Paper submitted for the:

Enterprise Risk Management Symposium

April 22-24 2013, Chicago, IL

Integration and use of Enterprise Risk Management (ERM) information

Type of Paper: Both theoretical and applied

Amelia Ho, CA, CRMA, CRISC, CIA, CISA, CFE, MBA

Email: Amelia.Ho@alumni.insead.edu

Amelia Ho is Country Audit Head of a global financial services company and has held compliance and risk management positions in financial services firms. She serves as a steering committee member of the Professional Risk Managers' International Association (PRMIA), which organizes events to promote risk management. She is also a Subject-Matter Expert, reviewer, speaker, writer and trainer for professional risk management, accounting and audit bodies. She has written articles on compliance management and Emerging Risk Audits (ERAs) published in the Information Systems Audit and Control Association (*ISACA) Journal* and the *Internal Auditor* periodical of professional audit bodies. She was a speaker or presenter on Enterprise Risk Management (ERM), risk identification and assessments, and business continuity risks for professional accounting and risk management organizations. She has also reviewed and contributed to risk management publications.

Abstract:

It is important to identify, measure, analyze and monitor risks such that risks can be properly managed with appropriate risk management decisions and actions to be taken on a timely basis. This paper describes ways to identify and measure various types of risks for management purpose. It suggests methods that can be used to report and/or integrate measurements of different types of risks to facilitate analysis, comparison, discussion and monitoring of risks by various parties. Through communication and monitoring of relevant, reliable and up-to-date risk information, management can make effective risk management decisions such as decisions on risk management actions/tactics for each risk identified, and prioritization of risk mitigation.

Integration and use of Enterprise Risk Management (ERM) information

Introduction

There are many types of risks within the Enterprise Risk Management framework and different methods are available to identify and measure risks. It is important that pertinent risks are appropriately identified, measured, reported, integrated, analyzed, monitored, communicated and managed by an entity so that its enterprise risk management can deliver good value to an entity.

Definition of risks

There are various definitions of risks. For instance, ISO31000:2009 Risk Management Standard defines risk as the "effect of uncertainty on objectives". In this definition, uncertainties include events (which may or not happen) and uncertainties can be caused by ambiguity or a lack of information. It also includes both negative and positive impacts on objectives. This definition refers to the probability of an event happening which can cause certain impact on objectives. From this definition of risk, it can be seen that two common elements of risks are probability and impacts.

Types of risks

With the broad definition of risks, there can be different types and categories of risks. For instances, there are strategic risks, market risks, credit risks, and operational risks. Operational risks cover risks in Human Resources (HR), financial management, information management, transaction processing, legal & compliance, fraud, etc. Also, there are various categories of risks such as inherent risks, residual risks and emerging risks which are described below.

Inherent risk is the susceptibility of information or data to a material misstatement assuming that there are no mitigating controls. They arise due to the inherent nature of the risks. Factors to consider in determining inherent risks include materiality, nature of operations, external factors, fraud factors, and operational changes. For instance, inherent risk of cash is high as it is susceptible to theft. Inherent risk is useful information for the auditors and risk management teams to determine the extent and nature of reviews required for various inherent risks faced by an entity. Based on the inherent risk level, management can also determine the level of controls required to mitigate the risks to an acceptable risk level.

Inherent risk is a factor to be considered when determining the residual risk. Residual risk is defined as the risk remaining after management takes action to reduce the impact and/or likelihood of an adverse event, including control activities in responding to a risk.

Integration and use of Enterprise Risk Management (ERM) information

Residual risk is determined after taking into account of the inherent risks, identified control weaknesses and risk incidents experienced by the entity, and controls or other risk mitigation measures in place. For instance, the residual risk of cash can be reduced if the cash is stored in a safe with dual control for its physical access together with monitoring over the access to the safe via Closed Circuit TVs (CCTVs). Residual risks are useful information for management to determine whether the existing risk management strategy is adequate and whether additional risk management actions are required to address the residual risks. For instance, if the residual risk is beyond the acceptable tolerance range set for the risk, the risk should be rejected, mitigated or transferred.

Another category of risk is emerging risk. Emerging risks can arise due to certain types of events and/or changes such as changes in regulatory, technology, operation, life style and external environment. For instance, event such as the 2008 global financial crisis which had widespread effect of systemic risks in the financial industry can make credit risk an emerging risk for any financial institution. The inherent risk for credit risk was high during such period. On the other hand, emerging risks can have low inherent risks as the risks are still at their infancy stage. Examples of such emerging risks include cloud computing and wireless security for entities which do not have important or production Information Technology (IT) systems built on cloud computing or wireless communication.

