

Continuous Risk Monitoring and Assessment (CRMA): Framework for Risk based CA

Daehyun Moon

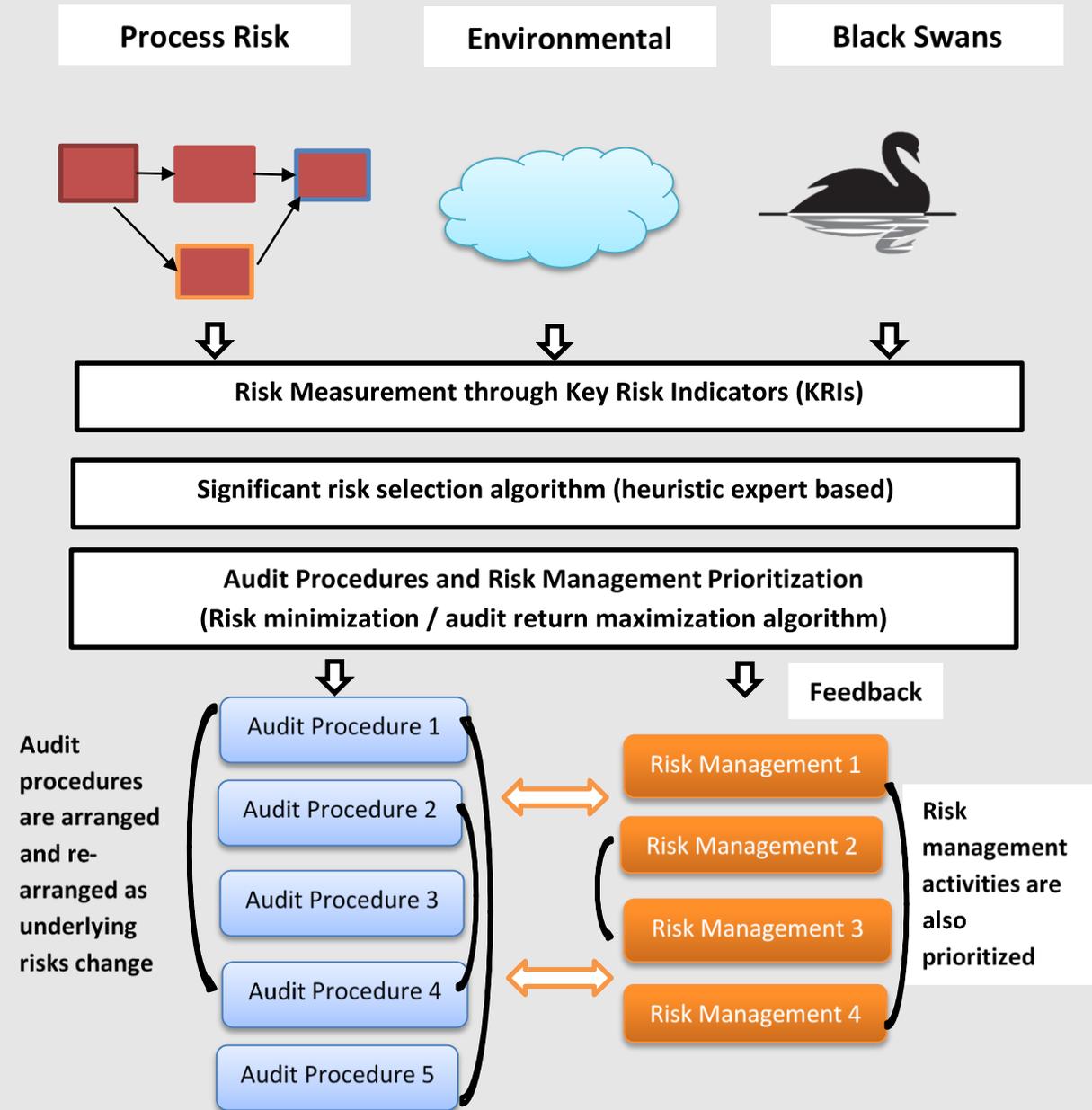
Introduction

- Continuous Assurance as two procedural components
 - Continuous Data Assurance + Continuous Control Monitoring (Alles et al. 2008)
 - Not adopt to changes in audit risks and related business environments → static procedures (Vasarhelyi et al., 2010)
- Vasarhelyi et al. (2010) introduce a concept of Continuous Risk Monitoring and Assessment (CRMA)
 - New CA procedure for risk based CA
 - Continuously assess and monitor the audited entity's risks
 - Dynamically prioritize audit procedures and risk management activities as value-added feedback for the entity.

