IT Audit Report 2022-2023

NAGINDAS KHANDWALA COLLEGE (AUTONOMOUS)

Appendix

I. Audit Checklist: List of Documents for understanding the system

No.	List of documents
1	Brief background of the organization
2	Organizational chart
3	Personnel policy
4	List of applications and their details
5	Network and application architecture
6	Organizational structure of the IT department with job descriptions
7	IT department's responsibilities with reference to the specific application
8	Details of hardware and Internet Connectivity
9	Details of software (including whether developed in-house etc.)
10	Database details
11	Details of interfaces
12	Systems manual, User manual and Operations manual
13	List of users with permissions
14	Security Setup

II. Audit Checklist: Criticality Assessment Tool

1	**Does the system relate to any of the following**		
	Business Critical Operations	Yes / No	Evaluation Remarks
	Support Functions		
	For example, Payroll, Inventory, Financial Accounting, Procurement, Marketing etc.	Yes	
2	**Investment made in the System**		
3	**General state of computerization in the entity. The entity has computerized**	Yes	
	Most of the Business processes	Yes	
	Most of the Accounting and Financial Processes	Yes	
4	**Number of PCs/Desktops used for the system**		
	More than 100	Yes	
	More than 50, less than 100		
	More than 20, less than 50		
	More than 10 less than 20		
	Less than 10		
5	**Is the system on the network?**		
	Yes	Yes	
	No		
	If the system is on the network, is it connected to		
	Internal LAN and/or on intranet?	Yes	
	WAN and MAN and/or on extranet?		
	Web based /public domain?		
6	**The system is functioning at**		
	Only one location	Yes	
	More than one, less than 5 locations		
	Name of the Office: Nagindas Khandwala College		
	Preliminary Information		
	More than 5 locations		
	Is proposed to be expanded in more than one location	No	
7	**The entity is dependent on the system in as much as**		
	Outputs are used for business-critical operations /revenue generation	Yes	
	Outputs are manually checked before making payments/raising bills	Yes	
	Outputs are used to prepare Financial Statements	Yes	
	Outputs are not used at all for payment/revenue		
8	**Do the public have access to such data either through web or any other means?**		
	Yes, Public can view the data in a dynamic manner	Yes	
	No, Public cannot view the data	Yes	

	Public can transact on-line	Yes	
	Note- The access is limited to the stack holders with authentic Login credentials		
9	**Does the System make use of direct links to third parties e.g. ERP/MIS**		
	Yes	Yes	
	No		
10	**Does the Organization have dedicated IT Staff?**		
	Less than 10	Yes	
	More than 10, less than 30		
	More than 70		
11	**Approximately how many persons can be termed as the end-users of the system?**		
	Name of the Institution: Nagindas Khandwala College		
	Preliminary Information		
	Less than 5		
	More than 5, less than 25		
	More than 25, less than 70	Yes	
	More than 70, less than 150		
	More than 150		
12	**The system is in operation for**		
	More than 10 years	Yes	
	Less than 10 years but more than 5 years		
	Less than 5 years but more than 2 years		
	Less than 2 years		
13	**The system is based on**		
	Batch Processing		
	On Line Transaction Processing	Yes	
14	**Are there formal change management procedures?**		
	Yes	Yes	
	No		
	How often changes are made to the applications		
	More than 5 times in a year	Yes	
	Less than 5 times in a year more than twice in a year		
	Less than twice in a year		
	Not even once in a year		
15	**Does the entity have a documented and approved security policy?**		
	Yes	Yes	
	No		
16	**Does the entity have a Systems Security Officer?**		
	Yes	Yes	
	No		
	Name of the Officer: Dr. Sindhu P. M. (Academics), Ms. Kalpana Divekar (Administration)		
	Preliminary Information		
17	**Does the entity have a documented and**		
	Disaster Recovery Plan?		

	Yes	Yes	
	No		
18	**Volume of data in the system (including offline data) is**		
	More than 10 GB	Yes **(10 TB)**	
	More than 2 GB less than 10 GB		
	Less than 2 GB		
	Less than 1 GB		
Remarks and Observations (At the end of the document)			

III. Audit Checklist: Collection of specific information on IT Systems

Form 1

1. Name of the auditee organization:	Nagindas Khandwala College of Commerce, Arts and Management Studies and Shantaben Nagindas Khandwala College of Science. (Autonomous)
2. Date on which information collected:	01/03/2023
3. Name of the IT Application and broad functional areas covered by the IT Application:	Mastersoft ERP All areas including Admission, Examination, Administration
4. Auditor I	Dr. Hiren Dand Head, Department of Information Technology Mulund College of Commerce, S. N. Road, Mulund West, Mumbai 400080

5. Department Head of the Auditee Organization: Name: Phone No: Email:	Prof. Dr. Moushumi Datta Nagindas Khandwala College (Autonomous) 28072262 Principal@nkc.ac.in
6. Information Systems in-charge: Name: Phone No: Email:	Dr. Sindhu P.M. (Academic) Kalpana S. Divekar (IT Administration) 28072262 kalpana@nkc.ac.in
7. What is (are) the location(s) of the IT system installation(s)?	Nagindas Khandwala College (Autonomous)
8. State the category of IT system architecture:	Education
9. State the category of IT application. (Please indicate the choice(s) applicable):	--
10. Whether the above IT application has got a bearing on the financial and accounting aspects of the organization?	--

