

Information Systems Audit Checklist

SYSTEM AUDIT CHECKLIST

ORGANISATION AND ADMINISTRATION

Audit Objective

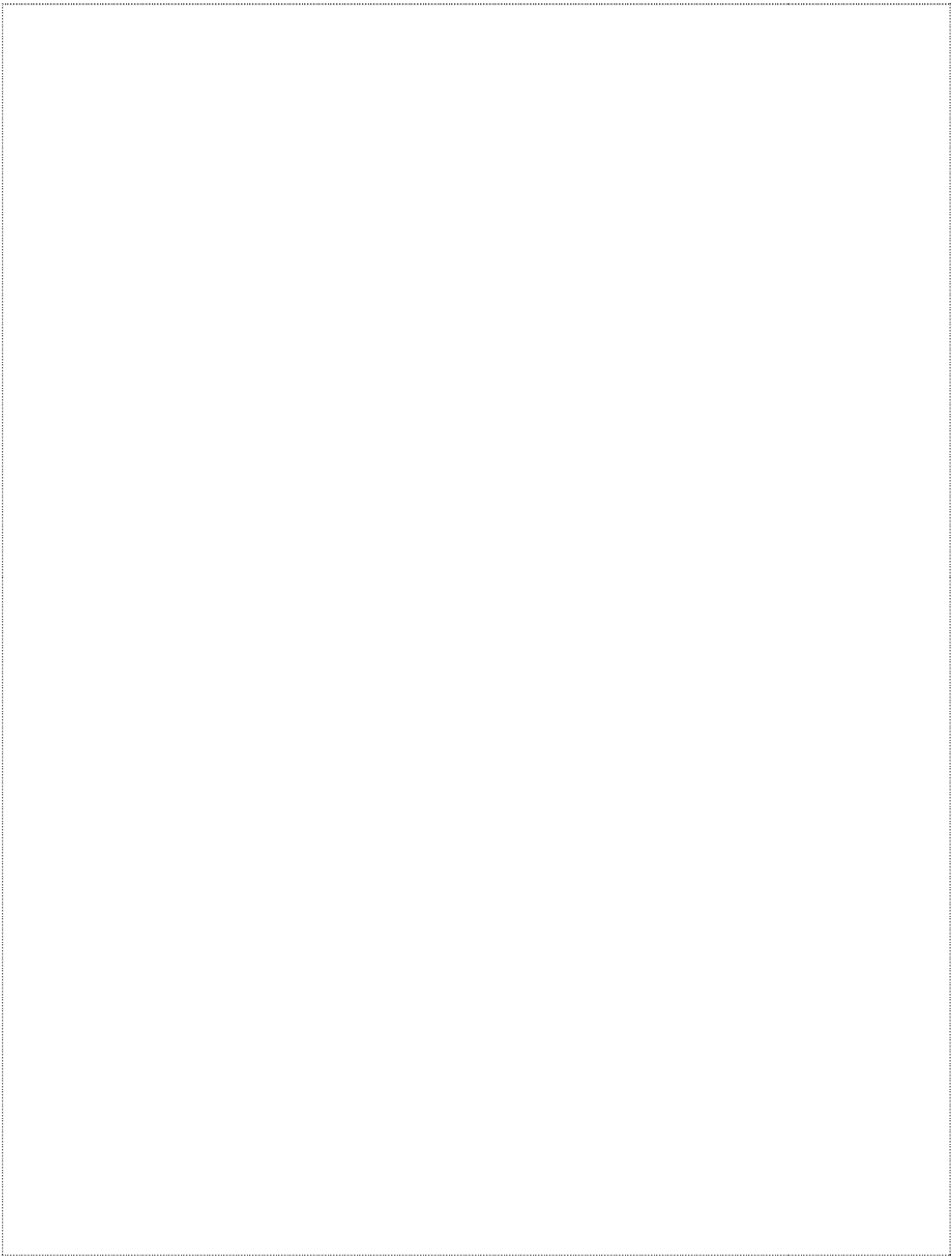
Does the organisation of data processing provide for adequate segregation of duties?

