

Larry's Cheat Sheet – Latest Developments in IA

Changes to Standards

Now called International Professional Practices Framework (IPPF). Non-mandatory guidance changed to consist of Practice Advisories, Position Papers, and Practice Guides. No changes to Code of Ethics or Definition.

1. Interpretations have been added to certain *Standards* to clarify terms or concepts. All interpretations are considered mandatory guidance and are integrated into each relevant standard. It is necessary to consider both the *Standards* and their interpretations to understand and apply the guidance correctly.

2. Six new *Standards* have been added:

1010 - The mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* must be recognized in the internal audit charter. The chief audit executive should discuss the Definition of Internal Auditing, the Code of Ethics, and the *Standards* with senior management and the board.

1111 - The chief audit executive must communicate and interact directly with the board.

2110.A2 - The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

2120.A2 - The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

2120.C3 - When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

2430 - Internal auditors may report that their engagements are conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support the statement.

3. Some amended wording of the current *Standards* has been introduced. Of particular significance is the replacement of should (which previously expressed a mandatory requirement) with must.

4. New requirements in existing *Standards* (partial list):

- 1110 – CAE must confirm independence to board annually
- 1210.A2 – "IAs must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization" ... replaced identify "indicators of fraud."
- 2010.A1 – Annual risk assessment must be documented
- 2060 – Periodic reporting to the Board now includes senior management, and fraud risks.
- 2330.A2 – Added "regardless of the medium in which each record is stored" to record retention.
- 2600 – Dropped "and senior management" from CAE discussion of unacceptable level of residual risks.

5. In most places, "irregularities" replaced with "fraud" and "record" replaced with "document."

6. Modifications to existing terms within the Glossary have been added. It now includes definitions for must, risk appetite, should, etc.

Guidance on Monitoring Internal Control Systems

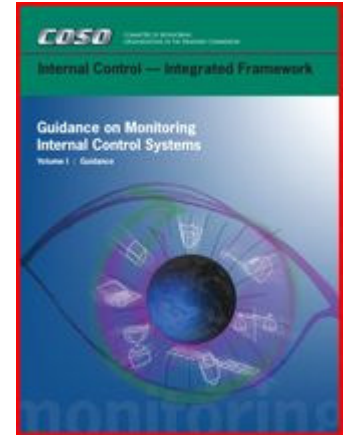
February 4, 2009 - COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is pleased to announce the release of its *Guidance on Monitoring Internal Control Systems*.

Developed by COSO and led by a diverse Grant Thornton LLP team, the guidance is designed to help organizations to better monitor the effectiveness of their internal control

systems and to take timely corrective actions if needed. The Introduction can be downloaded for free from COSO's Web site at www.coso.org. The guidance is available from the www.cpa2biz.com. The three-volume set includes:

- **Volume I:** Presents the fundamental principles of effective monitoring and develops the linkage to the COSO Framework
- **Volume II:** Presents in greater detail the principles outlined in Volume I and provides guidance to those responsible for implementing effective monitoring
- **Volume III:** Contains examples of effective monitoring



S&P Risk Management Rating Comments

The agency has announced that it will start to incorporate ERM into its discussions with the companies it rates starting in the third quarter of 2008, and it will add commentary in its reports in the fourth quarter. It won't be scoring organizations based on ERM, though -- at least, not yet. "We explicitly will not be doing that during 2008, and if we do score companies it will probably not be before the start of the second quarter of 2009," said Steven J. Dreyer, managing director of corporate ratings for S&P, in a teleconference.

Recent Headlines:

- **"Why risk management is letting down companies and what to do about it."**
- **"Why Risk Management Failed; How to Fix It."**
- **"What Happened? They All Had ERM and Risk-Based Internal Auditing."**

Internal Control Maturity Model

In audit reporting, a Maturity Model can be used to rate internal control maturity instead of rating risks or potential impacts as High, Medium, Low. Audit reports can report the status of internal controls, not be reports of only the exceptions. Possible levels of maturity:

Level 1: Unreliable

Unpredictable environment where controls are not designed or in place

Level 2: Informal

Controls are designed and in place but are not adequately documented; Controls mostly dependent on people; No formal training or communication of controls

Level 3: Standardized

Controls are designed and in place; Controls have been documented and communicated to employees; Deviations from controls may not be detected

Level 4: Monitored

- Standardized controls with periodic testing for effective design and operation with reporting to management; Automation and tools may be used in a limited way to support controls

- **Level 5: Optimized**

An integrated internal control framework with real-time monitoring by management with continuous improvement (Enterprise-Wide Risk Management); Automation and tools are used to support controls and allow the organization to make rapid changes to the controls if needed

