Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

IT Audit Bootcamp

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Overview

Identify planning considerations for an audit of internal control over financial reporting, including likely sources of misstatement and testing design effectiveness. Identify testing operating effectiveness and concluding on effectiveness of controls. Recognize how IT affects flows of transactions, identify relevant technology elements, assess risks arising from IT. Understand, identify and test relevant GITCs and evaluate deficiencies in GITCs and assess the impact of GITC deficiencies on the audit.

What you will learn

- The law that establishes the requirements for management to assess the effectiveness of ICFR and to have an independent audit of its ICFR are set forth in Section 404 of the Sarbanes-Oxley. PCAOB AS 2201 establishes the requirements for an audit of ICFR. An integrated audit accomplishes the objectives of both an audit of ICFR and audit of financial statements.
- The “measuring stick” for assessing effective ICFR is the framework selected by management (generally, COSO).
- Identification of the risks of material misstatement includes the consideration of the risk of fraud.
- PCAOB AS 2201.34 requires us to identify the controls implemented to address potential misstatements.
- For relevant controls, we evaluate design effectiveness; and, we test the operating effectiveness of these controls
- Use Higher or Not Higher classifications when concluding on the risk associated with the control. Document the conclusion and the basis for the classification of the risk associated with the control.
- Plan the nature, timing and extent of tests of operating effectiveness based on the risk associated with the control.
- Document nature of tests of operating effectiveness as inquiry, observation, inspection of documentation, and/or reperformance.
- The understanding of IT (along with understanding of other areas of internal control) helps identify if we are placing reliance upon automated controls, system generated reports, data, & substantive procedures not enough, that is an input into the scoping process for GITCs.
- General IT controls are the policies and procedures that serve to support the effective functioning of applications, including the effective operation of automated controls embedded in the applications, the integrity of reports generated from the applications, and the security of data housed within the applications. Areas of GITC are evaluated across technology layers.
- We typically consider the following elements when testing IPE - Source Data, Report Logic, Report Parameters. Testing GITCs alone is not enough to address IPE.
- When considering the design of a control, determine whether there is information used in the control (IUC). We must test controls over accuracy and completeness of IUC.

- When using the work of others, consider whether such work is sufficient to meet our needs.
- Align with the audit team on relevant automated controls and obtain a clear understanding to appropriately test the control
- If IT monitoring/review controls are relevant to the audit, obtain a clear understanding through walkthroughs and determine if the control is designed appropriately including consideration of segregation of duties and completeness and accuracy of logs.
- Segregation of duties divides functions and reduces chance that someone could commit and conceal fraud.
- If the user auditor plans to use an SSAE18 SOC1 report as audit evidence, the auditor should evaluate the report period, the sufficiency of audit evidence, and assess the complementary user entity controls and identified deficiencies.
- If a tool is used within an entity's GITCs, perform relevant procedures over that tool
- If your client experiences a cyber breach , consult!
- Document the nature and cause of identified deviations. Evaluate whether identified deviations are control deficiencies. Recognize that it is rare for deviations to not result in a control deficiency. Use decision trees from the Internal Control Guide while evaluating deficiencies
- There are key differences between an AICPA/ISA audit and a PCAOB audit.

Domains (Syllabus)

Domain 1: Planning considerations related to an audit of ICFR

domain 2: Identify and understand entity-level controls

Domain 3: Identify the relevant flows of transactions (processes) and the relevant IT environments.

Domain 4: Internal control planning considerations in an integrated group audit

Domain 5: Understand likely sources of misstatement

Domain 6: Select Controls using a Top-Down Approach

Domain 7: Test and conclude on design effectiveness

Domain 8: Assess the risk associated with the control

Domain 9: Plan the nature, timing, and extent, and perform tests of operating effectiveness

Domain 10: Assess findings and conclude on the effectiveness of the control

Domain 11: Role of IT Specialists & Process Flow for General IT Controls

Domain 12: Understand How IT Affects the Flow of Transactions and Identify Relevant Technology Elements

Domain 13: Identify and Assess Risks Arising from IT

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Domain 14: Identify and understand entity-level controls

Domain 15: Understand, Identify and Test Relevant General IT Controls

Domain 16: Conclude on Risks Arising from IT and Determine Audit Response & Evaluate Deficiencies in General IT Controls

Domain 17: Considerations for audits in accordance with AICPA/ISA standards

Domain 18: Documentation Considerations and Key Resources for General IT Controls
Review and wrap up

Domain 19: Question and answer session