Certified Information Technology Professional (CITP)
Content Specification Outline

The content of the Certified Information Technology Professional (CITP) examination has been developed to test a candidate’s overall understanding of the fundamental sections of the CITP body of knowledge. The content of each of the five topical sections is described in outline form and provides an overview of the knowledge and skills needed to be tested on the CITP Examination.

The examination questions are intended to test each content area and its logical extensions. The percentage range following each major content area in the outline represents the approximate weighting for that content area.

The examination is fully computerized and only consists of multiple choice questions.

CITP Body of Knowledge

Section 1 – Risk Assessment (10 to 15% of exam content)
Section 2 - Fraud Consideration (5 to 10% or exam content)
Section 3 – Internal Control and IT General Controls (25 to 30% of exam content)
Section 4 – Evaluate, Test, and Report (15 to 20% of exam content)
Section 5 – Information Management & Business Intelligence (35 to 40% of exam content)
### Primary Readings

**Content Applicable to most Sections**

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA/ITEC.</td>
<td>“Information Technology Considerations in Risk-Based Auditing”. 2007.</td>
</tr>
<tr>
<td>AICPA.</td>
<td>“Managing the Business Risk of Fraud: A Practical Guide”</td>
</tr>
<tr>
<td>AICPA Statement of Auditing Standards No. 94, 99, 104-111, 115, 440</td>
<td></td>
</tr>
<tr>
<td>AICPA</td>
<td>Trust Services Principles, Criteria, and Illustration.2010</td>
</tr>
</tbody>
</table>

**COBIT 4.1 IT General Controls and Application Controls**

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
</table>

**2012 AICPA CITP Content Specification Outline**
Section 1 – Risk Assessment (10% - 15%)

This section covers the 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.

Risk Assessment Outline

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)

Additional Referenced Readings
Section 1

| Deterring & Detecting Financial and Reporting Fraud: A Platform for Action, October 2010 (published by the Center for Audit Quality) |
| Federal Reserve - Framework for Risk Focused Supervision of Large Institutions, August 8, 1997 |
| Information Technology Control & Audit, 2nd Edition by Frederick Gallegos, CGFM,CISA,CDE |
| International Standards on Auditing No. 400 |
| National Institute of Standards and Technology No. 800-30 |
Section 2 - Fraud Consideration (5% - 10%)

This section considers the knowledge related to defining the various risks of material misstatement due to fraud and determining specific IT techniques to detect fraud.

Fraud Considerations Outline

a. Prevention and Deterrence
   i. Forensics basics
   ii. Use of IT in fraud investigations
b. Digital Evidence
   i. e-discovery rules and processes
   ii. 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)

Additional Referenced Readings
Section 2

| Computer-Aided Fraud Prevention and Detection, A step by Step Guide by David Coderre, Wiley & Sons |
| Fraud Examiners Manual.2009 |
| Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations by Jarrett and Bailie |
Section 3 – Internal Control and IT General Controls (25% - 30%)

This section outlines the knowledge supporting Internal Controls, Information Technology General Controls and Information Security. The Internal Controls segment consists of providing reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes/use. Information Technology General Controls cover control objectives related to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise. Information Security relates to understand, identify, design, implement, and monitor processes/systems used to enable security of information.

1) Internal Controls Outline
   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) Information Technology General Controls Outline
   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 Outline
   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

Additional Referenced Readings
Section 3

- Computer World: The difference between e-business and e-commerce, Andrew Bartels, October 30, 2010
- Core Concepts of Information Technology Auditing, James Hunton
- Department of Health and Human Services Enterprise Performance Life Cycle Framework V1.0: http://www.hhs.gov/ocio/eplc/eplc_framework_v1point2.pdf
- Eliminating Spreadsheet Risks: A Guide for Internal Auditors to Regain Control and Limit Exposure by Richard Blaustein
- Information Technology Control & Audit, 2nd Edition by Frederick Gallegos, CGFM,CISA,CDE
- Information Technology Management, Efriam Turban
- Global Technology Auditing Guide 14: Auditing User-Developed Applications, IIA
- Lockheed Martin, Open Architecture Enabling Sea Power 21 October 26, 2010 (World Wide Web), white paper
- Network World Vulnerability management: The basics by Bill Brenner, CSO September 09, 2010
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act - July 2004 PWC</td>
</tr>
</tbody>
</table>
Section 4 – Evaluate, Test, and Report (15% - 20%)

This section captures the types of Audit and Attest Services, Auditing Techniques & Procedures, Assessment of Controls and Information Assurance. **Types of Audit and Attest Services** provide assurance to the public on financial statements, a client service, a specific segment or piece of an entity’s operations. **Auditing Techniques & Procedures** highlight the techniques and options used to design and execute testing procedures. **Assessment of Controls** covers the knowledge in evaluating process of controls and the entity’s environment after examination and testing. **Information Assurance** provides assurance on the presentation, timeliness, and auditability of information.

