CS4050 – WEEK 11: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

CHAPTER 4: INFORMATION SYSTEMS OPERATIONS & BUSINESS RESILIENCE

- Part A: Information Systems Operations
  - Common Technology Components
  - IT Asset Management
  - Job Scheduling & Production Process Automation
  - System Interfaces
  - End-User Computing
  - Data Governance
  - Systems Performance Management
  - Problem & Incident Management
  - Change, Configuration, Release and Patch Management
  - IT Service Level Management.
  - Database Management
- Part B: Business Resilience
  - Business Impact Analysis
  - System Resiliency
  - Data Backup, Storage and Restoration
  - Business Continuity Plan
  - Disaster Recovery Plans

IT ASSET MANAGEMENT

- IT Inventory: The inventory record of each information asset should include:
  - Owner
  - Designated custodian
  - Specific identification of the asset
  - Relative value to the organization
  - Loss implications and recovery priority
  - Location
  - Security/risk classification
  - Asset group (where the asset forms part of a larger information system)

JOB SCHEDULING & PRODUCTION PROCESS AUTOMATION

- Job Scheduling Software
- Scheduling Reviews – Key areas to review as auditor:
  - Regularly scheduled applications
  - Input deadlines
  - Data preparation time
  - Estimated processing time
  - Output deadlines
  - Procedures for collecting, reporting and analyzing key performance indicators
  - Daily Job Schedule
  - Console Log
  - Exception Processing Logs
  - Re-executed Jobs & Personnel

SYSTEM INTERFACES

- ***System interfaces*** exist where data output from one application is sent as input to another, with little or no human interaction. Interfaces that involve humans are usually called ***user interfaces***.
- **System-to-system interfaces**: When data is transferred between two systems, whether internal or external. Data may also be transferred to specialized tools for analysis.
- **Partner-to-partner interfaces**: when two partners are continuously transferring data back and forth across agreed-upon systems. These transfers are generally done on a regular basis.
- **Person-to-person interfaces**: They can be as easy as attaching a data file to an email and sending it. These forms of transfer tend to be more difficult to observe, manage, secure and control.

CONTROLS ASSOCIATED WITH SYSTEM INTERFACES

IS auditors should ensure that the interface review covers the following:

- Manage multiple file transfer mechanisms.
- Use multiple protocols.
- Automatically encrypt, decrypt and electronically sign data files.
- Compress/decompress data files.
- Connect to common database servers.
- Send and retrieve files via email and secure email.
- Automatically schedule regular data transfers.
- Analyze, track and report any attributes of the data being transferred.
- Ensure compliance with appropriate regulatory laws and mandates.
- Offer a checkpoint or restart capability for interruptions.
- Integrate with back-office applications to automate data transfers as much as feasible.

END USER COMPUTING

- ***End-user computing*** (EUC) refers to the ability of end users (who typically are not programmers) to design and implement their own application or information system using computer software products.
- The lack of IT department oversight of EUC may lead to security risk:
  - Authorization—There may be no secure mechanism to authorize access to the system.
  - Authentication—There may be no secure mechanism to authenticate users to the system.
  - Audit logging—This is not available on standard EUC solutions (e.g., Microsoft Excel and Access).
  - Encryption—The application may contain sensitive data which have not been encrypted or otherwise protected

DATA GOVERNANCE

- Stakeholder needs, conditions and options are evaluated to determine balanced, mutually agreed enterprise objectives to be achieved through the acquisition and management of data/information resources.
- Direction is set for data/information management capabilities through prioritization and decision making.
- Performance and compliance of data/information resources are monitored and evaluated relative to mutually agreed-upon (by all stakeholders) direction and objectives.

DATA MANAGEMENT

- **The Data Management Body of Knowledge** (DMBOK) defines data management as "*the planning and execution of policies, practices, and projects that acquire, control, protect, deliver, and enhance the value of data and information assets.*"
- Data Quality is key to data management. There are three subdimensions of quality, i.e., (i) *intrinsic*, (ii) *contextual*, and, (iii) *security/accessibility*
  - **Intrinsic**: Accuracy, Objectivity, Believability, Reputation
  - **Contextual:** Relevancy, Completeness, Currency, Appropriate Amount, Consistent Representation, Interoperability, Understandability, Ease of manipulation
  - **Security/Accessibility**: Availability, Restricted Access

SYSTEM PERFORMANCE MANAGEMENT

- Information Systems Architecture & Software
- Access Control Software
- Data Communications Software
- Utility Programs
- Software Licensing Issues
  - **Free Software Licensing Types**: Open Source, Freeware, Shareware
  - **Paid Software Licensing Types**: Per CPU, Per Seat, Concurrent Users, Utilizations, Per Workstation, Enterprise
- Source Code Management
- **Capacity Management & Monitoring**: Plan Development, Monitoring, Analysis, Tuning, Implementation, Modeling, Sizing

PROBLEM & INCIDENT MANAGEMENT

- Difference Between Problem & Incident Management - *Problem management's objective is to reduce the number and/or severity of incidents, while incident management's objective is to return the affected business process back to its normal state as quickly as possible, minimizing the impact on the business*
- Problem Management Reporting Reviews:
  - Interviews with IT operations personnel
  - Procedures and documentation used by the IT department
  - Performance records, outstanding error logs
  - Helpdesk call and record logs

THE TOP QUALITIES OF SOLUTION-ORIENTED LEADERS

1. They Know When To Take Action — And When To Take A Step Back
2. They Keep Their Focus Forward
3. They Inspire Their Team To Focus On Solutions
4. Ask For Feedback
5. Ask The Questions To Find The Right Answers
6. Stop Playing The Blame Game