Audit Procedures

Review the company organisation chart, and the data processing department organisation chart.

	Yes/No	Comments
1 Is there a separate EDP department within the Company?		
2 Is there a steering committee and their duties and responsibilities for managing MIS are clearly defined?		
3 Has the Company developed an IT strategy linked with the long and medium term plans?		
4 Is the EDP Department independent of the user department and in particular the accounting department?		
5 Are there written job descriptions for all jobs Within EDP department and these job descriptions are communicated to designated employees?		
6 Are EDP personnel prohibited from having incompatible responsibilities or duties in user departments and vice versa?		
7 Are there written specifications for all jobs in the EDP Department?		
8 Are the following functions within the EDP Department performed by separate sections:		
System design		
Application programming		
Computer operations		
Database administration		
Systems programming		

	☐ ☐ ☐ ☐ Data entry and control?	_____	
			Yes/No Comments
9	Are the data processing personnel prohibited from duties relating to:		
	☐ Initiating transactions?	_____	_____
	☐ Recording of transactions?	_____	_____
	☐ Master file changes?	_____	_____
	☐ Correction of errors?	_____	_____
10	Are all processing prescheduled and authorised by appropriate personnel?	_____	_____
11	Are there procedures to evaluate and establish who has access to the data in the database?	_____	_____
12	Are the EDP personnel adequately trained?	_____	_____
13	Are systems analysts programmers denied access to the computer room and limited in their operation of the computer?	_____	_____
14	Do any of the computer operators have programming knowledge?	_____	_____
15	Are operators barred from making changes to programs and from creating or amending data before, during, or after processing?	_____	_____
16	Is the custody of assets restricted to personnel outside the EDP department?	_____	_____
17	Is strategic data processing plan developed by the company for the achievement of long-term business plan?	_____	_____
18	Are there any key personnel within IT department whose absence can leave the company within limited expertise?	_____	_____
19	Are there any key personnel who are being over - relied?	_____	_____
20	Is EDP audit being carried by internal audit or an external consultant to ensure compliance of policies and controls established by management?	_____	_____



PROGRAM MAINTENANCE AND SYSTEM DEVELOPMENT

Audit Objective

Development and changes to programs are authorised, tested, and approved, prior to being placed in production.

Program Maintenance

Audit Procedures

- (i) Review details of the program library structure, and note controls which allow only authorised individuals to access each library.
- (ii) Note the procedures used to amend programs.
- (iii) Obtain an understanding of any program library management software used.

	Yes/No	Comments
1 Are there written standards for program maintenance?	_____	_____
2 Are these standards adhered to and enforced?	_____	_____
3 Are these standards reviewed regularly and approved?	_____	_____
4 Are there procedures to ensure that all programs required for maintenance are kept in a separate program test library?	_____	_____
5 Are programmers denied access to all libraries other than the test library?	_____	_____
6 Are changes to programs initiated by written request from user department and approved?	_____	_____
7 Are changes initiated by Data Processing Department communicated to users and approved by them?	_____	_____
8 Are there adequate controls over the transfer of programs from production into the programmer's test library?	_____	_____
9 Are all systems developed or changes to existing system tested according to user approved test plans and standards?	_____	_____

		Yes/No	Comments
10	Are tests performed for system acceptance and test data documented?		
11	Are transfers from the development library to the production library carried out by persons independent of the programmers?		
12	Do procedures ensure that no such transfer can take place without the change having been properly tested and approved?		
13	Is a report of program transfers into production reviewed on a daily basis by a senior official to ensure only authorised transfers have been made?		
14	Are all program changes properly documented?		
15	Are all changed programs immediately backed up?		
16	Is a copy of the previous version of the program retained (for use in the event of problems arising with the amended version)?		
17	Are there standards for emergency changes to be made to application programs?		
18	Are there adequate controls over program recompilation?		
19	Are all major amendments notified to Internal audit for comment?		
20	Are there adequate controls over authorisation, implementation, approval and documentation of changes to operating systems?		

