University of Dar es Salaam

Lecture 6 – Auditing Entity-Level Controls

Aron Kondoro

Introduction

- Auditing of IT areas such as
  - Strategic Planning and technology roadmaps
  - Performance indicators and metrics
  - Project approval and monitoring processes
  - Policies, standards, and procedures
  - Employee management
  - Asset and capacity management
  - System configuration change management

Introduction

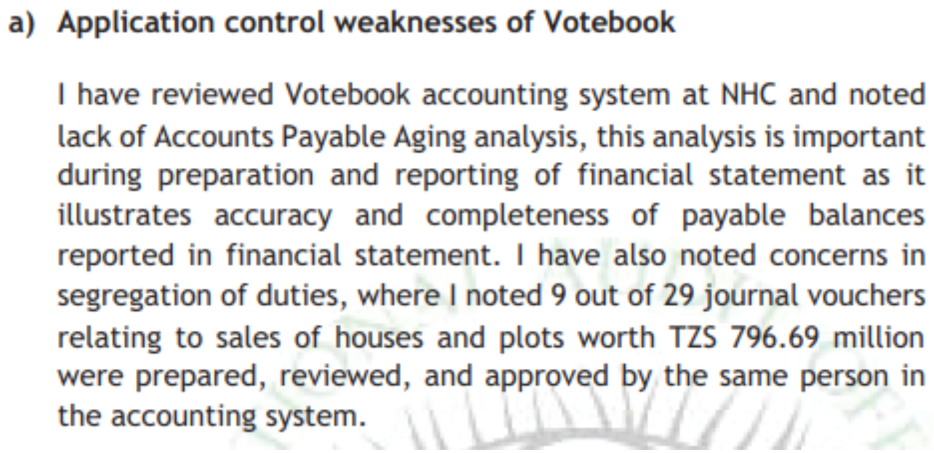
- Entity-level controls are **pervasive** across an organization
- Any critical IT process that is **centralized** falls under entity-level controls review
  - E.g. company with centralized data centre
- Entity levels controls provide for the core principles of IT governance

Auditing Steps for Entity-Level Controls

1. Review the overall IT organization structure

- Ensure it provides clear assignment of authority and responsibilities over IT operations
- Ensure it provides adequate segregation of duties
- Potential Impact:
  - confusion regarding responsibilities
  - disagreements on authority to make final decisions
- Method
  - Review org charts to ensure they clearly indicate reporting structures
  - Review org charts to ensure they clearly delineate areas of responsibilities
- Example Guidelines
  - IT personnel should not perform data entry
  - Programmers should not be able to modify production code, data
  - Programmers should be separate from IT operations support
  - Information security organization should be responsible for setting policies and monitoring compliance

Excerpt from CAG report 2019/20



a) **Application control weaknesses of Votebook**

I have reviewed Votebook accounting system at NHC and noted lack of Accounts Payable Aging analysis, this analysis is important during preparation and reporting of financial statement as it illustrates accuracy and completeness of payable balances reported in financial statement. I have also noted concerns in segregation of duties, where I noted 9 out of 29 journal vouchers relating to sales of houses and plots worth TZS 796.69 million were prepared, reviewed, and approved by the same person in the accounting system.

2. Review IT strategic planning process

- Ensure it aligns with business strategies
- IT must be aware of future business needs and changes so that it can prepare
- Method
    - Look for evidence of a strategic planning process
    - Determine how company strategies were used to develop IT strategies
    - Review documented short & long term IT priorities
    - Evaluate processes for periodic monitoring

3. Determine existence of tech/app strategies and roadmaps

- Ensure there are processes for long-range technical planning
- It is important for IT understand and plan for change
  - i.e. take advantage of new developments in tech
- Method
  - Look of evidence of long-term technical planning process
  - Determine the existence of processes to monitor relevant technology changes

4. Review performance indicators and measurements for IT

- Ensure that processes and metrics are in place for measuring performance of day to day activities
- Ensure tracking of performance against SLAs, budgets, and other operational requirements
- Method
  - Obtain copy of captured IT metrics e.g. system uptime, response time etc
  - Determine goals of metrics and evaluate their performance
  - Review any SLAs i.e. ensure measurements and corrective processes are in place
  - Ensure processes for establishing and enforcing budget adherence are in place i.e. budget vs actual analysis

5. Review IT process for approving and prioritizing new projects

- Ensure this process can prevent unapproved system development or acquisition projects
- Ensure management & key stakeholders can periodically review project status, schedule, and budget
- Method
  - Review any available documentation regarding project proposal and approval process
  - Sample active IT projects and obtain evidence they went through appropriate process
  - Ensure project approval process involves thorough cost analysis i.e. start-up costs, software & hardware maintenance, support (labour costs), power requirements etc.
  - Review evidence that management periodically reviews project status

6. Evaluate standards for governing execution of IT projects

- Standards for ensuring quality of developed or acquired products by IT
- Determine how these standards are communicated and enforced
- Method
  - Determine the scope of standards. i.e. ensure it covers **project management**, **software development**, **system configuration**, **hardware and software**, **quality assurance standards**
  - Look for evidence of communication and enforcement of standards

