CHAPTER-1 AUTOMATED BUSINESS PROCESSES

Enterprise Business Processes

Enterprise ↓ Multi-national company or very large Scale Organisat^n Eg- BIG BAZAR

Business Processes ↓ set of Activities ↓ that will accomplish goals of an Org.

BIG BAZAAR

Categories of Business Process.

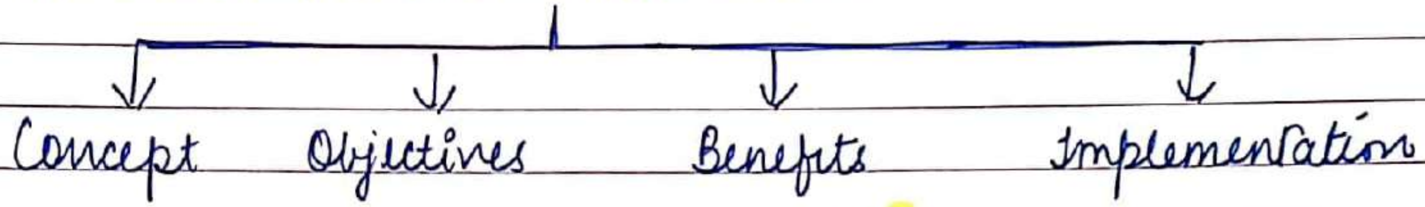
↓ Operational Processes

↓ Supporting Processes

↓ Management Processes.

Operational	Supporting	Mgt
(Sale/Purchase)	HRM	Policies बनाने वाले
• Core Business Activities • Other Name PRIMARY PROCESS	• Back Core Business Process/Activities/f's. • Other name SECONDARY PROCESS	• Measure, Monitar • Control • Making policies.
Example Order to Cash (OTC)	Example Human Resource Mgt	Example Budgeting
Customer Order ↓ Order fulfillment ↓ Delivery Note ↓ Invoicing ↓ Collections ↓ Accounting	- Recruitment ↓ Staffing ↓ Training & Devp ↓ Compensation ↓ Career Devp/ Promotions.	Vision ↓ Straltegic Plan ↓ Revenue, Cost, Profit Projection ↓ Board Approval ↓ Budget Review.

Business Process Automation



Concept

- Technology Enabled automation of activities
- like Sales, Supply chain etc.

" It consists of integrating applications & Using Software applications through out the Organisatn".

Objectives of BPA

Confidentiality	to Ensure data is only available to right persons.
Integrity	to Ensure no un-authorized amendments can be made
Availability	to Ensure that data is available when asked.
Timeliness	to Ensure data is made available at right time (as & when required
MC: CIAT	

Benefits

Quality	Since every Action is performed identically, it results in high Quality & Reliability
Time Saving	Automation reduces the no. of tasks as compared to manual process
Reduced Costs	Costing as compared to manual processing Wn is quite less. Automation allows you to accomplish more by utilizing fewer Resources.
Visibility	Automated processes are done accurately within defined timeline, This gives Visibility of the process status to Org.
Efficiency	Automation reduces the time taken for the accomplishment of task resulting in efficiency
Governance	Automation helps in Governance as Information is accurately processed

MC: Qtr. VEG

Implementation of BPA

Step 1 : Define Why we plan to Implement BPA	• Errors in manual process • Poor Customer Service, debtor mgt • Paying for G&S not received • Not able to find documents quickly
	The answer to this question will provide Justification for implementing BPA
Step 2: Understand the Rules/Regulations under which it needs to Comply with	• Entity needs to ensure that BPA adheres to the Requirement of Law. • Documents may be required to be retained for a specified pd. of time & in specified format
	The issue is that any BPA created needs to comply with Applicable LR
Step 3: Document the process we wish to automate	• All documents which are currently being used needs to be documented in the format like PDF, Word. • Benefit - clarity in the process.
	The current processes which are planned to be automated need to be correctly documented.

* BPC: Business Process Consultant

Step 4 Define Objectives / goals to be achieved by Implementing BPA	Goals need to be SMART S Specific: clearly defined M Measurable: Achievable A Attainable: Easily Quatifiable R Relavant : With refrence to Entity T Timely: Achieved within a given pd. This enables to understand the reason for going for BPA.

Step 5 Engage BPC	Evaluate "CWA" of BPC
	C = Competency, Capability & Objectivity
	W = Work Understanding
	A = Appropriateness
	Once the Entity has been able to define the above (steps). Entity needs to appoint an EXPERT, who can implement it for the Entity

Step 6 Calculate ROI for Project	• BPA shall lead to cost savings, Efficiency & Effectiveness. The answer to this question can be used for convincing top mgt to say "YES" to BPA exercise

Step 7 Development Of BPA	• BPC develops BPA • to meet the Goals of Org. Once the mgt (top) grant their approval, the right business solution is developed & Implemented.
Step8 Testing BPA	• Testing allows room for improvements (prior to official launch) • It helps to determine how well it works • It helps in Identifying where additional "exception processing" steps are need to be included. Before making the process live, the BPA should be throughly tested

Business Process Automation additional topics

(Added May 2021)

Which Business Processes should be automated?

following are the few examples of processes that are best suited for Automation

- Processes involving high volume of tasks/Repetitive tasks
  Automating these processes results in Cost & work effort reductions. Eg Purchase Order

- Processes requiring Multiple people to execute tasks
  Automating these processes results in reduction of waiting time & costs Eg Help desk Services

- Time Sensitive Processes
  Business process automation results in streamlined processes which eliminate wasteful activities
  Eg Online banking System

- Processes involving need for Compliance & audit trail
  Every detail is automatically recorded which can be used during audits. Eg Invoice issue to vendors

- Processes having Significant Impact on other Process/System
  Automating process results in sharing Information, resources & Improving efficiency & effectiveness of the related process/system. Eg Mktg dept & Sales dept.

Challenges Involved in BPA (MC: AIDS)

- Automating Redundant Processes

Sometimes org start off an automation project by automating the processes they find suitable without considering whether such processes are necessary ie creating value or not

- Defining Complex Processes

BPA requires re-engineering of some business processess that requires significant amount of time & detailed understanding which seems to be complex.

- Staff Resistence

In most cases, human factor issues are the main obstacle to the acceptance of automated processes. Staff may see process automation as a way of reducing their decision making power / substitute.

- Implementation Cost

The cost of Implementation of BPA might be relatively higher as compared to the fruits or benefits arriving from such automation. This cost Includes acquisition/ development cost as well as the cost of running.