System Development

1	Are there formalised standards for system development life cycle procedure?		
2	Do they require authorisation at the various stages of development – feasibility study, system specification, testing, parallel running, post implementation review, etc.?		

	Yes/No	Comments
3 Do the standards provide a framework for the development of controlled applications?		
4 Are standards regularly reviewed and updated?		
5 Do the adequate system documentation exist for:		
☐ Programmers to maintain and modify programs?		
☐ Users to satisfactorily operate the system?		
☐ Operators to run the system?		
6 Have the internal audit department been involved in the design stage to ensure adequate controls exist?		
7 Testing of programs - see Program Maintenance.		
8 Procedures for authorising new applications to production - see Program Maintenance		
9 Are user and data processing personnel adequately trained to use the new applications?		
10 Is system implementation properly planned and implemented by either parallel run or pilot run?		
11 Are any differences and deficiencies during the implementation phase noted and properly resolved?		
12 Are there adequate controls over the setting up of the standing data and opening balances?		
13 Is a post implementation review carried out?		
14 Are user manuals prepared for all new systems developed and revised for subsequent changes?		
15 Is there a Quality Assurance Function to verify the integrity and acceptance of applications developed?		

**Purchased
Software**

	Yes/No	Comments
1 Are there procedures addressing controls over selection, testing and acceptance of packaged softwares?		
2 Is adequate documentation maintained for all softwares purchased?		
3 Are vendor warranties (if any) still in force?		
4 Is the software purchased, held in escrow?		
5 Are backup copies of user/operations manual kept off-site?		

ACCESS TO DATA FILES

Audit Objective

Is access to data files restricted to authorised users and programs?

Access to Data

1 Is there any formal written data security policy? Consider whether the policy addresses data ownership, confidentiality of information, and use of password.		
2 Is the security policy communicated to individuals in the organisation?		
3 Is physical access to off line data files controlled in:		
☐ Computer room?		
☐ On-site library?		
☐ Off-site library?		
4 Does the company employ a full-time librarian who is independent of the operators and programmers?		
5 Are libraries locked during the absence of the librarian?		
6 Are requests for on-line access to off line files approved?		

		Yes/No	Comments
7	Are requests checked with the actual files issued and initialled by the librarian?	_____	_____
8	Are sensitive applications e.g. payroll, maintained on machines in physically restricted areas?	_____	_____
9	Are encryption techniques used to protect against unauthorised disclosure or undetected modification of sensitive data?	_____	_____
10	Are returns followed up and non returns investigated and adequately documented?	_____	_____

Computer Processing

11	Does a scheduled system exist for execution of programs?	_____	_____
12	Is there a comparison between actual and scheduled processing?	_____	_____
13	Are non-scheduled jobs approved prior to being run?	_____	_____
14	Is the use of utility programs controlled (in particular those that can change executable code or data)?	_____	_____
15	Are program tests restricted to copies of live files?	_____	_____
16	Is access to computer room restricted to only authorised personnel?	_____	_____
17	Are internal and external labels used on files?	_____	_____
18	Are overrides of system checks by operators controlled?	_____	_____
19	Are exception reports for such overrides pointed and reviewed by appropriate personnel?	_____	_____
20	Are sufficient operating instructions exist covering procedures to be followed at operation?	_____	_____

Database

	Yes/No	Comments
21 Does the position of database administrator (DBA) exist? If not note who is responsible for:		
☐ Defining user and program access	_____	_____
☐ Mediating between users who share data	_____	_____
☐ Maintaining the integrity of the database	_____	_____
☐ Setting standards of backup and recovery	_____	_____
22 Is the DBA restricted from:		
☐ Having control over company assets	_____	_____
☐ Initiating and recording transactions	_____	_____
23 Are logs maintained of the use of utilities, changes to access methods, etc.?	_____	_____
24 If so, are these independently reviewed?	_____	_____
25 Does the DBMS have the facility to abort jobs when two users, with the same priority, are locked out from the same chain of data?		
26 Is integrity checking programs run periodically for checking the accuracy and correctness of linkages between records?	_____	_____

Password and other online controls

Audit Procedure

- (i) Note procedures for issuing, amending, and deleting passwords. (ii) Obtain an understanding of any access control software used.