11. Software used (the Version may also be specified):							
Operating system(s)	Windows 7, 10, 11						
Network software	Tally Erp						
Communication Software	--						
DBMS / RDBMS	--						
Programming Language(s)	--						
Bespoke (Vendor developed)	CIMS, SLIM, DMS						
Utility Software	--						
12. Is the IT system a mission critical system or an essential system?	ESSENTIAL						
13. Has the application system been developed in house or by outsourcing?	Outsourcing						
14. In case of outsourcing, specify the name of agency and the contracted amount:							
15. When the system was made operational?	**MM**		**YYYY**				
	0	9	1	9	9	4	
16. Number of persons engaged for operation of the system.	07						
17. What is the average volume of transactional data generated on a monthly basis in terms of storage space?	5 GB						
18. Does the system documentation provide for an audit trail of all transaction processed and maintained?	Yes						

19. Are the manuals as indicated available?	
a. Users' documentation manual	Yes
b. Systems and programming documentation manual	NA
20. Is there any system in place to make modifications to the application being used on a regular basis to support the function?	Yes (Through Email)
21. Does the organization transmit/receive data to/from other organizations?	No.

Form 2

22. Details of all Hardware items including the number of terminals etc. employed:
    - Separate Record file is maintained.

23. Details of networking hardware employed:

Switches	32
Wi-Fi Routers	39
Server	05

24. Are more than one IT Application(s) running on the same Hardware? If yes, specify the name(s) of such IT Application(s)
    NO

IV. Audit Check List: Check list for risk assessment

No	Item	Response	
		Y	N
1.	Is there a strategic IT plan for the organization based on Business needs?	Y	
2.	Is there a steering committee with well-defined roles and Responsibilities?	Y	
3.	Does the IT department have clear cut and well-defined goals and targets?	Y	
4.	Is there a system of reporting to top management and review in vogue?	Y	
5.	Is there a separation of duties and well-defined job Characteristics in the IT Department?	Y	
6.	Are there appropriate policies and procedures in relation to Retention of electronic records?	Y	
7.	Where the organization uses third parties to process data, does It have appropriate procedures in place to address associated risks?	Y	
8.	Are there procedures to update strategic IT plan?	Y	
	Personnel policy		
9.	Whether criteria are used for recruiting and selecting Personnel?	Y	
10.	Whether a training needs analysis is done at periodical Intervals?	Y	
11.	Whether training programmers are periodically held to update Knowledge?	Y	
12.	Whether organization's security clearance process is adequate?	Y	
13.	Whether employees are evaluated based on a standard set of Competency profiles for the position and evaluations are held on a periodic basis?	Y	
14.	Whether responsibilities and duties are clearly identified?	Y	
15.	Whether backup staff is available in case of absenteeism?	Y	
16.	Whether there is a rotation of staff policy in key areas where uninterrupted functioning is essential	Y	
	Security		
17.	Is there a strategic security plan in place providing centralized? Direction and control over information system security?	Y	
18.	Is there a centralised security organization responsible for Ensuring only appropriate access to system resources?	Y	
19.	Is there a data classification schema in place?	Y	
20.	Is there a user security profile system in place to determine Access on a "need to know basis"?	Y	
21.	Is there an employee indoctrination/training system in place That includes security awareness, ownership responsibility and virus protection requirements?	Y	
22.	Whether cryptographic modules and key maintenance Procedures exist, are administered centrally and are used for all external access and transmission activity?	Y	
23.	Whether preventative and detective control measures have Been established by management with respect to computer viruses?	Y	
24.	Whether change control over security software is formal and Consistent with normal standards of system development and maintenance?	Y	
25.	Whether password policy exists	Y	

