Integration and Use of Enterprise Risk Management (ERM) Information

By Amelia Ho

Presented at the:
2013 Enterprise Risk Management Symposium
April 22-24, 2013

Integration and Use of Enterprise Risk Management (ERM) Information

Amelia Ho[*]

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 purposes. 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 and tactics for each risk identified and prioritization of risk mitigation.

[*] 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 has been a speaker or presenter on ERM and business continuity risks for professional accounting and risk management organizations. She has also reviewed and contributed to risk management publications. Her e-mail address is Amelia.Ho@alumni.insead.edu.

1. Introduction

Many types of risks are found within the Enterprise Risk Management (ERM) framework, and different methods are available to identify and measure risks. It is important that pertinent risks are properly and timely identified, measured, reported, integrated, analyzed, monitored, communicated, and managed by an entity to facilitate management in making the appropriate risk management decisions.

2. Definition of Risks

Risks are defined in different ways. For instance, the ISO31000:2009 Risk Management Standard defines risk as the "effect of uncertainty on objectives." In this definition, uncertainties include events (which may or may 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 that can cause a certain *impact* on objectives. From this definition of risk, it can be seen that two common elements of risks are probability and impacts.

2.1. Types of Risks

Within the broad definition of risks, different types and categories of risks can be identified. For instance, one finds strategic risks, market risks, credit risks, and operational risks. Operational risks cover risks in Human Resources (HR), finance, Information Technology (IT), transaction processing, legal and compliance, fraud, etc. Also, we see various categories of risks such as inherent risks, residual risks, and emerging risks.

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 because it is susceptible to theft. Inherent risk is useful information for people involved in audit or risk management 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. IIA (2013) defines residual risk is defined as the risk remaining after management takes action to reduce the impact and/or probability of an adverse event, including control activities in responding to a risk. Residual risk is determined after taking into account 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 controls for its physical access together with continuous monitoring of access to the safe via closed circuit TVs (CCTVs) and any other tool for physical access controls. 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. Ho (2012) describes emerging risks can arise due to certain types of events and/or changes, such as changes in regulations, technology, operations, life styles, and external environment. For instance, events such as the 2008 global financial crisis that had a widespread effect of spreading systemic risks in the financial industry can make credit risk an emerging risk for any financial institution. The inherent risk for credit risk is high during such periods. It is possible for emerging risks to have low inherent risks because the risks can still be in their infancy stage. Examples of such emerging risks include cloud computing and wireless security for entities that do not have important IT systems built on cloud computing or wireless communication.

3. Risk Information

For the various categories of risks, various sources of information can help identify the risks.

3.1. 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 occurring 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 personnel, compliance officials, regulators, and service providers
- Input provided by the Board of Directors, 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 that can give rise to emerging and/or strategic risks (e.g., regulatory, industry, accounting, technology, operational, or strategy changes)

3.2. External Sources of Risk Information

- Requirements or requests from regulators

- External loss database (with loss events from entities in the industry)
- News on other companies' fraud incidents, 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, and professional and industrial associations
  - Peer networking

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

4. Identification of Risks and Risk Inventory

Based on the various sources of risk information, risks can be identified for an entity. For instance, control reviews conducted by the corporate governance functions can identify risks. IT personnel can participate in IT security conferences and forums and identify certain IT risks and/or emerging risks. People can identify risks for their entities in different ways.

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 ERM or 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, for example, based on the results of periodic Risk Control Self-Assessment (RCSA), Key Risk Indicator (KRI) monitoring, etc., or on an ad hoc basis, for example, based on risk incidents or identified emerging risks.

5. Measurements of Risks

As stated in the definition of risk, the two key components of risks are probability or frequency and impact. One way to measure risks is to measure risks by its constituents, namely, probability and impact. Probability or frequency 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, or entity. For example, certain countries are more prone to natural disasters (e.g., earthquakes) than other countries, a retail bank has a higher chance of data privacy issues compared to an industrial company, etc.

Impacts, on the other hand, can be assessed in terms of materiality and strategic, reputational, financial, or regulatory impacts. A business unit is material to a business group if it constitutes a large portion of the business group in terms of sales and profits and/or it has a strategic impact for the entity (e.g., a certain product, service, or market has strategic value for an entity). Reputational impact can be significant if an entity makes a significant mistake and the incident is 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 a certain regulatory requirement is not met by the entity. Probability or frequency assessments and impact assessments are one way to measure inherent risks and residual risks, with the latter taking into account the controls while the former does not.