1 Do formal procedures exist for the issue and subsequent control of passwords?	_____	_____
---	-------	-------

		Yes/No	Comments
2	Is there any proper password syntax in-force i.e. min. 5 and max. 8 characters and include alphanumeric characters.		
3	Are there satisfactory procedures for reissuing passwords to users who have		
4	Are procedures in place to ensure the compliance removal of terminated employee passwords?		
5	Are system access compatibilities properly changed with regard to personnel status		
6	Are individual job responsibilities considered when granting users access privileges?		
7	Is each user allocated a unique password and user account?		
8	Are there procedures in place to ensure forced change of password after every 30 days?		
9	Is application level security violations logged?		
10	Do standards and procedures exist for follow up of security violations?		
11	Do formal and documented procedures exist for use and monitoring of dial up access facility?		
12	Is use made of passwords to restrict access to specific files?		
13	Do terminals automatically log off after a set period of time?		
14	Is there a limit of the number of invalid passwords before the terminal closes down?		
15	Are there any administrative regulations limiting physical access to terminals?		
16	Are invalid password attempts reported to user department managers?		
17	Are restrictions placed on which applications terminals can access?		

	Yes/No	Comments
18 Are keys, locks, cards or other physical devises used to restrict access to only authorised user?	_____	_____

APPLICATION CONTROLS

Input

Audit Objective

Do controls provide reasonable assurance that for each transaction type, input is authorised, complete and accurate, and that errors are promptly corrected?

1 Are all transactions properly authorised before being processed by computers?	_____	_____
2 Are all batches of transactions authorised?	_____	_____
3 Do controls ensure unauthorised batches or transactions are prevented from being accepted i.e. they are detected?	_____	_____
4 Is significant standing data input verified against the master file?	_____	_____
5 Is maximum use made of edit checking e.g. check digits, range and feasibility checks, limit tests, etc.?	_____	_____
6 Are there procedures to ensure all vouchers have been processed e.g. batch totals, document counts, sequence reports, etc.?	_____	_____
7 Are there procedures established to ensure that transactions or batches are not lost, duplicated or improperly changed?	_____	_____
8 Are all errors reported for checking and correction?	_____	_____
9 Are errors returned to the user department for correction?	_____	_____
10 Do procedures ensure these are resubmitted for processing?	_____	_____

		Yes/No	Comments
11	Is an error log maintained and reviewed to identify recurring errors?	_____	_____
12	Are persons responsible for data preparation and data entry independent of the output checking and balancing process?	_____	_____
13	Are persons responsible for data entry prevented from amending master file data?	_____	_____

Output and Processing

Audit Objective

The controls provide reasonable assurance that transactions are properly processed by the computer and output (hard copy or other) is complete and accurate, and that calculated items have been accurately computed:

1	Is there any formal written output distribution policy?	_____	_____
2	Are hard copy reports:		
	☐ Headed	_____	_____
	☐ Pages numbered	_____	_____
	☐ Dated	_____	_____
	☐ Identified by report/program number	_____	_____
	☐ Adequately totalled/control totalled	_____	_____
	☐ Designed to give an "End of Report" message, if not obvious?	_____	_____
3	Are significant reports distributed to only authorised personnel in line with an approved distribution list?	_____	_____
4	Are there formal procedures for checking, filing and retention of reports?	_____	_____
5	Where output from one system is input to another, are run to run totals, or similar checks, used to ensure no data is lost or corrupted?	_____	_____