Risk information

For the various categories of risks, there are various sources of information to help identifying the risks:

Internal Sources of risk information

- Information from internal processes or systems, for example:
  - Risk incident reports, fraud investigation reports, internal loss database (with loss events occur within the entity) and compliance issue database
  - Continuous monitoring of risk indicators
- Reports of control weaknesses based on reviews conducted by parties such as auditors, risk management teams, compliance, regulator, and service providers
- Input provided by the Board of Directors (BoD), Audit Committee, business management or other corporate governance functions (e.g. compliance, enterprise risk management, IT, security) on their views of risks
- Internal information on changes occurring within the entity which can give rise to emerging and/or strategic risks (e.g. regulatory/industry/ accounting/technology/operational /strategy changes)

Integration and use of Enterprise Risk Management (ERM) information

External Sources of risk information

- Requirements / requests from regulator(s)
- External loss database (with loss events from entities in the industry)
- News on other companies' frauds, court cases, pending investigations, control weaknesses, etc.
- Ongoing research and monitoring of:
  - Forums or conferences organized by external parties
  - Publications by risk rating agencies, consulting firms, audit service providers, professional and industrial associations
  - Peer networking

For a summary of the sources of risk information for inherent risks, residual risks and emerging risks, please refer to the Appendix.

Identification of risks and risk inventory

Based on the various sources of risk information, risks can be identified for an entity by parties such as business functions, corporate governance functions and management. For instances, control reviews conducted by the corporate governance functions can identify risks. IT personnel can participate in IT security conference/forum and identify certain IT risks and/or emerging risks. There are different ways for people to identify risks for their entities.

Once risks are identified, risk data should be created and updated in a controlled and timely manner to increase the usefulness of the risk data. For instance, a risk inventory can be kept manually or in the Enterprise Risk Management (ERM)/Governance, Risk Management and Compliance (GRC) system to be accessed by interested parties such as corporate/regional/local management and corporate governance functions. Update of risk data can be conducted periodically (e.g. based on the results of periodic risk control self assessment, Key Risk Indicator (KRI) monitoring, etc.) or on an ad hoc basis (e.g. based on risk incidents or identified emerging risks). Update of risk data should include retirement of risk data which are no longer relevant to an entity. Risk inventory should be properly maintained with proper controls over its management.

Measurements of risks

As stated in the definition of risk, the two key components of risks are probability and impact/severity. One way to measure risks is to measure risks on its constituents, namely probability and impact/severity. Probability assessment can be based on the inherent risk,

trend analysis and past history of control review results and/or risk incidents occurred in a country/industry/entity. For examples, certain countries are more prone to natural disaster (e.g. earthquakes) than other countries, a financial institution has a higher chance of data privacy issue compared to an industrial company, etc. Impacts, on the other hand, can be assessed in terms of materiality and strategic/reputational/financial/regulatory impacts. A business unit is material to a business group if it constitutes a big portion of the business group in terms of sales/profit and/or it has a strategic impact to the entity (e.g. certain product/service/market has strategic value to an entity). Reputation impact can be big if an entity makes fatal mistake where the incident was widely published (e.g. a retail bank's misrepresentation in selling a financial product to its retail customers). Financial impact can be in the forms of fines, penalties, compensations and loss due to fraud. An example of regulatory impact can be the loss of an entity's business license if certain regulatory requirement is not met by the entity. Probability assessments and impact/severity assessments is one way to measure inherent risks and residual risks, with the latter taking into account of the controls while the former does not.

Risk measurements of probability and impacts/severity can be reported separately or in combination. Probability/frequency, impact/severity and risks can all be measured by assigning a ranking such as Very High/High/Medium/Low/Very Low, etc. For examples, interest rate risk can be assessed as high for probability and very high for impact/severity. The overall interest rate risk can be assessed as High. There can also be agencies which assigned risk rating based on their defined criteria. For instance, credit rating agency can assign credit risk ratings to countries, institutions, financial products, etc. An overall risk rating can be derived and assigned to a risk.