Risk measurements of probability and impacts can be reported separately or in combination. Probability or frequency, impact, and risks can all be measured by assigning a ranking such as very high, high, moderate, low, very low, etc. For example, interest rate risk can be assessed as high for probability and very high for impact. The overall interest rate risk can be assessed as high. Also we often find agencies that assign risk rating based on their defined criteria. For instance, a 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.

Emerging risks 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 high value for uncertainty. For instance, when social media is at its early stage and not many people have adopted its usage, the value in time is low and uncertainty is high because entities are unsure of 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 because the impact of possible risk becomes more apparent 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 significant credit risk. Hence, in that case 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 measured in monetary terms based on the combined effect of probability and impact (measured in dollar terms). Financial measurements of risks are common practices because they provide useful information to facilitate decision making. For instance, Value at Risk (VAR) is a measure of risks that can be used for measuring market risks, credit risks, and operational risks. VAR is a statistical measure of total portfolio risk and one way to describe it by Allen (2004) is it is taken as the worst or maximum loss at a specified confidence level over a target time horizon, such that there is low and prespecified

probability that the actual loss will be larger. Similar to previous descriptions of risk measurement, VAR is a measure describing the impact (i.e., dollar amount of loss) with a specified probability. Measurements of risks in monetary terms provide information to various stakeholders on the potential amount of dollar that is at risk, and the information can be useful for decision-making purposes.

For a summary of risk measurements for emerging risks, inherent risks, and residual risks, 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, regulatory requirements may specify certain types of risk measurements. For instances, the Basel regulation requires 99 percent probability and VARs to be used for measuring market risks for banks. Comparability may be increased when the same risk measurement is used, but the impact can be large 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 or inaccurate risk measurements.

6. 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, moderate, or low, red, yellow, or green, etc.)
- Risk measurements (e.g., probability, impact, dollar amount)
- Trend of risks (e.g., stable, deteriorating, or 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, or 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, definitions should be documented 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, or deteriorating, or mitigation status can be stated as green, yellow, red, etc. Also, predefined scales should be used in measuring impact or probability and predefined thresholds for key risk indicators. Table 1 shows a sample of description of the "capital adequacy and volatility" risk for a financial institution for illustration purposes; it is not necessarily a comprehensive description of the risk.

Table 1

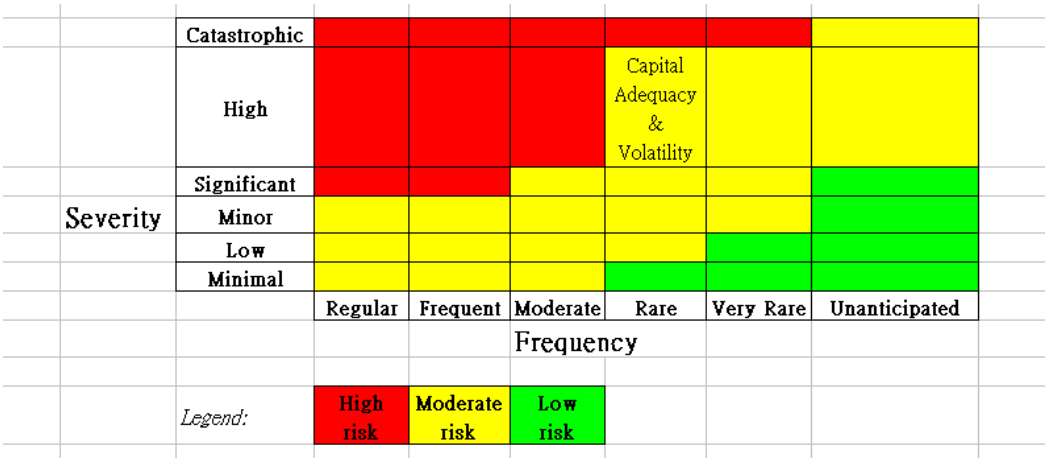
Capital Adequacy and Volatility Risk

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, moderate, or low)	Moderate
Risk measurement(s)	*Probability:* Rare *Impact:* Catastrophic
Trend of risk (stable, improving, or deteriorating)	Improving
Key Risk Indicator(s) (KRIs)	• Solvency measurements (e.g., solvency ratio) • Local capital sensitivity measures using predefined stress testing factors and scenarios • Liquidity ratio monitoring

<table>
<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 x% and (x+y)%, 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>Finance</td><td>Green</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
</table>
</td></tr>
</table>

Based on the measures of the probability or frequency and impact, Neil highlighted that risks also can be plotted in a risk map. Figure 1 illustrates how the risk of “capital adequacy and volatility” is reported via a risk map.