Enterprise Risk Mgt
(Amended May 2021)

- ERM Definition
- ERM Benefits
- ERM framework & its 8 Components

ERM definition

Process designed to Identify potential Events

↓

that may affect the Entity (whether profit/Non Profit)

↓

& to manage risk to be within Risk Appetitite

↓

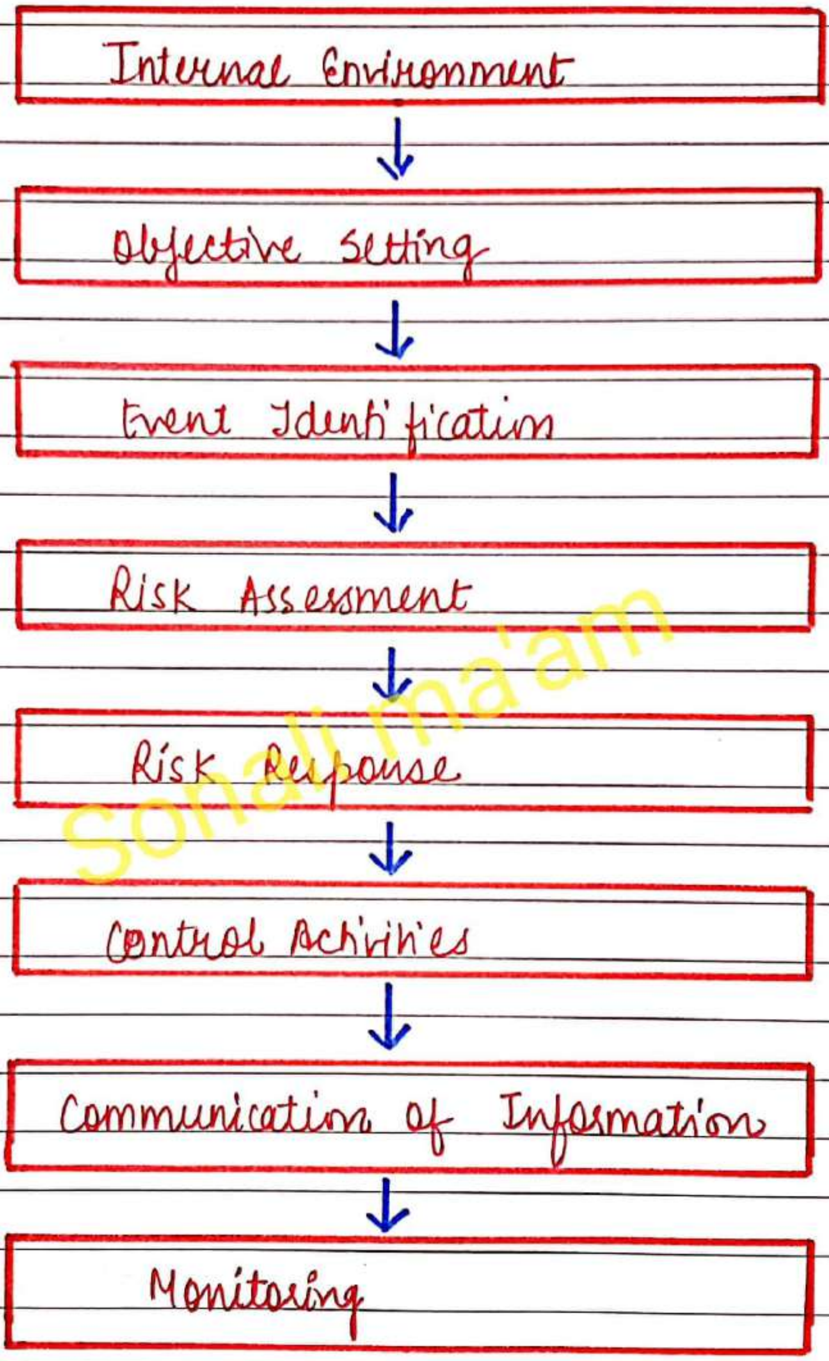
so as to provide reasonable assurance regarding the achievement of Org objectives.

ERM framework

ERM provides a framework for risk mgt which Includes
- Identifying potential threats/Risks
- determining it's Impact
- Implementing controls to mitigate it.

ERM framework consists of 8 inter-related Components.

⑧ Components



Internal Environment
↓
Objective Setting
↓
Event Identification
↓
Risk Assessment
↓
Risk Response
↓
Control Activities
↓
Communication of Information
↓
Monitoring

Internal Envt	"Mind set of Employees" - How the Risk is viewed & addressed by entity's people
Objective Setting	"What is to be achieved" -ERM ensure that mgt has a process to set Objectives
Event Identification	"Risky event are Identified" 'ERM includes identification of factors that may affect Entity.
Risk Assessment	"Prepare a Risk Assessment Table" Identified Risks are analysed in ERM
Risk Response	"Prepare Risk Response to Various Risks" Mgt Selects a way to approach set of actions to assessed Risk.
Control Activities	"Controlling should be Initiated." Policies & Procedures are established.
Communication Of Information	"Share the Information" Information transferred to appropriate Level of mgt
Monitoring	"Modify ERM as per need" Entire ERM process should be monitored & modifications if required shall be made accordingly.

Risk appetite :- degree Risk you are able to take

Cross = across enterprise

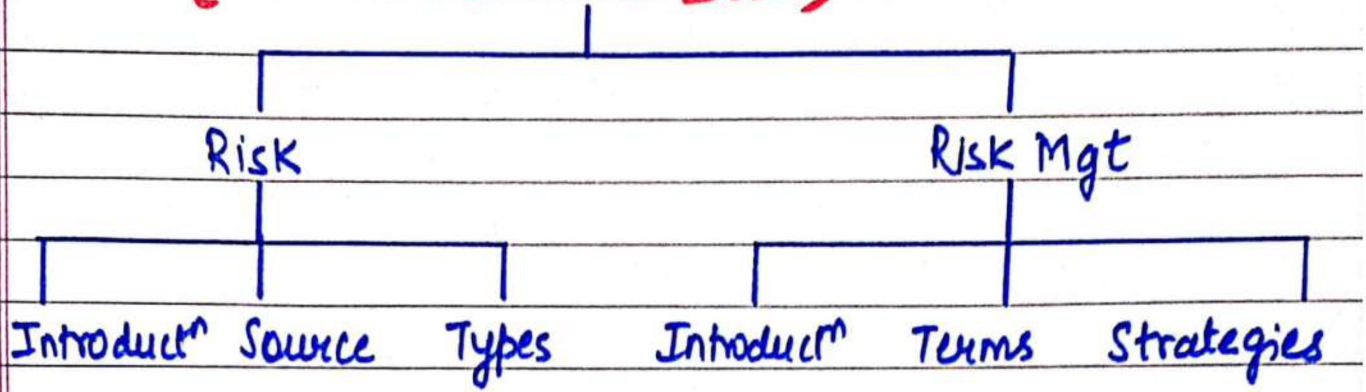
Multiple Risk = technological, Natural etc

Benefits

No entity operates in a risk-free Environment & ERM doesnot create such an Envt. Rather, it enables mgt to operate more effectively in Envts filled with Risks.

i) Align risk appetite* & Strategy	जो strategy adopt करो जो Risk appetite के साथ जा सकती है
ii) Link growth, Risk & Return	Growth ↑, Risk ↑ ERM helps to manage Risk
iii) Enhance Risk response decisions	ERM is helpful for decision making
iv) Minimize operational surprises & losses	Through ERM, we identify Risk, Losses are not surprises anymore.
v) Identify & manage cross* enterprise risks	Able to manage Risks affecting diff parts of Enterprise
vi) Provide integrated responses to multiple risks	ERM enables integrated solutions for managing the risks
vii) Seize opportunities	Helps to hold/grab opportunities.
viii) Rationalise Capital	Capital को Rationalise तरीके से use

Risk & its management (AMENDED MAY 2020)



RISK - Introduction

- Risk is any event that may result in SIGNIFICANT DEVIATION from a PLANNED OBJECTIVE resulting in an UNWANTED NEGATIVE CONSEQUENCE
- degree of Risk is determined by the probability of event occuring & its consequences.