For emerging risks, it can be measured by the degree of uncertainty versus time to illustrate the maturity of the risk. If the emerging risk is at its infancy stage, it will have a low value for time and the uncertainty will be high. For instance, when social media is at its early stage and not many people has adopted its usage, the value in time is low and uncertainty is high as it is unsure the impact of social media. When the risk is more mature, it will have a relatively higher value in time and lower value in uncertainty as it becomes more apparent of the impact of the risk with the progression of time. For instance, in 2008, it became obvious that there was widespread systemic risk during the global financial crisis which resulted in a significant credit risk. Hence, the degree of uncertainty is low and the value in time is high. This illustrates how emerging risks can be measured.

Risk can also be in monetary terms based on the combined effect of probability and impact/severity (measured in dollar terms). Financial measurements of risks are common practices as they provide useful information to facilitate decision making. For instance, Value At Risk (VARs) is a measure of risks which can be used for measuring market risks,

credit risks and operational risks. VAR can be defined as a threshold dollar amount value (the worst loss) such that the probability that the loss over the given time horizon exceeds this value is the given probability level. Similar to previous description of risk measurement, VAR is a measure describing the impact/severity (i.e. dollar amount of loss) with what probability. Measurements of risks in monetary terms provide information to various stakeholders on the potential amount of dollar that is at risk. The usefulness of such risk information depends on how good the risk estimation is (e.g. whether the estimated risk is closed to the actual amount of loss or not).

For a summary of risk measurements for emerging risks, inherent risks and residual risks, please refer to the Appendix.

With the different ways of measuring risks, one must decide the risk measurements to be used. For some industries and entities, there can be regulatory requirements for certain types of risk measurements to be used. For instances, Basel regulation requires 99% probability and Value at Risk (VARs) to be used for measuring market risks for banks. While comparability may be increased when the same risk measurement is used, the impact can be big if the wrong risk measurement is consistently and widely used. For instance, if the credit risk rating agency did not correctly assess and assign credit risk ratings to certain types of financial products and/or entities, wrong decisions can be made by investors and/or trading partners who based their decisions on the credit risk rating. Hence, one must be careful in choosing and calculating risk measurements to avoid situations where wrong risk management decisions are made based on inappropriate risk measurements.

Reporting of risks

After risks are measured, they should be reported to facilitate communication, monitoring and management of risks. For each risk identified, the following can be reported:

- type of risk
- risk description
- risk driver(s)
- overall risk level (e.g. high/medium/low, red/yellow/green, etc.)
- risk measurements (e.g. probability, severity/impact, dollar amount)
- trend of risks (e.g. stable/deteriorating/improving)
- risk indicators

- tolerance level of the risks for residual risks (e.g. threshold set for a Key Risk Indicator)
- risk strategy (e.g. risk avoidance/mitigation/transfer/acceptance) and its details (e.g. how risk is mitigated or transferred)
- mitigation status (where applicable) and accountabilities

To establish formal reporting process for risks, there should be documented definitions of key attributes of risks such as what criteria need to be met so that the trend of risk can be stated as stable/improving/deteriorating, or mitigation status can be stated as green/yellow/red, etc. Also, there should be pre-defined scales used in measuring severity or probability and pre-defined threshold for key risk indicators. Below is a sample of description of the "Capital adequacy and volatility" risk for a financial institution for illustration purpose and it is not necessarily a comprehensive description of the risk.

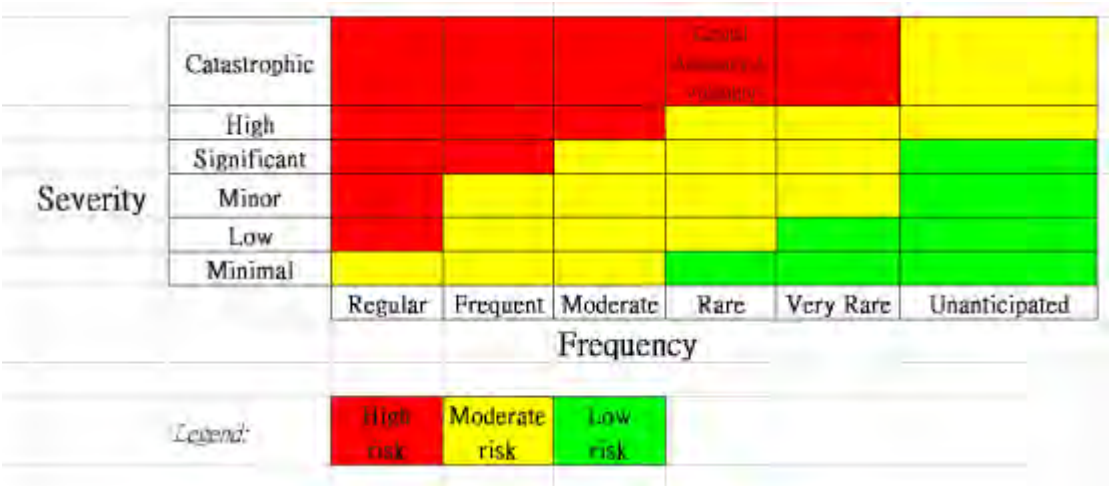
Name of risk:	Capital adequacy and volatility
Type of risk:	Financial risk and regulatory risk
Risk description:	Inadequate capital to meet regulatory requirements and/or to meet liabilities resulting in inability to operate as a financial institution
Risk driver(s):	Interest rate movement
Overall risk level: *(High/Medium/Low)*	High
Risk measurement(s):	*Probability:* Rare *Severity/Impact:* Catastrophic
Trend of risk: *(stable/improving/ Deteriorating)*	Stable
(Key) Risk indicator(s):	- Solvency measurements (e.g. solvency ratio) - Sensitivity analysis on solvency ratio

