CERTIFIED INFORMATION TECHNOLOGY PROFESSIONAL

BODY OF KNOWLEDGE - CONTENT SPECIFICATION OUTLINE

Section 1 – Risk Assessment

1) Risk assessment
    - Initial evaluation of risks that may impact the possibility of a material misstatement or the vulnerability of an organization's assets with initial assumptions, research, and uncertainties
    - a. Types of Risk Assessments
        - i. Financial Statement, Technology, and Security Audits
    - b. Understanding business environment & processes
        - i. Complexity of business
            - 1. Assess the level of IT sophistication, and degree of F/R reliance on IT
        - ii. Business or accounting change, such as within business process and cycles
    - c. Audit Risk Model for F/S Audits
        - i. Assessing Inherent Risk
            - 1. Entity (economy, industry, entity-specific)
            - 2. Control Environment
        - ii. Assessing Control Risk
            - 1. Manual versus automated controls, hybrid controls
            - 2. Preventive, detective, and mitigating controls
            - 3. Key versus non-key controls
        - iii. Risk of material misstatement
            - 1. combination of inherent and control risk
            - 2. Consider applicable account balances, classes of transactions, and disclosures
            - 3. Tie to relevant F/S assertions
    - d. Develop Walkthrough Plan
        - i. Determine business processes and controls to review
            - 1. Primary/ key controls
            - 2. Automated Controls w/in business processes and benchmarking of automated controls
    - e. Draft risk assessment report
        - i. Based on the evidence from walkthroughs and other procedures (example: Best practices)

Section 2 – Fraud Considerations

1) Fraud Considerations
    - Consider the risks of material misstatement due to fraud and determine specific IT techniques to detect fraud
    - a. Prevention and Deterrence
        - i. Forensics basics
        - ii. Use of IT in fraud investigations
    - b. Digital Evidence
        - i. e-discovery rules and processes
        - ii. Implications of federal and state-specific laws

c. Detection & Investigation
i. Proper digital acquisition procedures and tools
ii. Determine suitable digital sources
iii. Regulatory standards (SAS 99)

Section 3 – Internal Control and IT General Controls

1) Internal Controls
➢ Provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes/ use
a. Understanding of Internal Controls
i. Understanding of frameworks: COSO, CoBIT
ii. How the framework integrates with financial statement audits
b. Management Considerations
i. Management history at the organization and IT control reports filed in prior audits
c. Preparing an IT Audit Plan
i. Scoping of audit

2) Understanding of Information Technology General Controls
➢ Control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise
a. Control environment
i. Strategic planning
ii. Policies & procedures
1. Consider portfolio of systems utilized or in place
iii. Risk management
iv. HR management
1. Proper IT skill-set and performance evaluation
b. Systems Development, Deployment, and maintenance
i. Portfolio of Systems and Technologies Utilized
ii. System Development Lifecycle (SDLC)
1. Methodologies, Phases, and best practices
iii. Change management policies and procedures
1. Configuration management
2. Software management
3. Operating system and network management
iv. System maintenance
1. Application, database, and server
2. Network/ operations
v. Vulnerability management
vi. Systems Implications
1. Accounting & Financial Reporting Systems
a. Closed vs. custom/open accounting system packages
2. Enterprise Systems (or ERP)
3. E-business systems or applications
c. Logical and physical security
i. Logical Access
1. Application & financial system level
a. Evaluate and test application controls

b. Evaluate appropriate segregation of duties
c. Consider risks at spreadsheet level
2. Database and Server level
3. Network and operating system level
a. Firewalls, operating systems, finance directories
ii. Physical access
1. Access to server room, building facilities, and sensitive hardcopy records
d. Backup & recovery process
i. Backup procedures and disaster recovery plan
ii. Contingency plan
1. Incident response and contingency testing

3) Information Security: Identify, design, implement, and monitor processes/systems used to enable security of information
a. Understands Information Security policies, standards, and procedures to ensure information / data security
b. Understands hardware and physical controls over access to sensitive data
c. Understands software and other process controls to secure information
d. Understands concepts of security authentication and authorization
e. Understands concepts of encryption