Sources of Risk

(Areas from where risks can occur

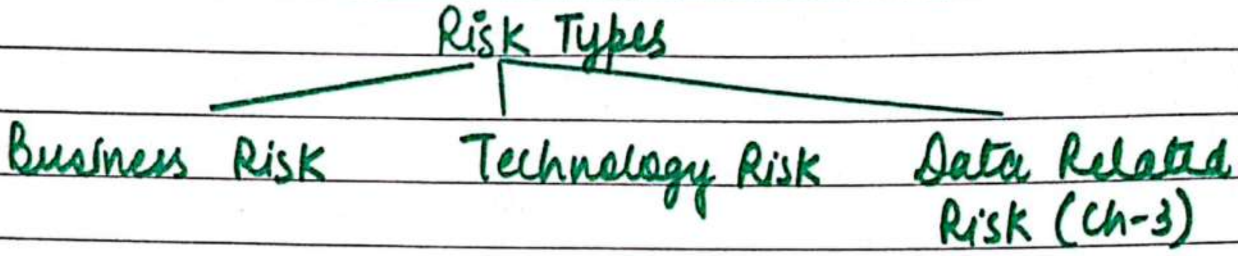
- Potential loss that exists as a result of threat or vulnerability
- Uncertainity of loss expected in terms of the probability of such loss
- probability that a threat may mount to specific attack against a particular system

Types of Risk

Risk can be broadly Categorized as-

- Business Risk
- Technology Risk
- Data R[illegible]

LR = Legal & Regulatory Requirements.



Business Risk

Business face all kinds of risks related from serious loss of profits to even bankruptcy & are discussed below-

Strategic Risk	Risks that would prevent an Org from achieving its objectives (because of Strategy failure)
Financial Risk	Risks that could result in a negative financial impact to Org.
Regulatory Risk	Risks that could expose the Org to fines & penalties from Regulatory Authorities due to non-compliance with LR.
Operational Risk	Risk that could prevent the Org from operating in effective/Efficient manner
Hazard Risk	Risks such as natural disasters, terrorism which brings damage to Org
Residual Risk	Risk remaining even after the counter measures are analysed & Implemented

Technology Risk (Amended In May 2020 & May 2021)

As technology is taking new forms & transforming as well, Enterprise, have to face following new set of IT Risk ie challanges.

Challanges are -

- Downtime due to technology failure
  - Informatⁿ system become unavailable due to technical problem / equipment failure
  - Eg server failure
- Frequent changes or obselence of technology
  - Technology = changing
  - Requires investment (Capital) for updation / Replacement
- Multiplicity & Complexity of System
  - Multiple digital platform
  - Requires Knowledge / Skills
- Diff types of Controls for diff types of technologies
  - It Give rise to new risks
  - These risks required to be mitigated by Controls
- Proper alignment with Business Objective & LR
  - Ensure Systems fulfill business Objectives & needs
  - And Legal & Regulatory requirements as well

- Dependence on Vendors due to Outsourcing of IT Services
  - Heavy dependency on venders give rise to Vendor risks
  - as specialized domain skills are required to manage IT.

- Vendor related Concentrat^{n} risks
  - Since Vendor पर concentrat^{n} है
  - Vendor = Single = Risk
  - Vendor = multiple = Also Risk

- Segregation of Duties (SOD)
  - High risk area
  - SOD conflicts can be a potential vulnerability for fraudulent activities.

- External threats leading to cyber crime
  - ∵ Providing anytime/ anywhere access using Internet
  - ∴ Risks from Hackers

- Higher Impact due to Intentional/ Unintentional acts of internal employees
  - Employees are weakest part of an Enterprise
  - Employees = trust / trust break
  - Extended privilges can be misused

- New Social-Engineering techniques employed to acquire Confidencial Credentials (NSET)
  - Fraudsters use NSET such as socializing with employees via fb, Whatsapp etc
  - Extract information about p/w etc to use it to commit frauds

- Need for Governance processes to adequately manage technology & information security.
  - Governance (TCWG) ie Senior management should be involved in directing technology-deploy.
  - & should approve policies as required

- Need to ensure continuity of business processes in the event of major exigencies (emergencies)
  - Ensure that failure of technology doesnot hamper business.
  - Ensure BCP [Business Continuity Plan] like Back up.

Data Related Risks

(AMENDED MAY 2022)

(It includes unauthorized implementation / modification of data & software)

It includes
→ Data Diddling
→ Bomb
→ Christmas Card
→ Worm
→ Rounding down
→ Salami techniques
→ Trap doors
→ Spoofing
→ Asynchronous Attacks.

(Includes unauthorized Implementation or modification of data & S/W)
It includes the following

Data Diddling	It Involves change of data before or after entering the System
Bomb	Bomb is a piece of bad-code deliberately planted by an Insider or Supplier of a program
Christmas Card	On typing the word 'Chritmas', it willdraw Christmas tree but, in addition, it will

Send the same to all other users connected to the network resulting in → other users cannot save their half-finished work Eg- IBM मे ऐसा हुआ था।

Worm

Worm program copies itself to another machine on the network. (Doesnot require a Host program) Eg Alark clock Worm

Rounding Down

This refers to rounding of small fractions of a denomination & transferring these small fractions into an authorized A/c. As the amt is small, it gets rarely noticed.

Salami Technique

Involves slicing of small amounts of money from a computerized transaction or a/c. A fixed amount is deducted

Trap Doors

It allows insertion of specific logic, such as program interrups that permit a review of data. They also permit insertion of unauthorized logic.

Spoofing

Involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Eg., a penetrator duplicates the login procedure, captures user's p/w & attemps uses login.

Asynchronous Attacks

- Data this is waiting to be transmitted is liable to unauthorized access called Asynchronous Attack
- These attacks are hard to detect because they are usually very small pin like Insertions.
- It includes -

Data Leakage

This involves leaking information out of computers by means of dumping files to paper or stealing computer reports & tape.

Subversive Attacks

These can provide intruders with imp. Informatn about messages being transmitted

Wire-tapping

This Involves spying on information being transmitted over communication networks

Piggybacking

This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts & alters transmissions.

AA. occur In environment where data is moved across Telecommunication Lines.

RISK MANAGEMENT - Introduction / Meaning

Risk mgt is the process of
↳ Assessing risk
↳ taking steps to reduce risk to an acceptable level &
↳ maintaining that level of Risk.

Terms

Asset	• Something of Value to Organisation • Eg, Information in Electronic form or physical form, software, etc. • Characteristics of Asset – Not Easily replaceable without cost – forms part of Org Identity • It is the purpose of Information Security Personnel to Identify threats / Risks that can cause damage to our Assets.
Vulnerability	• It is the weakness in the System that exposes Systems to threats. • Eg, Short passwords makes vulnerability via cracking or guessing. • Vulnerability forms / Allows an attacker to – execute commands as another user or – access data which has restrictions or – pose as another entity or – conduct a denial of service.