Integration and use of Enterprise Risk Management (ERM) information

<table>
<tr><td></td><td>- Local capital sensitivity measures using pre-defined stress testing factors and scenarios</td></tr>
<tr><td>Tolerance level of the residual risk:</td><td>Thresholds for the “solvency ratio’ KRI set by the regulator (i.e. regulatory minimum capital) and the entity (i.e. internal target level) are 150% and 200% respectively</td></tr>
<tr><td>Risk management actions, accountability and status:</td><td>
<table>
<tr><th>Mitigation action</th><th>Accountability</th><th>Status</th></tr>
<tr><td>Monitoring of liquidity ratios</td><td>Asset Liability Management (ALM) team</td><td>Green</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
</table>
</td></tr>
</table>

Risks can also be reported in a risk map. Based on the measures of the likelihood/probability and impact, risk can be plotted in a risk map. Figure 1 below illustrates how the risk of capital adequacy and volatility is reported via a risk map.

Figure 1: Sample of risk map for risk reporting purpose

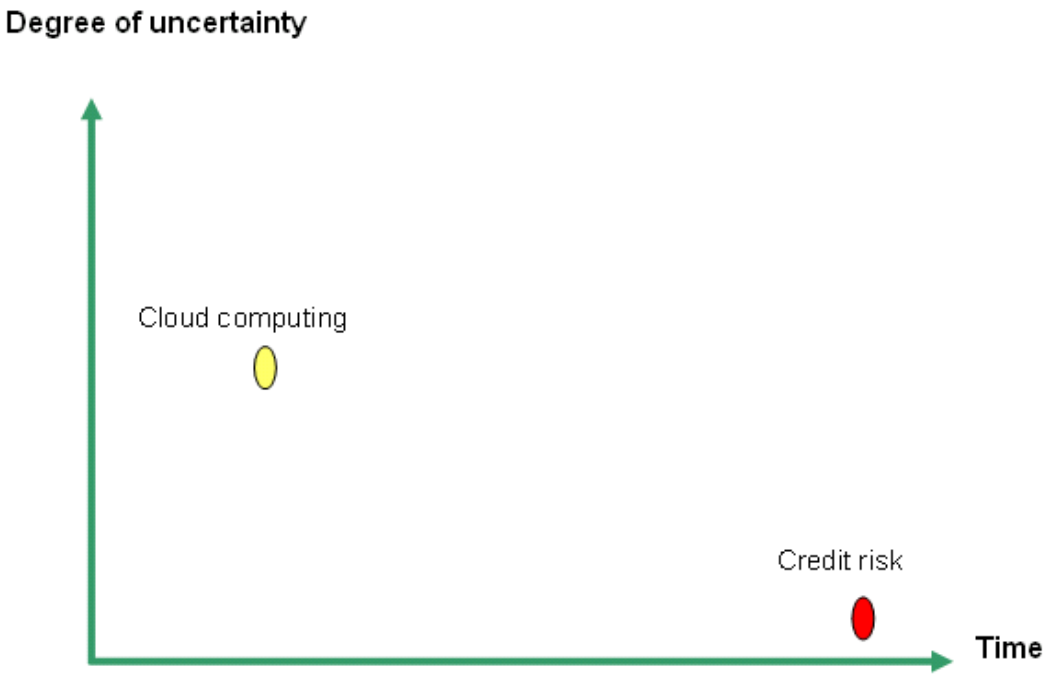


In risk reporting, it is reporting on the residual risks which take into account of risk mitigation once they are implemented. Risk mitigation strategy can potentially reduce probability and/or severity of a risk. For examples, if risks are hedged or insured, the risks in monetary terms can be reduced by the amount which is covered by the effective hedge(s)

