LLOYD'S

RISK MANAGEMENT TOOLKIT

CONTENTS

- **Section 1 – Introduction** **3**
- **Section 2 – Risk definition and language** **7**
- **Section 3 – Risk appetite** **33**
- **Section 4 – Risk governance, roles and responsibilities** **51**
- **Section 5 – Risk policy** **65**
- **Section 6 – Risk and control self assessment** **93**
- **Section 7 – Key risk indicators** **113**
- **Section 8 – Internal loss events** **129**
- **Section 9 – External loss data** **143**
- **Section 10 – Management information** **147**
- **Section 11 – Stress and scenario testing** **153**
- **Section 12 – Risk culture** **169**

LLOYD'S

INTRODUCTION

SECTION 1

1 INTRODUCTION

The risk management toolkit

Lloyd's has developed a risk management toolkit to help to **develop risk management practice across the Lloyd's market.** The toolkit provides a range of **tools, techniques** and **templates, worked examples**, and **practical advice** for key aspects of risk management. The toolkit supports the Lloyd's risk management **standards and guidance documents.**

Toolkit background and development

Lloyd's has worked closely with members of the market in developing the toolkit. In particular, Lloyd's would like to thank those members of the **toolkit working party** and the members of the **LMA Risk Management Committee** for their valuable contributions. The participation of both groups in helping to scope and shape the toolkit, in directing the development and by providing valuable feedback at every stage has been hugely helpful. As well as the individuals, we would like to thank their organisations for allowing them to participate. We would also like to thank **Deloitte** for their help and assistance in putting the material together, and all those that have been involved within the Franchisor.

Aims of the toolkit

Risk management practice varies considerably across the Franchise, and so will the use of the toolkit. For example, the tools could be used in the following ways:

- the tools can provide a **useful sense check to review current activity.** By comparing current practice against relevant tools, a **gap analysis** can be undertaken, providing comfort that existing practices are appropriate or highlighting areas for further consideration;
- where **further development is being considered,** the toolkit can help **inform and direct their development,** and provide tools which can be tailored to the organisation's needs; or
- where risk management practice is not in place, the toolkit can act as **a source of key building blocks** to **enable an organisation to identify, assess and manage risk,** and be a useful training tool.

Who are the tools aimed at?

The tools have been designed to complement organisations' existing risk management frameworks. Some of the tools are more applicable to small or less complex organisations and others, more relevant to large or more complex entities therefore the uses of the tools will differ between organisations.

We anticipate that the tools will be of **particular interest** to those responsible for the **management of risk on a day to day basis,** namely **Chief Risk Officers, risk managers, compliance officers, departmental managers** and **risk** and **control owners.**

The tools and their use

The tools cover key aspects of risk management and are designed to aid organisations with the ongoing review and development of risk management functions and processes. Sections 2, 3, 4, 5, and 12 can be considered "structural tools", covering key elements of a framework and context for managed risk taking, whereas section 6, 7, 8, 9, 10 and 11 are more "practical tools", designed to support the activities needed to identify, assess, control and manage risk.

Structure

With exception of section 9 and 12, each component section of the tools is split between four pages covering the following:

- **what is it? –** explains / defines the aspect of risk management that is discussed in this section;
- **why is it important? –** discusses why this is a key aspect of robust risk management;
- **some practical steps necessary for implementation –** highlights some key steps necessary for an organisation to take in order to implement and address this aspect of risk management; and
- **relevant toolkit contents –** presents the tools and gives a brief explanation of what each tools does / should be used for.

Tool downloads

Lloyd's is keen for managing agents and syndicates to use the toolkit to help review and, if necessary, improve their risk management functions, however **Lloyd's accepts no liability for incorrect use or subsequent risk management failure** from use of tools. Risk management is commensurate to the organisation in question and it is important to remember that even if all tools from the toolkit are used, this does **not necessarily** mean that an organisation will have **a perfect risk management function.**

The last page in each section, the **"Relevant toolkit contents"** page contains links to all associated tools. The tools are either in Word or Excel format and a range of tools can be tailored for use by organisations. There are also complete section documents available in Word format for editing and PDF format for printing. These complete section documents can also be found in section homepages along with, where applicable, zip files containing all the section Excel tools. A full PDF version of the toolkit can be found on the toolkit contents page, **"Risk management toolkit".**

Queries and updates – key contacts

If users of the toolkit have any queries or updates they should contact the following:

Queries, help – Please contact your appropriate risk executive with any queries.

Suggestions, amendments, updates – If you have any comments on the toolkit please contact either Olly Reeves, Lloyd's Risk Management at olly.reeves@lloyds.com or +44 (0)20 7327 6229 or Lyndsay Letty, Lloyd's Risk Management at lyndsay.letty@lloyds.com or +44 (0)20 7327 5993

Section introductions

The following a brief introductions to the various sections of the toolkit:

- **Section 2 – Risk definition & language:** Having a set risk definition and language in an organisation is an important step in providing a consistent framework for the organisation of risk management activity;
- **Section 3 – Risk appetite:** Articulating the amount of risk taking that is acceptable to the organisation and helping staff to understand the relative significance of the risks faced by the organisation allows for more efficient and effective risk management;
- **Section 4 – Risk governance, roles & responsibilities:** Effective risk management requires the appropriate definition and assignment of roles, responsibilities, accountabilities and authorities to support managed risk taking. Risk governance is an integral aspect of corporate governance.
- **Section 5 – Risk policy:** A risk policy sets out the approach to be adopted for the management of risk for a given risk group, which will typically include risk strategy and objectives, articulation of risk definition and language, appetite and the governance structure;
- **Section 6 – Risk & control self assessment:** A critical part of the risk management process is the regular identification and assessment of the key risks to the business objectives and the key controls which are in place to mitigate those risks. The results are recorded in a risk register, which acts as a central repository of the nature and status of the key business risks and controls;
- **Section 7 – Key risk indicators:** Using indicators to highlight the level of and potential change in the risk profile of an organisation can help to enable timely action to be taken in respect of risk;
- **Section 8 – Internal loss event data:** The tracking of actual loss, potential loss and “near-miss” events can contribute to the assessment and monitoring of risk, enable timely action on issues arising and be a key component of robust risk management;
- **Section 9 – External loss data:** Drawing on the loss experience of other organisations can give an indication of the size, frequency and sources of losses which could be experienced by organisations, providing a wider frame of reference when assessing potential risk exposures;
- **Section 10 – Management information:** Every organisation identifies and captures a wide range of information relating to events and activities, both internal and external, which is relevant to managing the organisation. Providing the right information to the right people at the right time enables better, more informed risk taking, as well as more effective monitoring of key risks within the business;
- **Section 11 – Stress & scenario tests:** Stress tests & scenario analyses help give a better understanding of the significant risks that an organisation potentially faces under extreme conditions and provide input into the determination of capital requirements. Stress tests and scenario analyses are therefore integral elements of an organisation’s risk management framework;
- **Section 12 – Risk culture:** Effective risk management requires a risk aware culture, where staff are encouraged and supported, throughout the organisation, to fulfil their risk management responsibilities in an open and honest manner.

LLOYD'S

RISK DEFINITION & LANGUAGE

SECTION 2

TOOLS

Tool 2.1 – Operational risk definition & categorisation

Tool 2.2 – Operational risk boundary examples

Tool 2.3 – Franchisor operational risk categorisation

Tool 2.4 – Basel II framework operational risk categorisation

Tool 2.5 – Common risk language & glossary

2 RISK DEFINITION & LANGUAGE

What is risk definition and language?

Risk definition – a detailed articulation of identified risks, designed to give a clearer understanding of the risks.

Risk category (or group) – risks identified can be **grouped** or **categorised** in order to facilitate monitoring and reporting. High level risk groups or categories (such as operational risk, credit risk etc.) are often broken down further into lower level **sub-groups** or **sub-categories** to facilitate monitoring and reporting, for example, the "risk of fraud" could be considered a sub-category or sub-group within "operational risk".

Risk language – details standard risk terms, vocabulary and abbreviations used across an organisation.

Why are they important?

Key roles

A common risk language provides a **consistent framework** for the definition and categorisation of risk and the organisation of risk management activities. It plays a key role in:

- helping to co-ordinate efforts on risk identification, assessment, and control;
- aiding **clarity and understanding** for all parties and enabling **consistency** of risk assessment;
- ensuring that **all risks are considered**;
- ensuring that information about significant risks, from different business areas, can be **aggregated**;
- assisting **management reporting** and **capital assessment**; and
- clarifying directors' and employees' **roles and responsibilities** in respect of defined risks. A common risk language is typically expressed through risk policies and terms of reference and assists strong governance practice.

Appropriate risk categorisation

In order for an organisation to manage its risks effectively, it is important that the significant risks inherent in the business strategy and objectives are **appropriately categorised**. For example:

- some organisations have adopted the FSA's six risk categories for their highest level risk categorisation (i.e. Insurance, Credit, Market, Liquidity, Group and Operational risk), considering that these are appropriate for the business; whilst
- other organisations, including the Franchisor, have adopted eight risk categories for their highest level risk categorisation (i.e. Strategic, Capital, Credit, Financial Market, Insurance, Liquidity, Operational and Regulatory risk), considering that these are appropriate for the business.

Practical steps for implementation

All organisations have some form of risk definition and language in place within their business. The attached tools help organisations review and enhance the status of those definitions, where appropriate, by:

- firstly, providing a health-check or benchmark against which to assess current risk definitions and language; and
- secondly, identifying options for development, drawing on the attached tools.

Notwithstanding the wide range in size and sophistication of organisations, it is anticipated that risk definition and language underpins **all risk management activity**, for **all organisations.**

Relevant toolkit contents

Relevant toolkit contents which may be of help include:

- **Tool 2.1** – **Operational risk definition and categorisation:** provides guidance on the Lloyd's, FSA and Basel II definitions of operational risk, and on how to determine the boundaries of operational risk by considering the primary causes of risk events;
- **Tool 2.2** – **Operational risk boundary examples:** helps explain operational risk boundary issues;
- **Tool 2.3** – **Franchisor operational risk categorisation:** a helpful point of reference;
- **Tool 2.4** – **Basel II framework operational risk categorisation:** a helpful point of reference;
- **Tool 2.5** – **Common risk language and glossary:** a helpful set of key definitions which could form the basis of a common risk language.

LLOYD'S

TOOL 2.1
OPERATIONAL RISK DEFINITION & CATEGORISATION

This tool provides a variety of **possible definitions** for operational risk and may help organisations **determine the boundaries** for operational risk. This is achieved by considering the root causes of operational risk.

Definition of operational risk

The most common definition of operational risk draws on the **Basel Committee**[1] definition:

> **"the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events"**

It is important to note that **differences exist** between what is and what is not included (or categorised) within this definition when used by different parties, for example:

Basel II – the Basel Committee defined operational risk for the banking sector. Its operational risk categorisation includes legal risk[2] but excludes strategic and reputational risk;

FSA – the FSA has adopted the Basel definition as above. Its operational risk categorisation, however, includes strategic and regulatory risks, but excludes capital risks, which are included within "group risk". The FSA has provided guidance on the factors to consider when assessing operational risk in PRU 2.3 and PRU 6.1 and guidance on systems and controls[3] for operational risk in SYSC 3A;

Franchisor – within the Lloyd's risk framework, strategic, capital and regulatory risks to the franchise objectives were considered to be of such significance that they merit their own distinct risk classes, rather than being categorised under operational risk.

The key issue for an organisation is that the categorisation adopted **matches** its key business risks.

Determining the boundaries of operational risk

The key issue when determining the categorisation of a risk event is its **primary cause**. A loss event will be considered an **operational risk event** if it arose as a result of inadequate or failed internal processes, people and systems or from external events.

---

[1] In its International Convergence of Capital Measurement and Capital Standards (ICCMCS) framework

[2] Per the Basel Committee, legal risk includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from FSA actions, as well as private settlements

[3] Senior Management Arrangements, Systems and Controls: Operational risk

Operational risk causes

Risk is expressed in terms of three components: **event, cause** and **effect**. This may be illustrated by a simple example, a worm virus:

Risk event – a virus enters your computer;
Cause – the **external** cause is a hacker, the **internal** cause is a lack of current virus protection software; and
Effect – computer software fails, data is lost, with potential financial and non-financial consequences.

Identifying the root cause(s) of a risk event helps to isolate the operational loss element from other losses and to understand **what action might be appropriate** to mitigate against exposure to the risk, for example, by amending a process, system, control or management approach. Some examples of operational risk causes include:

- lack of policies and procedures;
- inadequate segregation of duties;
- inadequate activity management;
- lack of management review;
- inadequate analyses;
- information processing errors;
- inadequate physical controls; and
- external events.

When an **internal issue** is at the root of a risk, **the focus should be on how to address the issue**. This generally involves modifying a business process or enhancing controls to reduce the potential likelihood and impact of a risk event. For example, if “miscommunication” of critical information caused exposure to a risk, consideration should be given to improving the frequency and quality of communications.

When an **external event** is at the root of exposure to risk, **focus should be on how leading indicators of the external event are monitored.** For example, while it may be difficult to prevent lightning from striking the Lloyd’s building, weather can be monitored for early warning signs of lightning and lightning conductors installed.

LLOYD'S

TOOL 2.2
OPERATIONAL RISK BOUNDARY EXAMPLES

Each organisation will need to determine **what risks it will include or "categorise" as operational risk**. This has the effect of determining the boundary between operational risk and other risk classes. The table below provides practical examples of what this might look like.

Risk group	Example of boundary issues
Insurance risk	In order to understand the operational risk arising from the controls and processes around insurance risk, agents should first consider the processes in relation to insurance risk. They should then identify the key controls specifically designed to mitigate insurance risk in each area. For example, an agent may address insurance risk with a number of key processes around areas such as underwriting, claims and reserving. The agent may place reliance on a number of key controls in these areas, for example: **Underwriting** • signed and regularly reviewed underwriting authorities for all underwriting personnel; • underwriting peer review / regular review of risks written; • war business policy and procedures; **Claims** • signed claims authorities and exception reporting; • procedures setting out the approach to claims management including service standards, complaints handling and the use of third party experts; • procedures for the regular review of dormant or non moving claims; and **Reserving** • periodic actuarial reserve estimation and reporting.

Risk group	Example of boundary issues
Credit risk	In order to understand the operational risk arising from credit risk, agents should first consider the key processes in relation to each counterparty. They should then identify the key controls specifically designed to mitigate credit risk in each area. For example, an agent may address third party credit risk with a number of processes around key areas such as reinsurance strategy, reinsurance purchase, reinsurance recoveries, coverholder / broker approval and outstanding third party balances. The agent may place reliance on a number of key controls in these areas, for example: **Credit controls** • an established credit risk committee, with clear terms of reference, which reviews and updates the credit ratings of reinsurers, brokers and coverholders on a regular basis; • controls to ensure that only approved reinsurers are used; • controls to ensure that only approved brokers are used; • policies regarding the maximum exposure to any one reinsurer, either actual or prospective; • controls to monitor exposures and to check that they are within the pre-agreed limits; • regular aged debt reporting; • controls and procedures in respect of dealing with reinsurer queries; • internal audit reviews of controls over third party credit risk; • a plan for managing cashflows / liquidity following a major catastrophe; and • ongoing management of the relationships with key counterparties.

Risk group	Example of boundary issues
Market risk	In order to understand the operational risk arising from market risk, agents should consider the processes in place in relation to the components of market risk and the key controls specifically designed to mitigate market risk. For example, an agent will address market risk with a number of processes around areas such as investment strategy, relationships with investment managers, and investment management reporting and monitoring. The agent will place reliance on a number of key controls in these areas, for example: **Investment controls** • formal investment management / custodian mandates and agreements, including details of reporting to be provided and performance benchmarks; • annual review of benchmarks and revision in light of changes to business strategy; • regular reporting on investment portfolio, including value of the portfolio by investment asset class, sales and purchases made in the period and cash movements; • monitoring of the portfolio against the limits established in the investment mandate; • regular reconciliation of investment holdings; • regular monitoring of the credit worthiness of counterparties and issues; and • periodic reviews of controls operated by counterparties.