Threat	• Any event which can cause harm to the software, system, through unauthorized access, destruction, modification etc. • Threats are prevented by appling some protection to assets
Exposure	• Extent of loss the enterprise has to face when a risk materializes. • Its not an Instant one, but occurs harm in long run. • Eg, violation of privacy policy.
Likelihood	• Estimation of probability that the threat will succeed in achieving an undesirable event.
Attack	• Attempt to Gain unauthorized access to the system • It is an intentional fault [External] • Intent : Exploiting vulnerability & making gains.
Counter Measure	• technique that reduces the vulnerability of a component / system • Eg, Threat " Spoofing the User identity" has 2 countermeasures – Strong authentication protocols – Secured mechanism for password storage.

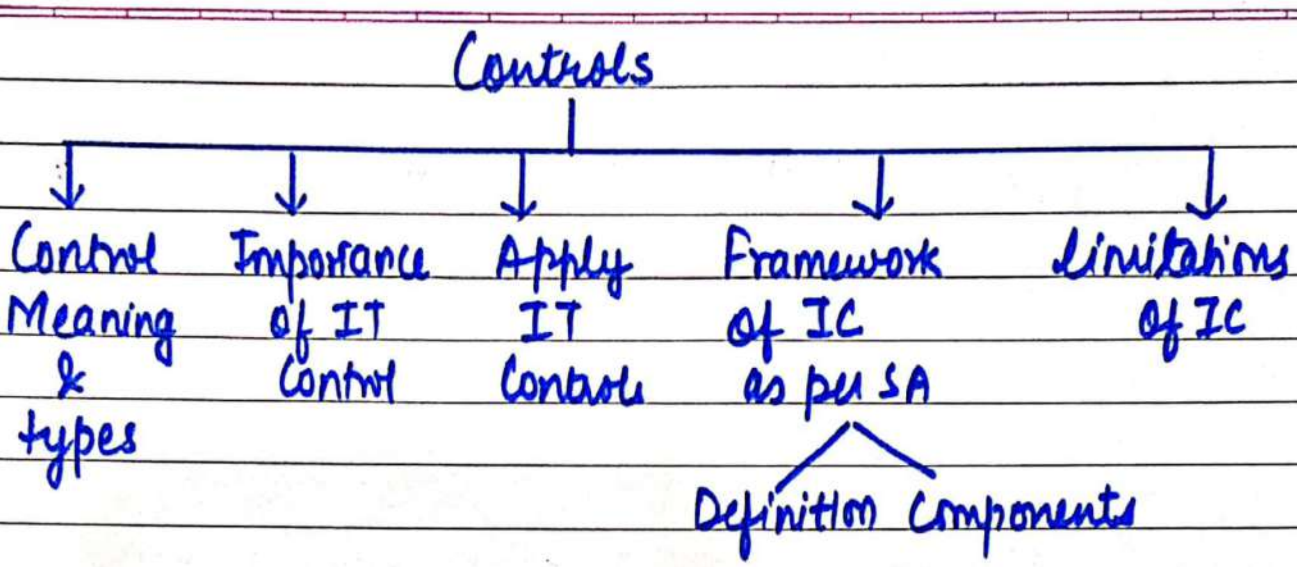
Risk Management Strategies

AMENDED MAY 2022

T4

Tolerate [Accept Risk] · Terminate [Eliminate] · Transfer [Share] · Treat [Mitigate Risk]

Tolerate	• Accepting the risk as a cost of doing busines • Risk should be viewed periordically so that its impact remains low. • Eg - planning for potential production delays since It is difficult to predict a precise delivery Schedule in advance.
Terminate	• In the cases of risk having high probability, its best to modify straligy to avoid it's risk. • Eg- Risk associated with use of a technology can be eliminated with more robust products from capable vendors.
Transfer	• Risk mitigation approaches can be shared with trading partners & suppliers. • Eg. - Outsourcing infrastructure mgt where supplier mitigate the risk by highly skilled staff
Treat	• Suitable controls must be derived & Implemented to prevent the risk from manifesting itself or to minimise its effects • Eg. - Planning for the eventuality in case an enterprise won't have sufficient capacity to deal with high demand, that allows them rapidly scale their capacity.


Controls

Control Meaning & types

Importance of IT Control

Apply IT Controls

Framework of IC as per SA

Definition

Components

Limitations of IC

Control Meaning

Control is defined as policies, procedures, practices that are designed to provide reasonable assurance that business objectives are achieved & undesired events are prevented/detected or corrected.

Types of control

- Manual control
- Automated Control
- Semi-automated Control

Importance of IT control

- They enable enterprise to achieve objective &
- they help in mitigating risks

Applying IT Controls

General Controls

[Infrastructure Controls]

- Impact pervades the IT Envt at different layers
- Apply to data process, HR mgt etc.

Examples:

- Information Security Policy
- Administration, access & Authentication
- Separation of key IT functions [SOD]
- Mgt of System Acquisition & Implementation.
- Change management Process
- Back up, Recovery, BCP
- Confidentiality
- Availability of Datafiles/ Software only to authorized

Application Controls

- Controls are specific to application software
- Implemented in an application to PDC errors [Prevent, Detect, Correct]

Examples:

- Data Edits allowed for permissible fields.
- Separation of duties
- Balancing of processing totals [Dr = Cr]
- Transaction logging process implementation
- Error reporting in processing, input, output immediately reported
- Exception Reporting also immediately Reported.

Framework of IC as per SA

Definition (as per SA 315)

The process DIM (Designed, implemented & maintained)

↓ By

TCWG & Other personnels

↓ to

provide reasonable assurance

↓ about

Entity's 4 aspects

- → Reliability of FR
- → effectiveness / Efficiency of operations
- → Safeguarding of Assets
- → Compliance with applicable LR.

Components of IC

i)

Control Environment	• Set of Standards that provides basis for carrying out activities in org. • The BOD & Senior mgt shall establish these parameters
Risk Assessment	• Whether the risk is assessed at mgt level or not • Whether mgt considers the Impact of possible changes in external envt?
Control Activities	• Includes whether transactions are authorized, duties are segregated, documents adequacy etc

	• It must be there to manage, mitigate, reduce the risks.
Informatn & Communication	• Where the information & its commn flows are clear (less barriers) • Since, decisions are based on the information so communicated.
Monitoring of Controls	•Evaluations are conducted periodically or not? • Whether deficiencies are traced & Communicated & taken action upon.

Key Indicators of Effective IT Control

- Upgradation of IT Infrastructure as & when required
- Cost Effectiveness (Within Budgets)
- Resource allocation is proper
- 24x7 [Consistent availability of IT Services
- Clear communicatn to mgt about indicators time to time
- Protection mechanism against vulnerabilities / threats
- Efficient help-desk
- Security awareness programs.

Limitation of Internal control Systems

- Cost of Internal Control exceeds the benefits
- Potential human error (mistakes), misunderstanding of instructions are unavoidable
- Cullusion with employees or outside party
- Person responsible for exercising an IC could misuse that responsibility
- Manipulations by mgt with respect txns/ Estimates/ judgements etc.