or insurance. Effectiveness of the hedge or insurance can vary at different points in time. For instance, during financial crisis where systemic risk is high, the counterparty offering the hedge or insurance may go out of business which means the probability of obtaining an effective hedge from another entity (e.g. financial institutions) can be reduced at times when systemic risk is high. Care must be taken when reporting risks as the level of risks can change at different points in time (e.g. during global financial crisis) as effectiveness of risk mitigation can change over time.

As mentioned in the previous section on risk measurement, emerging risks can be measured by the degree of uncertainty versus (vs.) time and be reported as such. Figure 2 below is a sample of report for emerging risks.

Figure 2: Sample of a 2008 report for emerging risks of a financial institution



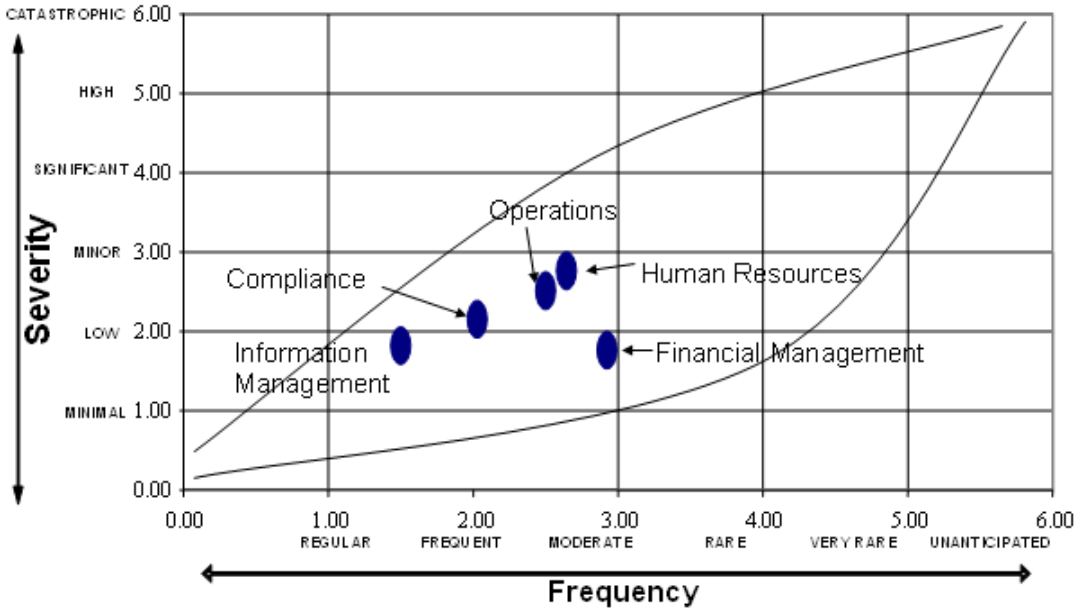
For a summary of risk reporting for emerging risks, inherent risks and residual risks, please refer to the Appendix.

Integration of risks

Besides measuring and reporting risks, integration of risks is a useful way to facilitate management in assessing and analyzing risks. In general, risks which are measured in the same way can be integrated. For examples, risks measured in monetary terms (e.g. Value at Risk, VARs) can be added. For risks which are measured as High/Medium/Low, etc., they can be integrated and displayed in a diagram. Risk map can be used for integrating and