Figure 1: Sample of Risk Map for Risk-Reporting Purposes

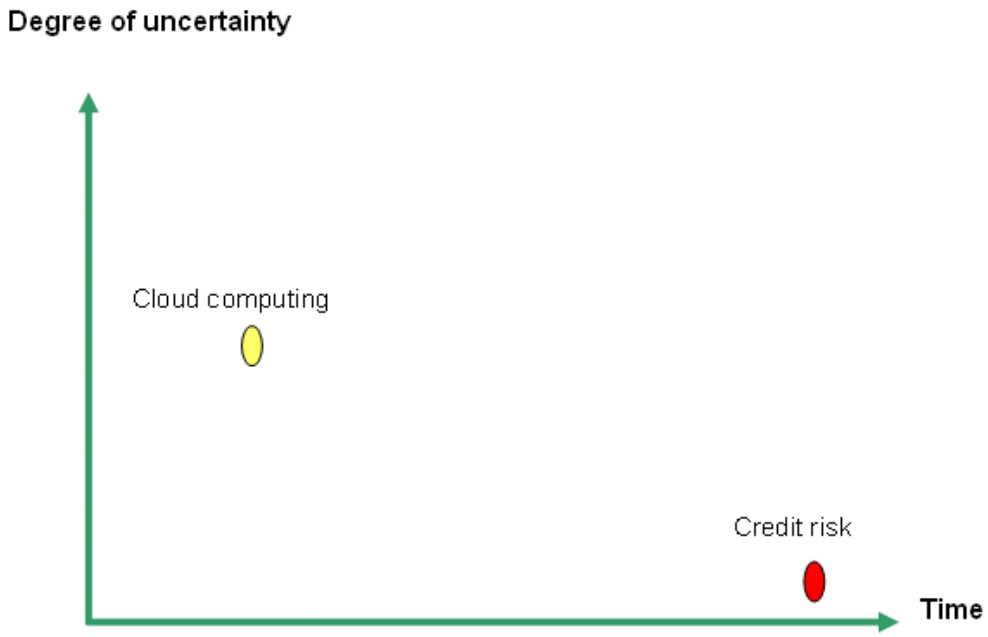


Risk reporting can be reporting on the residual risks, which take into account risk mitigation once they are implemented. Risk mitigation strategy can potentially reduce the probability and/or impact of a risk. For examples, if risks are hedged or insured, the risks in monetary terms can be reduced by the amount that 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 a 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 because the level of risks can change at different points in time (e.g., during a global financial crisis) because effectiveness of risk mitigation can change over time.

As mentioned in the previous section, emerging risks can be measured by the degree of uncertainty versus time and be reported as such. Figure 2 illustrates a report for emerging risks.

Figure 2: Illustration of a 2008 Report for Emerging Risks of a Financial Institution



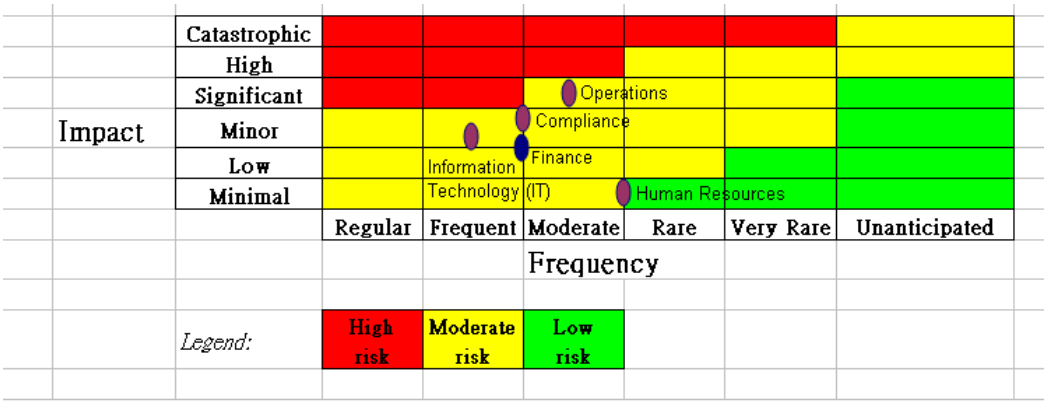
For a summary of risk reporting for emerging risks, inherent risks, and residual risks, refer to the Appendix.