		Yes/No	Comments
6	Are there adequate controls over forms that have monetary value?	_____	_____
7	Is maximum use made of programmed checks on limits, ranges reasonableness, etc. and items that are detected reported for investigation?	_____	_____
8	Where calculations can be 'forced' i.e. bypass a programmed check, are such items reported for investigation?	_____	_____
9	Where errors in processing are detected is there a formal procedure for reporting and investigation?	_____	_____
10	Is reconciliation between input, output and brought forward figures carried out and differences investigated?	_____	_____
11	Are suspense accounts checked and cleared on a timely basis?	_____	_____
12	Are key exception reports reviewed and acted upon on a timely basis?	_____	_____

Viruses

1	Is there any formal written anti-virus policy?	_____	_____
2	Is the policy effectively communicated to individuals in the organisation?	_____	_____
3	Is there a list of approved software and suppliers?	_____	_____
4	Is only authorised software installed on microcomputers?	_____	_____
5	Is there a master library of such software?	_____	_____
6	Are directories periodically reviewed for suspicious files?	_____	_____
7	Are files on the system regularly checked for size changes?	_____	_____

		Yes/No	Comments
8	Is anti-virus software installed on all microcomputers?	_____	_____
9	Is anti-virus software regularly updated for new virus definitions?	_____	_____
10	Are suspicious files quarantined and deleted from the terminal's hard drive and network drive?	_____	_____
11	Are diskettes formatted before re-use?	_____	_____
12	Have procedures been developed to restrict or oversee the transfer of data between machines?	_____	_____
13	Is staff prohibited from sharing machines?	_____	_____
14	Is software reloaded from the master diskettes after machine maintenance?	_____	_____
15	Has all staff been advised of the virus prevention procedures?	_____	_____
16	Are downloads from internet controlled by locking the hard-drive and routing it through network drive to prevent the virus (if any) from spreading?	_____	_____

INTERNET

1	Is there any proper policy regarding the use of internet by the employees?	_____	_____
2	Does the policy identify the specific assets that the firewall is intended to protect and the objectives of that protection?	_____	_____
3	Does the policy support the legitimate use and flow of data and information?	_____	_____
4	Is information passing through firewall is properly monitored?	_____	_____
5	Determine whether management approval of the policy has been sought and granted and the date of the most recent review of the policy by management.	_____	_____

		Yes/No	Comments
6	Is the policy properly communicated to the users and awareness is maintained?	_____	_____
7	Have the company employed a Firewall Administrator?	_____	_____
8	Is firewall configured as per security policy?	_____	_____
9	Is URL screening being performed by Firewall?	_____	_____
10	Is anti-virus inspection enabled?	_____	_____
11	Are packets screened for the presence of prohibited words? If so, determine how the list of words is administered and maintained.	_____	_____
12	Are access logs regularly reviewed and any action is taken on questionable entries?	_____	_____

CONTINUITY OF OPERATIONS AND PHYSICAL PROTECTION

1 Fire Hazard

Fire resistance:

☐ Building materials fire resistant	_____	_____
☐ Wall and floor coverings non-combustible	_____	_____
☐ Separation from hazardous areas (e.g. fire doors)	_____	_____
☐ Separation from combustible materials (e.g. paper, fuel)	_____	_____

	Yes/No	Comments
☐ Smoking restriction	_____	_____
☐ Fire resistant safes (for tapes, disks and documentation)	_____	_____
Fire detection:		
☐ Smoke / Heat-rise detectors		
☐ Detectors located on ceiling and under floor	_____	_____
☐ Detectors located in all key EDP areas	_____	_____
☐ Linked to fire alarm system	_____	_____
Fire extinction:		
☐ Halon gas system (for key EDP areas)	_____	_____
☐ Automatic sprinkler system	_____	_____
☐ Portable CO ₂ , extinguishers (electrical fires)	_____	_____
☐ Ease of access for fire services	_____	_____
Fire emergency:		
☐ Fire instructions clearly posted	_____	_____
☐ Fire alarm buttons clearly visible	_____	_____
☐ Emergency power-off procedures posted	_____	_____
☐ Evacuation plan, with assignment of responsibilities	_____	_____
Fire practices:		
☐ Regular fire drill and training	_____	_____
☐ Regular inspection/testing of all equipment	_____	_____