Schemata of CRMA (Vasarhelyi, 2011)

- Key steps of CRMA

1. Risks Identification
 - I. Process risk
 - II. Environmental risk
 - III. Black swans
2. Risks assessment and monitoring through KRIs
3. Selection of risks to be subject to subsequent audits.
4. Prioritization of audit procedures and risk management recommendations.



Research motivations and questions

- CRMA is an innovative concept shifting into risk based Continuous Assurance.
- But, it lacks underlying theories and methods to understand what CRMA does and how it works.
- This paper develops an extended framework for CRMA further explaining about its key components, purposes, theories, and methods.
- The present methodology would contribute to the completion of CRMA concept and its introduction to the field of CA.

CRMA definition

- CRMA is defined as a series of procedures that (1) identify risks facing the audited entity and allow given CA systems to (2) continuously assess and monitor the entity's business environments and related risks, (3) recognize significant risks that are more likely to materialize and/or whose underlying risk events may have already materialized and have been adversely affecting the entity currently, (4) prioritize relevant audit procedures to deal with audit risks coming from the entity's current significant risks, as well as the risk management activities to mitigate those significant risks as value-added feedback from the continuous risk monitoring and assessment.

Building blocks of CRMA

1. Risks Identification

- Purpose is to identify all potential risks that prevent the entity from accomplishment of its critical business objectives or performance targets.
 - Process risk
 - Environmental risk
 - Black swans

Process risk

- Process risk category includes possible risk events threatening the failure of the achievement of the audited entity's given objectives due to its inefficient internal environments, such as unsuccessful business processes, rogue employees or misaligned strategies.
- Example may include,
 - Budget risk
 - Human resource risk
 - Project management risk
 - Employee strike risk

Environmental risk

- This risk category includes potential risk events that are mainly from the entity's external environments, such as government, customers, third-party suppliers, market variables (interest rate, exchange rate, etc.), natural hazard, terrorist attacks, war, etc.
 - Third-party risk
 - Exchange risk
 - Competitor risk
 - Reputation risk

Black swans

- Black swan risk (Taleb, 2007) refers to risks that are extremely rare, thus unknown to the world, unknowable or unpredictable before they occur.
 - 9-11 terrorist attack
 - 9.0 earthquake in Japan and tsunami in 2011
 - 2007 financial market crisis
- Ignoring black swan events may end up with catastrophic damages causing significant losses not only to the entity's businesses, but also to auditor's reputation.
- It would be better if the auditor senses emerging black swans before they issue an opinion and communicate with the management.

Black swans in CRMA

- CRMA takes unique approach to identify potential black swans.
- Black swans are *imagined* with the entity's critical assets or most valuable things without which the entity cannot continue as going concern, such as major assets, main products and services, major customers, skilled employees or managements, etc. as extreme events that could severely destroy or disable those critical assets once happen, causing extreme damage to the entity.
- Example
 - Betrayal of trusted CEO selling out the entity's *secrete formula*.
 - A meteor hits the entity's major *manufacturing facilities*.
 - Breakout of unknown epidemic disease affecting the sales of the *main products*.