7. 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 that are measured in the same way can be integrated. For examples, risks measured in monetary terms (e.g., VARs) can be

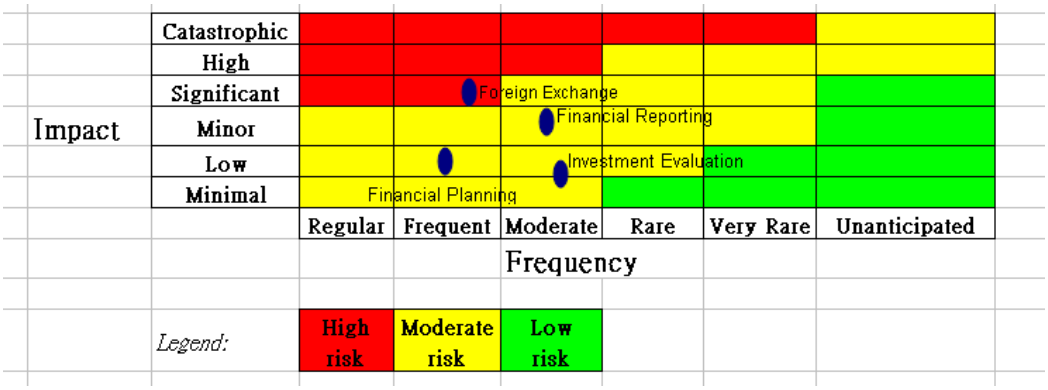
added. For risks that are measured as high, moderate, low, etc., they can be integrated and displayed in a diagram. A risk map can be used for integrating and reporting operational risks and emerging risks. Figure 3 demonstrates how a risk map is used for integrating different types of risks, such as finance risk, HR risk, etc.

Figure 3: Demonstration of How to Integrate Different Types of Risks in a Risk Map



One can also drill down within one type of risk (e.g., finance risk) where risks of that type can also be integrated and displayed in the risk map; see Figure 4 for an example.

Figure 4: Illustration of How to Integrate Various Finance Risks in a Risk Map



By integrating risks, stakeholders can have a view of risks faced by the entity, and this can facilitate risk analysis.

8. Analysis of Risks

After risks are measured, reported, and/or integrated, risks can be analyzed to identify the most appropriate risk management strategy (i.e., risk avoidance, acceptance, transfer, or mitigation) for each risk based on the risk appetite (e.g., risk limits). For different types of risks, the risk management decision rules or 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 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 the financial losses exceed a certain dollar limit, and avoid transactions related to financial products and/or counterparties whose credit ratings are below certain grades. For operational risks, the risk management decisions can be based on the risk rating (e.g., avoiding risk when the risk level is at a high-risk level, accepting risk if the risk level is very low, etc.).

Risk maps can facilitate risk analysis. For instance, one can easily see which region a risk is located in on a risk map, and the appropriate risk management strategy can be decided upon based on the region in which a risk lies on the risk map. Figures 5 and 6 are suggestions of applicable risk management strategies for different regions on the risk map. Figure 5 illustrates how an entity's risk management strategy is determined based on risk levels. For instance, a high risk would result in the risk management strategy of risk avoidance. Figure 6 displays a nonlinear curve for determining the regions of unacceptable risks, tolerable risks, and normal risks, which in turn can be used to determine the risk management strategies. For example, in the region of "unacceptable risks," the risk management strategy is risk avoidance.

Figure 5: Risk Map Highlighting Various Risk Management Strategies Determined Based on Risk Levels