Risks & Controls for specific Business processes

Controls should be checked at three levels, namely

Configuration | Masters | Transactions

Configuration refers to the way a software is setup. It will define how software will function & what menu options are displayed.

Example

- User Activation / deactivation
- User Access & Priviledges
- Password management
- Creation of customer type, year end process

Masters refers to the way various parameters are set up for all modules of software like Pur, Sale, Inventory, Finance etc. Eg- Employee Master

Transactions refers to the actual entries entered through menu's & functions in the application software. For Example

- Sales Transactions
- Purchase Transactions.

PROCURE TO PAY (P2P) Risk & Controls

Procure to Pay is the process of obtaining & managing the raw materials needed for mfg a product or providing a Service.

Masters P2P (Supplier Master file)

	Risk	Control
1.	Unauthorised changes to Supplier master file (User इच्छा)	Only authorised changes are made to SMF
2.	All changes to SMF are not input (छूटा)	All valid changes are entered (Input)
3.	Changes to SMF are not Correct (इच्छा)	Changes to SMF should be accurate
4	Changs to SMF are delayed (not on time)	Changes to SMF are processed in timely manner
5	SMF is "not" "uptodate"	SMF shall remain uptodate
6	"System access" not been restricted	System access should be given to requisite personnel

Transactions P2P

	Risk	Controls
1.	Purchase Order issued are not Input & processed	All P.O. Issued are input & processed
2	Amounts posted to A/c payable not correct	It should be calculated properly
3	Amounts for G&S received are recorded in Wrong pd	Record in appropriate pd.
4	Credit Notes not Recorded	Should be accurately recorded
5	Disbursements (Payments) not recorded in app. year, wrong amt, wrong personnel	Should be recorded in app year, accurate amt, app. supplier.

ORDER TO CASH (O2C)

It Includes receiving & fulfilling Customer requests for G&S.

Masters (O2C) - Customer Master file

	Risk	Controls
1.	Unauthorised changes to Customer Master file	Only authorized changes are made to CMF
2	All changes to CMF are not input	All valid changes are entered (Input)
3	Changes to CMF are not correct	Changes to CMF should be accurate
4	Changes to CMF are delayed	Changes to CMF are processed in timely manner
5	CMF is not uptodate	CMF shall remain uptodate
6.	"System Access" not been restricted	System access should be given to requisite personnel

Transactions O2C

	Risk	Controls
1.	Orders are not input & processed	All customer orders are Input & Processed
2.	Amounts posted to A/c Receivable not correct	It should be Calculated & posted properly.
3	Amounts for G&S given are recorded in Wrong period	Record in Appropriate period
4	Credit/Debit Notes are not Recorded	Should be recorded in appropriate manner
5	Receipts are not recorded in appropriate year, including wrong amt, wrong personnel	Should be recorded appropriate year, accurate amount & appropriate customer.

INVENTORY CYCLE

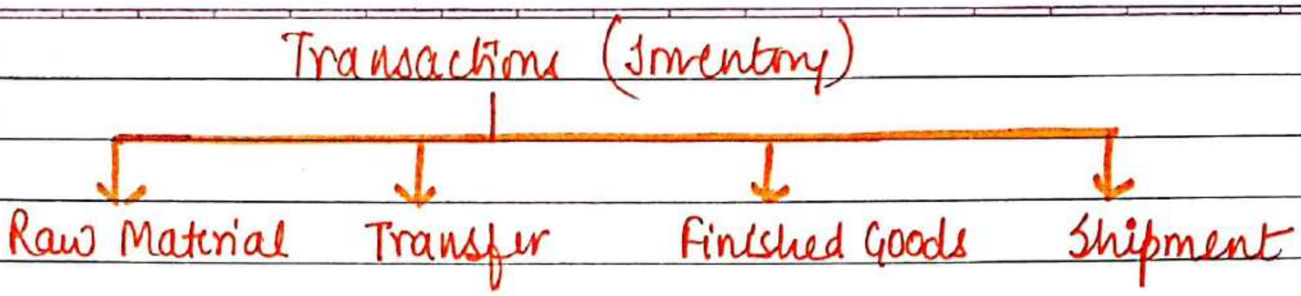
Inventory Cycle consists of -

- **Ordering phase** : the amount of time, it takes to order & receive raw materials.
- **Production phase**: The WIP phase (R/M → FG)
- **Delivery phase** : Delivery phase.

Inventory cycle is measured in NUMBER OF DAYS

Masters - Inventory Master File

	Risks	Controls
1	Invalid/Unauthorized changes made to IMF	Only valid changes
2.	Invalid changes to IMF are Input	All valid changes to be Input
3	Changes are IMF not accurate	Changes to be accurate
4	Changes not made in time	changes to be done in time
5.	IMF is not uptodate	Should be uptodate
6.	System Access given to everybody ie not restricted.	Should be restricted to Requisite personnel.



Transactions (Inventory)

Raw Material

Transfer

Finished Goods

Shipment

RISK	Controls
Raw material	Raw material
- accepted without valid purchase Orders	- should be accepted only if they have Valid pur Order
- Not recorded accuratily	- Recorded accuratily
- Not recorded In system	- All R/M should be recorded
Transfers	Transfers
- Not recorded completely	- should be recorded Completely
- Not recorded accureatily	- Should be recorded accurately
- Not in app. period	- in app. pd.
Finished Goods (Same as above)(Transfer)	Finished Goods (Same as above)
Shipment (Same as above)	Shipment (Same as above)

HUMAN RESOURCES - RISKS & CONTROLS

Human Resource Cycle covers all the stages of an employee's time within a specific Entity.

HRC Includes -

- Recruiting : Process of hiring new employee
- Orientation : Process by which employee learns his duties.
- Career Devp : Professional Growth & Devp.
- Termination : laying off / Removing employee

Configuration - HR.

Risks	Controls
Employee who have left the company continue to have system access	system access to be immediately removed as & when employees leave
Employees have system access in excess of their job requirements	RBAC → Need to know Basis

Sonali Jain | 8447-82-4414

Masters - HR (Payroll Master files)

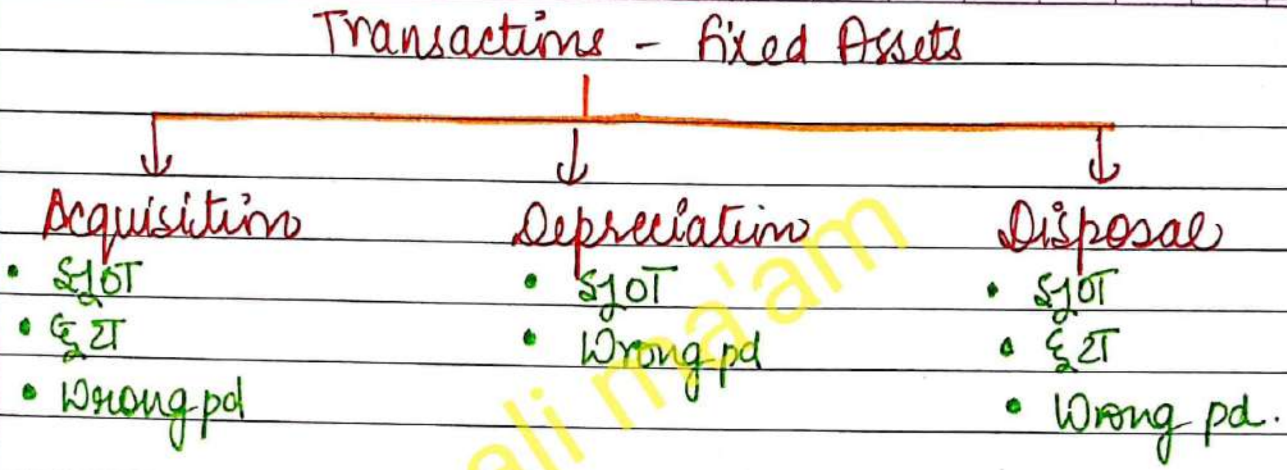
Risks	Controls
New Employees are not added to PMF	All Employees should be added to PMF
Terminated employees not removed from PMF	Terminated employees should be removed from PMF.
बाकी 6 "same"	