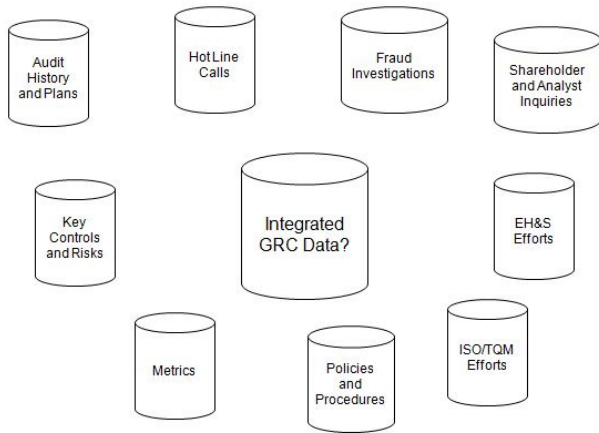
Larry's Cheat Sheet – Latest Developments in IA

Integrated Governance, Risks, and Compliance (GRC) Data and Software

Integrated GRC software can do for GRC data what Data Base Management Systems did for application data files – separate the data from the applications (like Auto Audit and Teammate) and the groups. All these corporate Groups have their own data ... now:

- Auditors
- ISO/TQM Efforts
- EH&S Efforts
- Consultants
- Sarbanes-Oxley Teams
- Security Reviews
- Regulators
- Etc, Etc, Etc

The distinctions between the sub-segments of the broad GRC market are often not clear. And, with a large number of vendors entering this market recently, determining the best product for a given business problem can be challenging. And, given that the analysts don't fully agree on the market segmentation, vendor positioning can increase the confusion.

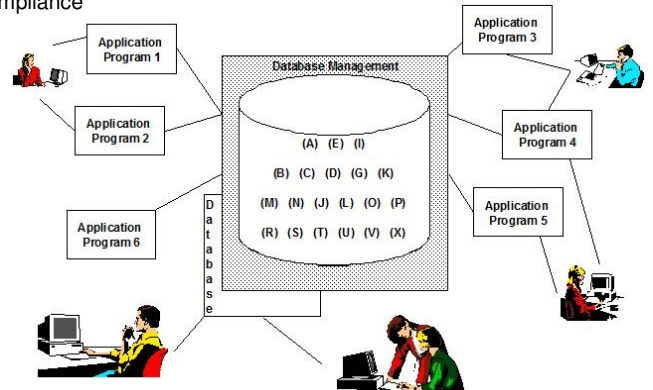


There are a large number of companies who offer a “GRC Platform” for managing and tracking GRC activities across an enterprise. These include large, enterprise software vendors such as CA, SAP AG, IBM, and Oracle Corporation as well as a variety of smaller companies who are targeting the GRC Platform market, including: ControlCase, ControlPath, Curulis, Proventsure, MetricStream, Bwise, Modulo Security, AXENTIS, OpenPages, Trintech, Paisley, QUMAS, Infogov, Security Weaver, MEGA, and several others.

The Forrester Wave: Enterprise Governance, Risk, And Compliance Platforms, Q4 2007 was released on December 21, 2007 and Forrester evaluated 15 leading enterprise governance, risk, and compliance (GRC) platform vendors across approximately 100 criteria. MetricStream, Bwise, AXENTIS, OpenPages, Paisley, and QUMAS rounded out the Leaders category.

However, due to the dynamic nature of this market, any vendor analysis is often out of date relatively soon after its publication.

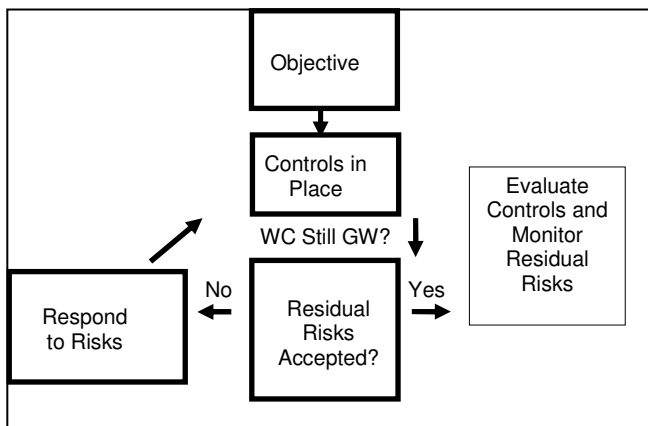
Text extracted from http://en.wikipedia.org/wiki/Governance,_Risk_Management,_and_Compliance



Risk Management Formulas

Typically documented using a Risk Matrix or Risk Register

Best Way – Residual Risks



This is also the format used in the COBIT IT framework.

Traditional Way – Good Theory – Inherent Risks