	Yes/No	Comments
2 <u>Water Damage</u>		
EDP area located above ground level	_____	
Building weather protected (eg. Storms, water leaks)	_____	_____
Computer room drainage facilities	_____	_____
3 <u>Air Conditioning</u>		
Monitoring of temperature and humidity in EDP area	_____	_____
Heat, fire and access protection of sensitive air conditioning parts (eg. cooling tower)	_____	_____
Air intakes located to avoid undesirable pollution	_____	_____
Back-up air conditioning equipment	_____	_____
4 <u>Power Supply</u>		
Reliable local power supply	_____	_____
Separate computer power supply	_____	_____
Line voltage monitored	_____	_____
Power supply regulated (For voltage fluctuation)	_____	_____
Uninterrupted power supply (eg. Battery system) available	_____	_____
Alternative power supply (eg. Generator)	_____	_____
Emergency lighting system	_____	_____

	Yes/No	Comments
5 <u>Communications Network</u>		
Physical protection of communications lines modems, multiplexors and processors	_____	_____
Location of communication equipment separate from main EDP equipment		_____
Back-up and dial-up lines for direct lines	_____	_____
6 <u>Machine Room Layout</u>		
Printers, plotters located in separate area	_____	_____
Printout preparation (eg. bursting) located in separate area	_____	_____
Tape/Disk library in separate area Machine room kept tidy	_____	_____
Practical location of security devices	_____	_____
Emergency power off switches	_____	_____
Alarms	_____	_____
Extinguishers	_____	_____
Environment monitoring equipment	_____	_____

B ACCESS CONTROL

1 <u>Entrance Routes (EDP areas):</u>		
No unnecessary entrances to the computer room	_____	_____
Non-essential doors always shut and locked to the outside (eg. Fire exits)	_____	_____
Air vent and daylight access location protected	_____	_____
Use of all open doors controlled	_____	_____

	Yes/No	Comments
2 <u>Access Control:</u>		
Access restricted to selected employees	_____	_____
Prior approval required for all other employees	_____	_____
Entrance door controlled by:		
☐ Screening by a guard	_____	_____
☐ Locks/combinations	_____	_____
☐ Electronic badge/key	_____	_____
☐ Other (specify)	_____	_____
Positive identification of all employees (eg. identification card)	_____	_____
All unknown personnel challenged	_____	_____
Verification of all items taken into and out of the computer room	_____	_____
Access controlled on 24 hours basis including weekends (e.g. automatic control mechanism)	_____	_____
Locks, combinations, badge codes changed periodically	_____	_____
Is access to copies of the documentation kept in a secure location?		
3 <u>Visitor Control:</u>		
Positive identification always required	_____	_____
Temporary badges issued, controlled and returned on departure	_____	_____
All visits logged in and out	_____	_____
Visitors accompanied and observed at all times	_____	_____

	Yes/No	Comments
4 <u>Terminal Security:</u>		
All terminals located in secure areas	_____	_____
Alarm system used to control microcomputers from being disconnected or moved from its location.	_____	_____
Sensitive applications e.g. payroll, maintained on machines in physically restricted area.	_____	_____
Terminal keys/locks used	_____	_____
Passwords changed regularly	_____	_____
Identification labels been placed on each terminal.	_____	_____
5 <u>General Security</u>		
Waste regularly removed from EDP area and sensitive data shredded	_____	_____
Window and door alarm system	_____	_____
Closed circuit television monitoring	_____	_____