Risk group	Example of boundary issues
Liquidity risk	In order to understand the operational risk arising from liquidity risk, agents should consider the processes in place in relation to liquidity risk (the potential gap between cash in flows and cash out flows) and the key controls specifically designed to mitigate liquidity risk. For example, an agent may address liquidity risk with a number of processes around key areas such as cashflow forecasting, credit control and cash calls. The agent may place reliance on a number of key controls in these areas, for example: **Finance controls** • regular formal cashflow forecasting, showing the cash position by month and currency and reflecting the likely effect of an RDS / catastrophe events; • monitoring actual levels of liquid assets against a benchmark; • the maintenance of sufficient (liquid) assets to meet expected / reasonable changes in regulators' financial requirements, or contingency plans to raise sufficient funds; • having formal agreements in place for borrowing facilities / funding arrangements; • credit control policies and procedures to target outstanding premiums and reinsurance recoveries for collection; and • personnel with sufficient skills and knowledge of the cash call process.

LLOYD'S

TOOL 2.3
FRANCHISOR OPERATIONAL RISK CATEGORISATION

Example operational risk categorisation

The Franchisor has adopted the following high level definition or categorisation of "operational risk":

> **"the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events".**

In order to facilitate monitoring and reporting, a number of risk sub-categories have been adopted by the Franchisor under "operational risk". These are summarised below in order to provide a helpful point of reference.

Operational risk sub-category	Description	Risk components
Failure by Franchisor to perform key processing functions to required service levels	Financial loss, inefficiency, brand damage / reputational loss due to failure by Franchisor to provide key processing functions at the required service levels	• failure in CIL process • failure in members' distribution process • failure of FPD business planning process • failure to adapt processes to changing requirements / environment • failure to modernise key processes • ineffective market reporting process • mismanagement of auction process • unsatisfactory management of Trust Funds • accounting & settlement project requires change by STFO and hence generates risk

Operational risk sub-category	Description	Risk components
Ineffective management of information or IT	Financial loss or damage to brand due to ineffective management of information by the Franchisor	• absence or poor management of data • breach of confidentiality of information such as leakage of commercially / price sensitive information • breach of data protection laws • data corruption or loss of data • inability to perform regulatory / statutory reporting • inability to proactively manage Franchise performance • inaccurate, untimely or poor quality management information hindering effective decision making / reporting • loss of intellectual property • multiple data sources / lack of definitive data source for key data • reliance on paper documentation • reliance on third parties for base data
Failure or loss of key infrastructure	Critical failure or loss of key elements of infrastructure, including systems, communications and physical infrastructure	• accidents or unintended damage including fire and water damage • data failure, including those resulting from hacking of systems and virus attacks • failure of critical utilities or other third party services • malicious acts or terrorism specific to Lloyd's, both internal and external • technical failure • widespread acts (denial of access, e.g. transport failure, chemical, biological, nuclear, radiological attack on London, cordon)

Operational risk sub-category	Description	Risk components
Failure of key service providers to deliver service levels to Franchisor	Failure of key service providers to deliver service levels to the Franchisor resulting in financial loss or the trading position of the Franchise being adversely affected (Note: excludes Xchanging – see risk 34)	• business failure of service provider • conflicts of interest within service provider • service provider has inadequate governance or resources • service providers fail to deliver cost effectiveness • service providers have poor systems, procedures and back office processing • service providers lack clarity of objectives
Ineffective Franchise governance structure	Financial loss or damage to brand resulting from ineffective governance structure	• failure to appropriately manage ongoing litigation • failure to comply with FSA requirements (whistle blowing etc.) • failure to effectively govern the decision making and governance processes • failure to understand risk associated with the decisions made • inappropriate or unclear delegations of authorities or approval process • inappropriate organisational structure (duplication, or omission of decisions) • ineffective business planning and objective setting • ineffective management information • lack of accountability • reporting lines unclear

Operational risk sub-category	Description	Risk components
Failure to define / implement Franchisor culture and competence	Failure to establish appropriate culture and competence for the Franchisor	• inconsistent information results in missed opportunities / misalignment of effort • HR policies and practice not carried out in accordance with legislation throughout the business • failure to develop people to meet individual and business objectives • failure to demonstrate core capabilities (management of information, projects, risk, people and relationships) • failure to demonstrate core values (flexible, commercial, accountable, excellence, clarity, collaboration) • failure to meet FSA training and competence commitments • failure to remove poor performers • failure to retain the key people / failure to plan succession of key people • inability to attract the right people • inappropriate allocation of responsibilities • inappropriate reward structure (not aligned to objectives of the Franchise) • over reliance on key people • poor perception of Franchisor culture and competence by franchisees resulting in strained working relationship

Operational risk sub-category	Description	Risk components
Ineffective external communication	Failure by Franchisor to communicate effectively to all external stakeholders (including franchisees, market associations, investment analysts, rating agencies, brokers, capital providers, key suppliers, customers, media, regulators, government)	• breakdown in relationship with key stakeholders • duplication or misalignment of effort • failure to attract or retain capital as a result of inaccurate, incomplete or untimely communication • key messages not being delivered appropriately • misleading or conflicting messages • mismarketing • poor media relations
Franchisee culture and competence	Failure to establish appropriate culture and competence for the franchisee	• culture not regularly reviewed • employment not carried out in accordance with legislation • failure to appropriately develop the people • failure to demonstrate core capabilities (management of information, projects, risk, people and relationships) • failure to live appropriate values • failure to meet FSA training and competence commitments • failure to remove poor performers • failure to retain the key people • inability to attract the best people • inappropriate allocation of responsibilities • inappropriate reward structure (not aligned to objectives of the organisation) • over reliance on key people

Operational risk sub-category	Description	Risk components
Failure of core processing systems	Failure of franchisees, Franchisor, brokers or third parties to deliver core insurance business service levels resulting in financial loss or the trading position of the Franchise being adversely affected	• brand undermined by poor policyholder service • business lost by Franchise due to poor reputation / process • franchisee unable to settle valid claims or reject invalid claims • failure of central accounting system • failure of central processing • failure of Franchisor to deliver regulatory reports • inability to force brokers, franchisees or third parties to improve or deliver quality standards • lack of viable alternative service provider • poor change management fails to identify and/or deliver key improvements • signed Premium data not provided to franchisees • franchisees unable to deliver policies or collect premiums • liquidity issues for franchisees resulting from failure of central accounting system
Failure to execute current strategy	Failure to execute current strategy through the business planning process, leading to lack of confidence	• failure of franchisees and Franchisor departments to align plans with Franchise • failure to effectively communicate current strategy • failure to execute business plan • failure to monitor delivery of business plan objectives • failure to translate strategy into an operational business plan

LLOYD'S

TOOL 2.4
BASEL II FRAMEWORK OPERATIONAL RISK CATEGORISATION

Basel II framework – Detailed loss event type classification (operational risk)

The following table sets out the Basel II loss event categorisation for operational risk in order to provide a helpful point of reference.

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity / discrimination events, which involves at least one internal party	Unauthorised activity	• transactions not reported (intentional) • transaction type unauthorised (w/ monetary loss) • mismarking of position (intentional)
		Theft and fraud	• fraud / credit fraud / worthless deposits • theft / extortion / embezzlement / robbery • misappropriation of assets, malicious destruction of assets, forgery, check kiting, smuggling, account take-over / impersonation / etc. • tax non-compliance / evasion (wilful), bribes / kickbacks, Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and fraud	• theft / robbery • forgery • check kiting
		Systems security	• hacking damage • theft of information (w/ monetary loss)

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee relations	• compensation, benefit, termination issues • organised labour activity
		Safe environment	• general liability (slip and fall, etc.) • employee health and safety rules events • workers compensation
		Diversity and discrimination	• all discrimination types
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product	Suitability, disclosure and fiduciary	• fiduciary breaches / guideline violations • suitability / disclosure issues (KYC, etc.) • retail consumer disclosure violations • breach of privacy • aggressive sales • account churning • misuse of confidential information • lender liability
		Improper business or market practices	• antitrust • improper trade / market practices • market manipulation • insider trading (on firm's account) • unlicensed activity • money laundering
		Product flaws	• product defects (unauthorised, etc.) • model errors

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
		Selection, sponsorship and exposure	• failure to investigate client per guidelines • exceeding client exposure limits
		Advisory activities	• disputes over performance of advisory activities
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events	Disasters and other events	• natural disaster losses • human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	• hardware • software • telecommunications • utility outage / disruptions
Execution, delivery and process management	Loss from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction capture, execution and maintenance	• miscommunication • data entry, maintenance or loading error • missed deadline or responsibility • accounting error / entity attribution error • model / system misoperation • other task misperformance • delivery failure • collateral management failure • reference data maintenance
		Monitoring and reporting	• failed mandatory reporting obligation • inaccurate external report (loss incurred)
		Customer intake and documentation	• client permissions / disclaimers missing • legal documents missing / incomplete

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
		Customer / client account management	• unapproved access given to accounts • incorrect client records (loss incurred) • negligent loss or damage of client assets
		Trade counterparties	• non-client counterparty misperformance • misc. non-client counterparty disputes
		Vendors and suppliers	• outsourcing • vendor disputes

LLOYD'S

TOOL 2.5
COMMON RISK LANGUAGE & GLOSSARY OF RISK TERMS

The following examples provide a **helpful set of key definitions** which could form the basis of a common risk language.

- **Backstop control –** A less frequent type of detect control, typically carried out on a monthly or quarterly basis, for example quarterly reviews of loss ratios across contract classes.
- **Basel II –** A framework developed by the Basel Committee on Banking Supervision to provide prudential risk management guidance to the global banking community, covering capital requirements, supervisory review and market discipline. The framework impacts banking groups both internationally and domestically. Within such groups there are capital requirements for majority-owned or controlled banking entities, securities entities and other financial entities (excluding insurance entities).
- **Capital –** There are four main types of capital:
    - **total capital (or equity or book capital),** defined in GAAP or IAS as common equity, preferred stock and subordinated debt;
    - **regulatory capital** as defined by the FSA using minimum rules for solvency capital for insurance businesses and used for prudential supervision (i.e. capital adequacy);
    - **rating agency capital,** defined by rating agencies as capital required to maintain the current debt or financial strength ratings; and
    - **economic capital** which represents the level of capital required to protect against unexpected losses, such that the market's underwriting liabilities can be met and Lloyd's credit rating maintained.
- **Cause –** The business condition that allowed a risk to occur. Causes generally fall into two categories: internal problems or external matters.
- **Control –** A preventative and/or detective activity, intended to manage the inherent risks identified within a business. This will normally relate to management of the potential impact and/or likelihood of risk exposure but may also involve risk transfer, mitigation or elimination.
- **Control activities –** Policies and procedures that ensure management directives are executed; they ensure necessary actions are taken to address risks to the achievement of corporate objectives.
- **Control environment –** The operating environment that comprises the integrity and competence of colleagues, management's philosophy and operating style and the way management communicates and delegates responsibility, and develops its people.

- **Control objective –** The primary goals of an internal control system. As defined by the Basel Committee on Banking Supervision, an internal control system can be expected to provide reasonable assurance of achieving the following four control objectives:
  - safeguarding of assets;
  - economy / effectiveness of process;
  - compliance with laws and regulations; and
  - integrity / reliability of data.
- **Control rating –** A score achieved through the risk and control self-assessment (RCSA) process that provides an indication of how the current control effectiveness is perceived.
- **Correlation –** A random event can have a different probability of occurring if a second random event has occurred. In this case, the events are dependent. If the probability is not affected by whether the other event takes place, the events are independent. Correlation is a simple measure of dependence. Other more complex measures exist.
- **Credit risk –** The risk of loss if another party fails to perform its obligations or fails to perform them in a timely fashion. For syndicates the key counterparties are reinsurers, brokers, insureds, reinsureds, coverholders and investment counterparties.
- **Diversification –** Because losses are not completely dependent, generally less capital is needed at a given confidence level for a pooled portfolio than for the separate components of the portfolio considered alone. The degree to which this happens is called diversification. Diversification depends heavily on the correlation of the parts of the portfolio and also on the way risk is measured.
- **Economic capital –** Represents the level of capital required to protect against unexpected losses, such that the market's underwriting liabilities can be met and our credit rating maintained.
- **Enterprise risk management –** A structured and disciplined risk management approach considering strategy, process, people, technology and knowledge with the purpose of continually evaluating and managing risks to business strategies and objectives on an enterprise-wide basis. Enterprise risk management is a continuous activity that aggregates and integrates risk management activities across all types of risk in order to achieve maximum risk-adjusted returns.
- **Escalation triggers –** A process whereby immediate reporting is instigated upon a particular indicator or variable moving outside an agreed range.
- **Group risk –** The potential impact of risk events, of any nature, arising in or from membership of a corporate group.
- **Individual Capital Assessment (ICA) –** Capital assessment performed by a managing agent under PRU 1.2.26R, LLD 18.2.1R, PRU 2.3 and LLD 19.4.1R(1) in respect of each syndicate managed by it.
- **Impact –** The effect that the risk would have on the organisation's ability to successfully achieve its objectives if the risk occurred.

- **In-Control –** The term used to describe a business area that understands its risk profile, has assessed the risks and, where it has been concluded that risks are under control, knows what the controls are and that they are working. Where risks have been assessed as not being under control, the business area knows the factors contributing to this and has plans to manage, mitigate or eliminate the contributing factors.
- **Inherent risk –** The risk in a business or process before the effect of any risk mitigation, control or transfer activities.
- **Insurance risk –** The risk of loss arising from the inherent uncertainties as to the occurrence, amount and timing of insurance liabilities.
- **Internal control –** The system of control, financial or otherwise, established by the management of an agent in order to:
    - carry on the business of the agent in an orderly and efficient manner;
    - ensure adherence to management policies;
    - safeguard the assets of the agent and other assets for which the agent is responsible; and
    - secure as far as possible the completeness and accuracy of the agent's records.
- **Internal loss database** – A database which records:
    - **Potential losses** – An incident that has been discovered, that may or may not ultimately result in a financial loss;
    - **Near misses** – An incident that was discovered through means other than standard operating practices and through good fortune or focused management action has resulted in nil or positive financial impact; and
    - **Actual losses** – An incident that has resulted in a negative financial impact.
- **KCI (Key control indicator) –** A measure of the performance of a specific control. Deterioration in KCIs can show an increase in residual risk. KCIs tend to be relevant to a particular control activity.
- **KRI (Key risk indicator) –** A key risk indicator is a measure of the status of an identified risk within a business, by measuring defined risk events.
- **Likelihood –** The probability that exposure to a risk will occur**.**
- **Liquidity risk –** The risk that sufficient financial resources are not maintained to meet liabilities as they fall due.
- **Market risk –** The risk that arises from fluctuations in values of, or income from, assets or interest or exchange rates.
- **Material –** In general terms, a material issue is one involving actual or potential significant financial loss or reputational damage, which has been or needs to be escalated to the Board of Directors or Board Committee level.
- **Mitigation –** To moderate or decrease the likelihood or potential impact of exposure to a risk.
- **Modelling –** Creation, parameterisation and interpretation of a representation of the syndicate's business. Usually includes probability assumptions and simulation ("stochastic model").

