IIA Executive Audit Tool

Control Matrix Template

Category: Executive

Purpose: How To

The Institute of Internal Auditors

Control Objective/Desired Control Activity	*Categoryof Objective O,F,C*	*Risk*	*Description of Specific Control Activity Identified*	*Client Documentation Reference (Policy or Procedure Reference, flowchart name,etc.)*	*Type of Control (Preventive /Detective)*	*Control Assertion (CAVR)*	*Evaluation*	*Work Program Reference*
1 Control Objective: Ensure that the financial statements are free ofmaterial misstatement	F,C							
Desired Control Activity: Documented controls are in place and operating effectivelythat mitigate the risk of financial statement misstatement.		Financial Statements contain material misstatements.						
2 Control Objective:Comply with Section 404 of the Sarbanes-Oxley Act, internal controls are documented.	F,C							
Desired Control Activity: Internal Controls supporting the objectives of the XXXX department are appropriately documented.		Controls that are in place and operating effectively are not documented.						
3 Control Objective: Comply with Section 404 of the Sarbanes- Oxley Act; documented internal controls are appropriately followed and operatingeffectively.	F,C							

Control Objective/Desired Control Activity	*Categoryof Objective O,F,C*	*Risk*	*Description of Specific Control Activity Identified*	*Client Documentation Reference (Policy or Procedure Reference, flowchart name, etc.)*	*Type of Control (Preventive /Detective)*	*Control Assertion (CAVR)*	*Evaluation*	*Work Program Reference*
Desired Control Activity: Documented controls are communicated, followed, and updated inorder to ensure the reliability of financial data.		Documented Controls are not followed and operating effectively.						
4 Add additional objectives, as necessary. (From Engagement Memo)								
EXAMPLES:								
Control Objective: Trades are executed within establishedpolicies and limits.	O							
Desired Control Activity Trading Responsibilities are segregated from middleand back office functions.	O	Employees perform incompatible Duties; Unauthorized access to automated processes.	Trading Controls and back office report to the Director, Trading Controls and Energy Marketing Accounting, who reports to the CFO.	0-2 Statement of Trading; 4-0 Trading ControlsRoles and Responsibilities	Preventive	R	Duties appear properly segregated	No testing/ Observation

Control Objective/Desired Control Activity	*Categoryof Objective O,F,C*	*Risk*	*Description of Specific Control Activity Identified*	*Client Documentation Reference (Policy or Procedure Reference, flowchart name, etc.)*	*Type of Control (Preventive /Detective)*	*Control Assertion (CAVR)*	*Evaluation*	*Work Program Reference*
Desired Control Activity All personnel involved in trading havesigned off as having read and willing to comply with establishedrisk policies.								

General Risk Analysis (GRA)Column Descriptions

Control Objective/Desired Control Activity [1] – ***Control objectives*** can be broadly defined as what the company strives to achieve by the control. For example, a control objective for cash disbursements may be that all disbursements of cash are properly authorized by management. ***Control activities*** are policiesand procedures that help management ensure the control objectives are met. Control activities may include: approvals; authorizations; reconciliations; verifications; management reviews; physical and electronic access security; and segregation of duties. At a minimum, the GRA should list the objectives stated in the engagement memo[2] [3]

Category of Objective O,F,C – Each objective should be classified into one of the following categories-Operational (O) Financial Reporting (F) or Compliance (C):

Operational – Pertains to the effectiveness and efficiency of the company's operations, includingperformance and profitability goals, and safeguarding resources against loss

Financial Reporting - Driven by external requirements, pertains to the preparation of reliablepublished financial statements including the prevention of fraudulent public financial reporting

Compliance – pertains to adherence to laws and regulations that the company is subject. Pertain to external factors, such as environmental regulations or internal factors, such as compliance with policiesand procedures

Risks – Risk, in this context, is defined as the consequences to the company if the control objective is notmet. Or in other words, what could go wrong.

Description of the Specific Control Activity Identified – The auditor should use this column to documentthe actual control activity in place as identified through a review of policies and procedures, flowcharts, interviews or other methods.

Client Documentation Reference – The auditor should use this column to cross reference the source documentation for the control activity, using specific references. Undocumented control activities shouldbe highlighted for future action.

Type of Control (Preventive /Detective) - Preventive controls are designed to prevent (1) invalid transactions from being processed, and (2) assets from being misappropriated. Detective controls are designed to (1) identify errors or irregularities in transactions already processed, and (2) identify missingassets or invalid disbursements.

Control Assertion (C,A,V,R) – Identify the control assertion associated with the control activity identified, asdefined below:

Completeness (C) – All information is input and processed once and only once, information is processed completely, duplicate transactions are identified and rejected, rejected transactions are activities" listed may be from a reference source, such as COSO, a SOA evaluation tool, other internal control checklist, or from the auditors knowledge.
Accuracy (A) – All valid transactions are accurate, consistent with the originating transaction data,and information is recorded in a timely manner.
Validity (V) – Transactions and updates are authorized and permitted by appropriate personnel, transactions display the actual circumstances, transactions are supported by valid source documents,and transactions comply with the legal requirements.
Restricted Access (R) – Information is restricted to appropriate personnel (physical and logical access protection), company assets are protected from theft and misuse, segregation of operationalareas, authorization and segregation of duties and confidentiality according to legal requirements

Evaluation – Document the initial evaluation of the control, or identified absence or a control. Determineif the control appears sufficient to accomplish the stated objective.

Work Program Reference - If the control will be tested in the fieldwork portion of the audit, cross reference toTeamMate procedure summary.

---

[1] The auditor may also use this column to list the ***Desired Control Activity*** that supports the control objective. Such control activities would represent the "desired control" that would help the auditor focus on identifying the controls that shouldbe present. "Desired control.

[2] Internal control and SOA based audits may have a large number of control objectives and associated control activities.

[3] Although the GRA is designed to capture risk analysis data, reference may be made to a protocol or other documentprepared by Audit Services that meets the same objective tracked, monitored and corrected, and all transactions are timely and comply with the legal requirements.

About The IIA Executive Membership

This tool is an exclusive benefit of The IIA Executive Membership. This membership delivers all IIA member benefits, plus exemplifies the preeminent membership for a high-level, seasoned internal audit executive. Members access customized tools, tailored content, and peer-to-peer networking focused on leadership, team development, performance, and problem solving.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.theiia.org.

Disclaimer

Copyright

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101