Section 4 – Evaluate, Test, and Report

1) Types of Audit and Attest Services
➢ Provide assurance to the public on financial statements, a client service, or a specific segment or piece of an entity's operations
a. Financial Statement audit
i. Regulatory bodies: PCAOB, SEC, AICPA (Peer Review)
ii. Standard setting bodies: FASB, ASB
iii. Risk-Based Auditing Standards (SAS 104-111, AS.5)
iv. IT Considerations (SAS 94)
b. Audits on Service Organizations (SSAE 16)
i. Conducting SSAE 16 audits
ii. Reviewing SSAE 16 reports
c. Trust Services engagement
d. Agreed-Upon procedures or other attestation services
i. Example: PCI and HIPAA
2) Auditing Techniques & Procedures
➢ Techniques and options to design and execute testing procedures
a. Planning for test of controls
i. System testing
ii. Application control testing
b. Evidence gathering
c. Sampling considerations
i. Sampling ITGCs and sample size
d. Technical tools/ techniques (CAATTs)
i. Simple to complex tools available
3) Assessment of controls
➢ Evaluation process of controls and the entity's environment after examination and testing

   a. Deficiency Evaluation for IT Related Controls
      i. Deficiency, Significant deficiency, and Material weakness
      ii. Aggregation of deficiencies
   b. Materiality/ Impact to the Entity
      i. Risk of material misstatement
   c. Assessment Reporting

4) Information Assurance
   a. Information Presentation
      i. Relevancy
      ii. Fitness for Particular Use
      iii. Disclosure
   b. Information Timeliness
      i. Latency
      ii. Currency
   c. Information Auditability
      i. Source Traceability
      ii. Transformation Traceability

Section 5 – Information Management & Business Intelligence

1) Information Management: Ensuring that information is managed such that it provides value in a number of aspects:
   a. Information Life Cycle Management
      i. Creation, Storage, Archival, and Destruction
      ii. Compliance
         1. Internal Policy / Internal Compliance
         2. Privacy
         3. Regulatory
         4. Other External Compliance

   b. Information and Data Modeling
      iii. Understands Data Modeling Concepts
         1. Understand the logical unit / structure of data
            a. Basic data types
         2. Understand need for data normalization, and consistency of data
            a. e.g.; master record for a single data element
         3. Understands conceptual data modeling
            a. E.g. entity-relationship, star/snowflake
      iv. Understands Information Architecture Concepts
         1. Business Information Architecture Components
         2. Business Information Types

2) Business Process Improvement: identifying opportunities and understand the value of using information technology to create work flows and processes that enable more effective use of resources.
   a. Business Process Management
      i. Understanding of business processes that impact data
      ii. Proper design and integration of internal controls into business processes
         1. Business Activity Monitoring (BAM) approach
         2. Continuous monitoring
            a. Approach

b. Techniques
c. Examples
b. System Solution Management
i. Definition of the system acquisition and evaluation lifecycle
1. Initial Phase: Requirements analysis, solution selection, business case management, and system design
2. Secondary phase: system deployment/ development, quality control, solution implementation
3. Last Phase: training & transition
ii. Risk associated with financial system management:
1. Customization
2. Purchase of packaged accounting/information system
c. Application Integration Management
i. Understand values of application integration relative to use of disparate applications and databases to manage information and transactions. Examples:
1. Integration among financial accounting modules (e.g.; GL, Accounts payable, purchasing)
2. Other related systems (e.g.; inventory management, MRP, Electronic Data Interchange, etc.)

3) Data Analysis & Reporting Techniques: process of gathering, modeling, and transforming data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making
a. Infrastructure/ platforms typically employed
i. ERP or other software as the source
ii. reporting tools as the vehicles to generate information for management/users
b. Data collection and aggregation
i. Data Mapping, data collection
1. Data structure and flows through an entity
a. within a system
b. among systems
c. manually
c. Available tools/ approaches and functionalities
i. Functionalities:
1. Extraction
2. Data mining
3. Querying
ii. Real-time data analysis or "buffered" database analysis
iii. Understanding the types of tools available:
1. Applicable Technology Resources / Business Intelligence
2. Other integration tools
3. Reporting tools
iv. Extract, Transform, & Load (ETL) Tools and Techniques
d. Tool Selection Process
v. Understanding which analysis and reporting tools are best for a given circumstance

4) Performance Management: apply data analysis and reporting concepts to analyze enterprise performance and help the organization achieve its accountability goals and objectives, using financial and non-financial information.

e. Budget & Profitability Management

vi. Types of systems-aided budget or cost management processes

vii. Examples include:

4. cost or revenue reporting automation
5. analysis by job or process
6. management information dashboards

f. Performance Metrics and Reporting

viii. Systems-aided alignment of measures/metrics to organizational objectives

ix. Financial measures through financial system outputs

x. Customer related measures through financial system outputs

xi. Key Performance Indicators (KPIs) and metrics

xii. operational or production reporting/ measurements

xiii. monitoring