Building blocks of CRMA

2. Risks Assessment

- Business risks drive audit risks (Lemon et al., 2001, Knechel, 2007)
 - Business Risk Audit or Strategic Systems Audit
 - KPMG's Business Measurement Process; E&Y's Audit Innovation (Knechel, 2007)
- A risk (or materialized underlying risk event) → likely to prevent the entity from achieving given objectives → likely to motivate management to manipulate financial data to hide underachieved objective → increase material misstatements risk.
 - Weak internal control environment.
 - Going concern issues

Likelihood of Risk vs. Effect of Materialized Risk

- CRMA determines the significance of a given risk to the audit by factoring in the likelihood of a risk and the effect of the materialized risk event.
- CRMA aims to assess and monitor these two distinct development status of a given risk event on real time basis, so that changes in its significance to the audit can be recognized and corresponding audit responses can be followed promptly.
- To this end, the proposed CRMA methodology utilizes Key Risk Indicators (KRIs) and Lagging Indicators.

Key Risk Indicators (KRIs) vs. Lagging Indicators

- A KRI is defined as any type of data (ratio, quantity, qualitative) that indicates current symptoms (signs) of a rising risk,
 - early warning signal for potential problem.
- A lagging indicator can be also any type of data that represents current effects of materialized risk events.
- The proposed CRMA methodology uses relevant KRIs to continuously (automatically) assess the likelihood of a given risk event and current effect of the materialized risk.
 - If KRIs are collected in real time, it would be possible to keep track of changes in the entity's business and risk environments in close to event time or near real time.
 - Advanced IT and integrated information systems enables real time data processing and cross-functional data analysis. This would facilitate the auditor collect relevant KRIs in real time to assess and monitor the entity's business and risk environments.

Threshold

- A threshold value represents a limit or range of values the relevant KRI or lagging indicator can take to be considered as normal.
- With a specific threshold value, the observed value a KRI or a lagging indicator can be normalized on common scale.

- If the threshold is set as *maximum* limit:

$$\text{Standardized score} = \frac{\text{Value observed}}{\text{Threshold (max)}}$$

- If the threshold is set as *minimum* limit:

$$\text{Standardized score} = \frac{\text{Threshold (min)}}{\text{Value observed}}$$

- If the threshold is set as a range limit *between a minimum and a maximum* value:

$$\text{Standardized score} = \frac{\frac{\text{Value observed}}{\text{Threshold (max)}} + \frac{\text{Threshold (min)}}{\text{Value observed}}}{2}$$

Building blocks of CRMA

3. Selection of significant risks

- **Significance of a Risk**

- CRMA measures the audit significance for each risk which indicate the extent to which a given risk event will drive related audit risks. The greater the audit significance score is, the higher audit risk it indicates.
- The significance of a risk is the weighted average of the standardized score of all KRIs and lagging indicators given for the risk.

$$\sum_{i=1}^n \text{standardized score } (i) * \text{weight } (i)$$

Example: Liquidity Risk at a bank

- For a bank, having sufficient liquidity would be a critical business objective to achieve for its smooth business operations without a significant funding problem.
- The event that the bank will not have sufficient liquidity at hand would be a major risk event threatening the bank's business operations.
- The liquidity risk may be classified as *Process* risk if the bank's liquidity problem is mainly driven by its inefficient internal processes, such as ineffective liquidity management, insufficient operational incomes, too much borrowings, or poor credit risk management, preventing the entity from accomplishing having a sufficient liquidity.

Some relevant KRIs and Lagging indicators for the liquidity

- KRIs (that indicate symptoms of the rising liquidity risk; *early warning signals*, there may be no problem yet)(Matz, 2007)
 - Spread between the entity's funding costs and its peers' costs
 - Decline in earnings
 - Increase in loan delinquency
 - Decline in the bank's stock price
 - Significant asset acquisitions
 - Increase in Exchange rate
 - Decline in the bank's minimum liquidity ratio
- Lagging indicators (that represent the current effect of the materialized liquidity risk problem; the problem has started)(Matz, 2007)
 - Increase in non-performing loan
 - Downgraded rating
 - Increase in number of turndown of borrowing requests