- **Operational risk –** The risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events.
- **Procedure –** A formal system or process set out to achieve policy or operational aims.
- **Process map –** The major steps in any process, usually portrayed as a flow chart, and depicting the inputs and outputs for each step in the process. Key controls may be depicted as process steps. Suppliers and customers of each process may also be identified.
- **Quantification of risk –** The determination of the scale of risk by the allocation of a metric, such as £ sterling cost, or impact on share price, relative to the frequency of occurrence. Most often, risk is quantified by reference to its potential impact on an organisation – e.g. loss of earnings, damage to profit, volatility of results – and the likelihood of its occurrence. Quantification can be derived from a combination of methodologies that can be qualitative in nature – particularly used in areas where the scarcity of needed data makes risk more difficult to measure, such as operational risk – or quantitative – used where precise measurement and statistical analysis is possible.
- **Regulatory risk –** The risk of loss arising from the organisation's dealings with both UK and overseas regulators.
- **Residual risk –** The potential impact and likelihood of an identified risk exposure, considering the effect of the existing (but excluding planned) controls.
- **Risk –** The potential for loss or failure to meet business objectives as a consequence of internal or external events.
- **Risk appetite –** The expression of the level of acceptable and/or unacceptable risk as defined by the Board of Directors and senior management. Risk appetite reflects Lloyd's willingness to take on risk as derived from its capacity to bear risk and the philosophy or attitude toward risk taking.
- **Risk capacity (or tolerance) –** The amount of risk, in aggregate, that an organisation is able to bear. Risk bearing capacity generally includes available capital, ability to raise capital and the capacity and strength of operational processes and related governance.
- **Risk category (or risk group / risk sub-group) –** Risks identified can be grouped in order to facilitate monitoring and reporting e.g. Insurance, Credit, Operational.
- **Risk components –** Examples of causes, effects and examples of the risk issue and instances when it may have occurred in the past. This may include process failures or inadequacies that may, in combination, result in the risk event occurring. The list of components under any one risk would normally be illustrative rather than exhaustive.
- **Risk description (or definition) –** A detailed articulation of a risk, designed to give clearer understanding of the risk.
- **Risk effect –** The consequence that the risk has to the company. The effect can be measured on a qualitative (high, low) or quantitative manner (dollar amount, number of transactions impacted).
- **Risk event –** A high level articulation of risk and potential or actual exposure often used in risk registers / portfolios.

- **Risk framework –** The overarching, unifying approach and process for the management of risk within an organisation, which is often expressed diagrammatically. The framework includes all the key building blocks for risk management which typically include a common language for risk, the organisation's risk policy and appetite, identification and assessment of risk, monitoring and assurance of risk and of the risk management process and reporting.
- **Risk map –** The visual representation of risk (which has been identified through a risk assessment exercise) in a way that allows priority ranking. This representation often takes the form of a two-dimensional grid with frequency (or likelihood of occurrence) on one axis, and severity (or degree of impact) on the other axis; the risks that fall in the high-frequency / high-severity quadrant are given priority risk management attention.
- **Risk policy –** Documented approach and rules to be followed in relation to a particular area or issue that has been agreed by the Board or a properly delegated committee.
- **Risk register –** A schedule or table capturing the list of significant risks facing the organisation.
- **Self-Assessment –** A process whereby each business / functional area proactively identifies the significant risks it is potentially exposed to, estimates the potential impact and likelihood, assesses the quality of control, and determines a mitigation plan for identified risks that are "high" and controls that need improving.
- **Stress and scenario tests –** Stress and scenario tests are carried out to determine the expected financial and non financial consequences of adverse circumstances and events arising within the relevant time horizon. Stress tests are generally defined with reference to movements in key financial parameters (such as interest rates, asset values or liability values), whereas scenario tests may make reference to the cause of the adverse developments (such as a material natural catastrophe or major industrial incident).
- **Threshold –** Represents a level of exposure that can be exceeded, but which, when exceeded, will trigger some form of timely response.
- **Unexpected loss –** Loss that is not budgeted for (expected) and is absorbed or buffered by an attributed amount of economic capital.

SECTION BREAK

LLOYD'S

RISK APPETITE

SECTION 3

TOOLS

Tool 3.1 – Key questions to consider when setting risk appetite

Tool 3.2 – Example appetite articulation via qualitative statements

Tool 3.3 – Example appetite articulation via quantitative statements

Tool 3.4 – Example appetite articulation via key risk indicators

Tool 3.5 – Examples of high level articulation of risk appetite

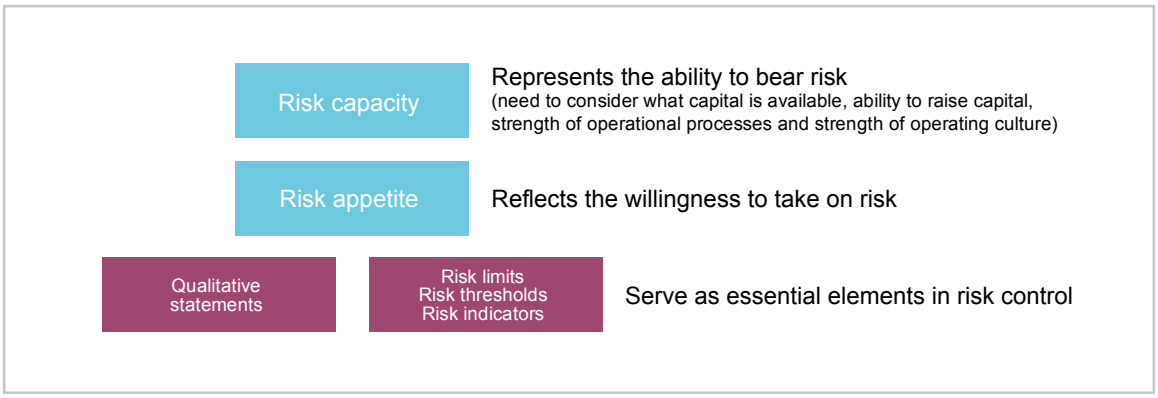
Tool 3.6 – Examples of low level articulation of risk appetite

3 RISK APPETITE

What is risk appetite?

Risk appetite reflects **the amount of risk taking that is acceptable to an organisation.** As a result, risk appetite refers to the organisation's attitude towards risk taking and whether it is willing and able to tolerate either a high or a low level of exposure to specific risks or risk groups.

As the diagram below illustrates, risk appetite, first and foremost, is a function of the organisation's capacity to bear risk and of its attitude towards managed risk taking. Risk appetite can also be viewed as **assigned or allocated risk capacity.**



Why is it important?

Among other things, risk appetite plays an important part in supporting risk assessment, monitoring and control activities. It does this by helping staff to understand the relative significance of the risks faced by the organisation and thereby **better prioritises risk monitoring and control activities.**

Risk appetite plays a key role in **maximising return on capital invested** as it acts as a driver for allocation of capital to identified risks. The better the understanding of risk appetite, the more efficient the allocation of capital across the organisation. Risk appetite should be a function of the capacity to bear risk and should not exceed it. Constraints on risk appetite include the capital which needs to be maintained to support a target rating agency's rating and regulatory capital requirements.

It is important to note that businesses trading at Lloyd's are subject to a number of guidelines in respect of risk appetite, through the operation of the **Franchise guidelines**.

What are the benefits of articulating risk appetite?

Organisations that effectively articulate their risk appetite and adequately fund their managed risk taking are better insulated against shock to future earnings, **better placed to allocate scarce resources** when and where needed, and better prepared to take advantage of changes in insurance cycles as they arise.

Specifically, **risk appetite plays two roles** in supporting the business objectives and risk management activities of an organisation:

- firstly, it establishes a benchmark from which transaction specific limits or thresholds can be set and monitored for an organisation's exposure to particular risks:

  - **a limit** reflects the absolute maximum level of exposure that is acceptable for a particular risk (i.e. it represents a level of exposure that should not normally be exceeded);
  - in contrast **a threshold** represents a level of exposure which, with appropriate approvals, can be exceeded, but which, when exceeded, will trigger some form of response (e.g. additional capital or expenditure on risk control, reporting the situation to senior management, etc.);
- secondly, as a **resource allocation tool,** risk appetite helps determine the degree of control that needs to be applied to a particular risk. For example:
  - if current exposure to a particular risk is considered to be acceptable there is usually little value, other than for efficiency reasons, in changing the extent of control (either in terms of using tighter controls or by increasing capital or the amount invested in risk control);
  - in contrast, where current exposure to a particular risk is considered unacceptable, an agent may decide that it needs to invest more capital and introduce more rigorous controls.

There are a number of **additional benefits** of articulating risk appetite:

- risk appetite is an essential element of risk governance and provides a framework for the business to operate within, as it provides **clear boundaries** regarding what is and is not acceptable to the organisation;
- articulating risk appetite **leaves room for creativity** within acceptable limits and reduces the possibility of exposure to unpleasant incidents due to a lack of awareness;
- **provides a framework** for considering and approving risk taking levels and activities that are outside the current appetite for risk; and
- assists in the identification and **prioritisation of areas** where additional resources or controls may be necessary to bring the risk into line with the stated risk appetite.

What practical steps are necessary for implementation?

The following guidance is intended to help you understand what is involved from a **practical standpoint** to implement this **risk appetite section:**

- **Staff resource and skills**
  - senior management buy-in is vital in order to establish and articulate an organisation's risk appetite
  - Board and senior management assessment of risk bearing capacity and risk appetite, as an integral part of business planning, with facilitation and proposals from the risk committee and risk management function
  - business unit and functional area management workshops to consider, interpret and cascade risk appetite for their function(s)
  - IT programming resource to develop and implement system limits, monitoring and exception reports, thresholds and KRIs as appropriate
  - internal audit review to give assurance that reliable monitoring systems against appetite are in place

- **Enabling technology**
  - underwriting system implementation of limits, thresholds, KRIs and/or other expressions of appetite
- **Time**
  - Board – extending the business planning process to articulate clearly the risk appetite
  - business unit managers – cascade and interpret board appetite for each business unit and functional area, e.g. via workshops, as part of business plan roll out
  - overall implementation time – an integral part of business planning cycle and performance monitoring process
- **Direct / indirect costs**
  - Board and senior management time – integral part of business planning and performance monitoring process
  - IT staff time – for programming limits, thresholds etc.
  - risk management time – proposals for risk appetite, facilitation of appetite setting, documentation, review and monitoring
  - internal audit / external consultants – review, technical support, assistance and assurance over appetite setting and resetting

Notwithstanding the wide range in size and sophistication of organisations, it is anticipated that setting risk appetite should be an **integral part of the business planning** process, including roll out and monitoring against plans, for **all organisations.**

Relevant toolkit contents

With regard to operational risk, there are a number of ways of expressing risk appetite. The toolkit provides explanations of each approach with advantages and disadvantages and worked examples covering:

- **Tool 3.1 – Key questions to consider when setting appetite:** highlights key questions organisations should consider when setting and expressing risk appetite;
- **Tool 3.2 – Example appetite articulation via qualitative statements:** provides examples of and advantages and disadvantages of risk appetite articulation using qualitative statements;
- **Tool 3.3 – Example appetite articulation via quantitative methods:** provides quantitative examples of and advantages and disadvantages of risk appetite articulation through limits and thresholds;
- **Tool 3.4 – Example appetite articulation via key risk indicators:** provides quantitative examples of and advantages and disadvantages of risk appetite articulation through key risk indicators;
- **Tool 3.5 – Examples of high level articulation of risk appetite:** an example high-level (Board level) articulation of risk appetite in terms of various operational risk classes; and
- **Tool 3.6 – Examples of low level articulation of risk appetite:** an example low-level (business function level) articulation of risk appetite in terms of various operational risk classes.

LLOYD'S

TOOL 3.1
KEY QUESTIONS TO CONSIDER WHEN SETTING RISK APPETITE

Consideration of the following questions will be of help when considering how to express risk appetite:

- When **setting risk appetite**, have the following been considered?
    - investor expectations;
    - the financial strength of the franchisee and/or parent;
    - the attitude to risk taking by the Board and senior management;
    - the proposed business plan, including risk classes, line sizes, territories, aggregates and exposures and potential gross and net RDS losses, particularly for high hazard classes, taking account of:
        - the range of expected performance;
        - expected losses consistent with the business classes (i.e. extent of high severity low frequency losses and low severity high frequency losses);
        - minimum legal and regulatory requirements; and
        - acceptable levels of retention:
            - including the **largest downside loss** which the Board would be prepared to accept;
            - subject to outwards **reinsurance availability and costs;** and
            - subject to ensuring **survival** in a catastrophe.
    - acceptable costs of:
        - risk control and risk financing (of retained losses); and
        - risk management administration.
- Is the **expression of appetite** clear in respect of what risks you are willing to accept and what risks are you unwilling to accept?
- Has risk appetite been **communicated** in a way that is readily understood by managers and staff?
- How are you **measuring performance** against stated risk appetite?
- Does the **measurement and reporting of risk** relate to stated risk appetite?
- **What can be improved** about the current risk appetite setting process and the way in which performance is measured?
- **What limits or thresholds are most relevant** for each risk and control?
    - e.g. reserving
    - e.g. staff turnover
    - e.g. reporting / escalation – at what point?

TOOL 3.2
EXAMPLE APPETITE ARTICULATION VIA QUALITATIVE STATEMENTS

Qualitative risk appetite articulation

One approach to articulating risk appetite involves a **series of qualitative statements** detailing the specific risks that a business is or is not prepared to tolerate, usually as a section within the relevant risk policy.

Worked examples include:

- the business has zero risk appetite for **fraudulent activity**;
- the business is an **equal opportunities employer**;
- the business has a **low operational risk appetite**. Where operational risks arise, these should be mitigated and controlled, as long as the cost of controlling the risk does not exceed the benefits derived from the lower risk level;
- the business has a very low appetite for **reputational risk** exposure. While it is recognized that inherent reputational risk is generally high due to the nature of the business, the business will always need to take all steps possible to minimize the likelihood of adverse reputational impact from all major sources; and
- the business has a low appetite for **business outages**. Business contingency arrangements and plans should be established, maintained and periodically tested which respond to any outage scenarios between 30 minutes and 1 month in duration. The business has zero tolerance for outages beyond 1 month in duration.

Advantages and disadvantages

Advantages	Disadvantages
• easy to define, useful in areas where quantification may be an issue • intuitively simple to create and understand	• no figures and can be difficult to measure unless key risk indicators are established and systematically monitored • by their very nature, and as can be seen from the above examples, operational risk limits tend to be “binary” statements. This can complicate the assessment of the relative significance of actual breaches or any assessment of what margin of safety the business is operating in • comparison / aggregation of appetites can be complicated • completeness. The implication is that for this to adequately cover appetite the business may need to generate a long list of what they do and do not do in practice

LLOYD'S

TOOL 3.3
EXAMPLE APPETITE ARTICULATION VIA QUANTITATIVE METHODS

Quantitative risk appetite articulation through limits and thresholds

A second approach to articulating risk appetite involves quantitative statements, which are typically expressed in terms of **limits, thresholds and key risk indicators** (discussed in detail later in the toolkit).

Limits

Limits may be set by the Board for operational risk outcomes:

- **example aggregate limit –** total annual operational risk losses, arising from both expected and unexpected events, is not to exceed £[TBD]m;
- **example single event limit –** no single unexpected operational risk loss in a single year should exceed £[TBD]m.