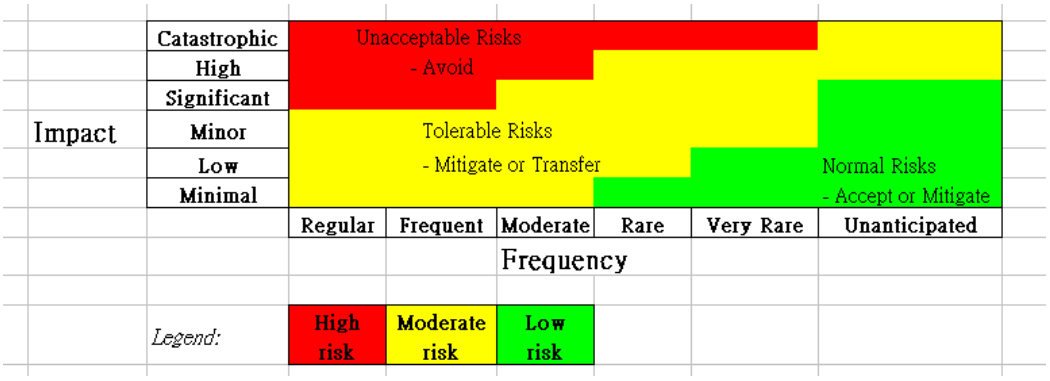
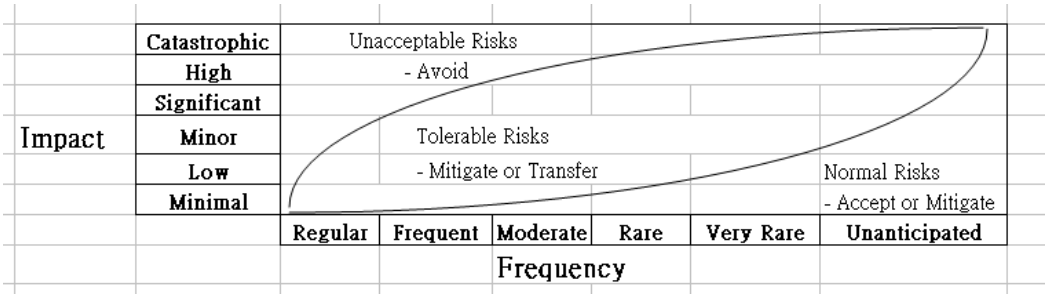
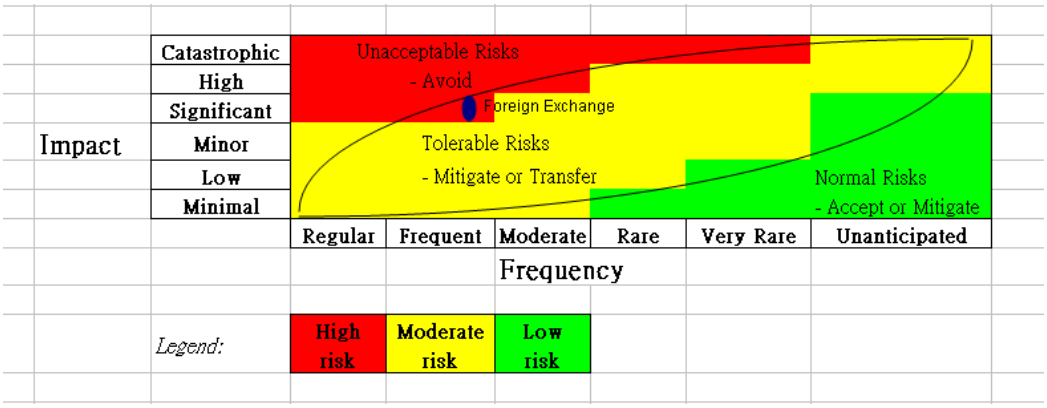


Figure 6: Risk Map Showing Nonlinear Curve for Determining Regions of Unacceptable Risks, Tolerable Risks, and Normal Risks and Their Corresponding Risk Management Strategies



Depending on the risk appetite of the company, it is possible that a risk can be an unacceptable risk for one entity but it can be a tolerable risk for another entity, as illustrated in Figure 7. Figure 7 combines the information shown in risk maps in both Figures 5 and 6. In Figure 7 one can see that the risk of "foreign exchange" is to be avoided if an entity's risk management strategy is determined based on the risk level (i.e., avoiding risk if risk level is high). However, the same "foreign exchange" risk can be tolerated if an entity has a risk map shown in Figure 6 where the "foreign exchange" risk is within the range of tolerable risks.

Figure 7: Risk Map Showing Risk Levels and Regions of Unacceptable Risks, Tolerable Risks, and Normal Risks



For risks that are at the boundary of tolerable risks and unacceptable risks, 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.

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 was approaching the peak point in the 2008 global financial crisis, the financial institution might have had a lesser chance of reducing its credit risk by obtaining an 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 during the early stage of a financial crisis compared to the later stage of the crisis) at a relatively lower cost (e.g., lower transaction cost) compared to the point when the emerging risk peaks. Actuarial Standards Board (ASB) (2012) commented that one tool that can be used to analyze emerging risk is to conduct stress and scenario testing, which considers an extreme event scenario with extreme results. Different tools are available for analyzing risks, and the usefulness of the tool depends on the type of risks, the quality of the tool, and the experience of the person using the tool.