FIXED ASSETS - RISKS & CONTROLS

It Includes -
- Procuring an Asset / Acquisition
- Registering / Adding an Asset
- Adjusting an Assest (Depreciation)
- Transferring an Asset (Sold)

Masters → Fixed Asset Register

	Risks	Controls
1	Unauthorised changes made to FAR / Master file	Only authorised changes are made to FAR
2	All changes to FAR are not Input	All valid changes are entered (Input)
3	Changes to FAR are not correct	Changes to FAR should be accurate
4	Changes to FAR are delayed	Changes to FAR are processed in timely manner
5	FAR is not uptodate	It shall remain uptodate
6	System access not been restricted	should be restricted to required personnel



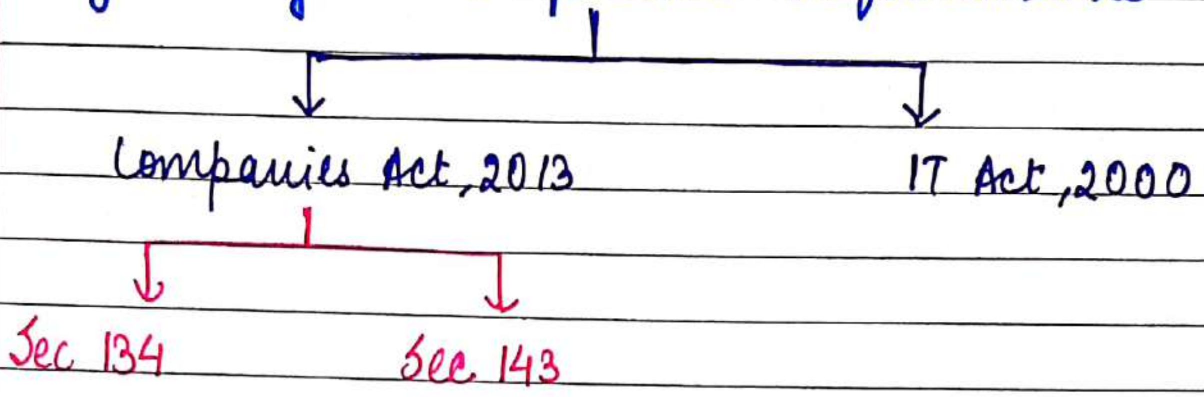
Transactions - Fixed Assets

Acquisition
- SJOT
- ξ2T
- Wrong pd

Depreciation
- SJOT
- Wrong pd

Disposal
- SJOT
- ξ2T
- Wrong pd.

Regulatory & compliance Requirements



Sec 134 (Director Responsibility Statement)

- The DIRs had Taken Proper & sufficient Care for the maintenance of Adequate accounting Records & accordance with the provisions Of the act for
  - Safe guarding Of Assets
  - P, D, C the frauds & I.C.

Sec 143 (Auditor Report)

- Sec 143(3) Contains the Auditor's report which states " Whether the Company has Adequate IFCS in place & the operating effectiveness Of Such controls"

IT Act, 2000

IT Act Provision contain many Advantages

- E-filing
- E-mail
- E-commerce
- E-Governance
- Digital Signature

Information technology Act
(Amended May 2020 & 2021)

- Cyber Crime
- IT Definition
- Key Provision Of IT
- Computer Related Offences
- Advantages of Cyber Law
- Privacy Policy of Online Data

CYBER CRIME

- The term 'Cyber Crime' is not mentioned in any Law including IT Act.
- It is not different than the traditional Crime.
- The only point is that it is Computer technology related & thus, it is a Computer related Crime.
- IT Act aims to provide legal structure for E-commerce in India so that, legal sancity is accorded to all electronic records & other activities carried out by electronic means.

SOME DEFINITION IN IT ACT (Sec 2)

Access	Computer	Computer Network	Data	Informatn
Sec 2(a)	2(i)	2(j)	2(o)	2(v)

C	- computer
CS	- computer system
CN	- Computer Network
CR	- Computer Resource

CSD - includes codes for Running Programes.

KEY PROVISIONS OF IT RELATED OFFENCES

The IT Act recognises Risks of IT deployment, various types of computer-related offences & provides a legal framework for prosecution for these offences.

Sec No.	Description	Penalty
Sec 43	Penalty & Compensation for damages to Computer, Computer system etc. If any person without permission of owner/Incharge of a computer, CS, or Network or Comp Resource - - Access to C, CS, CN or CR - Downloads, Extracts any data stored in Removable storage medium - Damages to C, CS, CN or CR - Disrupts to CS, CN - Deletes/ Alter information	"Sec 66"
Sec 65	Tampering with Computer Source Documents. (CSD) Whoever knowingly concels, destroys or alters any CSD used for CS, CN, CR shall be punishable.	3yrs Jail, 2 Lacs Fine Or Both

Camlin Page

sec 66	Computer Related offences If any person does any act referred in sec 43, he shall be punishable	3 yrs/ 5 Lacs or Both
sec 66B	Punishment for dishonestly receiving stolen CR or Communication device Whoever dishonestly receives/retains any stolen CR or Communication device shall be punishable	3 yrs/ 1 Lac or Both
sec 66C	Punishment for Identity theft Whoever, fraudulently making use of electronic signature, or any unique Identification feature of any other person shall be punishable	3 yrs/ 1 Lac or Both
sec 66D	Punishment for cheating by Personation by using computer Resource Whoever by any CR or device Cheats by personation, shall be punished	3 yrs/ 1 Lac or Both
sec 66E	Punishment for violation of privacy Whoever knowingly captures, publishes the images of private area of a person without his/her consent violating the privacy of that person, shall be punishable.	3 yrs/ 2 Lacs or Both

ADDED MAY 2021 -

Sec 66F	Punisment for Cyber terrorism • Whoever with intent to threaten the unity, Integrity, security or sovereignty of India Or strike terror in the people by - denying access to authorized person or - Attempting access to computer resource without authorizatn or - Exceeding authorized access or - doing any computer contaminant (Causing damage to the life of people) • Whoever knowingly obtains access to informatn or using the informatn [Restricted info for Security reasons] so obtained for the injury to the interest of India.	Life time Imprisonment |———| 0 ∞
Sec 67	Punishment for publishing/transmitting obscene (attracting lust) material in Electronic form Whoever publishes/transmit in Electronic form any material - which Is Lascivious - appeals to the prurient interest - Effect is to deprave/Corrupt persons by reading, seeing, hearing the matter contained	Ist time |———| 0 3yrs + 5Lacs II time |———| 0 5yrs + 10Lacs