26.	Whether access to the VoiceMail service and the PBX system Are controlled with the same physical and logical controls as for computer systems?	Y	
27.	Whether access to security data such as security management, Sensitive transaction data, passwords and cryptographic keys is limited to a need-to-know basis?	Y	
	Physical & Logical access		
28.	Whether facility access is limited to least number of people?	Y	
29.	Whether "Key" and "including ongoing card reader" Management procedures and practices are adequate, update and review on a least-access-needed basis?	Y	
30.	Whether access and authorisation policies on entering/leaving, Escort, registration, temporary required passes, surveillance cameras as appropriate to all and especially sensitive areas are adequate?	Y	
31.	Is there a periodic and ongoing review of access profiles, Including managerial review?	Y	
32.	Whether security and access control measures include Portable and/or off-site used information devices?	N	
33.	Whether review occurs of visitor registration, pass assignment, escort, person responsible for visitor logbook to ensure both check in and out occurs and receptionist's understanding of security procedures?	N	
34.	Is there a system of reviewing fire, weather, electrical warning and alarm procedures and expected response scenarios for various levels of environmental emergencies?	Y	
35.	Is there a system of reviewing air conditioning, ventilation,	Y	
36.	Whether health, safety and environmental regulations are Being complied with?	Y	
37.	Whether physical security is addressed in the continuity plan?	Y	
38.	Whether specific existence of alternative infrastructure items necessary to implement security: • uninterruptible power source (UPS) • alternative or rerouting of telecommunications lines • alternative water, gas, air conditioning, humidity resources	**No power failure**	
39.	Are there procedures to update physical and logical access Procedures?	Y	
	Business Continuity & Disaster Recovery		
40.	Have the business-critical systems been identified?	Y	
41.	Has an appropriate business continuity plan been developed, Documented and approved?	Y	
42.	Whether regular review and update of the plan has been Carried out?	Y	
43.	Are back up copies of data files and programs taken Regularly?	Y	
44.	Are the documents of the system and disaster recovery plan Appropriately backed up?	Y	
45.	Are back up copies held in secure locations both locally and Remote from the computer site?	Y	
46.	Are the back-up and recovery procedures appropriately Tested?	Y	
47.	Are the business systems and operations effectively designed to minimize disruption?	Y	

48.	Are there procedures to update business continuity and Disaster recovery plan?	Y	
	Hardware		
49.	Is there an organization policy for upgrading the hardware based on technology changes?	Y	
50.	Is there an effective preventive maintenance program in place for all significant equipment?	Y	
51.	Is equipment downtime kept within reasonable limits (say <5%)	Y	
52.	Is a reasonable effort made to acquire data centre and networking hardware that is compatible with the existing environment?	Y	
53.	Is anyone in the IT organization responsible for identifying potentially unnecessary equipment and taking appropriate action?	Y	
54.	Is a formal inventory of all IT hardware available?	Y	
55.	Are there procedures to update documentation whenever Changes made in the hardware?	Y	
	Software		
56.	Is the software used covered by adequate licences?	Y	
57.	Is the source code available and if so, accessible at what level?	Y	
58.	Is there a system of recording changes to the applications?	Y	
59.	Are these changes properly authorized?	Y	
60.	Whether emergency change procedures are addressed in Operation manuals?	Y	
61.	Whether proper testing was carried out and results recorded before final implementation of application?	Y	
62.	Is there an exception reporting system in place?	Y	
63.	In the case of bought out software, are there agreements in place for maintenance and service?	Y	
64.	Is there a system of obtaining user feedback and reporting action taken thereon to management?	Y	
65.	Is the application design documented?	NA	
66.	Whether the programs are documented?	NA	
67.	Is the testing methodology documented?	Y	
68.	Whether operations procedures are documented?	Y	
69.	Whether user manuals are available?	Y	
70.	Do manuals include procedures for handling exceptions?	Y	
71.	Are there procedures to update documentation when an application changes?	Y	
	Data Management		
72.	Whether for data preparation the following exist: • data preparation procedures ensure completeness, accuracy and validity • authorisation procedures for all source documents • separation of duties between origination, approval and conversion of source documents into data • periodic review of source documents for proper completion and approvals occurs	Y	

	• source document retention is sufficiently long to allow reconstruction in the event of loss, availability for review and audit, litigation inquiries or regulatory requirements		
73.	Whether for data input whether the following exist: • appropriate source document routing for approval prior to entry • proper separation of duties among submission, approval, authorisation and data entry functions • audit trail to identify source of input • routine verification or edit checks of input data as close to the point of origination as possible • appropriate handling of erroneously input data • clearly assign responsibility for enforcing proper authorisation over data	**Y**	
74.	For data processing: Whether programmes contain error prevention, detection, correction routines	**Y**	
75.	Whether error handling procedures include: • correction and resubmission of errors must be approved • individual responsibility for suspense files is defined • suspense files generate reports for non-resolved errors • suspense file prioritization scheme is available based on age and type	**Y**	
76.	Whether logs of programmes executed, and transactions Processed/rejected for audit trail exist?	**Y**	
77.	Whether there is a control group for monitoring entry activity and investigating non-standard events, along with balancing of record counts and control totals for all data processed?	**Y**	
78.	Whether written procedures exist for correcting and Resubmitting data in error including a non-disruptive solution to reprocessing?	**Y**	
79.	Whether resubmitted transactions are processed exactly as Originally processed?	**Y**	

Remarks:

1. The Systems are in place and well maintained
2. The office is effectively using the IT for all the day-to-day activities
3. The library is automated with iSLIM and it is being effectively used
4. The computer laboratories are well-maintained

Suggestions:

1. The RAM in the computer lab used for M.Sc. I.T may be increased from 8 GB to 32 GB for all the software to work efficiently
2. The RAM of the computer lab used of B.Sc. CS and IT be increased from 8 GB to 16 GB

1/3/2023

Dr. Hiren Dand
Head, Department of Information Technology
Mulund College of Commerce
S. N. Road, Mulund West, Mumbai 400080

Date : 01.03.2023