1) **Types of Audit and Attest Services Outline**
   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 Outline**
   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 Outline**
   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 Outline**
   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

### Additional Referenced Readings

<table>
<thead>
<tr>
<th>Section 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA Facts about Financial Accounting Standard Board</td>
</tr>
<tr>
<td>Control Self-Assessment: A Practical Guide by Larry Hubbard</td>
</tr>
<tr>
<td>Management Information Systems, Kenneth Laudon, chapter 2</td>
</tr>
<tr>
<td>Management Information Systems, Marshall Romney</td>
</tr>
<tr>
<td>Model Driven Software Development, Haase.2005</td>
</tr>
</tbody>
</table>
Section 5 – Information Management & Business Intelligence (35% - 40%)

This section covers the knowledge supporting Information Management, Business Process Improvement, Data Analysis & Reporting Techniques and Performance Management. **Information Management** ensures that the information is managed such that it provides value in a number of aspects. **Business Process Improvement** identifies opportunities and understands the value of using information technology to create work flows and processes that enable more effective use of resources. **Data Analysis & Reporting Techniques** recognize the process of gathering, modeling, and transforming data with the goal of highlighting useful information, suggesting conclusions and supporting decision making. **Performance Management** covers the understanding of applying data analysis and reporting concepts to analyze enterprise performance and helping the organization achieve its accountability goals and objectives, using financial and non-financial information.

1) Information Management Outline
   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 Outline
   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 Outline
   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 Outline
   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

<table>
<thead>
<tr>
<th>Additional Referenced Readings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 5</strong></td>
</tr>
<tr>
<td>ACM SIGMOD Record Volume 32 Issue 2, June 2003 by Lukasz Golab</td>
</tr>
<tr>
<td>Business Intelligence Dashboard, Business Analytics:</td>
</tr>
<tr>
<td>Business Intelligence For Dummies Swain Scheps, paperback, January 2008</td>
</tr>
<tr>
<td>Business Process Management (BPM) Definition and Solutions, Mark Cooper, founder, and Paul Patterson, managing partner, Athens Group Fri, April 27, 2007:</td>
</tr>
<tr>
<td>Business Insight Through Real-Time Analysis on Data in Motion Jul 15, 2010</td>
</tr>
<tr>
<td>Computer Word, QuickStudy: Extract, Transform and Load (ETL):</td>
</tr>
<tr>
<td>Gartner Inc., Business Activity Monitoring: Calm Before the Storm, David W. McCoy, 2002</td>
</tr>
<tr>
<td>Gartner Inc., Gartner Identifies Seven Major Guidelines to BPM Project Success</td>
</tr>
<tr>
<td><a href="http://www.gartner.com/it/page.jsp?id=1297313">http://www.gartner.com/it/page.jsp?id=1297313</a></td>
</tr>
<tr>
<td>Handbook of EDP auditing, Halper, Davis, O'Neil/Dunne, Pfau, Warren, Gorham and Lamont, Coopers and Lybrand, 1985</td>
</tr>
<tr>
<td>Haag, 8th edition, MIS for the Information Age, chapters 2, 3.</td>
</tr>
<tr>
<td>Information Lifecycle Management for Business Data An Oracle White Paper June 2007</td>
</tr>
<tr>
<td>Info World, To build or to buy IT applications: <a href="http://www.infoworld.com/d/applications/build-or-buy-it-applications-676">http://www.infoworld.com/d/applications/build-or-buy-it-applications-676</a></td>
</tr>
<tr>
<td>Title</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>approach not only saves money, but also allows auditors to focus on more high-risk areas, April 2009</td>
</tr>
<tr>
<td>Practical IT Auditing, Jack Champlain, Warren, Gorham and Lamont, 2005 Edition</td>
</tr>
<tr>
<td>Real Time Data Warehousing: Challenges and Solutions, Justin Langseth:</td>
</tr>
<tr>
<td>Selecting a Development Approach, Centers for Medicare &amp; Medicaid Services, Department of Health &amp; Human Services, 3/27/2008</td>
</tr>
</tbody>
</table>