

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES- MANILA

IT AUDIT
GUIDE QUESTIONS

LEADER: MAUI A. ESGUERRA

MEMBERS:

HANZ JOSHUA ANCUNA

SOPHIA NICOLE M. BENAVIDES

LANZ COLICO

MARIA ANGELA DAYAWON

BACKGROUND

I. Has your organization experienced any data breaches in the past 12 months?

a. Yes

☒ b. No

II. Have you conducted a formal risk assessment of your IT infrastructure in the last year?

☒ a. Yes

June, virus

b. No

III. Do you have a documented incident response plan in place for handling data breaches?

a. Yes

☒ b. No

IV. Have you encountered any unplanned server downtime that lasted more than 24 hours in the past year?

a. Yes

☒ b. No

6 Strong password
June last change

V. Do you regularly update your software and security patches on all servers and workstations?

- (a) Yes windows security
b. No windows firewall
every 3 months update

SYSTEM SECURITY

1. Is the antivirus software updated regularly to protect against the latest threats?

(Reference: NIST SP 800-83 Rev 1)

- ☒ Yes 3 months
☐ No
☐ Partially

2. Are periodic scans conducted, and how frequently? (Reference: ISO/IEC 27001:2013)

- ☐ Daily
☐ Weekly Quarterly
☐ Monthly
☐ Never

3. Is there a documented process for reviewing and updating firewall rules? (Reference: CIS Controls v8)

- ☐ Yes checklist
☒ No
☐ Occasionally

4. Are there multiple layers of firewall protection implemented (e.g., perimeter and internal firewalls)? (Reference: CIS Controls v8)

- ☐ Yes
☒ No
☐ Unsure

5. Is there an inventory management system in place for tracking hardware assets?

(Reference: NIST SP 800-53 Rev 5)

- ☐ Yes

- ☒ No
- ☐ Partially

6. Are regular maintenance and updates performed on critical hardware components?

(Reference: ITIL)

- ☒ Yes
- ☐ No
- ☐ Occasionally

7. Are there policies enforcing the use of strong, complex passwords? (Reference: NIST SP 800-63B)

- ☒ Yes they
- ☐ No
- ☐ Partially

8. Are password changes mandated at regular intervals, and how frequently? (Reference: CIS Controls v8)

- ☐ Monthly
- ☒ Quarterly every 3 months, last time they've change was June 2024
- ☐ Yearly
- ☐ Never

9. Are dormant accounts removed after deactivation?

- ☒ Yes they do remove accounts, to optimize their storage and tech resources
- ☐ No
- ☐ Partially

10. Is account information transmitted via encrypted formats only?

- ☒ Yes gmail zip pass
- ☐ No
- ☐ Partially

11. Are admin privileges granted on an as-needed basis?

- ☒ Yes
- ☐ No

according to him, all accounts are admin, since they use personal technological resources to provide for their work.

Wala namang CCTV eh

- ☐ Partially

12. Are all company properties equipped with locks on all windows and doors?

- ☒ Yes
- ☐ No
- ☐ Partially

13. Is there full security camera coverage at the office?

- ☒ Yes
- ☐ No
- ☐ Partially

Yes, every department has ^{camera coverage} ~~at least~~ inside the offices

14. Are mobile hardware devices locked and checked in/out for use?

- ☐ Yes
- ☒ No
- ☐ Partially

Too

15. Do mobile devices have remote wipe software installed in case of theft?

- ☐ Yes
- ☒ No
- ☐ Partially

After, pandemic the brgy remove the use of mobile for work.. sin

16. Do remote employees' home networks meet minimum security requirements?

- ☐ Yes
- ☒ No
- ☐ Partially

too

17. Are unauthorized system access alerts enabled?

- ☐ Yes
- ☒ No
- ☐ Partially

Since isa lang yung it and siya lang may access and may CCTV naman to check kung sino gumamit

18. Are unplanned system modification alerts active?

- ☒ Yes ~~the notification only~~
- ☐ No
- ☒ Partially Since ~~the~~ every dept has an it that is the only one who uses the system

19. Do you have a system or physical security intrusion alerts? Do you monitor it 24/7?

- ☒ Yes They have physical security intrusion alerts,
- ☐ No
- ☒ Partially they have cctv but they don't have system alerts.

20. Are background checks required for system access?

- ☒ Yes they ~~they~~ do background checks since the data
- ☐ No
- ☐ Partially they have is sensitive

21. Do employees acknowledge and sign security policy agreements before accessing secure systems?

- ☐ Yes
- ☒ No Since it is public and they just only have a verbal agreement.
- ☐ Partially

22. Do employees participate in annual security awareness and training?

- ☐ Yes
- ☒ No not all employees participate especially the
- ☐ Partially old^{ones} since they are not techy.

23. How often is the business emergency plan documented and updated?

- a. Monthly
- b. Quarterly Backup
- c. Annually
- d. As needed 3 months / was made

24. How frequently do employees undergo emergency response training?

- a. Monthly
- b. Biannually
- c. Annually
- d. Only during onboarding

wala / isa lang

25. How is the emergency chain of command communicated to employees?

- a. Verbally during meetings.
- b. Posted on the company intranet.
- c. Included in the employee handbook.
- d. All of the above.