C PERSONNEL POLICIES

1	New employees recruited according to job description and job specification	_____	_____
2	Employee identity cards issued	_____	_____
3	Performance evaluation and regular counselling	_____	_____
4	Continuing education program	_____	_____
5	Training in security, privacy and recovery procedures	_____	_____
6	All functions covered by cross training	_____	_____
7	Critical jobs rotated periodically (e.g. operators, program maintenance)	_____	_____

	Yes/No	Comments
8	Clean desk policy enforced	_____
9	Fidelity insurance for key personnel	_____
10	Contract service personnel vetted (e.g. cleaners)	_____

D INSURANCE

1	Does adequate insurance exist to cover:	_____
	☐ Equipment?	_____
	☐ Software and documentation?	_____
	☐ Storage media?	_____
	☐ Replacement / re-creation cost?	_____
	☐ Loss of data/assets (eg. Accounts receivable)?	_____
	☐ Business loss or interruption (business critical systems)?	_____
2	Is adequate consideration given to cover additional cost of working and consequential	_____

E BACK-UP PROCEDURES

1	<u>Equipment (computer and ancillary):</u>	
	Regular preventive maintenance	
	Reliable manufacturer service	_____
	Arrangements for back-up installation	_____
	Formal written agreement	_____
	Compatibility regularly checked	_____
	Sufficient computer time available at back-up	_____
	Testing at back-up regularly performed	_____

	Yes/No	Comments
2 Outside Suppliers (non continuance / disaster):		
(eg. suppliers of equipment, computer time, software)	_____	_____
Alternative sources of supply / maintenance / service available	_____	_____
Adequate and secure documentation/back-up of data and programs	_____	_____
Are backup copies of system documentation kept in a secure location?		
3 <u>Off-site Storage:</u>		
Secure separate location	_____	_____
Adequate physical protection (see section A)	_____	_____
Log maintained of off-site materials		
Off-site Inventory regularly reviewed	_____	_____
File transportation under adequate physical protection	_____	_____
Back-up files periodically tested	_____	_____
4 <u>Data Files:</u>		
File criticality and retention procedure regularly reviewed	_____	_____
<i>Tape</i>		
At least three generations of important tape files retained	_____	_____

Yes/No

Comments

Copies of all updating transactions for above retained

At least one generation and all necessary updating transactions in off-site storage

Disc

Checkpoint/restart procedures provided for

Audit trail (log file) of transactions updating on-line files (data base) maintained

Regular tape dumps of all disc files stored off-site

Audit trail (log file) regularly dumped and stored off-site

5 Software:

Copies of following maintained at off-site storage:

Production application programs

Major programs under development

System and program documentation

Operating procedures

Operation and system software

All copies regularly updated

Back-up copies regularly tested

6 Operations

Back-up procedure manual

Priority assignments for all applications

Procedures for restoring data files and software

Procedures for back-up installation

Yes/No

Comments

F DISASTER RECOVERY PLANS

1	Is a comprehensive contingency plan developed, documented and periodically tested to ensure continuity in data processing services?		
2	Does the contingency plan provide for recovery and extended processing of critical applications in the event of catastrophic disaster?		
3	Has any Business Impact Analysis carried out by the company?		
3	Are all recovery plans approved and tested to ensure their adequacy in the event of disaster?		
4	Communicated to all management and personnel concerned		
5	Critical processing priorities identified (eg. Significant accounting applications)		
6	Are disaster recovery teams established to support disaster recovery plan?		
7	Are responsibilities of individuals within disaster recovery team defined and time allocated for completion of their task?		
8	Operations procedures for use of equipment and software back-up		
9	Has the company developed and implemented adequate plan maintenance procedures?		
10	Are priorities set for the development of critical systems?		
11	Does a hardware maintenance contract exist with a reputable supplier?		

Yes/No

Comments

12 Does the recovery plan ensure, in the event of failure:

- ☐ No loss of data received but not processed
- ☐ No reprocessing of data already processed
- ☐ Files not corrupted by partially completed processing

13 Are recovery plans regularly tested?

CA SATISH KUMAR V
9885328512