9. 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 thresholds 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 an Automatic Teller Machine (ATM) 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. If the financial exposure to a single customer or industry or country exceeds the risk limit set by the entity, an entity may need to reduce transactions (e.g., trading or investment) from that customer or industry or country to ensure its exposure is reduced to an acceptable level. Financial VAR can also be monitored.

Trends of risks can be monitored to ascertain whether the risk stays stable, improves, or deteriorates. Management can take appropriate actions based on the risk trend; for example, more timely actions may be required if a risk is deteriorating compared to a risk that is improving or stable. Timely and regular 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 an online securities trading system should be monitored during the trading hours of the markets it serves. Another example is during times 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.

10. Communication and Discussion of Risks

Risk information is of little value if it is not communicated to relevant parties. Risk information can raise awareness among 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, discussing, analyzing, monitoring, communicating, and managing risks.

For instance, 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 are 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, analyze, monitor, and communicate risks for risk reporting and risk management purposes, etc.

In discussing risks, different types of risks can be discussed, and various parties can examine the appropriateness of risk value, risk rating, and risk ranking. For example, discussions can be held on emerging risks and determination of whether any action is required besides monitoring the emerging risks. Discussions can also address the expected effectiveness of the risk management strategy (e.g., insurance and/or hedges) for each risk. For instance, during a financial crisis, the probability that an entity can obtain effective hedges and/or insurance from a financial institution may be reduced because systemic risk is high during a 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 risk ranking because 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 or risk mitigation regions or risk mitigation or risk acceptance regions (e.g., on the risk map), the risk needs 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 ranking 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 in a local office can also exist in overseas offices because they may have similar systems, process, and policies and procedures. Hence sharing of risk information can assist in timely and effective implementation of 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, a risk management team can produce newsletter or guides for distribution within the entity to promote awareness and management of these risks. By communicating risks and making different parties aware of risks, the chance improves 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 the risks). Risk communication and risk awareness are very important because staff would be encouraged and equipped to implement risk management in their day-to-day work.

11. Conclusion

Information on risk is important for risk management purposes. By examining a wide range of sources of risk information available internally and externally, an entity has a better chance to identify all the pertinent risks at any point in time. Although different types of risks may be faced, risks can always be decomposed into two components: probability and impact. Risks can be measured and reported by probability and impact separately or in combination, and they can be measured by qualitative ratings and/or monetary terms. Appropriate and accurate risk measurements can enable management to make correct risk management decisions (e.g., reject or avoid risks that exceed the entity's risk appetite, accept risks that are low, and mitigate or transfer risks that are tolerable). With consistent risk measurements among 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 the various parties maintain full communication and discussions 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). An entity making appropriate decisions throughout the entire ERM process would create effective ERM.

Appendix: Summary of Potential Sources of Risk Information, Risk Measurements, and Risk Reporting for Different Categories of Risks

The table gives 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 Measurement Examples	Examples of Risk Reporting
Inherent risks	External information sources (e.g., rating agency on country or corruption risk, communication with industrial and professional bodies and partners, external loss database) Views of corporate, regional, or local management and business functions such as corporate governance functions	High, moderate, or low Impact vs. probability	Inherent risk assessments
Residual risks	Control review results Risk incidents and internal loss databases	High, moderate, or low Impact vs. probability Financial measures (e.g., VARs)	Reports on risks and/or controls (e.g., risk map, RCSA reports, KRI reports)
Emerging risks	External information sources (e.g., news, conferences, forums, peer networking, external loss database, communication with industrial bodies) KRI results Views and inputs of	Degree of uncertainty vs. time Impact vs. probability	Reports of emerging risks (e.g., risk map, degree of uncertainty vs. time, etc.)

	Potential Sources of Risk Information	Risk Measurement Examples	Examples of Risk Reporting
	Board of Directors, corporate, regional, and local management and business functions Business plan and strategy plan		

References

Actuarial Standards Board. 2012. Actuarial Standard of Practice (ASOP) No. 46, Risk Evaluation in Enterprise Risk Management. September.

Allen, L., J. Boudoukh, and A. Saunders. *Understanding Market, Credit and Operational Risk: The Value at Risk Approach.* Oxford: Blackwell, 2004.

Ho, A. 2012. Emerging Risk Audits. *Internal Auditor*. June.

Institute of Internal Auditors (IIA). 2013. Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning.

Neil, M. 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.