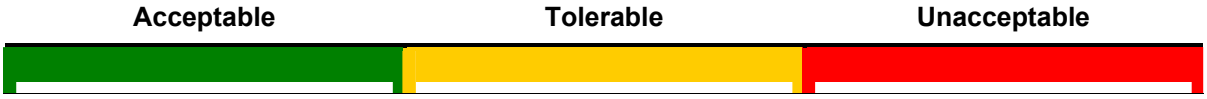
Limits – advantages and disadvantages

Advantages	Disadvantages
• aggregate limits provide an overall measure of acceptable outcome in any one year or other timeframe • single event limits provides clear direction on levels of acceptable exposure and that which is considered unacceptable • expected losses can be tied in to the budget process • facilitates monitoring	• ability to articulate operational risk appetite by way of limits is dependent on Board and senior management having defined overall appetite for risk and being able to attribute an acceptable volatility to operational risk

Thresholds

Thresholds may be set, above which specific requirements are identified for the management, escalation and approval of the risk and/or incident. For example, thresholds could be set according to what level is deemed acceptable, tolerable and unacceptable, and a **red, amber, green approach** applied. The benefit of the "traffic light" approach is that it can be easily used to determine practical ranges of acceptability, tolerability and unacceptability. Exposures that are in the:

- **"green" range** are acceptable and probably do not need to change;
- **"amber" range** may be tolerated but need to be monitored closely to ensure that the level of exposure does not worsen; and
- **"red" range** are unacceptable, and will require an immediate response to ensure that they are reduced or eliminated. This is illustrated in the diagram below:



Worked examples

Examples of expressing risk appetite numerically include:

- **yearly (or quarterly) loss amounts** (for example, the total levels of internal fraud losses) that are acceptable, tolerable and unacceptable in the specified period;
- the **number of operational risk events** that are acceptable, tolerable and unacceptable in a given year (or quarter);
- the **size of any one single operational loss** that is acceptable, tolerable and unacceptable;
- the size of any one single operational loss that is tolerable or which would be unacceptable **in a given time period** (say over a 10, 20 or 50 year period, etc.);
- the degree to which operational loss levels or the number of operational risk events can **increase in a given year** (for example, an increase of 5% in external fraud losses might be acceptable, 10% tolerable and 15% unacceptable); and
- the level of an **individual key risk indicator** that is acceptable, tolerable and unacceptable in a given year.

Thresholds – advantages and disadvantages

Advantages	Disadvantages
• facilitates monitoring • thresholds can potentially factor in reputational impacts e.g. regulatory, customer etc • permits assessment of relative significance of breaches • permits aggregation and comparison • flexible. As the organisation matures and / or the risk profile changes thresholds can be adjusted to provide the “right level” of Board oversight	• method of deriving may be subjective; some areas may find it difficult to define and relate to thresholds

Examples of where numerical expression may be difficult to derive include:

- media and reputation effects;
- regulatory interest and the potential for intervention;
- the effect that an operational risk event could have on the organisation’s customers;
- the effect that an operational event could have on staff (in terms of morale, turnover etc.); and
- opportunity costs in terms of diverted management resources to deal with loss events.

TOOL 3.4
EXAMPLE APPETITE ARTICULATION VIA KEY RISK INDICATORS

Quantitative risk appetite articulation through key risk indicators

Key risk indicators (KRIs) are:

- parameters that are assumed to be **highly predictive** regarding changes in the risk profile; and
- designed to **monitor the development** of significant risks. Tolerance levels are therefore set and monitored and breaches escalated.

These are discussed in more detail in the **KRI section (7)** of the toolkit.

Worked example

A key risk indicator for monitoring the development of resourcing risks in respect of staff levels is staff turnover levels:

- **below 24% – No risk.** The risk is not materialising and we are comfortable with the level of staff turnover. No escalation or treatment required;
- **above 24% – Potential risk.** The risk is a concern and HR would be expected to monitor actively, establish causes and actions. Escalation required to raise awareness but explanatory report not required; and
- **above 28% – Risk.** Action and escalation with explanatory report required.

Advantages and disadvantages

Advantages	Disadvantages
• easy to monitor performance, quick view of overall performance against target • tolerable ranges can be set around any measurable indicator and can be tailored to different parts of the business • flexible. As the organisation matures and/or the risk profile changes the thresholds can be adjusted to provide the "right level" of Board oversight	• requires planning and in-depth knowledge of risk areas and operational processes, which may take time to develop • KRIs may be difficult to derive or establish in some risk areas and operational processes • does not permit assessment of relative significance of breaches across different KRIs • does not permit aggregation of risk appetite

LLOYD'S

TOOL 3.5
EXAMPLES OF HIGH LEVEL ARTICULATION OF RISK APPETITE

The Board will set the overall risk appetite for a business. Some examples of high level operational risk appetite are illustrated in the table below. In practice, risk appetite would be set for each major risk group.

This is typically interpreted and **cascaded** down by senior management into more detailed expressions of appetite or limits applicable to each business function (see separate example).

Operational risk class	*ABC* Board level articulation
People	• *ABC* employs sufficient, suitably skilled and experienced staff • staff roles and responsibilities are clearly defined • staff performance is reviewed and training needs met • *ABC* is an equal opportunities employer • *ABC* has zero appetite for fraudulent activity • potential conflicts of interest are avoided and/or disclosed
Processes	• *ABC* has a low operational risk appetite for process failure • zero tolerance of business outside plan and RI programme • zero tolerance for high priority internal audit / regulator issues • no single operational risk loss to exceed £50,000 / year • annual aggregate operational risk losses not to exceed £100,000 / year • *ABC* is Turnbull compliant
Systems	• no more than 2 IT system outages / month for more than 1 hour • no more than 1 IT virus caused outage / month for more than 1 hour • zero tolerance of IT & data security breaches • effective and tested DRP to be in place
External events	• tolerate up to 20% gross RDS exposure against capacity • tolerate up to 5% final net RDS exposure against capacity • very low appetite for business outages • effective and tested BCP arrangements in place • responding to outages 30 minutes to 3 months in duration

Reputational	• very low appetite for reputational risk
	• *ABC* takes immediate action to resolve
	  • policyholder complaints
	  • UK and overseas regulator concerns
	  • high priority internal and external audit concerns
	• *ABC* actively contributes to the community

Legal	• *ABC* seeks contract certainty prior to written risks incepting • zero appetite for legal action against the organisation • *ABC* complies with all relevant legislation

Strategic	• *ABC* actively monitors its business strategy against:
	  • insurance cycle and class rating changes
	  • political, regulatory and economic environment changes
	• *ABC* actively manages change

LLOYD'S

TOOL 3.6
EXAMPLES OF LOW LEVEL ARTICULATION OF RISK APPETITE

Once the Board has set the **overall risk appetite**, it is typically **cascaded down by senior management** into more meaningful and detailed expressions of appetite or limits applicable to each business function.

Some examples of **low level operational risk appetite** are illustrated in the table below (i.e. potential weaknesses or failures in respect of people, systems and processes and external events, wherever located in a business).

In practice, risk appetite would be set for each major risk group.

Cause	Potential causes	Example articulation of appetite
People	**Staff recruitment / training / supervision** • recruitment screening failure • inadequate staff training • inadequate staffing levels • lack of management supervision • lack of escalation to management	• recruitment screening for all potential recruits • CPD and training development to be met • less than 20% staff turnover • less than 5% sickness rates per division • less than 5% average use of contract staff • 100% referral rates where appropriate • succession plans in place for all staff
	Staff activity • internal theft or fraud / other unauthorised activity	• zero fraud or theft tolerated • full disclosure of conflicts of interest required • less than 5% of complaints referred to Ombudsman

Cause	Potential causes	Example articulation of appetite
Processes	**Basic underwriting processes** • inadequate risk capture – not complete, accurate and timely (i.e. risk recording system / copy slips, declarations and endorsements / long term contracts / aggregates) • slips not underwritten within authority (agent & Lloyd's) / signatures & stamps controlled • failed referral process / reporting lines and authority limits inappropriate • underwriting guidelines not followed or inadequate • underwriting objectives unclear or inappropriate (for class underwriters)	• 100% slips recorded within 24 hours • less than 2% slip entry error rate • 100% endorsements recorded • 100% aggregates (or proxy for max aggregate) recorded within 24 hours • 100% of slips underwritten within authority • 100% referral where appropriate • 100% underwriting guidelines to be followed, subject to referral
	Underwriting review • lack of detailed, inexperienced or untimely peer review (including endorsements) • ineffective underwriting meetings (updates on developments) • inadequate supervision and performance review of class underwriters	• 100% of slips with more than £1m premium or more than £10m exposure to be peer reviewed within 10 days • quarterly underwriting review of all accounts • technical underwriting review if class loss ratios are more than 20% above expected

Tool 3.6 Examples of low level articulation of risk appetite

Cause	Potential causes	Example articulation of appetite
	Monitoring of underwriting • performance against plan not reviewed (including premium income) • exception reports inadequate, untimely or not reviewed • outstanding premiums not reported or chased • large claims not reviewed • performance not reviewed (at contract level) • aggregates not up to date and monitored • outstanding facultative reinsurance recoveries not chased • wording not finalised or issued	• zero tolerance of business written outside approved plan and reinsurance programme • zero tolerance of class premium income greater than 110% of business plan • all premium and reinsurance debt more than 90 days outstanding to be chased • all claims over £10m to be reviewed • all non-moving claims to be reviewed every 6 months • all contracts with loss ratio greater than 110% to be investigated, (subject to de-minims £1m premium) • all exposures to be recorded within 1 month of underwriting • less than 100 binders to be written, with minimum income £100k • zero tolerance of outstanding wordings over 1 month
	Agency level underwriting controls • independent review covered the class • compliance monitoring covered the class (inc. internal audit / other reviews) • Board reporting of major issues (via monitoring committee / active underwriter)	• 75% of major contracts to be independently reviewed within 1 month of underwriting • internal audit to review all key businesses processes over a rolling 2 year period • compliance review to cover all key business areas annually • key business issues to be considered by the Board or sub delegated to an approved sub committee
	Placement of reinsurance programme • insufficient scrutiny of reinsurers' quotes • errors on reinsurance order forms, e.g. through lack of scrutiny • errors on cover notes undetected through lack of scrutiny (against order) • partial or revised placements not communicated to management or underwriters	• all reinsurance order forms and cover notes to be reviewed against requirements • 100% accuracy on reinsurance orders and cover notes • the Board monitors the progress of placement

Cause	Potential causes	Example articulation of appetite
	Agency level reinsurance purchase controls • lack of clear guidelines / authorities for individuals purchasing reinsurance • lack of guidelines on acceptable security (including exotic / financial reinsurance) and maximum exposures to reinsurers • lack of monitoring of exposures, amounts due, disputes and delinquency of reinsurers • lack of reinsurance erosion reporting to management	• set authorities for staff reinsurance purchase • set limits on our exposures to reinsurers (e.g. less than 10% premium to be placed with 1 reinsurer) • maintain up to date security ratings for reinsurers • monitor all material exposures / recoveries from reinsurers / erosion of reinsurance
	Claims processes • Board / management uninformed of significant claims / disputes / complaints • lack of referral where underwriters are solely responsible for adjusting claims which they underwrite themselves • lack of regular reconciliation between Xchanging and the reserves held by the syndicate • lack of monitoring the progression of claims advice or reserves • administrative delays in processing claims payments and reporting to reinsurers • delayed / omitted collection note issue / reinsurance recoveries • lack of chasing outstanding debts / review of doubtful debt provisions • unresolved dispute with actuaries or accountants	• 100% material claims / disputes / complaints reported to senior management / Board • second adjustor review for material claims greater than £10m • monthly reconciliation of claims reserves • all claims advice reviewed within 2 days • pay claims promptly, on presentation of appropriate evidence of claim • all collection notes issued within 30 days • all outstanding debts chased after 90 days • zero appetite for ongoing dispute with syndicate actuaries or accountants
	Liquidity processes • lack of regular cash flow forecasts produced, e.g. monthly, by currency, by year of account • lack of consideration of cash needs for RDS scenarios and other major losses • lack of contingency planning for potential or expected cash shortfalls • lack of regular cash flow reporting to the Board / senior management	• undertake monthly cash flow forecasting for all material currencies • forecast potential and expected cash needs for RDS scenarios and other material losses • established contingency plans for all potential or expected cash shortfalls • quarterly reporting of cash flow forecast and shortfalls to the Board

Tool 3.6 Examples of low level articulation of risk appetite

Cause	Potential causes	Example articulation of appetite
	Generic process failures • manual errors • inadequate segregation of duties • inaccurate / incomplete management information • inadequate functionality / supporting software • inadequate / inappropriate polices • process failure affecting insureds / intermediaries	• less than 2% manual input errors • no underwriting staff to have access to accounting system • MI and exception reporting to be produced and reviewed within 2 days of month end • IT system queries to be responded to within 24 hours • established policies in place for all key processes • complaints resolved within 1 month of receipt • zero tolerance for adverse press comment • zero tolerance of outstanding external and internal audit / compliance / regulatory report points
Systems	**IT outage** • hardware or software failure • network / telecommunications failure • third party IT provider failure • inadequate virus protection • inadequate system security / information risk management • insufficient processing capacity • other system error • insufficient / untested business continuity processes • inadequate update / release management	• no more than 1 IT system outage per month • zero tolerance of IT security breaches • no more than 1 IT virus caused outage per month • zero tolerance for IT supplier failure • no more than 1 day a year tolerance for server failure • 100% testing of IT disaster recovery procedures and systems
External events	**Natural or man made disaster** • local terrorist attack / other external event • power outage	• less than 24 hours IT system outage following a disaster event • less than 24 hours non availability of office facilities following a disaster event
	Supplier failure • third party provider failure	• no failure tolerated from outsource providers
	External theft or fraud • fraud • external breach of system security	• zero appetite for fraud • zero appetite for IT system security breaches

Cause	Potential causes	Example articulation of appetite
Reputational	**Regulatory environment**	
	• FSA findings	• zero tolerance of regulator action / concerns • zero tolerance of outstanding Lloyd's operational risk review points raised
Legal	**Contract certainty**	
	• poorly completed slips / wordings	• 99% of slips to be LMP compliant first time • all wordings to be agreed prior to inception
Strategic	**Changes from business plan**	
	• business written outside plan or reinsurance programme	• no tolerance of business outside plan or reinsurance programme, without prior authorisation

SECTION BREAK

LLOYD'S

RISK GOVERNANCE, ROLES & RESPONSIBILITIES

SECTION 4

TOOLS

Tool 4.1 – Example risk governance framework

Tool 4.2 – The “three lines of defence” model

Tool 4.3 – Example roles and responsibilities

Tool 4.4 – Example roles of a Chief Risk Officer

Tool 4.5 – Example risk governance principles

4 RISK GOVERNANCE, ROLES & RESPONSIBILITIES

What is governance?

Risk governance is an integral aspect of corporate governance which focuses on the structures, processes and approach to the management of the significant risks to the business objectives. This includes:

- clearly defined **accountabilities and expectations** for all relevant parties, including the **roles and responsibilities** of the Board, management, and employees;
- clearly defined **policy** for the management of all significant risks. See separate toolkit section on "Risk policy" (5);
- the rules and process for **risk based decision making**;
- a sound system for **internal control**; and
- an appropriate **assurance** process.

In summary, risk governance is the system for directing and controlling the management of risk within the organisation.

Why is it important?

Having **clear roles and responsibilities** for all relevant parties:

- clarifies which parties are responsible for **accepting and managing risk** and **setting the parameters** for managed risk taking;
- clarifies how the organisation will **balance business opportunities** against the **cost, risk and upside potential** of risk taking; and
- provides a basis for objective risk adjusted **performance measurement and management**.

There is **no "one size fits all"** model applicable for businesses.

Practical steps for implementation

All organisations will have some form of risk governance in place. The attached tools help organisations review and enhance the status of their governance framework, where appropriate, by:

- firstly, providing a **health-check or benchmark** against which to assess current risk governance; and
- secondly, to **identify options for development,** by drawing on the attached tools.

Notwithstanding the wide range in size and sophistication of organisations, it is anticipated that risk governance underpins **all risk management activity**, for **all organisations**. The example roles for a Chief Risk Officer and example risk governance principles however, are more likely to be of interest to larger organisations.

