PROCESS - IDENTIFICATION, ASSESSMENT, CONTROL AND MITIGATION

The organisation has a process by which it can identify, assess and mitigate the significant risks to the achievement of its business objectives.

- **Process to identify all significant risks**

  Lloyd's expects its businesses to be 'in control' of significant risks. This means:

  - Understanding the risk profile and identifying and assessing the significant risks contained within it. Where it has been concluded risks are 'under control' (ie managed to within appetite), having controls that are documented, appropriate, and work consistently and effectively.
  - Where risks have been assessed as not being under control, the factors contributing to this are known and plans to manage them are in place.

  Risk identification is a key component of a robust framework. In the absence of a risk identification process, the organisation is unable to effectively manage its key risks and demonstrate whether they are 'in control'.

  An effective risk identification process would typically:

  - Identify the significant risks to the achievement of its business objectives.
  - Identify all types of risks, associated major components and controls currently in place, from all sources, across the entire scope of the organisation's activities.
  - Identify risks around opportunities as well as threats, to increase the organisation's chance of maximising the benefit of those opportunities when they arise.
  - Ensure that the organisation is aware of its major risks at any point in time, and include elements to update the organisation's understanding of risk on an ongoing basis, such as key indicators.
  - Be systematic, disciplined and documented, ie methodical and well-organised and in a format that is capable of being communicated and understood by all.

  It may also be worth considering;

  - Focussing on the root causes and influencing factors of risk, both internal and external, as well as its effects and outcomes: financial, reputational or other.
  - Looking forward, as well as drawing on past experience, by including elements such as horizon scanning.

  The organisation should consider carefully the risk categorisation that it adopts. Risk categories aid effective, systematic and comprehensive risk identification:

  - When categorising risk, an organisation should understand how its categories map to those of the FSA.
  - Each of these categories then forms the basis for a more detailed identification process to ascertain individual risks and their components.

  Organisations may wish to employ a combination of 'bottom up' (typically starting with data analysis, building up into an aggregate view) and 'top down' (eg starting with the consideration of influencing factors or risk groups) tools according to the size and complexity of the business.

  See also

Risk management toolkit - Section 6 - Self assessment

Risk management toolkit - Section 2 - Risk language

- ## Risk assessed using appropriate techniques

Risk assessment provides greater understanding of risk, and is vital to the process of making risk-based decisions, by enabling:

- Comparison of risks against each other, thereby helping to prioritise risk events.
- Comparison against appetite, prompting remedial action and providing assurance towards the 'in control' status of the organisation.
- Cost v benefit analysis of risk taking activities and alternative control options.
- Valuable input into the ICA process.

An effective assessment of risk would typically:

- Assess the impact and probability of risks, using metrics or scales that are suitable and appropriate to the business, commonly understood across the organisation, and in line with its risk policy.
- Be reviewed regularly to ensure it stays relevant and appropriate to the nature and level of risk within the organisation. The frequency of review should reflect the risk profile of the organisation, and might typically be quarterly or six-monthly.
- Use an appropriate assessment method which might be qualitative or quantitative, or a combination of both. The appropriate method will depend on a number of factors, including the nature of the risk and the organisation's risk policy. Whatever methods are chosen, the organisation should be able to demonstrate the effectiveness and appropriateness of its assessment criteria and techniques.
- Identify potential aggregations of risk and risks that interact or correlate either positively or negatively across the organisation.

Qualitative methods are often used to perform initial screenings of risks due to low cost and time requirements. They are also used when there is insufficient data to perform more scientific assessments. Factors to consider when employing qualitative assessment techniques include:

- The need to use the right people, with the appropriate competence and experience.
- If self assessment methods are being used, there should be procedures to provide challenge and oversight to ensure judgment is being consistently applied across the organisation. This is important as there can be a significant diversity in judgmental perceptions of risk from person to person.
- Key indicators and loss analysis may be of benefit to corroborate or challenge judgmental assessments.

Quantitative tools rely on the availability of a sufficient amount of reliable historical data. Factors to consider when employing quantitative assessment techniques include:

- Where there is insufficient internal data, the use of an external loss database may provide some benefit. Careful consideration should however be given as to whether that external data is appropriate to the risk profile of the organisation itself, and relevant to the particular risks being assessed. Furthermore, an organisation has relatively little control over the completeness and accuracy of information compiled in an external database.
- The use of internal data should also be treated with an element of caution since historical performance is not necessarily an indication of future events. Consideration should therefore be given to potential changes to the risk environment, risk causes, impacts and probabilities over time.
- The organisation should also be able to demonstrate that parameters and assumptions used in modelling techniques are suitable and robust, and that time horizons are appropriate, and consistent with related strategy and objectives.