KRIs & Lagging Indicators	Threshold	Observed value	Weight	Standardized score	Standardized score * Weight
Decrease in earnings (KRI)	5% (max)	3%	1/9	0.6	0.07
Decrease in stock price (KRI)	5% (max)	2%	1/9	0.4	0.04
Increase in asset acquisition (KRI)	10% (max)	2%	1/9	0.2	0.02
Spread between the entity's funding costs and its peers' costs (KRI)	0.5% (max)	0.3%	1/9	0.6	0.07
Increase in loan delinquency (KRI)	5% (max)	10%	1/9	2	0.22
Increase in Exchange rate (KRI)	20%(max)	5%	1/9	0.25	0.03
Increase in non-performing loans (lagging)	10% (max)	15%	1/9	1.5	0.17
Downgraded rating (AAA: 6; AA: 5; A:4; BBB: 3; BB:2; B:1) (lagging)	BBB:3 (min)	BB:2	1/9	1.5	0.17
Increase in number of turndown of borrowing requests (lagging)	10% (max)	30%	1/9	3	0.33
Significance of liquidity risk $\sum_{i=1}^n deviation(i) * weight$				=	1.12

Significant risk ranking

- CRMA computes the significance score for each risk in a continuous manner and ranks them according to their significance scores automatically.
- The rankings would refer to the entity's most significant risks in order and be kept always current and updated on ongoing manner.

Risks	Significance score	Rankings
Liquidity Risk	1.12	1
Litigation Risk	1.05	2
IT security Risk	0.35	3

Building blocks of CRMA

3.1 Prioritization of audit procedures

- CRMA prioritizes subsequent audit procedures that deal with audit risks related to the entity's most significant risks first.
 - as the rankings are updated in real time, the audit procedure priorities will always reflect the entity's current risk environments.
- Audit risks are defined as potential material misstatements and internal control weaknesses in the entity's business processes that are expected to be affected by a given risk event.
- For example, if the entity with liquidity problems or likely to have ones the liquidity risk, audit risks would be greater for the valuation process and disclosure about the fair value of collateralized debt obligation (CDO) assets.

Building blocks of CRMA

3.2 Prioritization of risk management priorities

- CRMA also prioritizes the risk management activities according to the entity's current significant risk rankings.
- Suggested risk management activities would be the auditor's feedback from the continuous risk assessment and monitoring to strengthen its risk management process particularly for the identified significant risks.
 - When the entity's significant risks profile changed
 - Value-added feedback for the management.

Risk Management Priorities

1/31/2018

From our continuous risk monitoring and assessment of the entity's risks, we identified following changes in the significant risks facing the entity.

1. Liquidity risk
2. Litigation risk
3. IT security risk

Our relevant KRIs and lagging indicators analysis indicate that

1. The liquidity problem has started, review contingency liquidity plan;
2. Number of non-performing loan has increased; reinforce credit risk management

Conclusion

- Propose an extended framework
 - Methodology
 - Theories
- Innovative concept to incorporate risk assessment and monitoring process into Continuous Assurance systems.
- With CDA and CCM, CRMA shifts into risk based CA systems.
- Reduce the risk of audit failure due to the abrupt changes in the entity's business and risk environments.

1. Risk Identification

- 1.1 Understand and recognize a client's each key business objective
- 1.2 Identify risk events that could adversely affect the achievement of those key business objectives by Process, Environmental, and Black swans.
- 1.3 Select risks that would bring serious impacts when they materialized.

2. Risk Assessment

- 2.1 For each risk identified and selected, develop or choose relevant risk indicators which provide relevant information about current status of risk in terms of Leading risk indicator and Confirmatory risk indicators.
- 2.2 Determine threshold for each indicator.
- 2.3 Use algorithmic procedure to compare actual observed value against the threshold for each risk indicator.
- 2.4 Compute the weighted average of the deviations of all risk indicators as a significant score for the given risk.

3. Significant risks selection

- 3.1 Use algorithmic procedure to assign a ranking to each risk monitored based on its significant score.
- 3.2 Continuously update the significant risk rankings as the significance risk scores change.

4. Prioritization of subsequent assurance procedures

- 4.1 Develop pre-established linking schedule that relates each risk to relevant assurance procedures to examine its related business processes and the risk management controls.
- 4.2 Use algorithmic procedure to prioritize assurance procedures by mapping each risk in order of its significant risk ranking to corresponding assurance procedures in the pre-established linking schedule.

Thank you!