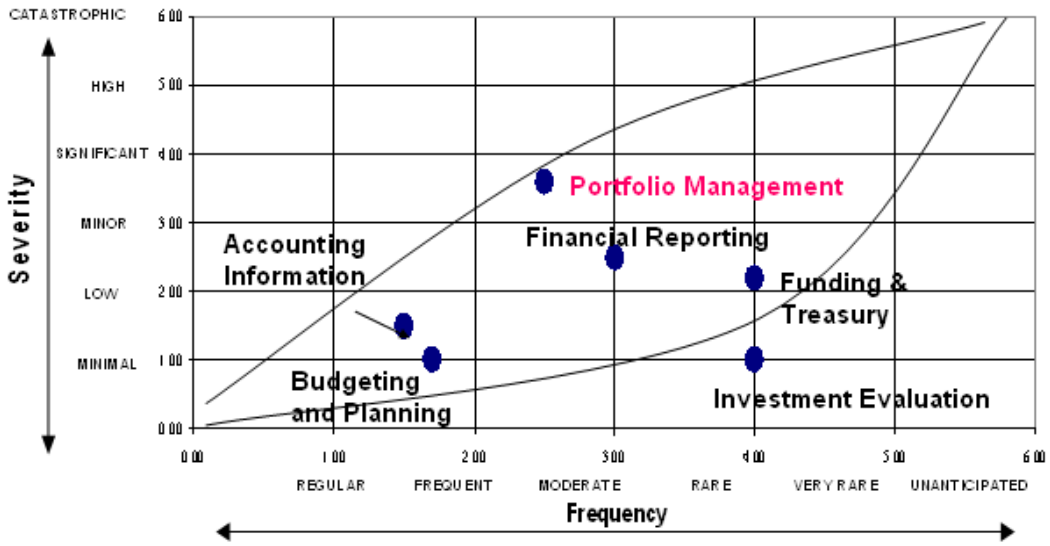
reporting operational risks and emerging risks. Figure 3 below demonstrates how a risk map is used for integrating different types of risks such as Human Resources (HR) risks, compliance risks, etc.

Figure 3: Demonstration of how to integrate different types of risks in a risk map



Within one type of risk (e.g. financial management risk), risks can also be integrated and displayed in the risk map and this is illustrated in Figure 4 below.

Figure 4: Illustration of how to integrate various financial management risks in a risk map



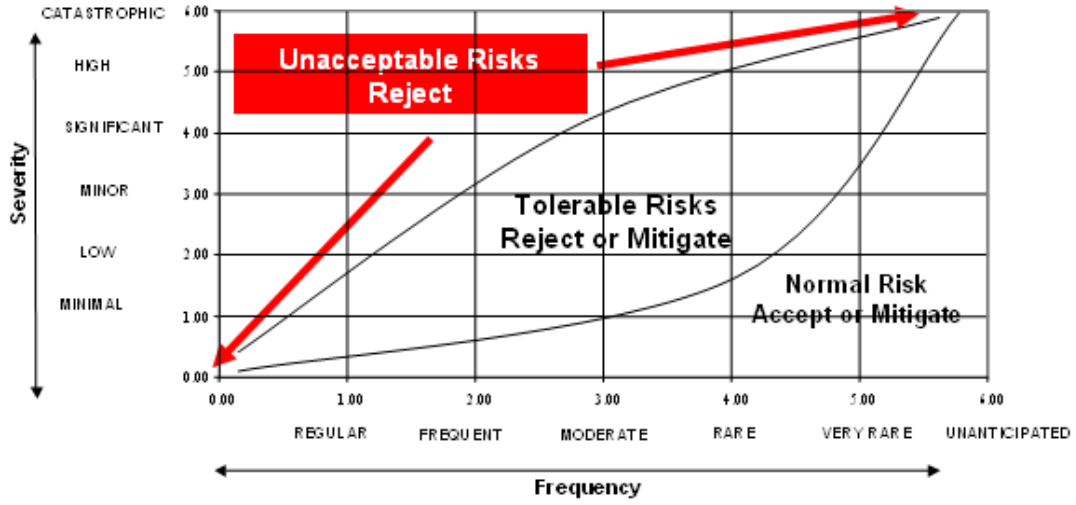
Integration and use of Enterprise Risk Management (ERM) information

Analysis of risks

After risks are measured, reported and/or integrated, risks should be analyzed to identify the most appropriate risk management strategy (i.e. risk avoidance/acceptance/transfer/mitigation) for each risk based on the risk appetite (e.g. risk limits) of the entity. For different types of risks, the risk management decision rules/heuristics can vary. For instance, for strategic risks, the risk management decisions can be based on discussions with senior management who can take into account of scenario analysis, consultants' reports, etc. For market risk and credit risks, the risk management decision rules can be very specific such as cut loss for securities trade transactions where losses exceed certain dollar limit. Another example of risk management decision rule is entities do not transact on financial products and/or trade with counterparties whose credit ratings are below certain grades. For operational risks, the risk management decisions can be based on the risk rating (e.g. avoids risk when the risk level is at catastrophic level, accepts risk if the risk level is very low, etc.). There are different tools for analyzing risks and the appropriateness of the tool depends on the type of risks, the quality of the tool and the experience of the person using the tool.