Sec 67A	Punishment for publishing / transmitting material containing sexually explicit act in electronic form Whosoever publishes / transmit in electronic form any material which contains sex intercource / abuse etc.	Ist ⊢⊣ 5yrs + 10 Lacs IInd ⊢⊣ 7yrs + 10 Lacs
Sec 67B	Punishment for publishing / transmitting material depicting children in any sexually explicit act in Electronic form Whosoever - publishes/transmit material which depicts children engaged in sexually explicit act or - Creates text/ digital images/advertises or distributes any material in EF - Cultivates or induces children for online relationship with another - facilitates abusing children online - Records sexually explicit act	Ist ⊢⊣ 0 5 yrs + 10 Lacs IInd ⊢⊣ 7yrs + 10 Lacs.

3 Provided that (Sec 67 & Sec 67A)

- the publicat^n is in interest of science, art, learning
- which is kept for bonafide purposes

Sec 43A

SPDI (Sensitive Personal Data Information)

- SPDI consists of passwords, financial Informat^n. (including bank account, Credit Card, Debit Card or other payment details), physical, physiological, mental health conditions, sexual orientation, medical Records etc.

- Sec 43A of IT Amendment Act imposes responsibility for protection of Stakeholders information by body corporate.

- It states that, where a body corporate processing, dealing or handling any SPDI in a Computer Resource is negligent in implementing & maintaining resonable security practices & procedures & thereby causes wrongful loss to any person

⇓

such body corporate shall be liable to pay damages by way of Compensation to the person so affected.

Computer Related Offences Examples (ADDED MAY 2021)

IT Act 2000

Example	Section Attracted
Harassment via fake public profile on social networking site & he/she labelled as 'prostitute' or a person of "loose character"	Sec 67
Email Account Hacking & obscene emails are sent	Sec 43, 66, 66A, 66C, 67, 67A, 67B
Credit Card fraud to make Online transactions	Sec 43, 66, 66C, 66D
Web Defacement (Homepage of Website is replaced with pornographic image or defamatory page.	Sec 43, 66 Sometimes 66F & 67
Introducing Viruses, Worms, Bugs, Trojans - used to destroy/gain access	Sec 43, 66
Cyber Terrorism conducted in cyberspace where criminals attempt to damage Computer systems or Telecommunication Networks	Sec 43, 66, 66A
Cyber Pornography specifically child pornography	Sec 67, 67A, 67B

Phishing - fraudently acquiring sensitive informatn like passwords	Sec 66, 66C, 66D
Theft of Confidential Information (stored by business Organisations) by rivals, criminals, dissatisfied employees	Sec 43, 66, 66B
Source Code Theft Asset of the company (most imp ie Crown Jewel)	Sec 43, 65, 66, 66B

Advantages of Cyber Laws.

- IT Act 2000, attempts to change outdated laws & provides ways to deal with Cyber crimes.
- The act offers the much needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in electronic form of records.

PRIVACY POLICY – Online Data

Information

Non- Personal (NPI)
When a Customer visits the website of Bank, Information about
- IP Address of device
- Browser Used
- Browser Version
- Operating System Used

Personal (PI)
Information which is provided by Customer Such as
- Name, address
- Mobile no, Email
- Date of Birth etc

- Every Bank captures PI of customers. Hence, it is mandatory to ensure security of PI. This information must be protected by relavant Safeguards
- further, the Employees of Banks should be trained properly in handling of Personal Information.
- Even when such services are outsourced, the vendor company is required to protect the confidentiality of PI they receive & process.

DIAGRAMMATIC REPRESENTATION

☞ AMENDED MAY 2021 (THEORY)

Data Flow Diagram (DFD's)

- DFD uses few Simple Symbols to Illustrate flow of data among external entities (such as people or other Org.)
- Flow = Informat^{n} from one place to another
- It provides overview of
  - What data a System process
  - What transformations are performed
  - What data are stored
  - What results are produced & where they flow

Flowcharts

Why?

- for controlling org. effectively, it is important to have understanding about the processes, which can be done through BPM (Business Process mapping)
- "BPM refers to gathering extensive information about the current process in an Organisation."

What?

- Flowchart is a diagram that describes a process or operation
- It includes multiple steps, through which the process "flows" from start to finish

Advantages?

Quicker grasp of R/ship	Help to depict a lengthy procedure more easily
Effective analysis	•Helps to identify problems easily • New approaches may be suggested by flowchart
Communicat^{n}	Aid/Help in Communicating the facts Easily
Efficient Coding	•Act as a guide during programming • Further, Instructions coded in programme may be checked against flowchart to see, if any omission.

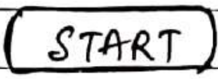
Program Debugging	Helps in detecting, locating, removing mistakes
Efficient program maintenance	Help programmer to concentrate on that part of Informat^n which needs to be modified

Limitations ?

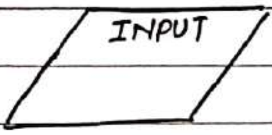
Complex	Flowchart becomes complex & clumsy where the problem logic is complex.
Modificat^n	In case of Modificat^n, it may require complete re-drawing.
Reproduct^n	Reproduct^n is often a problem bcoz Symbols used in flowchart can't be typed
Linkages	Sometimes difficult to establish link b/w various conditions & action reqd.
Standardizat^n	Flowcharts are expressed in a natural way which can't be standardized for all

Flowchart

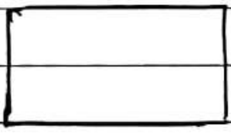
Important Symbols

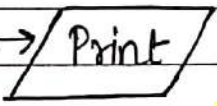
① Beginning = 

[Capsule Shape]

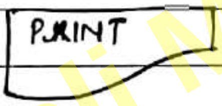
② Input /Read = 

[Parallelogram]

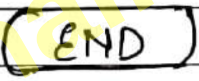
③ Processing/ working = 
[Rectangle]

④ Output ——⟹ 

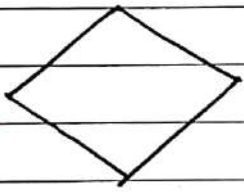
(Screen) [Parallelogram]



(Paper) [Whistle]

⑤ Ending/Stop = 

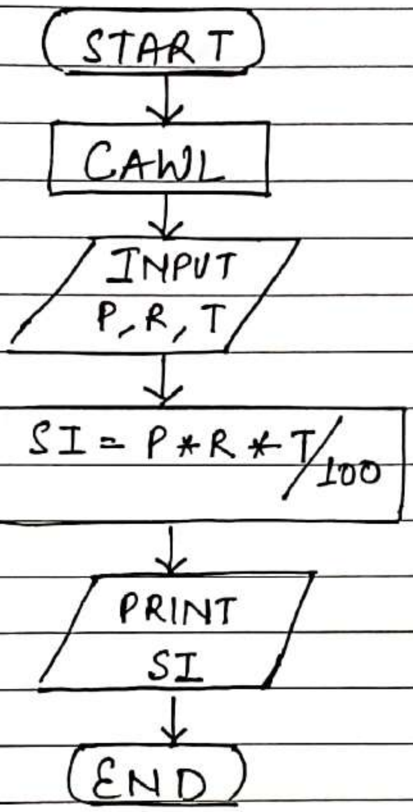
[Capsule shape]

⑥ Decision 
[Diamond/ Kaju Katli]

Important points to Remember

① Use BLOCK / CAPITAL letters
② * = Multiplicatn | / = Division
③ % Sign Not allowed (Use division/decimals)

Q1 Draw a flowchart to calculate Simple Interest (P*R*T/100)



List of abbreviations :

CAWL	=	Clear all working Locations
P	=	Principle
R	=	Rate
T	=	Time
SI	=	Simple Interest

Q2 ABC & Co of Delhi has announced a special Discount policy for all its customers.