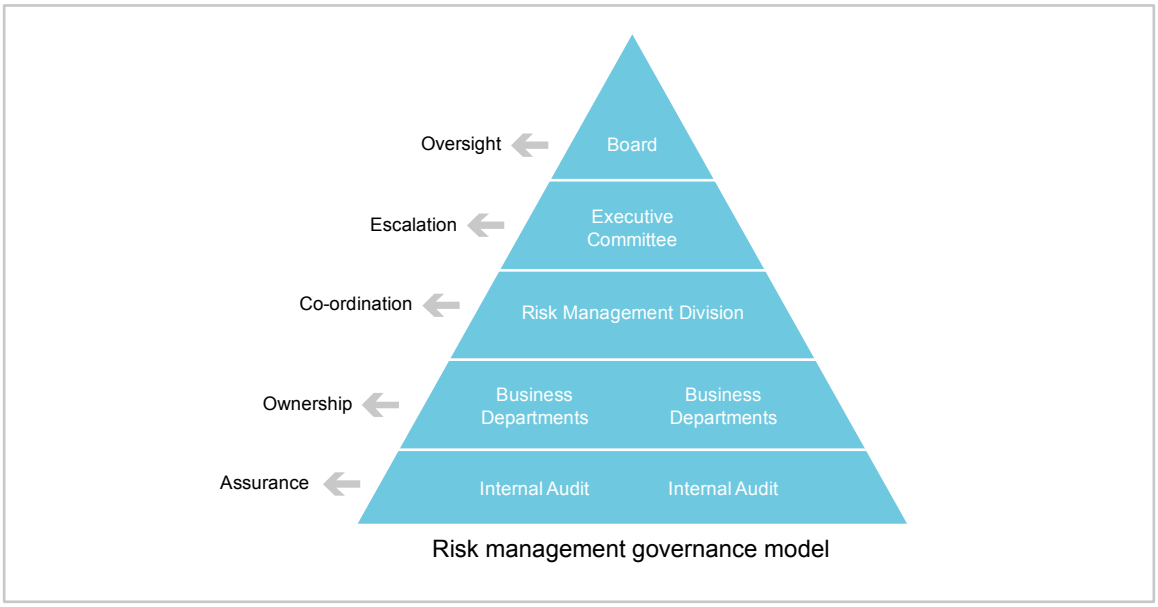
Relevant toolkit contents

Relevant toolkit contents to aid the understanding and development of risk governance, roles and responsibilities include:

- **Tool 4.1 – Example risk governance framework:** a possible approach to a risk governance framework using a pyramidal structure;
- **Tool 4.2 – The "three lines of defence" model:** a second possible approach to a risk governance framework. This illustrates and provides a high level explanation of the "three lines of defence" model;
- **Tool 4.3 – Example roles and responsibilities:** a breakdown of typical roles and responsibilities which could be used by an organisation when developing their risk governance model;
- **Tool 4.4 – Example roles of a Chief Risk Officer:** this discusses the typical roles of a Chief Risk Officer in more detail than previously provided; and
- **Tool 4.5 – Example risk governance principles:** principles that may assist an organisation when considering what risk governance principles to adopt.

TOOL 4.1
EXAMPLE RISK GOVERNANCE FRAMEWORK

A high level example of a possible **risk governance framework** is illustrated below.



Risk management governance model

In this illustrative model, each party has the following roles:

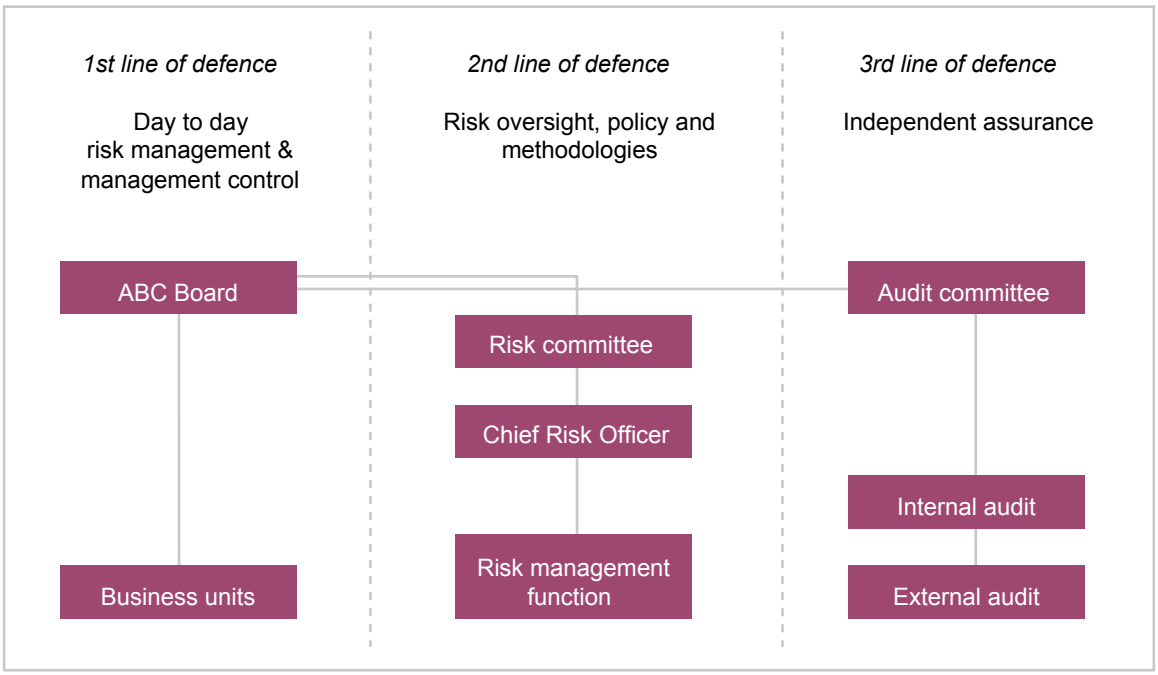
- **The Board,** on the top of the pyramid, has the ultimate accountability for the risk and related control environment, and is responsible for approving and reviewing risk policies;
- **The Executive Committee** is responsible for reviewing and challenging risk information and escalating issues to the Board;
- **The Risk Management Division** is responsible for the facilitation and co-ordination of risk management activity across the organisation;
- **Business Departments** are the “risk-takers” and are responsible for identifying, assessing, measuring, monitoring and reporting risk associated with their businesses or functions; and
- **Internal Audit** is responsible for independently assessing the effectiveness of risk management processes and practices and for providing timely objective assurance on the control of risk.

NB: It is possible to view risk management as providing pro-active control over risk and internal audit as providing more reactive control over risk.

TOOL 4.2
THE "THREE LINES OF DEFENCE" MODEL

The "three lines of defence" model

One common governance model is the **"three lines of defence" model,** which is diagrammatically illustrated below. This model may assist franchisees by providing a basis to develop and document its risk governance framework.



The **three lines of defence** framework operates as follows:

- staff in the **first line of defence** have direct responsibility for the management and control of risk (i.e. staff and management working within or managing **operational business units** and the **Board**);
- staff in the **second line of defence** co-ordinate, facilitate and oversee the effectiveness and integrity of the risk management framework (i.e. the **risk committee** and **risk management division**); and
- staff in the **third line of defence** provide independent assurance and challenge across all business functions in respect of the integrity and effectiveness of the risk management framework (i.e. **internal and external audit**).

LLOYD'S

TOOL 4.3
EXAMPLE ROLES AND RESPONSIBILITIES

The following table provides a breakdown of **typical roles and associated responsibilities** which could be used by an organisation when developing their risk governance model.

Role	Responsibilities
The Board	• sets business strategy • sets risk appetite • agrees risk policy, in alignment with strategy • sets governance structure • sets risk management framework • makes business decisions • delegates actions • defines the methodology by which risk management is reviewed (e.g. reports, annual assessment) • obtains assurance on risk management effectiveness and compliance with set risk policy • reports to stakeholders on risk management • approves public disclosures
Risk committee	The risk committee is a sub-committee of the board and oversees the development, implementation and maintenance of risk management across the business as follows: • proposes the approach to risk management • proposes risk policies • proposes risk appetite • monitors compliance with risk policies • monitors the adequacy of controls • monitors the overall risk profile against appetite • escalates issues • reports to Board • oversight and challenge of risk management • does not make decisions (may do so where delegated authority)

Role	Responsibilities
Chief Risk Officer	The Chief Risk Officer leads the development and implementation of risk management across the business (more detailed terms of reference attached): • develops risk management strategy, principles, framework and policy • implements appropriate risk management processes and methodologies • advises and coaches management and business units on risk management • monitors the application and effectiveness of risk management processes • coordinates appropriate and timely delivery of risk management information
Risk management function	The risk management function leads the development and implementation of risk management across the business. The risk management function: • drafts risk policies and risk management standards • develops and implements the risk framework • develops and distributes tools, techniques, methodologies, common risk language, risk framework, analysis, reporting, communication and training • coordination, aggregation, facilitation and enabling function • monitors the overall risk profile, including accumulations of risk, trends, and risks from internal and external market changes • escalates high priority issues to senior management and Board • collates, challenges and reports on aggregate risk profile, control effectiveness and actions taken to risk committee and Board
Business units	• own risks and controls • assess risks and the effectiveness of controls in line with documented risk policy • design, operate and monitor a suitable system of control • manage and review risks as part of day to day business activity
Audit committee	The audit committee is a sub-committee of the Board, which: • monitors and reviews the activities of internal audit, ensuring that internal audit has the necessary resources and access to information to perform its role • ensures that the financial activities of the business are subject to independent review and external audit, appointing the external auditor and monitoring the independence, objectivity, effectiveness and cost effectiveness of the audit • reviews the half-year and annual financial statements and other formal announcements on financial performance and principal regulatory returns before submission to the Board

Role	Responsibilities
Internal audit	Provides assurance to the Board that risk is being managed and that controls are working effectively. Internal audit: • monitors effectiveness of the risk management processes • tests controls • validates risk information and risk reporting • identifies corrective actions • liaises with the risk management department • reports to the audit committee and Board
External audit	Reports on risk and control process failings, including corporate governance weaknesses, if identified during the external audit

LLOYD'S

TOOL 4.4
EXAMPLE ROLES OF A CHIEF RISK OFFICER

More and more organisations are introducing a **Chief Risk Officer** role into their governance structures. The Chief Risk Officer typically has overall leadership of risk management across a business and may typically undertake the following roles:

Example roles for a Chief Risk Officer

Development of risk management strategy, principles, framework and policy

- provides overall leadership, vision and direction for risk management throughout the business
- develops company risk management strategy and framework
- instils risk management principles and raises awareness of risk management
- develops risk management policy statements
- develops a commercial and cost effective "business wide approach" to risk management
- guides the risk committee and Board through the formulation of risk strategy, appetite, policies, delegated authorities and limit structures
- develops a culture of managed risk taking

Implementation of appropriate risk management processes and methodologies

- leads development, selection, implementation, validation and maintenance of processes, procedures and systems for risk management
- develops, with Finance, processes for determining, allocating, monitoring and managing capital requirements and measuring risk adjusted performance
- manages the activities of the risk management function, ensuring adequacy of resource
- coordination of different risk management areas
- preparation of manuals / guidelines
- reviewing risk management standards / guidelines
- formation and support of risk management committee structures and processes
- design of self assessment procedures for business units
- setting up a committee to look at the wording of contracts
- developing corporate emergency procedures, developing health and safety standards and performance improvement programmes

Advice and coaching to management and business units on risk management

- informed and objective challenge to executive line management on risk management
- techniques for risk identification
- change management
- addressing HR risks
- investment proposals
- contractual terms and conditions (warranties, indemnities, insurance aspects)
- disaster recovery
- insurance matters, reducing the cost of insurance
- institute training courses
- site surveys / inspections
- build awareness of continuity risks
- encourage preparation of continuity plans

Example roles for a Chief Risk Officer

Monitors the application and effectiveness of risk management processes

- approving risk financing strategies
- ensuring particular risks are being managed
- identifies examples of good practice
- identification of (under managed) risks
- ensuring escalation processes are working
- ensuring identified corrective action is followed through
- take account of internal audit findings over risk management systems and practice
- bench-marking studies

Co-ordinates appropriate and timely delivery of risk management information

- provision of management information on risk management, including loss statistics
- identifies, escalates and oversees the resolution of risk management issues
- reports quarterly to the Board on the management of risk and aggregate risk profile
- produces in-house publications
- advises on sources of good practice and (outside) expertise
- maintains effective working relationships with internal and external stakeholders, including regulators

This table is based on Ward, S. (2001). Exploring the role of the corporate risk manager. *Risk Management: an international journal*, 5(4), 7-23

LLOYD'S

TOOL 4.5
EXAMPLE RISK GOVERNANCE PRINCIPLES

The following principles may assist organisations when considering what **risk governance principles** to adopt for their organisation.

Example Board commitments

The Board is committed to achieving its goals and will seek to:

- operate in an open, constructive and flexible manner;
- take into account the views of individual stakeholders;
- encourage regular dialogue and consultation with stakeholders and with the market associations. The Board will develop effective working arrangements with the market associations to achieve this;
- adopt a cost effective, commercial and efficient approach;
- actively support market initiatives relating to business process reform, such as LMP, leading to improved service standards and reduced costs;
- allocate charges, as far as possible, on an activity based cost basis;
- deliver high levels of service to policyholders and develop a performance culture amongst employees;
- rationalise the frequency and manner in which data and information is collected, from brokers and policyholders, and streamline the number of IT systems for increased efficiency;
- protect the confidentiality of commercially sensitive information provided to it by customers and stakeholders in accordance with published guidelines; and
- assist underwriters to manage underperforming business lines and improve their performance but take firm action where an underwriter is unable or unwilling to respond to that approach.

Combined code commitments

The combined code sets out a number of principles of good governance and best practice within the following recommendations:

- **Directors** – listed companies should have an effective Board with clear division of duties between Chairman and Chief Executive Officer, a balance of executive and non-executive directors, with relevant information, and a formal, transparent appointment process with directors submitting themselves regularly for re-election;
- **Directors' remuneration** – there should be appropriate levels of remuneration with a formal and transparent process for fixing said remuneration and details in the company's annual report;
- **Relations with shareholders** – companies need to enter into a dialogue with institutional shareholders and use the annual general meeting to communicate with private investors;
- **Accountability and audit** – the company should present a balanced and understandable assessment of its position, maintain a sound system of internal control and establish formal and transparent arrangements for the review of financial reporting and internal control principles; and

- **Institutional investors** – investors should make considered use of their vote, be ready to enter into a dialogue with companies and should give due weight to all factors when evaluating a company's governance arrangements.

Companies listed on the London Stock Exchange have to report on how they apply the principles of the code and either confirm that they have complied throughout the financial year with the code provisions or, where they do not, provide an explanation.

Example employee commitments

The Board expects employees to operate in accordance with the following principles:

- deal with customers, stakeholders and other employees in an open, constructive and cooperative manner;
- protect:
    - the brand and reputation of the business;
    - the security rating;
    - the security behind the organisation's insurance policies including the funds at Lloyd's; and
    - Lloyd's licences and authorisations to conduct insurance business in the UK and overseas.
- deliver high levels of service to brokers and policyholders in accordance with set service standards, systems and protocols;
- prepare high quality business plans, in accordance with the relevant guidelines, with a view to achieving the Board's long term profitability targets;
- operate and underwrite in accordance with agreed business plans;
- accurately report syndicate performance in a timely manner and understand the factors which may have affected syndicate performance;
- notify senior management, in good time, of any matters which may have a material effect on the business, managed syndicates or on Lloyd's as a whole; and
- protect the confidentiality of information, not to be disclosed, throughout the business.

SECTION BREAK

LLOYD'S

RISK POLICY

SECTION 5

TOOLS

Tool 5.1 – Example risk policy template

Tool 5.2 – Example comprehensive risk policy

Tool 5.3 – Example corporate social responsibility policy

5 RISK POLICY

What is a risk policy?