The organisation assesses both inherent risk (before controls) and residual risk (after controls). Assessment of inherent risk provides a number of benefits:

- It assists the understanding of exposure level in the event of a significant control failure.
- It helps identify key controls and their effectiveness.
- It provides better understanding of the nature of interaction between risks and their associated controls.
- It provides assistance in the development of effective key indicators as well as controls.

A sensible assessment of inherent risk would be one that is appropriate to the organisation's risk profile as well as the type and complexities of the appropriate risks. Such an assessment would typically be:

- Practical and commensurate.
- Relative to other risks.
- More qualitative / subjective; it may not be necessary or appropriate to associate a monetary value to the risk.

See also

Risk management toolkit - Section 6 - Self assessment

Risk management toolkit - Section 8 - Internal loss events

Risk management toolkit - Section 9 - External loss data

- ## System of internal control

Effective risk management aims to manage risk to within acceptable levels, finding a suitable balance between the positives (opportunity and reward) and negatives (threats and losses), in line with the agreed risk appetite.

Risks that exceed capacity form an immediate threat to the viability of the organisation and should be identified and dealt with immediately.

Risks that exceed appetite form a threat to the successful achievement of the organisations objectives and consideration should be given to the required response.

Control activities operate at all levels within the organisation to
mitigate risks to risk appetite. Controls may include policies, procedures, systems and processes in place throughout the organisation. Effective controls are typically:

- Appropriate and commensurate with the key risks faced at all levels across the organisation in order to provide cost effective mitigation of those risks to risk appetite.
- A normal part of day to day activity, systems and procedures, management and decision making processes throughout the organisation.
- Co-ordinated across the organisation.
- Subject to regular evaluation (ie are the controls effective at mitigating the key risks, did they work throughout the period under review, and if not, identify corrective action).
- Subject to an overall assurance process, which also addresses the
wider control environment.

The control environment encompasses the wider governance approach, management style, organisational

structure and culture within which control activities take place.

Controls are often categorised into two broad types although a combination will usually be needed:

- Prevent – controls reduce the likelihood of a risk event occurring in the first place. They include planning and strategy setting, authorisation limits and data input controls.
- Detect – controls identify occurrences of risk events after they have occurred and enable remedial action to be taken to limit the extent of damage. Examples include exception alerts and reports, and reviews of actual results against expectation.

Assessment of controls is typically done by assessing the effectiveness with which they mitigate risk. One method is to consider the design of a control and its performance:

- Design – considers how well the control should work if it is always applied in the way it is intended to work.
- Performance - considers the way in which the control is operated in practice; if it is applied when it should be and in the way intended by its designer.

See also

Risk management toolkit - Section 6 - Self assessment

- ## Identification and assessment

The organisation can respond to risk in a number of ways, including:

- Transfer part of the risk elsewhere; for example by buying insurance or reinsurance.
- Treat or mitigate the risk; ie reduce the likelihood and / or impact of it.
- Accept or tolerate the current level of risk, where risk is already at a level that is within appetite. It may also sometimes be appropriate to accept the current level of risk where the cost of mitigating it is disproportionate to the benefits to be gained by doing so.
- Eliminate or terminate; for example by exiting a class of business altogether.

When determining the appropriateness of risk responses the following should be considered:

- The feasibility and relative costs (direct, indirect and opportunity) and benefits of alternative risk response options, the cost to design and implement a new control, and the ongoing cost of operating the control.
- How to ensure responses are based on a comprehensive understanding of risk and its components, particularly the causes of risk to ensure that they are addressed.
- How risk events and their controls interact with one another. In determining the most appropriate response a portfolio view of risk and control can enable management to determine whether the organisation's overall level of risk is commensurate with its risk appetite.
- Whether risks that cannot be controlled to within acceptable levels should be avoided, or contingency plans developed.

Action plans are typically developed and implemented to address unacceptable levels of risk and / or remediation of control weaknesses.

The organisation should consider how the assurance processes can ensure the effective operation of controls and the implementation of action plans.

See also

Risk management toolkit - Section 6 - Self assessment

- ## Risk register

A risk register brings together the output of its risk identification process and that reflects the size and complexity of the business and its risk policy. An effective risk register typically:

- Gathers together risk information to enable effective sharing and communication of that information.
- Focuses attention on the key risks and therefore drives action.
- Is linked to the capital requirements of the organisation.
- Assists in developing a portfolio view of risk.
- Forms the core of an organisation's risk knowledge database and is the basis for risk analysis and reporting.
- Facilitates monitoring and review.
- Evidences a systematic and comprehensive approach to risk identification.
- Is subject to regular review and update.

With respect to significant risks, a risk register typically captures:

- A description of the risk.
- The assessment of risk and control.
- Causes and influencing factors, both internal and external.
- Effects and outcomes, financial, reputational and other.
- Controls and actions currently in place to manage elements of the risk.