7. Review and evaluate risk-assessment processes

- Ensure risk assessment processes are in place to help IT take appropriate measures to mitigate
- Method
  - Look for evidence that IT is assessing risks and making conscious decisions on how to handle them
  - These risks assessment mechanisms include
    - Monitoring internal controls
    - Performing formal threat and risk assessment of data centres and systems
    - Performing periodic reviews of strategic IT plans
    - Monitoring compliance with information security policies

8. Review IT personnel skills and knowledge

- Evaluate processes for ensuring IT employees have the necessary skills and knowledge to perform their tasks
  - Mechanisms to maintain and enhance knowledge/skills of IT
- Method
  - Review IT-related human resources (HR) policies i.e. ensure qualified people are hired
- Examples
  - Ensure that job descriptions exists and are referred during hiring
  - Review IT training policies and ensure the provide opportunities for trainings/seminars
  - Review performance-review processes

9. Ensure compliance with laws and regulations

- Ensure there are processes for complying with laws/regulations and maintaining awareness changes in the legal environment
- Non-compliance can lead to penalties/fines, damaged reputation, lawsuits etc
- Method
    - Look for single point of contact responsible for identification, monitoring, and compliance with regulations/laws
    - Evaluate effectiveness of processes for monitoring regulatory environment
    - Look for evidence of responsibility assignment and compliance

10. Review end users involvement mechanisms

- Evaluate processes for ensuring end users of IT can report problems, are involved in IT decisions, and are satisfied with IT services
- Method
  - Ensure helpdesk allows end users to report problems
  - Evaluate processes for capturing and tracking reported problems
  - Sample recent tickets and verify resolution
  - Look for evidence management follows-up on user feedback
  - Ensure helpdesk does not compromise security in favour of customer satisfaction
  - Verify the existence of customer steering teams for IT projects

11. Review third-party services

- Evaluate processes for managing third-party services to ensure roles and responsibilities are clearly defined and performance is monitored
  - E.g. PC support, web server hosting, system support, programming etc
- Method
  - Review the process of selecting vendors i.e. multiple competitive bids, pre-defined criteria, proper procurement personnel, thorough cost analysis etc
  - Ensure contracts define roles/responsibilities and include SLAs
  - Ensure contracts include non-disclosure and right-to-audit clauses
  - Review processes for monitoring performance of third party services

12. Review non-employee access

- Evaluate processes for controlling non-employee logical access
  - E.g. contractors, third-party vendors
- Method
  - Ensure policies require approval and sponsorship from employee
  - Review processes for communicating IT policy to non-employees i.e. signed agreements/statements
  - Review and evaluate access revocation processes for non-employees i.e. validate sample accounts of current non-employees
  - Ensure non-disclosure agreement (NDAs) are signed by non-employees
  - Ensure data access restrictions for non-employees have been considered
    - E.g. access to financial data, system administration capabilities etc

13. Review software licence compliance

- Evaluate processes for ensuring company is in compliance with applicable software licences
  - Illegal use can lead to penalties, fines, lawsuits
- Method
  - Look for evidence company maintains and monitors list of enterprise software licences
  - Determine how decentralized (non-enterprise) licences are monitored
  - Test effectiveness of licence management method i.e. centralized database, scan of computers

14. Review remote access controls

- Evaluate controls over remote access into the company’s network e.g. VPN, dedicated external controls
  - Lack of strong controls can lead to compromised network
- Method
  - Ensure strong authentication (multifactor) is required for remote access
  - Determine the existence of approval/revocation processes for remote access accounts
  - Evaluate controls for removing dedicated external connections
  - Evaluate controls for prevention of unauthorized connections
  - Ensure policies for minimum security requirements for remote access machines e.g. OS patches, antimalware protection, not dual-homed etc

15. Review hiring and termination procedures

- Ensure that hiring and termination procedures are clear and comprehensive
  - Background checks, confidentiality agreements etc for new hires
  - Access revocation to facilities and systems after termination i.e. physical and logical, return of company-owned equipment
- Method
  - Review HR policies and procedures

16. Review procurement procedures

- Evaluate policies and procedures for controlling the procurement and movement of hardware
    - Asset management i.e. controlling, tracking, and reporting
    - Lack of proper management can lead to increased expense due to duplicate equipment, unnecessary lease expenses, missing end-of-life conditions, missing theft of equipment
- Method
    - Evaluate asset management policies and procedures
        - asset procurement process - appropriate approvals
        - asset tracking - tags, asset management database
        - Inventory – asset number, location, warranty status, lease expiration, life-cycle
        - Asset move and disposal procedures – secure storage, secure erasure of data

17. Review system configuration changes

- Ensure system configurations are controlled with change management
  - Prevents unnecessary system outages
  - Planning, scheduling, applying, and tracking
- Configuration management procedures should include processes for
  - Requesting changes
  - Scheduling approved changes
  - Testing and approving changes before implementation
  - Communicating planned changes
  - Implementing changes
  - Rolling back wrong changes

18. Review media management policies and procedures

- Ensure media transportation, storage, reuse, and disposal are addressed by company-wide policies and procedures
    - Data-storage media remains confidential and protected from premature deterioration e.g. Loss of back-up media in transit
- Method
    - Ensure sensitive information is encrypted before transport
    - Ensure proper digital shredding of magnetic media
    - Ensure proper physical shredding of optical and paper media

Further Reading

- Lecture 6 Readings