The policy is an under-

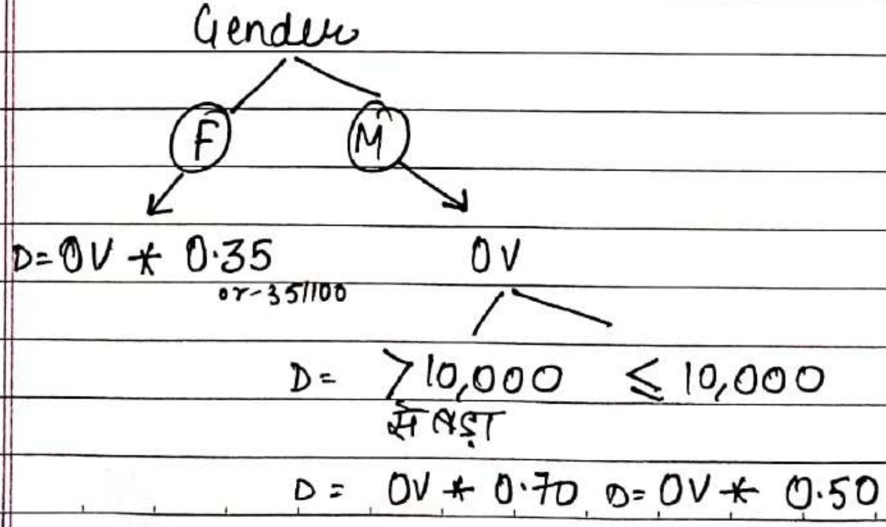
a) If the ~~policy~~ customer is female, a flat discount Of 35% is given

b) If the customer is male, a flat discount of 50% is given and, if the Value of order is more than ₹ 10,000, an additional discount of 20% (70% effective) is also given

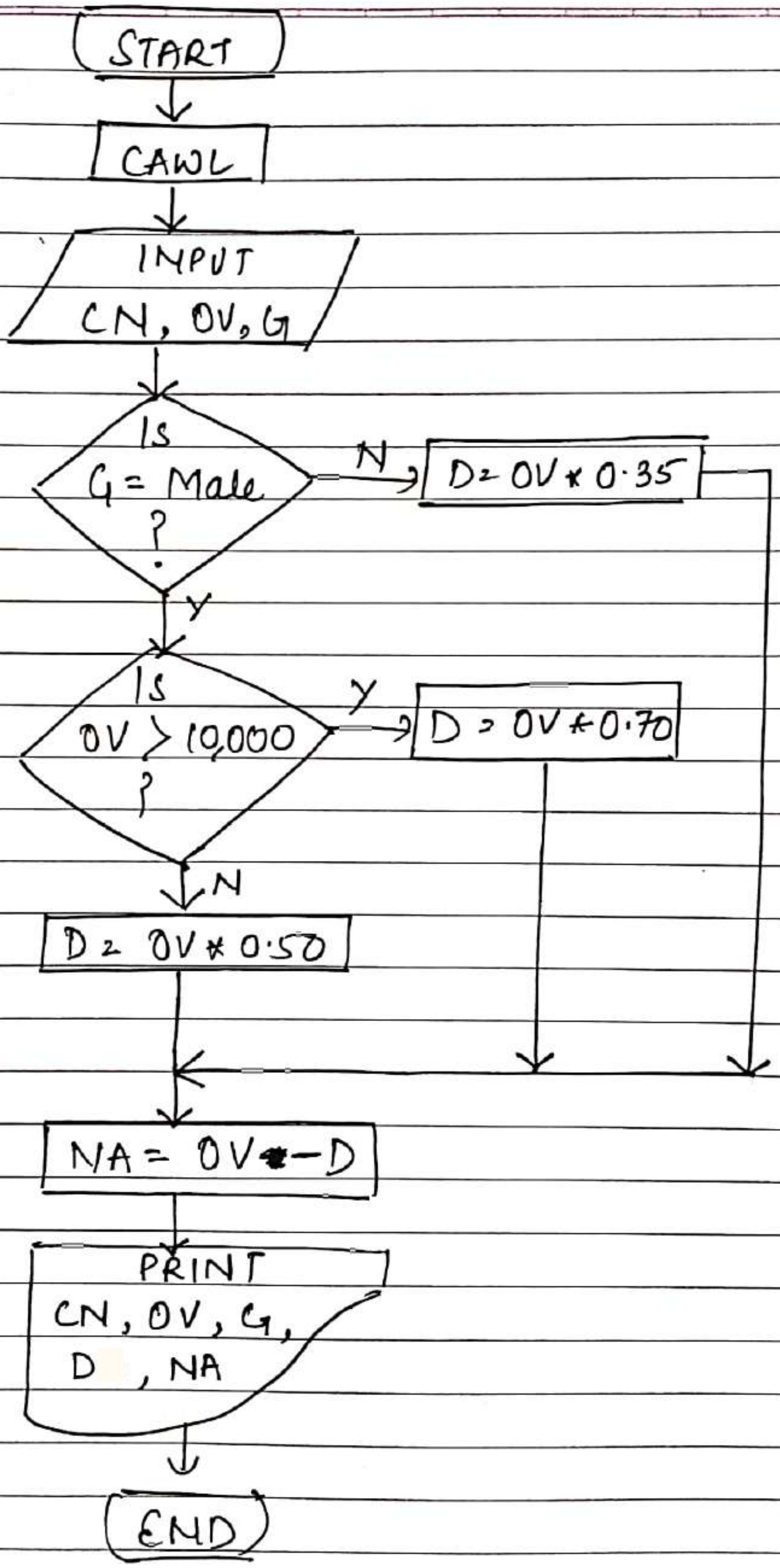
Draw a flowchart to PRINT out customer name, Order value, Gender, discount amount & Net amount for every Customer.

Workings

Input Reqd = Gender, Order Value, customer Name
= Discount Rate Automatic
= Discount Amt
= Net ~~Value~~



Solution


START
CAWL
INPUT
CN, OV, G
Is
G = Male
?
N
D= OV * 0.35
Y
Is
OV > 10,000
?
Y
D = OV * 0.70
N
D = OV * 0.50
NA = OV - D
PRINT
CN, OV, G,
D , NA
END