insurance to mitigate risk.
- INSURED ⟹ INSURANCE COMPANY

LOSS IS TRANSFERED TO INSURANCE CO.

- Banks are allowed to recognise risk mitigating impact of the insurance up **to 20% of total operational risk.**

OUTSOURCING:

- Organisation may transfer some of its function to an outside agency.
- Careful assessment to be done whether **only process is transferred** or the **risk.**
- For example: **outsourcing of telecommunication lines.** Entity must consider the compensation clause must be conditioned in such a manner that organisation is able to mitigate risk.

SERVICE LEVEL AGREEMENT:

- Risk can be mitigate by entering into service level agreement.
- Service agreement can be entered with **EXTERNAL SUPPLIERS, USERS & CUSTOMERS.**
- Service agreement WITH **CUSTOMER**

Limit responsibility of entity for **loss suffered** by customer **to technological failure**	Example: **Bank is not responsible for non working of ATM's subject to service availability.** Service delivery is conditioned upon **system functionality.**

RISK CONTROL

-- Risk is the probability that an event will have adverse effect on the organisation.

-- In order to reduce the risk it is imperative to develop control procedures.

-- Following shows the effect of excessive risk & controls:

Excessive Risks	Excessive Controls
Loss of assets, donor or grants	Increased bureaucracy
Poor business decisions	Reduced productivity
Non-compliance	Increased complexity
Increased regulations	Increased cycle time
Public scandals	Increase of no-value activities

-- Internal controls should be **proactive** to maintain balance between risk & control