Risk maps can facilitate risk analysis. For instance, one can easily see which region a risk is located in a risk map and the appropriate risk management strategy can be decided based on the region a risk lies in the risk map. Figure 5 below is an illustration of applicable risk management strategy for different regions in the risk map.

Figure 5: Risk map which highlights various risk management strategies for different regions in the risk map



From the risk map at Figure 4 shown in the previous section, it can be seen that the risk of "Portfolio Management" is at the boundary of tolerable risk and unacceptable risk.

Integration and use of Enterprise Risk Management (ERM) information

Management should analyze and monitor such risks carefully so that an appropriate risk management strategy is chosen to ensure the risk does not create undesirable exposure for the entity. When analyzing portfolio management risks, one can assess the entity's exposure to risky countries/industries/companies/financial products, etc. If one has assets in a foreign currency, one can analyze the impact of depreciation of a country's currency and determine whether hedging or asset liquidation is required to manage or avoid the risks. Risk can be analyzed in details depending on the significance of the risks.

Risk analyses for emerging risks are different. In particular, options for actions can decrease with time. For example, if the emerging risk for a financial institution is credit risk, when it is approaching the peak time in the 2008 global financial crisis, the financial institution may have a lesser chance of reducing its credit risk by obtaining extra line of credits or additional credit limits, etc. The earlier the emerging risk is identified, analyzed and managed, the more options are available (e.g. there is a higher chance that an entity can liquidate its assets to obtain cash) at a relatively lower cost (e.g. lower transaction cost) compared to the time when the emerging risk peaks. One tool that can be used to analyze emerging risk is to conduct catastrophic scenario stress testing (where necessary).

Monitoring of risks

Risk analysis is not a one-off exercise and risks should be monitored regularly and on a timely basis. To facilitate monitoring of risks, risk indicators and acceptable threshold can be defined for each risk. If actual risk level exceeds the tolerance level, one should analyze the risk and determine the appropriate risk management strategy. Follow up actions can be taken where necessary. For instance, if the availability of a retail banking system is below its target level, then the risk should be analyzed to address its root cause and risk mitigation should take place to raise the system availability level to an acceptable level at a minimum. Trends of risks can also be monitored to ascertain whether the risk keeps stable, improving or deteriorating. Management can take appropriate actions based on the risk trend (e.g. more timely actions may be required if a risk is deteriorating compared to a risk which is improving or stable). Timely risk monitoring is important in risk management.

Monitoring of risks can take place at different frequencies depending on the types of risks and external environment faced by an entity. For instance, availability of online system for customers should be monitored continuously. Another example is during time of financial crisis, the frequency of monitoring capital adequacy can be increased from monthly to weekly or even daily. Frequency of risk monitoring should be revisited where necessary to ensure risks are monitored on a timely basis.

Integration and use of Enterprise Risk Management (ERM) information

Communication and discussion of risks

Risk information is of little value if it is not communicated to relevant parties. Risk information can raise awareness amongst stakeholders and facilitate identification and communication of risks. By providing risk information and/or consolidated view of risks to various parties, it can facilitate parties such as management and corporate governance functions in identifying, comparing, analyzing, discussing, monitoring and communicating risks. For instances, it is possible for the corporate governance functions or business functions to identify risks for an entity if they are made known of risks experienced by an entity's competitor (e.g. via an external loss database). By describing risk levels of various risks, management would find it easier to compare risks. Furthermore, when details of risk incidents provided, one can analyze the root causes of risk incidents and devise risk mitigation actions accordingly. If risk inventory and integrated view of risk is given to various parties including management, relevant parties can discuss, monitor and communicate risks for risk reporting and risk management purposes, etc.

In discussing risks, various parties can examine the appropriateness of risk value, risk rating and risk ranking. There can also be discussion on the expected effectiveness of the risk management strategy (e.g. insurance and/or hedges) for each risk. For instance, during financial crisis, the probability that an entity can obtain effective hedges and/or insurance from a financial institution may be reduced as systemic risk is high during financial crisis. The reduced expected effectiveness of insurance and/or hedges can increase the value of risk and risk rating which may result in a risk management decision of risk avoidance instead of risk mitigation or risk transfer via insurance. In addition, it is important to discuss and have consensus on risk ranking as risk ranking can affect prioritization of mitigation of various types of risk. Also, for risks whose values are near the boundary of the risk avoidance/risk mitigation regions in the risk map or risk mitigation/risk acceptance regions, the risk need to be examined and discussed to ensure that the correct risk management strategy is chosen for the risk. By having various parties involved in discussing the risk values and order of risks, a better and more informed decision can be made on the appropriate risk management strategy for each risk and prioritization of mitigation of various risks.