A risk policy formally outlines an organisation's **risk management strategy and objectives** for a given risk class and documents the roles, responsibilities, accountabilities and authorities that support the **approach** and **processes** adopted to achieve those objectives. It encompasses the following areas:

- a common risk language, including risk definitions and their categorisation;
- key principles to guide risk based decision-making;
- an articulation of risk appetite illustrating the level of acceptable risk taking (risk limits and thresholds which are derived from appetite, and which may change frequently, would normally be documented in a separate "standard" which relates to the policy); and
- the risk governance framework, including accountabilities, roles and responsibilities for oversight committees (at the management or Board levels), business units, divisions and departments which take risk, the risk policy and supporting functions (e.g. the risk management function) and internal audit (which provides timely, objective assurance about the management and control of risk).

Why is it important?

A risk policy is important as it:

- outlines the organisation's **approach to a specific risk class** for the benefit of all stakeholders; and
- provides for **clear, unambiguous accountability** for the various participants in the overall management of risk.

Practical steps for implementation

All organisations will have some form of risk policies in place. The attached tools help organisations review and enhance the status of those policies, where appropriate, by:

- firstly, providing a health-check or benchmark against which to assess current risk policies; and
- secondly, to identify options for development, by drawing on the attached tools.

Notwithstanding the wide range in size and sophistication of organisations, it is anticipated that risk policies underpin **all risk management activity**, for **all organisations.**

Relevant toolkit contents

Relevant toolkit contents which may be of help include:

- **Tool 5.1 – Example risk policy template:** an example risk policy template with suggested headings and content (illustrated for operational risk);
- **Tool 5.2 – Example comprehensive risk policy:** a comprehensive example of a risk policy statement (illustrated for operational risk). This example draws on each section of the toolkit to form a comprehensive example policy statement; and
- **Tool 5.3 – Example corporate social responsibility policy:** an example CSR policy statement in respect of the marketplace, workplace, environment and the community. This may help organisations to manage their ethical, social and environmental risks which can often be overlooked but which increasingly are a source of reputational risk.

Please note that Lloyd's has developed its own **corporate social responsibility policy**, from which the above tool 5.3 has been derived. For further details, please contact Vicky Mirfin, Manager, Lloyd's Community Affairs.

LLOYD'S

TOOL 5.1
EXAMPLE RISK POLICY TEMPLATE – OPERATIONAL RISK

The following template headings and content may provide a helpful starting point for the development of a risk policy statement, as illustrated for operational risk.

Section 1: Introduction and context

Purpose & scope of policy

- describes what the policy document is intended to achieve and sets out the risk management strategy and objectives
- may include the rationale behind the policy, including any related regulatory requirements for and of the policy

Definition and grouping for operational risk

- the definition of operational risk adopted (i.e. the scope of operational risk)
- any exclusions / additions to the definition of operational risk
- description of the risk group, including the significant risks within the risk group

Interactions and boundaries with other risk classes

- explains the importance of the distinction as well as the interrelationship or correlation between operational risk and other risk groups (insurance, credit, market and liquidity risk) and how this is manifested

Ownership, review and update of policy statement

- ownership of the policy and review / update cycles
- how frequently it is to be reviewed and approved by the Board (i.e. should be at least annually)
- requirement for internal audit review or other compliance / assurance processes

Dispensations

- what happens when the policy is not complied with (i.e. the process for dealing with and approving any exceptions to the policy)
- what criteria should be used for reporting any instances of non-compliance to the Board

Unauthorised deviations from policy statement

- describes the process for escalating unauthorised deviations from the policy statement to management, the Board, the risk management function and internal audit

Section 2: Governance and policy

Policy

- explains that responsibility for compliance with the standards set out in the policy statement lies with relevant staff at all levels throughout the organisation and aims to ensure:
    - the ongoing management and control of operational risk is in accordance with “good practice” principles; and
    - compliance with all relevant legislation, regulatory requirements and appropriate codes of practice / conduct.

Objectives

- sets out the objectives of operational risk management
- explains how operational risk will be embedded within the organisational operating culture
- explains the management of potential and actual risk exposures and incidents in line with good practice principles

Risk appetite

- the organisation’s expression of risk appetite based on its capacity to bear or take on risk
- explains the qualitative and quantitative statements, limits and thresholds, or key risk indicators used in the expression of risk appetite

Guiding principles

- basic assumptions made and principles to be followed by the organisation with respect to operational risk management

Ethical / behavioural conduct of business

- ethical behaviour which the organisation expects in respect of operational risk issues

Operational risk governance and responsibilities

- explanation of the risk governance structure, e.g. via a structure diagram (for example, the 3 lines of defence model), key responsibilities table, role profiles and job objectives

Section 3: Execution

Operational risk management methodologies (note that all of the following are required for a robust operational risk management framework)

Risk and control self-assessment (RCSA)

- methodology and approach, with reference to practical guidance / templates / rating for the risk and control self assessment exercise

Internal loss data

- tracking of loss data, including actual losses, near misses and potential losses, in accordance with risk policy and management reporting requirements

Key risk indicators (KRIs)

- key attributes of and purpose for KRI monitoring and reporting
- explanation of the monitoring and reporting of KRIs

Stress and scenario testing

- performing stress / scenario testing on severe unexpected events or tail losses in order to:
    - aid testing of the financial and non financial impact of potential operational risk exposures; and
    - ascertain the related responsiveness of the existing control environment to the scenarios.

External operational risk data

- approach to the use of external data
- limitations of available existing external data

Section 4: Management information

Management information

- routine reporting
- frequency of reporting
- exception reporting
- document retention standards

Economic capital

- explains the link between operational risk management and the capital assessed to cushion against unexpected losses arising from operational risk

Disclosure

- explains the basic standards to be adhered to with respect to operational risk management

TOOL 5.2
EXAMPLE COMPREHENSIVE RISK POLICY – OPERATIONAL RISK

ABC Operational Risk Policy

This illustrative comprehensive operational risk policy statement may provide a helpful point of reference when **developing or reviewing** your own operational risk policy.

It is vital, however, that policy statements are **tailored** to each organisation's risk definition, categorisation, principles, appetite and governance arrangements.

***ABC* Managing Agent Ltd**
Operational Risk Policy Statement
Version 1.0

June 2005

Document history

Created by

Name	Date	Department / role	Version
A. N. Other	10/06/05	ORM / Manager	1.0

Reviewers

Name	Date	Department / role	Version

Sign off

Name	Date	Department / role	Version

Distribution list

All *ABC* staff

Introduction

This policy statement outlines *ABC*'s **strategy** and **objectives** for operational risk management and the **approach** and **processes** by which *ABC* achieves those objectives.

The policy takes account of and is **consistent** with operational risk policy guidance issued by the FSA in the Integrated Prudential Sourcebook: Prudential Systems and Controls – Operational Risk (PRU 6.1).

This policy has been approved by the Board of Directors and is applicable to **all business units and functional areas**, including the underwriting, claims and reserving teams, finance, risk management, legal services, personnel, operations and compliance divisions of *ABC*. All **managers and staff** are expected to abide by the policies and rules set out in this policy statement.

Definition and categorisation

ABC has adopted the following **definition** of operational risk:

> **"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"**

Operational risk presents significant exposures to *ABC,* including potentially **high severity low frequency losses**, such as catastrophic losses, which may threaten its survival and capital adequacy.

ABC has established a **common risk language** to provide a consistent framework for the definition and categorisation of risk and the organisation of its risk management activities.

Within this framework*, ABC* **categorises** operational risk into seven sub-categories, as summarised below. *ABC's* detailed risk categorisation is set out in the ***ABC* risk register.**

Level 1	Level 2
People	• manual input errors – slip, premium & claims entry • errors in the use of models / systems – rating, reserving & capital • inadequate management oversight – underwriting & claims • inadequate management decision making • inadequate staff training • inadequate staffing levels • processes / procedures not followed • lack of escalation to management • internal theft or fraud • recruitment screening failure • miscommunication – internal / external

Level 1	Level 2
Processes	• inadequate processing control – premiums / claims • inadequate control over outsourced activities – IT / finance • failure of outsource provider • inadequate segregation of duties • inaccurate / incomplete management information • inadequate supporting software • inadequate / inappropriate polices • inaccurate / incomplete trading data • failure in corporate governance
Systems	• hardware failure • software failure • network / telecommunications failure • third party IT provider failure • inadequate virus protection • inadequate system security / information management • insufficient processing capacity • insufficient / untested disaster recovery processes • inadequate system upgrade management
External events	• natural disaster / catastrophic loss • man made disaster / catastrophic loss • third party / supplier failure • external theft or fraud • external breach of system security • terrorist attack / denial of access to building • power outage
Reputational	• breach of overseas licences – by coverholder • US or other overseas regulatory action • identify theft / abuse of brand • rating downgrade • corruption, intimidation or coercion of staff • failure to comply with UK legislation • regulatory breach, fine, bad press
Legal	• insurance & reinsurance policy dispute • dispute over service level agreements • public and employers' liability • breach of fiduciary duty • change in law / failure to interpret law correctly
Strategic	• adverse insurance cycle developments • technological developments in trading platform and distribution • adverse political developments • adverse developments in the wider economy • failure to manage change • failure to deliver business strategy

Boundaries with other risk classes

ABC determines the categorisation of a risk event on the basis of its **primary cause.**

ABC therefore considers a loss event to be an **operational risk event** if it arose as a result of inadequate or failed internal processes, people and systems or from external events.

Ownership, review and update

ABC's **risk management function** and **risk committee** is responsible for the ownership of and proposed revisions to this operational risk policy statement.

The *ABC* **Board** reviews and approves the policy statement on an annual basis in order to ensure that the policy remains aligned with *ABC's* overall **business** and **risk management objectives,** current or future planned **changes in the operations** of *ABC* and the **annual business plan.**

On an ongoing basis, **internal audit** provides timely, objective assurance regarding the continuing appropriateness of the policy statement and the adequacy of compliance with the policy statement.

Dispensations for non-compliance

Dispensations for **non-compliance** with this policy statement must be **documented** and **approved by the risk committee** (operating under delegated authority from the Board). Such dispensations are **reported to the Board** at its quarterly board meetings.

Dispensations for **significant non-compliance** with this policy statement must receive **prior Board approval.**

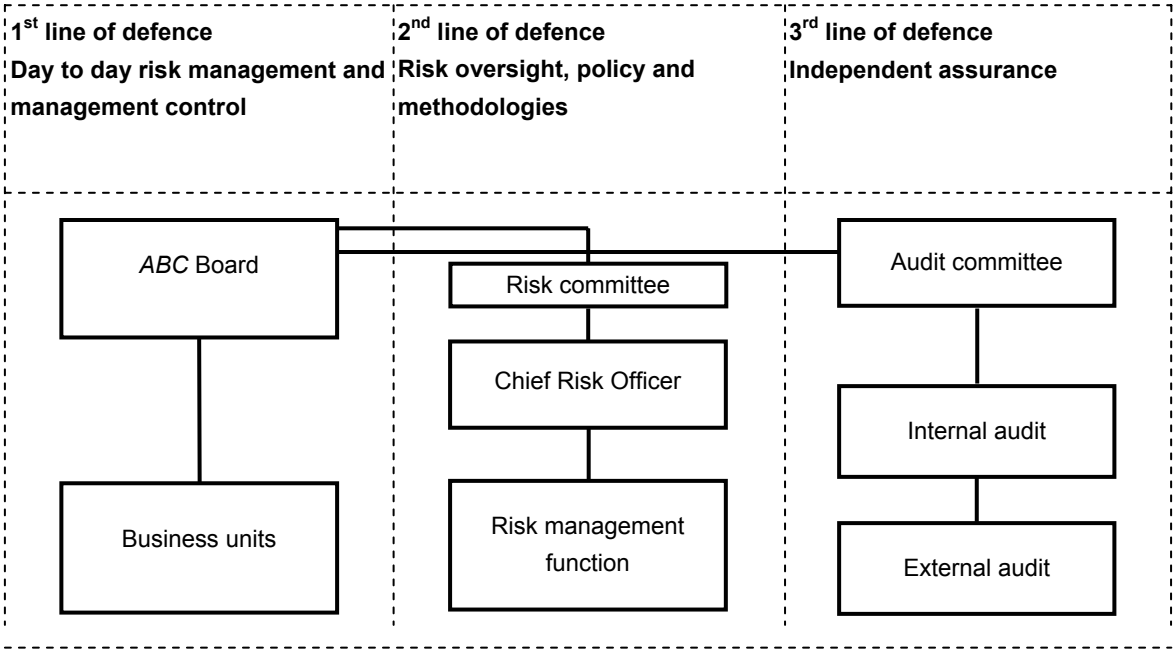
Unauthorised deviation

All **unauthorised deviations** from the standards set out in this policy statement are reported to the risk committee, risk management function and the Board.

Depending on the **nature** and **severity** of non-compliance, the issue may be considered to be a matter of disciplinary conduct.

Governance

ABC has adopted a **"three lines of defence"** governance framework, as illustrated and explained below:



The **three lines of defence** framework operates as follows:

- staff in the **first line of defence** have direct responsibility for the management and control of operational risk (i.e. staff and management working within or managing **operational business units** and the **Board**);
- staff in the **second line of defence** co-ordinate, facilitate and oversee the effectiveness and integrity of *ABC's* operational risk management framework (i.e. the **risk committee** and **risk management division**); and
- staff in the **third line of defence** provide independent assurance and challenge across all business functions in respect of the integrity and effectiveness of the operational risk management framework (i.e. **internal and external audit**).

Roles and responsibilities for each of these functions and parties are described in detail below.

Stakeholder	Roles and responsibilities
The Board	• sets business strategy • sets risk appetite • agrees risk policy, in alignment with strategy • sets governance structure • sets risk management framework • makes business decisions • delegates actions • defines the methodology by which risk management is reviewed • obtains assurance on risk management effectiveness & compliance with set risk policy • reports to stakeholders on risk management • approves public disclosures

Stakeholder	Roles and responsibilities
Risk committee	• proposes the approach to risk management • proposes risk policies • proposes risk appetite • monitors compliance with risk policies • monitors the adequacy of controls • monitors the overall risk profile against appetite • escalates issues • reports to Board of Directors • oversight and challenge of risk management • does not make decisions (unless delegated authority)
Chief Risk Officer	• develops risk management strategy, principles, framework and policy • implements appropriate risk management processes and methodologies • advises and coaches management and business units on risk management • monitors the application and effectiveness of risk management processes • co-ordinates appropriate and timely delivery of risk management information
Risk management function	• drafts risk policies • defines risk management standards • develops and distributes tools, techniques, methodologies, common risk language, risk framework, analysis, reporting, communication and training • coordination, aggregation, facilitation and enabling function • reports on aggregate risk profile, control effectiveness and corrective actions taken
Business units	• own business risks and controls • identify, assess and accept risks – underwriting • design, operate and monitor suitable internal controls • manage and review risks • follow policy for risk management • operate the business within set risk appetite & tolerances
Audit committee	• monitors and reviews the activities of internal audit, ensuring that internal audit has the necessary resources and access to information to perform its role • ensures that the financial activities of the business are subject to independent review and external audit, appointing the external auditor and monitoring the independence, objectivity, effectiveness and cost effectiveness of the audit • reviews the half-year and annual financial statements and other formal announcements on financial performance and principal regulatory returns before submission to the Board

Stakeholder	Roles and responsibilities
Internal audit	• monitors effectiveness of risk management processes • tests controls • validates risk information and risk reporting • identifies corrective actions • liases with risk management department • reports to the audit committee and Board
External audit	• reports on risk and control process failings, including corporate governance weaknesses, if identified during the external audit

Objectives

ABC's **objectives for operational risk management** are as follows:

- all **significant operational risks** are identified, measured, assessed, prioritised, managed, monitored and treated in a consistent and effective manner across the organisation;
- appropriate and reliable risk management tools (including key risk indicators, loss databases, risk and control self assessments and stress and scenario testing) are deployed to **support operational risk management**, particularly **management reporting, decision making** and **capital assessment**;
- all directors, management and staff are **accountable** for managing operational risk in line with the roles and responsibilities set out in this policy;
- **compliance** with all relevant legislation, regulatory requirements, guidance and codes of practice; and
- key stakeholders receive timely, dependable **assurance** that the organisation is managing the significant operational risks to its business.

