Agenda

- Background – T Simon
- Definitions
- Risk, CM & CA
- Risk Intelligent Enterprise
- Risk as Foundation for Internal Audit Planning
- Role of analytics in CM & CA
- Examples of Application of Analytics in CM/CA
- Questions
Definitions

What does Continuous Monitoring do?

- Continuous monitoring enables management to continually review business processes for adherence to and deviations from their intended levels of performance and effectiveness.

- CM is an automated, ongoing process that enables management to:
  - Assess the effectiveness of controls and
  - detect associated risk issues
  - Improve business processes and activities while adhering to ethical and compliance standards
  - Execute more timely quantitative and qualitative risk-related decisions
  - Increase the cost-effectiveness of controls and monitoring through IT solutions

- CM is gives management greater visibility into, and more timely information on, business processes designed to achieve strategic and operational goals.
Definitions

What does Continuous Auditing Do?

• Continuous auditing enables internal audit to continually gather from processes, data that supports auditing activities.

• CA is an automated, ongoing process that enables internal audit to:
  • Collect from processes, transactions, and accounts data that supports internal and external auditing activities
  • Achieve more timely, less costly compliance with policies, procedures, and regulations
  • Shift from cyclical or episodic reviews with limited focus to continuous, broader, more proactive reviews
  • Evolve from a traditional, static annual audit plan to a more dynamic plan based on CA results
  • Reduce audit costs while increasing effectiveness through IT solutions

• CA enables internal audit to move from sampling accounts and transactions to coverage of 100 percent of accounts and transactions (when and where desired).
Risk, CM, and CA

• CM and CA can improve the risk management and control activities of virtually any large enterprise.

• Key Questions:
  • How do we currently monitor controls?
  • How well do the enterprise's controls currently function?
  • How do we currently allocate internal audit resources?
  • How do we determine that this allocation is optimal?
  • What costs and unintended risks do our current methods of controls monitoring and auditing create?

• Deloitte's approach to CM and CA supports, and is supported by, the principles of the Risk Intelligent Enterprise™
The Risk Intelligent Enterprise

• Risk intelligence is Deloitte's philosophy of and approach to risk management, and it consists of practices that:
  
  • Address the full spectrum of risks, including strategic, operational, compliance, reporting, security, environmental, and other risks across the enterprise
  
  • Acknowledge the need for specialization by business and function, but also across organizational "silos"
  
  • Consider the interaction of multiple risks rather than focusing on a single risk or event, and consider the potential impacts of multiple threats
  
  • Create common terms and metrics for risk, and a culture in which people account for risk in every activity
  
  • Support risk taking for reward and value creation, rather than pure risk avoidance
  
• A risk Intelligent enterprise will therefore implement a risk management framework
Risk Management Cycle

1. Identify Objectives
2. Identify and Understand risks
3. Set risk threshold
4. Identify Control Gaps
5. Identify Solutions Strategy
6. Implement Solutions Strategy
7. Measure & Monitor
8. Continuous Improvement

ASSESS
TRANSFORM
SUSTAIN

Risk Management Cycle
Risk Management’s Relationship to Internal Control

**RISK**
Risk is the uncertainty that is inherent in the range of possible outcomes (losses or gains) which occur as a result of the choices and decisions required throughout an extended enterprise.

**RISK MANAGEMENT**
Mechanism that creates stability in the organization by enabling the identification, prioritization, mitigation and measurement of the implications of each decision.

**Internal Control**
Foundation of an Internal Audit Coverage Plan

To package an appropriate assurance plan, the macro, business and internal environments an organisation have to be considered in order to ensure that:

- A holistic business perspective on the challenges that affect the organisation is adopted.
- Identify the relevant and appropriate response to the challenges and complexities that the organisation faces.

**Business environment analysis:**

- Organisations can only **respond** to these challenges.
- Organisations can **influence** these challenges.
- Organisations can **control** these challenges.

**Macro Environment / Industry including Regulatory Environment**

**Business Environment**

**Internal Environment**
The Role of data Analytics In CM and CA

Data Analytics and CM

Key Questions:

• What are the key risks over transactions?
• What controls are in place to manage the risk?
• What data is available to identify any control breaches?
• What breaches should be monitored continuously?
• What tools are available to monitor these breaches?
The Role of data Analytics In CM and CA

Data Analytics and CM

• Management can implement tools to detect significant breaches, and take immediate corrective action eg
  – Exception reporting
  – Dashboard systems

• Where data is not readily available, other monitoring tools can be implemented eg, control self assessment
The Role of data Analytics In CM and CA

• Data Analytics and CA

  • Auditors can implement CAATs to perform efficient wider scope audits on a more frequent basis
  • CAATs will assist auditors to detect control failures through analysis of historical transactional data by:
    – Performing trend analyses
    – Creating relationships between data from disparate systems
    – Identifying, gaps in controls eg, missing document numbers, duplicate transactions, breaches of credit terms, breaches in password controls etc
The Role of Data Analytics In CM and CA

Data Analytics and CA

- CAATs will assist auditors to detect control failures as they occur through embedding data analysis tools to the organisations’ IT systems to identify on an hourly daily, weekly or monthly basis:
  - Dashboard systems
  - Exception reporting on a frequent basis eg daily, hourly
  - Use of IT systems reporting capability for exception reporting
Example of Application of Data Analytics to CM

Example 1

- A lender wanted comfort that the pricing of each loan it extended was in keeping with its underwriting policies, in order to ensure profitability. Its practice had been to calculate loan price on a defined set of business and credit rules, but to allow manual override of these rules. However, when implemented by the lender's agents, that manual override could occur without detection, causing a potential control failure.

- The solution was to continually monitor loan prices and to report deviations from the price calculated only on the basis of the business and credit rules. (Any significant deviation is now detected and reported, and exceptions are investigated and resolved.)
Example of Application of Data Analytics to CM

Example 2

• An operating manager needed to detect unnecessary freight payments, which were set by the trucking company per the weight of the goods being shipped. The contract between the enterprise and the trucking company included clauses that guaranteed a minimum payment if the weight of a delivery fell short of the truck's maximum load. Generally, the minimum cost was set at 0 percent of the cost of a truck's maximum load. Thus, the manager needed to ascertain when trucks were being loaded at less than 0 percent of the vehicle's capacity, situations that would represent inefficiency and excess costs.

• The solution was to automatically identify and report trucks that had been loaded at less than 0 percent of capacity on the same route or destination within a given period of time.
Example of Application of Data Analytics to CM

Example 3

• A comptroller wanted to be able to detect limit-of-authority breaches in areas such as purchases, payables, and sales discounts. The enterprise had established systemic preventive controls to support approval levels in some processes, but those controls could be circumvented. For example, if a person authorized to sign for individual purchases of up to $2,000 wanted to approve a purchase of $10,000, he could input and approve five purchase orders for $2,000 for the same supplier and thus complete the transaction.

• The solution was to continually monitor approvals of expenditures or disbursements to the same entity by each individual with spending authority and to compare the individual and total amounts authorized for a specific entity in a specific period, such as one day or five business days.