Risks can also be communicated to regional or corporate management such that the overseas offices are made aware of the risks for detection, prevention, correction and monitoring purposes. It is possible that risks exist in a local office can apply to overseas offices as they can have similar systems, process, and policies and procedures. Hence sharing of risk information can assist in timely and effective risk management measures. Besides communicating risks to management, there can be other forms of communication of risks. For instance, for risks faced by the entity or the industry, risk management team can produce newsletter or guides for distribution within the whole entity to promote awareness

and management of these risks. By communicating risks and making different parties aware of risks, there is an increased chance that the risks are properly managed and staff can make use of the risk information in their day-to-day work (e.g. watch out for certain risks or perform controls to mitigate risks). Risk communication and risk awareness are very important as staff would be encouraged and equipped to implement risk management in their day-to-day work.

Conclusion

Risk information is important for risk management purpose. By examining a wide source of risk information that is available internally and externally, an entity has a better chance to identify all the pertinent risks at any point in time. Although there are different types of risks which an entity can face, risks can always be decomposed into two components, namely probability and impact/severity. Risks can be measured and reported by probability and impact/severity separately or in combination and they can be measured by qualitative ratings and/or monetary terms. With consistent risk measurements amongst various types of risks, risks can be easily reported and integrated in risk maps or in monetary terms to facilitate comparison, ranking, analysis, monitoring and communication of risks.

Throughout the risk management process, it is very important that there are full communication and discussion amongst various parties to ensure that appropriate decisions are made on the identification, measurement, analysis and ranking of risks, the risk management strategy chosen for each identified risk, and the prioritization of risk mitigation (if any). Making appropriate decisions throughout the entire enterprise risk management process would result in an effective enterprise risk management.

Integration and use of Enterprise Risk Management (ERM) information

Appendix: Summary of potential sources of risk information, risk measurements and risk reporting for different categories of risks

The table below is a summary of sources of risk information and examples of risk measurements and risk reporting for various categories of risk:

	Potential sources of risk information	**Risk measurements examples**	**Examples of risk reporting**
Inherent risks	- external information sources (e.g. rating agency on country/corruption risk, communication with industrial and professional bodies and partners, external loss database) - views of corporate/regional/local management and business functions such as corporate governance functions	- High/Medium/Low	- inherent risk assessments (e.g. by auditors)
Residual risks	- control review results - risk incidents and internal loss databases	- High/Medium/Low - severity vs. probability/frequency - financial measures (e.g. Value at Risk, VARs)	- reports on risks and/or controls (e.g. risk map, Risk Control Self Assessments (RCSA) reports, Key Risk Indicator (KRI) reports)
Emerging risks	- external information sources (e.g. news/conference/forum, peer networking, communication with	- degree of uncertainty vs. time - severity vs. probability/frequency	- reports of emerging risks (e.g. risk map, degree of uncertainty vs. time, etc.)

Integration and use of Enterprise Risk Management (ERM) information

	Potential sources of risk information	**Risk measurements examples**	**Examples of risk reporting**
	industrial body, external loss database) - Key Risk Indicator (KRI) results - views and inputs of Board of Directors, corporate/regional/local management and business functions - business plan/strategy plan		

References

Allen, Linda; Boudoukh, Jacob and Saunders, Anthony, *Understanding Market, Credit and Operational Risk: The Value at Risk Approach,* 2004

Bank for International Settlements (BIS), "Basel Committee on Banking Supervision, Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches", June 2011

Ho, Amelia, "Emerging Risk Audits", *Internal Auditor*, The Institute of Internal Auditors, June 2012

Jorion, *Value-at-Risk: The New Benchmark for Managing Financial Risk, 3rd Edition,* 2006

The Institute of Internal Auditors, *Practice Advisory* 2010-2: *"Using the Risk Management Process in Internal Audit Planning",* 2013

Neil, Martin, "Using 'Risk Maps' to visually model and communicate risk", Agena Ltd. & Risk Assessment and Decision Analysis Research Group, Department of Computer Science, Queen Mary, University of London, United Kingdom