Guiding principles

ABC has adopted the following **principles to guide decision making** throughout the organisation:

- *ABC* conducts its business with **integrity** and observes high standards of market conduct;
- *ABC* conducts its business with **due skill, care and diligence**;
- *ABC* **organises and controls its affairs** responsibly and effectively with sound risk management systems and procedures.
- *ABC* treats its **policyholders** fairly and communicates with them in a way which is clear, fair and not misleading;
- *ABC* manages **conflicts of interest** fairly, both between itself and its policyholders and between policyholders;
- *ABC* **manages operational risk** in a cost effective manner, subject to compliance with applicable legislation and regulatory requirements and effective management of operational risk exposures;
- *ABC's* **staff** all play an active role in the management of operational risk; and
- *ABC* **deals with its regulators** and other supervisory bodies in an open and co-operative way, making full and open disclosure of operational risk events where appropriate.

Risk appetite

The **Board** articulates **statements** of operational risk appetite, namely the amount of risk that is acceptable and/or unacceptable to *ABC*:

- divisional heads and business unit managers **interpret and cascade down** more detailed expressions of appetite / limits for their division / business function; and
- underwriting divisions / business functions **interpret, apply and operate within** these more detailed statements of appetite, with guidance from the risk management function.

ABC articulates its risk appetite via a combination of **qualitative statements**; **limits and thresholds** – above which specific requirements are identified for escalation and approval; and **key risk indicators** – with identified tolerance levels and escalation points. The Board's high level statement of operational risk appetite is set out below.

Operational risk class	***ABC* Board level articulation**
People	• *ABC* employs sufficient, suitably skilled and experienced staff • staff roles and responsibilities are clearly defined • staff performance is reviewed and training needs met • *ABC* is an equal opportunities employer • *ABC* has zero appetite for fraudulent activity • potential conflicts of interest are avoided and/or disclosed

Operational risk class	*ABC* Board level articulation
Processes	• *ABC* has a low operational risk appetite for process failure • zero tolerance of business outside plan and RI programme • zero tolerance for high priority internal audit / regulator issues • no single operational risk loss to exceed £50,000 / year • annual aggregate operational risk losses not to exceed £100,000 / year • *ABC* is Turnbull compliant
Systems	• no more than 2 IT system outages / month for more than 1 hour • no more than 1 IT virus caused outage / month for more than 1 hour • zero tolerance of IT & data security breaches • effective and tested DRP to be in place
External events	• tolerate up to 20% gross RDS exposure against capacity • tolerate up to 5% final net RDS exposure against capacity • very low appetite for business outages • effective and tested BCP arrangements in place • responding to outages 30 minutes to 3 months in duration

Reputational	• very low appetite for reputational risk
	• *ABC* takes immediate action to resolve:
	  • policyholder complaints
	  • UK and overseas regulator concerns
	  • high priority internal and external audit concerns
	• *ABC* actively contributes to the community

Legal	• *ABC* seeks contract certainty prior to written risks incepting • zero appetite for legal action against the organisation • *ABC* complies with all relevant legislation

Strategic	• *ABC* actively monitors its business strategy against:
	  • insurance cycle and class rating changes
	  • political, regulatory and economic environment changes
	• *ABC* actively manages change

Operational risk management methodologies

In order to meet its operational risk management objectives, **each business function** within *ABC* is required to identify, assess, measure and control its operational risk in line with the policy set by the Board.

The following **tools and techniques** are used by each business unit, in line with the nature and scale of the business risks.

a) Risk and control self assessment (RCSA)

RCSA is a key component of *ABC*'s operational risk framework and involves, on a quarterly basis, each business unit within *ABC* proactively identifying and assessing its significant operational risks and the controls in place to manage those risks.

RCSA is intended to **add value** to *ABC* by providing a prioritised assessment of the significant risks and controls to its business objectives, which:

- draws on the input of management and staff across *ABC*;
- draws on the output of loss event data, key risk indicators and stress and scenario testing (see below);
- is updated quarterly, by means of a series of assessment workshops, meetings or questionnaires;
- focuses on the root causes of risk, rather than just its effects;
- draws on the *ABC* common risk language and categorisation for risk in order to analyse and aggregate the results of the self assessment; and
- allocates ownership or accountability to the key risks and related controls to managers and staff best placed to manage them.

The results are **reported** as part of quarterly management reporting, collated by the risk management function.

b) Internal loss data

The tracking of **internal loss event data** is a key component of *ABC*'s operational risk framework. Internal loss events are categorised into **actual loss, potential loss and near miss** events as follows:

- **actual loss** – an incident that has resulted in a financial loss;
- **potential loss** – an incident that has been discovered, that may or may not ultimately result in a financial loss; and
- **near miss** – an incident that was discovered through means other than normal operating practices and through good fortune or focused management action resulted in no loss or a gain.

ABC has applied the following **thresholds** for loss event recording:

Event type	Reporting to risk committee	Threshold amount
Actual loss	Monthly	> £10,000
Potential loss	Monthly	> £50,000
Near miss	Monthly	> £25,000
Any	Immediately	> £100,000

Sources of loss events may arise from:

- **new risks** to *ABC*; and
- a **lack of control or control failure** surrounding a known risk.

In either case, loss events should be fed into the next self assessment exercise to identify any **corrective action** which may be necessary.

c) Key risk indicators (KRIs)

KRIs are measures which track the risk profile of *ABC*.

Each business unit within *ABC* develops and monitors key risk indicators for its significant risks, which:

- target key operational risk exposures for the business unit;
- enable management of the underlying causes of risk exposures;
- use thresholds aligned to *ABC*'s risk appetite and enable risk based decision making;
- are monitored with a frequency that matches the nature of the risks;
- compliment the self assessment and loss event collection processes; and
- are reported as part of monthly management reporting.

d) Stress and scenario testing

ABC analyses the impact of unlikely, but not impossible events by means of **scenario analysis,** which enable *ABC* to gain a better understanding of the risks that it faces under extreme conditions:

- scenario analysis is the process of evaluating the impact of specified scenarios on the financial position of *ABC*;
- both **historical and hypothetical** events are tested; and
- scenario analyses are conducted **at least annually**, or more often if there is a change in *ABC*'s operations or operating environment.

Scenario analysis results are also an important input to the determination of *ABC's* **regulatory and economic capital** for operational risk in *ABC*'s business (see section Capital assessment).

e) External loss data

An **external loss database** potentially provides an indication of the size and spread of losses experienced by other insurance companies and thus a wider frame of reference when assessing potential exposures as part of the quarterly self assessment exercise.

Each business unit is therefore encouraged to collect and periodically monitor **relevant external loss data.**

Management information

ABC's **risk management function** oversees the collation, aggregation, and analysis of business unit management information and challenges it prior to submission to the risk committee and the Board.

ABC requires **monthly management information** from each business unit in respect of:

- loss events, near misses and potential losses;
- key risk indicators;
- risk profile;
- new or significantly changed risk exposures;
- key risks with significant control weaknesses;
- deviations from the risk policy; and
- overdue agreed action for treating significant risks.

ABC requires **immediate escalation** to the risk committee and Board in the following instances:

- **unauthorised deviations** from any of the standards set out in this risk policy statement; and
- likely or actual **breaches of thresholds** agreed by the risk committee, *ABC* Board and risk management function.

Capital assessment

ABC uses scenario analysis as an important input to the determination of the amount of regulatory and economic **capital** required to support the level of operational risk in its business:

- the *ABC* **risk categorisation** is initially mapped to the risk groups defined by the FSA for the purposes of the capital assessment;
- a reasonable set of **realistically possible severe events** is then identified, drawing on the *ABC* risk framework, risk register, executive management and subject matter experts from relevant business units;
- **the impact and probability** of the various risk scenarios is then assessed, including the direct and indirect effects and the impact of control failures, via facilitated assessment workshops;
- **wider "ripple" or knock on effects** are then considered when quantifying the overall effects of each risk scenario (e.g. a large loss event which leads to reinsurer failure);
- scenario test **results are then aggregated** for operational risk in order to deal with correlation effects between the scenarios, by means of a **correlation matrix,** i.e.:
    - each risk scenario test is considered and quantified in isolation and a correlation matrix is then specified between scenarios (for example, senior management judgementally allocating a high/medium/low correlation). The results are then aggregated to provide input to determining an overall capital figure for operational risk; and
    - as a separate exercise, the overall results for each risk group are aggregated via a second correlation matrix, to help derive an overall capital assessment number.

The capital assessment methodology is addressed in more detail in *ABC's* Individual Capital Assessment 2005.

LLOYD'S

TOOL 5.3
EXAMPLE CORPORATE SOCIAL RESPONSIBILITY POLICY

ABC corporate social responsibility policy

The following illustrative corporate social responsibility (CSR) policy statements provide a point of reference when **developing or reviewing** your own CSR policy. These policy statements (marketplace, workplace, environment and community policies) may help organisations to manage their ethical, social and environmental risks which can often be overlooked, but which increasingly are a source of reputational risk. It is vital, however, that policy statements are **tailored** to each organisation.

Marketplace policy

ABC is **regulated by the FSA** and, as such, must comply with a variety of FSA requirements. *ABC* seeks to ensure that these are adhered to within its business. All employees within *ABC* are expected to act in a manner which is consistent with the FSA's Principles for Business (see below).

1	**Integrity**	A firm must conduct its business with integrity
2	**Skill, care and diligence**	A firm must conduct its business with due skill, care and diligence
3	**Management and control**	A firm must take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems
4	**Financial prudence**	A firm must maintain adequate financial resources
5	**Market conduct**	A firm must observe proper standards of market conduct
6	**Customers' interests**	A firm must pay due regard to the interests of its customers and treat them fairly
7	**Communications with clients**	A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading
8	**Conflicts of interest**	A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client
9	**Customers: relationships of trust**	A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment
10	**Clients' assets**	A firm must arrange adequate protection for clients' assets when it is responsible for them
11	**Relations with regulators**	A firm must deal with its regulators in an open and co-operative way, and must disclose to the FSA appropriately anything relating to the firm of which the FSA would reasonably expect notice

ABC also plays a role in ensuring full compliance with all relevant laws and regulations. Within *ABC* there is active promotion of awareness and understanding of a variety of policies aimed at protecting the interests of our customers and monitoring of compliance with these policies. It is expected that all business units would adopt measures to ensure full compliance with all relevant laws and regulations.

The areas covered by these policies include:

- client confidentiality and handling of sensitive information (Data Protection Act);
- promotional communications to ensure they are fair, clear and not misleading;
- whistle blowing (reporting on concerns relating to possible wrongdoing or malpractice);
- financial crime (money laundering, advance fee fraud, suspicious transactions); and
- conflicts of interest (accepting and giving of gifts or benefits).

ABC monitors and deals with complaints concerning insurance policies to seek a reduction of such complaints.

As a responsible organisation, *ABC* strives for clear communications with all its customers and is committed to providing a more financially intelligible and transparent market. To this end we are moving towards annual accounting which will be in place during 2005.

Workplace policy

ABC recognises that the ultimate source of value of the organisation lies with its employees. *ABC* is committed to treating its employees with fairness, respect and integrity.

ABC has in place a set of policies relating to the treatment of its employees. They cover the following areas:

Recruitment

ABC's recruitment policy is to ensure we recruit the highest quality people having regard to both immediate and future needs. *ABC* will recruit from within the organisation where possible and will give fair consideration to all applicants regardless of ethnic origin, religion, nationality, sex, sexual orientation, age or marital status. *ABC* will also ensure full and fair consideration is given to applications from disabled people having regard to ability rather than disability. We do not just avoid discrimination as required by law but adopt policies and practices that treat as irrelevant all factors which do not genuinely affect a person's ability to undertake a particular job.

Remuneration

ABC is committed to rewarding its people fairly and to providing remuneration which will attract, retain and motivate the high calibre people the business requires. *ABC* recognises that employees all have different benefit needs and priorities at different stages in their lives and careers and provides a flexible benefits programme with this in mind. *ABC's* remuneration policy is based on providing a package of rewards (salary plus benefits) which is competitive, fair and flexible. The remuneration policy is regularly monitored by means of external remuneration surveys. Decisions on remuneration are based on rewards for performance and not a position in a hierarchy. *ABC* ensures employees understand the criteria by which rewards are determined and reviewed.

Training and development

ABC encourages all employees to improve their skills and expertise and develop to their full potential, thereby raising performance and the level of professional competence throughout the organisation. *ABC* views learning as a continuous process and therefore emphasises the importance of each member of staff engaging in some form of relevant development each year. *ABC* Training Programme exists to promote and recommend programmes of training and education to support the improvement of professional standards throughout the company. Bonus payments are awarded to employees who successfully complete relevant professional examinations.

Equal opportunities and diversity

ABC takes steps to ensure that all applicants and employees receive equal treatment regardless of sex, sexual orientation, race, colour, ethnic or national origins, religion, trade union membership, age, marital status or disability. In *ABC's* view the only criteria in selecting employees for recruitment, promotion and development are competence and performance. *ABC* is committed to encouraging a diverse workforce, recognising that everyone is different and that these differences result in a variety of valuable perspectives and experiences.

Work / life balance

ABC supports the need for employees to strike a balance between working life and home life and respects its employees' commitments outside of work. *ABC* values an employee for results rather than hours worked and operates a discretionary flexible working policy (see below). *ABC* also supports employees wanting to take time to do voluntary work with up to x days paid leave a year available for employees.

Flexible working practices

ABC encourages flexible working and will positively consider requests from any employee. Those with 26 weeks' continuous employment who are responsible for children aged under 6 or disabled children under 18 have a legal right to request flexible working. The flexible arrangements that will be considered are part-time and home working, job share arrangements and early or late starts with correspondingly early or late finishes. The aim is to provide maximum flexibility consistent with achieving objectives and meeting the needs of the business.

Communications and employee involvement

ABC actively promotes the understanding and involvement of employees in its business objectives by a variety of means. Currently these include: CEO briefings for all employees at open forums; regular team meetings to keep employees informed and to provide feedback to management; and an Intranet which provides information rapidly to all employees and also for employees to communicate directly with the CEO.

Job security

ABC is sympathetic to the need for job security amongst its workforce. *ABC's* policy is to avoid redundancy occurring whenever possible and to make employees redundant only when their position no longer exists and redeployment procedures have been followed without success. Where redundancy is inevitable, *ABC* will give employees as much warning as possible.

Grievances

The aim of the *ABC* grievance procedure is to resolve grievances quickly and informally where possible. Employees with any cause for concern or complaint are encouraged to raise the issue, particularly in the case of alleged discrimination or harassment on the grounds of race, sex, disability or otherwise.

Health and safety

ABC is committed to meeting all health and safety requirements and providing employees with a safe and healthy working environment. *ABC* provides information and training required for this purpose. *ABC* also provide free medical insurance for all employees and a programme of free health screening is available for all employees.

ABC fully supports the principles set out in the Universal Declaration of Human Rights and respects the dignity and rights of each individual who works for us and with us. *ABC* views observance of these principles as a basic requisite for a company which seeks to conduct its business in a socially responsible manner. The policies outlined above demonstrate that *ABC* not only complies with the relevant principles but exceeds them.

