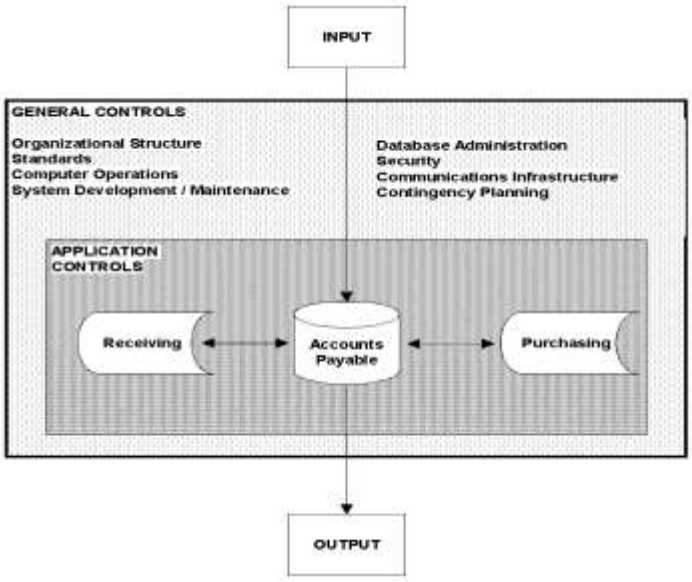
Larry's Cheat Sheet – IT for Auditors (COBIT 4.1)



COBIT 4.1 is available for download at www.ISACA.org.

COBIT's 4 Domains and 34 Processes (Control Objectives for IT)

- Plan and Organize (PO) (10 processes)
- Acquire and Implement (AI) (7 processes)
- Deliver and Support (DS) (13 processes)
- Monitor and Evaluate (ME) (4 processes)

Application Review Steps

1. Understand the general controls of the IS infrastructure in which the application runs
2. Understand the business objectives of the process, and identify the application level risks related to the 7 COBIT information criteria
3. Document the flow of transactions, focusing on the controls to achieve the COBIT Application Control Objectives AC 1 to AC 6
4. Identify the controls that mitigate the identified application risks – logical security will always be an important control

Every application can be broken into three related components. All three components can reside on a single machine, host, or workstation or the application can be split among two or more computers: User interface; Business process; Data management.

General Control Audit Steps

1. Identify and agree the COBIT processes (of the 34) that are applicable to the area under audit.
2. Identify the impact of pervasive IT controls.
3. Identify the specific controls that achieve the Detailed Control Objectives applicable to the audit. (Program change controls are always key – COBIT AI 7.)
4. Test the important specific controls (after considering the strength of the pervasive controls) to determine if they are operating as designed.

COBIT Information Criteria (for Data)

- Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.
- Confidentiality concerns the protection of sensitive information from unauthorized disclosure.
- Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- Compliance deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria, as well as internal policies.
- Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

IIA Practice Advisories 2100-9 and 2100-11

- Pervasive IS Controls – General control areas related to the management and monitoring of IS. These affect the reliability of Detailed IS Controls
- Detailed IS Controls – Other general control areas, plus application controls
- Relevant Controls – Those Pervasive and Detailed controls that have an effect on the specific audit assignment.

Larry@LHubbard.com
In the USA: (301) 529-8118

COBIT Application Controls

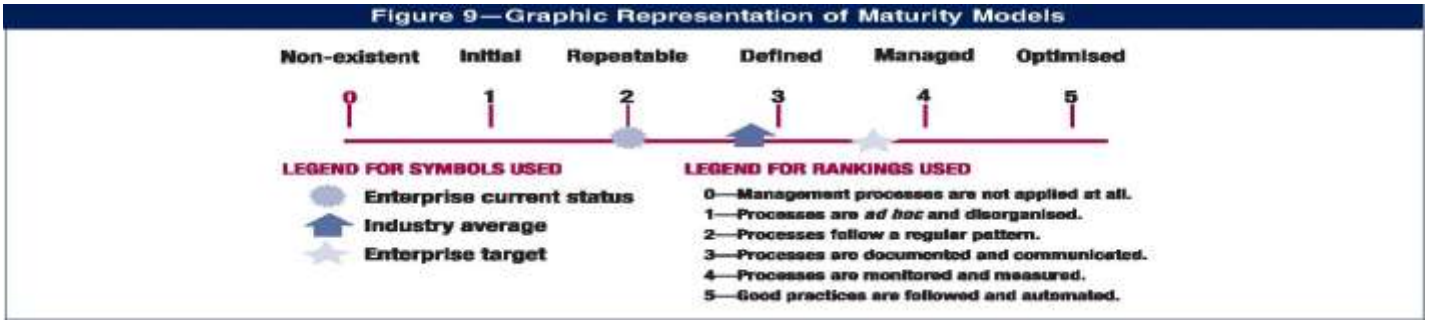
AC1 Source Data Preparation and Authorisation
AC2 Source Data Collection and Entry
AC3 Accuracy, Completeness and Authenticity Checks
AC4 Processing Integrity and Validity
AC5 Output Review, Reconciliation and Error Handling
AC6 Transaction Authentication and Integrity

Logical Security Basics
(Primarily from COBIT DS 5)

1. Each user uniquely identified.
2. Every user authenticated. (For passwords: complex, regularly changed, limited number of invalid attempts.)
3. Active violation reporting and follow-up
4. Regular updates of user rights and attributes
5. Restricted access to sensitive data files (resource protection or encryption)
6. Protection from malicious software (viruses, spam) and up-to-date program patches.
7. Defined procedures for security events
8. Regular backup of important data files.

Other Thoughts

- IT is a normal part of business, and something every auditor must include in their auditing
- The IT professionals are actually more worried about controls than anyone else – controls keep the data center running
- IT controls are part of COSO's Control Activities
- In a Risk Matrix, almost all responses to risks, or controls, are IT-based in some way.
- You don't need lots of controls over passwords – you just need the right controls. (PW history, length, complexity, minimum days are often not well thought out)
- If users can avoid changing passwords, they will.
- Everyone writes down their passwords somewhere.
- Be sure you identify all the logon steps – most users go through at least two or three logons to get to what they need.
- A Help Desk is often TOO helpful – worry about them, not the technical experts.
- Most IT problems that can handicap the business are not technical
- Any backup plan that is not regularly tested will not work the way it is intended
- "IT Audits" mean general controls reviews and other infrastructure audits – done by IT auditors. These are usually on a separate annual audit plan.
- Violation reports MUST be actively reviewed to be effective



Larry@LHubbard.com
In the USA: (301) 529-8118