No emergency plan

26. What happens to sensitive physical documents when they are no longer needed?

- a. They are stored indefinitely.
- b. They are shredded.
- c. They are recycled without shredding.
- d. They are discarded in regular trash.

- stored in an open cabinet

27. How are shredded documents stored before disposal?

- a. In a regular trash bin.
- b. In a locked container.
- c. In an open area.
- d. Not stored, immediately disposed of.

binibanta / other drawer
for composed w/

28. What procedure is followed for devices before changing users or disposal?

- a. They are cleaned and reused.
- b. They are factory reset.
- c. They are sold without any changes.
- d. They are thrown away without any action before being changed to a new user or disposed of to protect sensitive information.

Save mga ung files / then dispose

(treasurer na young
naka charge)

29. How often is critical data backed up?

- a. Weekly
 - b. Daily
 - c. Monthly
 - d. Only when necessary
- every 3 months

30. How frequently are backups checked and validated?

- a. Monthly
 - b. Weekly
 - c. Annually
 - d. Only after a data loss incident
- - Quarterly

31. How many separate locations are files backed up to?

- a. One
- b. Two or more
- c. Only in the cloud
- d. Not specified

by isa ilwuni

32. How often are security protocols updated?

- a. After every incident.
 - b. Regularly and after system modifications.
 - c. Annually.
 - d. Only when requested.
- Quarterly

3 months

33. How does your organization secure IT logs to prevent tampering?

- a. Stored in a secure database.
- b. Access restricted to authorised personnel only.
- c. Both A and B.
- d. No specific measures in place.

hala / hilde pg

REA - encounter

34. How often are IT logs reviewed?

- a. Daily

- b. Weekly
- c. Monthly
- d. Annually

35. For how long are IT logs retained?

- a. 3 months
- b. 6 months
- c. 1 year
- d. Indefinitely

2 years | depends on data

36. What information is recorded in incident reports?

- a. Only the incident description.
- b. Incident descriptions, times, and dates.
- c. Only the solutions.
- ☒ d. No specific information is recorded.

37. How are causes and solutions documented in incident reports?

- a. Only causes are recorded.
- b. Causes and solutions are recorded, and procedures are updated if necessary.
- c. No updates are made.
- d. Only solutions are recorded.

— No updates or record are made

PERFORMANCE MONITORING

38. How does your organization track outage frequency?

- a. Only planned outages are tracked.
- b. Both planned and unplanned outages are tracked.
- c. No tracking is done.
- d. Only unplanned outages are tracked.

*they have
war panel*

39. What is the mean time to resolve outages in your organization?

- a. Less than 1 hour
- b. 1-3 hours
- c. 3-6 hours
- d. More than 6 hours
- not applicable

40. How is total system downtime measured?

- a. By service only.
- b. By infrastructure only.
- ☒ c. Total downtime is tracked across all services.
- ☐ d. Not measured.

41. How is RAM utilization monitored in your organization?

- a. Manually checked.
- ☒ b. Automated monitoring tools.
- c. Not monitored.
- d. Only during system upgrades.

42. How does your organization track hard drive storage utilization?

- Regular audits.
- Automated alerts for capacity limits.
- Not tracked.
- ☒ • Only when issues arise.

43. How is cloud storage utilization managed?

- No specific management.
- Regular reviews and audits.
- ☒ • Only monitored during incidents.
- Managed by third-party vendors only.

44. How do you measure upload speeds on the network?

650mbps Fiber globe plot

45. What is the typical upload speed, and is it meeting expectations?

yes

46. Are there any limits or slowdowns on upload speeds during heavy usage?

no

47. What steps are taken when download speeds are slower than expected?

no limit

48. What steps are taken when download speeds are slower than expected?

no limit

49. What is the average delay (latency) when sending data across the network?

43 pps

50. Does network delay vary depending on the time of day or traffic load?

random 20 min

51. What actions are taken to reduce delays, especially for time-sensitive activities like video calls?

limit

52. What is the total IT budget or expense for the organization annually? Ex. Less than 500,000php

less than million
not enough

53. How does this year's total IT expenses compare to previous years?

(a) Increased by 10% or more compared to last year

b) Remained the same

c) Decreased by 5% or more

54. What is the average IT expense per employee?

minimum

55. Does the IT expense per employee include training and support costs?

yes

56. What is the cost per unit of data storage (e.g., per GB or TB)?

40k per unit computer

8gb ram 1tb ssd

57. How does the cost of data storage compare to other IT assets (e.g., hardware, software)?

other assets 618k

58. Have there been any changes in data storage costs over the last year?

no

SYSTEM DEVELOPMENT

59. Who is involved in determining system development needs?

treasurer, captain, IT

60. Are system design and development procedures documented and accessible to all team members?

IT

61. How are team members trained to follow these procedures?

No

62. Who is responsible for approving each stage of the development process?

None

63. Are there any delays or bottlenecks in getting necessary approvals?

No

64. At which stages are approvals required during the development process?

a) Initial design

b) Before testing

c) Final deployment

d) All of the above

not applicable

65. Are data entry documents comprehensive and easy to understand for users?

yes

66. How comprehensive are the tests conducted on new systems or updates?

Choices:

- a) All critical components and edge cases are tested thoroughly.
- b) Most key features are tested, but some areas are skipped due to time constraints.
- c) Testing is minimal, focusing only on primary functions.
- not applicable

67. What types of testing are used to ensure system reliability?

Choices:

- a) Unit testing
- b) Integration testing
- c) Performance and load testing
- d) User acceptance testing (UAT)
- e) All of the above
- not applicable

68. Are automated tests part of the process to ensure consistency?

Choices:

- a) Yes, we use automated tests for regression and repetitive tasks.
- ☒ b) No, all testing is done manually. no testing
- c) A mix of both automated and manual tests.

69. Are test environments separate from production environments?

Choices:

- a) Yes, we use a dedicated test environment for system testing.
- b) No, testing is often done in the live environment.
- c) A mix of both, depending on the type of test.
- not applicable

70. Is load or performance testing performed to evaluate system stability under high usage?

Choices:

- a) Yes, load testing is a standard part of the testing process.
- b) No, we do not conduct specific load testing.
- c) Only if the system is expected to handle high traffic.

- not applicable

71. Who is responsible for managing and overseeing the testing process?

Choices:

- a) A dedicated QA team
- b) Developers conduct their own tests.
- c) A mix of QA team, developers, and end-users

- not applicable

72. Is the implementation process fully documented and accessible to relevant team members?

Choices:

- a) Yes, the process is fully documented and stored in a central repository.
- b) Partially, some steps are documented, but not all.
- c) No, documentation is minimal or informal.

- not applicable

73. Are industry standards or internal guidelines followed during the implementation process?

Choices:

- a) Yes, we adhere to industry standards (e.g., ITIL, ISO) and internal policies.
- b) No, implementation is based on internal practices only.
- c) We follow a mix of internal guidelines and industry standards.

- not applicable

74. What is the process for approving changes during implementation?

Choices:

- a) A formal change control process with approvals from senior management.
- b) Approval is required only for major changes.
- c) Changes are implemented without formal approval.

- not applicable

75. What security controls are in place during the implementation process to protect sensitive data?

not applicable

76. Are security policies updated to reflect changes made during implementation?

no security policies

77. Is there a documented post-implementation review process to evaluate system performance?

Choices:

- a) Yes, the post-implementation review is fully documented and mandatory.
- b) No formal review is done, but feedback is gathered informally.
- c) Reviews are conducted but not always documented.

not applicable

78. Who is responsible for conducting the post-implementation review?

Choices:

- a) The project manager and IT team
- b) A third-party consultant or auditor
- c) A combination of both internal teams and external reviewers

not applicable

Student IT Auditors
Ayala Boulevard, Ermita, Manila
Technological University of the Philippines
October 20, 2024

Mrs. Amelia Concepcion Chua
Barangay Captain
Brgy. North Fairview, Quezon City, Metro Manila

Subject: Request for Permission to Conduct IT Audit at Barangay North Fairview

Dear Mrs. Amelia Concepcion Chua,

We are a group of five students from the Technological University of the Philippines-Manila, currently pursuing our Bachelor of Science in Computer Science. As part of our term project, we would like to seek your permission to conduct an IT audit for Barangay North Fairview.

Our aim is to thoroughly examine the existing information technology infrastructure and processes at Barangay North Fairview. By conducting this audit, we hope to pinpoint potential areas for enhancement and ensure that these systems align with current IT governance standards and industry best practices. We believe that this analysis will not only help streamline operational workflows but also improve data security, system reliability, and overall service quality. The insights gained could contribute to optimizing the efficiency of daily operations and enhancing the company's performance.

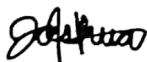
We are committed to carrying out the audit with the highest level of professionalism and respect for Barangay North Fairview's resources, staff, and time. We would be grateful for the opportunity to collaborate with you and your team in this endeavor.

Thank you very much for considering our request. We look forward to your positive response.

Sincerely,



Maui A. Esguerra
Leader



Hanz Joshua V. Ancuna
Member



Sophia Nicole M. Benavides
Member



Lanz Andrei C. Colico
Member



Maria Angela S. Dayawon
Member

Acknowledgment and Approval:

SGD Jasmin Niguidula


Department of Computer Studies

Technological University of the Philippines-Manila

Acknowledgment and Permission

I, Mrs. Amelia Concepcion Chua, Barangay Captain of Barangay North Fairview Quezon City, hereby acknowledge and give permission for the Student IT Auditors from the Technological University of the Philippines to conduct an IT audit of the company's information technology infrastructure and processes, subject to the conditions mutually agreed upon.

Signature: _____
Name: Mrs. Amelia Concepcion Chua
Position: Barangay Captain
Date: _____


Patricia F. Mondragon
IT Officer