Environment policy

ABC recognises that its business activities have an impact on the environment and that it has a clear responsibility to manage this impact as effectively as possible. The aim of *ABC's* environment policy is to provide guidance for business units so that they are able to protect and improve the environment locally. In turn, this will impact on environmental conditions nationally and indeed globally in line with *ABC's* commitment to good environmental practice and innovation.

The policy addresses a number of *ABC's* activities that impact on the environment:

Energy

ABC is committed to reduce the use of energy, water and other natural resources and implement regular maintenance and improvement programs to ensure that the buildings operate at their optimal environmental efficiency.

Waste

The reduction of waste is a key objective. Where possible, waste materials are recycled and separated for collection by specialist organisations. Where waste cannot be recycled, the disposal is in strict compliance with the law and according to the best practicable environmental option.

Built environment

The management of buildings is best engineering practice to minimise any risks to human health and to the environment. *ABC's* property services maintain clean drinkable water and the supply of air to the offices to a high standard, while minimising any hazardous effects from emissions or materials.

Catering

Catering services ensure that food is produced within the statutory food hygiene regulations and that the storage of food meets the mandatory requirements. Caterers take all reasonable precautions to ensure that none of their food contains genetically modified ingredients. Where possible and with regard to economic constraints, caterers source their products from environmentally caring foodstuffs such as tuna fish caught in dolphin friendly nets, free range eggs, etc.

Procurement

Suppliers are encouraged to minimise the amount of packaging used on incoming goods and to use biodegradable or recyclable materials or reusable systems, e.g. recyclable paper. The purchase of timber and timber products are from legal and sustainable managed sources.

Transport

ABC's vehicles comply with emission regulations, and the use of alternative types of low polluting transport as a means of travelling to the building is encouraged.

Communication

Property services will communicate openly with staff, tenants and users of the premises to encourage them to support the environmental policy and involve them in relevant environmental initiatives.

Community policy

ABC takes its responsibilities to the wider community seriously and believes that the success of *ABC* is affected by the health and prosperity of the communities of which it is a part – on a local, national and international level. *ABC* supports wide-ranging charitable involvement in the local community.

ABC is committed to facilitating the community involvement and charitable giving through providing staff resource to co-ordinate the schemes.

Time and Skills

ABC encourages and supports employees to volunteer their time and skills to the local community.

Volunteering involvement is directed through the *ABC* Community Programme, managed and administered by *ABC*. The *ABC* Community Programme is committed to improving the opportunities and environment of local residents.

ABC does this through building strong, long-term relationships with key community partners in the local area and identifying suitable projects where volunteer time can make a positive impact. It manages and supports volunteers to ensure that they are fully briefed, trained and supported in their volunteering.

ABC also supports its own employees wanting to take time to do voluntary work with up to x days paid leave a year available.

Charitable Funding

ABC supports the charitable activity of its employees through a dedicated charity budget which is managed and administered by a charitable committee.

The charitable committee has a specific set of aims which are determined by its members. The members of the committee are drawn from across *ABC*.

ABC also encourages charitable giving amongst its employees by running a payroll giving scheme and covering the administrative costs of that, ensuring that all monies donated go directly to employees' chosen charities.

More information on the *ABC* Community Programme and its charitable donations can be found at *ABC*.com.

SECTION BREAK

LLOYD'S

RISK & CONTROL SELF ASSESSMENT

SECTION 6

TOOLS

Tool 6.1 – Self assessment methodology

Tool 6.2 – Self assessment cycle of activity

Tool 6.3 – Roles and responsibilities

Tool 6.4 – Risk assessment criteria

Tool 6.5 – Control assessment criteria

Tool 6.6 – Risk assessment template

Tool 6.7 – Excel spreadsheet template for risk assessment

Tool 6.8 – Risk assessment output

Tool 6.9 – Risk profile tool

Tool 6.10 – Risk register tool

Tool 6.11 – Underwriting process maps

Tool 6.12 – Binding authority process map

6 RISK & CONTROL SELF ASSESSMENT

What is self assessment?

Self assessment is the process of identifying and assessing risk within a business and evaluating the effectiveness of the controls that are in place to manage these risks.

Self assessment is, therefore, a key component of a robust risk framework. It adds value to management by providing a prioritised assessment of the key risks and controls to the business objectives, which:

- draws on the input of both **management and staff** across the business;
- is updated **at least annually**, but often quarterly, by means of a series of workshops, meetings or questionnaires;
- may be undertaken at either **high or low level**, for example, in respect of projects, processes, business units, functions, or the entire business;
- focuses on the **root causes** of risk, rather than just its effects;
- draws on a **common risk language** and **categorisation** for risk in order to analyse and aggregate the results of the self assessment; and
- **allocates ownership** of the key risks and controls to staff best placed to manage them.

The output of the self assessment will have most meaning if it reflects and highlights the **key business risks** (e.g. the “top 10” risks) which the Senior Management and Directors are worried about, and does not “miss the wood for the trees” through excessive detail.

Why is it important?

The results of self assessment enable management to:

- understand the risks inherent in key business processes and the business objectives;
- evaluate the effectiveness of internal controls;
- assess the risk profile against risk appetite;
- provide internal audit with prioritised areas of work; and
- agree action plans to address risks in excess of the agreed risk appetite (for example, to address identified weaknesses in internal control or risk management).

It is important to note that **rapid change** or **rapid business growth** will have a significant impact on the risk profile of the business.

Some practical steps for implementation

The following guidance is intended to help organisations understand what is involved from a practical standpoint to implement a risk and control self assessment.

- **Staff resource and skills**
    - business units to identify key risks and controls drawing on the skills and experience of various staff
    - individuals to fully understand the nature and impact of, and to take responsibility for specific risks and controls
    - relevant business units and staff, as well as risk and control owners to undertake contol activities
    - risk management function to facilitate the risk and control self assessment process, as well as provide appropriate training / workshops to identify key risks and aid design of appropriate controls
- **Enabling technology**
    - appropriate risk management software (may be Excel, Access or similar, may be bespoke risk management software / product) to assess and record various risks and controls
- **Time**
    - will depend on the size of an organisation, the level of detail, type of risk, etc.
    - time to hold training / familiarisation sessions before any workshops, workshops for appropriate groups, review and analysis of results, playback and amendment, etc.
- **Direct / indirect costs**
    - risk management function for workshops, training, etc.
    - appropriate management and committee time to discuss major risks to the organisation
    - systems capability and support

It is important to remember that risk and control self assessment should be commensurate to the business. As one key risk my be critical to a small organisation, the same risk may be of low impact to a larger firm and should require less focus during a risk and control self assessment.

Relevant toolkit contents

Relevant toolkit contents which may be of help include:

- **Tool 6.1 – Self assessment methodology:** explanations of the various stages necessary within a risk and control self assessment;
- **Tool 6.2 – Self assessment cycle of activity:** an explanation of a typial risk management cycle of activity;
- **Tool 6.3 – Roles and responsibilities:** descriptions and examples of risk and control owners' roles and responsibilities;
- **Tool 6.4 – Risk assessment criteria:** examples of risk assessment scoring systems;
- **Tool 6.5 – Control assessment criteria:** examples of control assessment scoring systems;
- **Tool 6.6 – Risk assessment template:** example ratings tables and guidance and explanations for tool 6.7;
- **Tool 6.7 – Excel spreadsheet template for risk assessment:** example risk assessment template that can be edited and tailored to fit an organisation;
- **Tool 6.8 – Risk assessment output:** an example risk assessment output – a graphic heatmap / matrix;
- **Tool 6.9 – Risk profile tool:** a working risk profile heat map and template tool;
- **Tool 6.10 – Risk register tool:** a generic risk register tool for a small business operation;
- **Tool 6.11 – Underwriting process maps:** example structure and contents of an underwriting process map;
- **Tool 6.12 – Binding authority process map:** details what can go wrong with a binding authority process map.

LLOYD'S

TOOL 6.1
SELF ASSESSMENT METHODOLOGY

There are three main parts to risk & control self assessment ("self assessment"), which are explained below, namely **risk identification, risk assessment** and **control evaluation**.

Risk identification

The initial risk identification stage seeks to identify the sources and root causes of key risks which may affect the business objectives, examples of which may include (for operational risk):

- a change in existing products, processes or key staff;
- development of new products or processes;
- new projects or initiatives; and
- a potential terrorist attack affecting the business premises.

In practical terms, there are several common methods of identifying the key risks:

- **self assessment questionnaires** – this is a bottom-up approach, whereby business managers identify and assess the areas that present most risk to the business as a whole. A standard self assessment questionnaire, with instructions, is provided to the managers and staff best placed to understand the key risks and the results are compiled by the risk management function.
    - Care is needed to achieve consistency in ratings across business units and to manage poor response rates. Regular communication between the business managers and risk management function can help mitigate these weaknesses.
- **process and risk mapping** – this is a systematic and analytical approach which considers the major steps in key business processes as a prompt to identify the major risks. It may be performed at either a high or low level to identify "what can go wrong" with key business processes and results in a visual portrayal of the key risks and controls, for example by means of a flow chart.
    - Care is needed not to exclude risks arising from interdependencies between different processes.
- **facilitated workshops** – a series of workshops is undertaken to consider each business risk category and involves those staff who are best placed to understand the risk category i.e. the company experts for that risk. Relevant material (see below) is circulated in advance for review and, with the aid of a facilitator, a structured discussion takes place in which the group seeks to reach a consensus on the key risks faced by the business.

The methods described above are not mutually exclusive and can be used in combination. The simplest option is a self assessment questionnaire, while a more sophisticated approach is process mapping. In practice, **a combination of a top-down and bottom-up approach to risk identification is needed**, with a combination of both executive management and business unit identification and assessment of the key risks. The nature of risks identified will also differ depending on the business level, i.e. department, division, senior management or board level.

Supporting material which may assist the various risk assessment approaches above includes:

- business goals and objectives;
- business risk appetite;
- process and risk maps;
- loss event data;
- key risk indicator data;
- risk event categorisation and causation analysis;
- prior risk assessments;
- regulatory reports;
- audit reports; and
- prior risk management plans.

Risk assessment

In order to be meaningful to management, identified risks need to be prioritised and considered against the current control environment:

- the use of standard **risk assessment templates** provides a helpful structure for this process, for example, assisting staff to consider the risk descriptions, causes and drivers, different types of risk effects and the most appropriate risk owner;
- **standard criteria for assessment** are helpful in order to aggregate the results across risk classes, for example risks may be assessed for probability and impact;
- risks may be assessed on an **inherent basis** (before the controls are applied), or on a **residual basis** (after controls have been applied). However, in practice it can be difficult to disregard the controls in place in order to make an inherent risk assessment. Whichever approach is adopted, most value will be obtained if:
    - there is clear prioritisation of risks, identifying the more significant risks which should be the focus of board attention; and
    - there is clear identification of those areas where the business is very reliant on the effectiveness of its controls.
- the measurement of inherent and residual risk may also be undertaken by **stress and scenario testing**.

It is important to allocate **ownership of risks** to owners with the authority and resources to manage them effectively. The owner may delegate these tasks to others as and when appropriate, but remains accountable for the completion of the assessments.

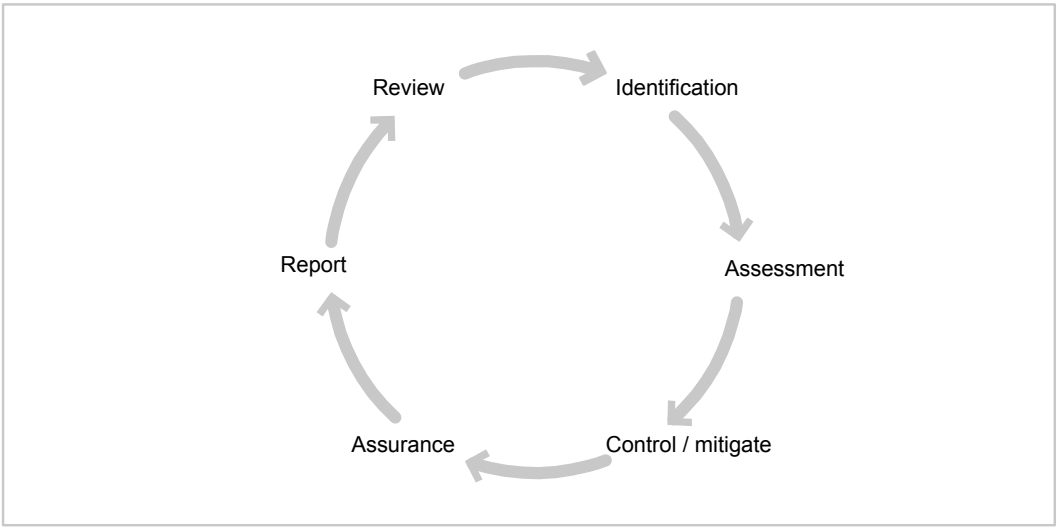
Control evaluation

Once identified and prioritised, the risks may be considered against the current control environment in order to understand the residual **risk profile** of the franchisee:

- the use of standard **control assessment templates** provides helpful structure to this process (see attached risk profile tool with example self assessment template);
- **standard criteria for assessment** are necessary in order to aggregate the results, for example, controls may be assessed for their design and performance;
- controls may be **preventative or detective**, for example, the use of recruitment criteria is a preventative control and quarterly staff reviews are a detective control. It is helpful to consider the balance of preventative and detective controls in place against key risks, given that preventing losses is more effective than detecting them once they have occurred:
    - **front line prevent controls** are high level controls aimed at preventing risk causes from occurring at a very early stage. Examples might include the business planning process, franchise guidelines or admissions criteria;
    - **back stop detect controls** are a less frequent type of detect control and would typically be carried out on a monthly or quarterly basis. Both the issues identified and the remedial action prompted by back stop controls can be relatively serious due to the potential time lag since the risk event. Examples may include various quarterly reviews, reinsurance debtors' return or a review of solvency deficits.
- it is important to allocate **ownership of controls** to capable owners with the authority and resources to manage them effectively. The owner may delegate these tasks to others as and when appropriate, but remains accountable for their completion;
- the resulting **risk profile** of scored residual risks may then be reviewed against the risk appetite and, if the level of risk exposure is higher than the franchisee appetite for any risks, **mitigation strategies** / **action plans** may be developed to reduce the level of risk, for example by reducing the risk exposure (e.g. writing less business through delegated authorities) or by implementing additional controls (e.g. more frequent audit review); and
- the action plans may then be agreed by management and reported against as part of ongoing **management reporting.** This will ensure that the exposure is limited and that there is cost / benefit in the mitigation strategy.

TOOL 6.2
SELF ASSESSMENT CYCLE OF ACTIVITY

The following diagram and supporting text may assist organisations by explaining a **typical risk management cycle of activity.**



The identification, assessment, monitoring and control of risk are continuous processes.

Risk identification – the process begins with the identification of risks and an analysis of the nature of each risk. Everyone within the organisation is involved at this stage of risk management, whether for new or existing risks. The aim is for all employees to be aware of the risks to the business objectives and to be able to highlight any new risks that may be developing over time or changes in existing risk levels such that they are reported and responded to appropriately.

Risk assessment – following on is the assessment of the likely frequency and severity of risks, by means of qualitative or quantitative measurement. This stage of the cycle is likely to involve the participation of the risk owners.

Risk mitigation – the level of each risk must then be transferred or controlled down to a satisfactory level. This stage will not only involve both risk and control owners but also many other departments that are involved in undertaking control activities.

Assurance – once the key business risks have been identified, assessed and are subject to controls throughout various parts of the business, it is important to obtain confirmation that these activities are being performed as expected and that the risk and control scoring is valid. Typically, assurance is provided over risks and controls by resources which are independent of line management, e.g. Internal Audit.

Reporting – relevant information for each key risk should be seen by the "right people at the right time" across the business. This information is most likely to be provided by risk and control owners as they are closest to the issues and should be reported on a regular, timely and consistent basis. Reporting is often consolidated or reviewed by a risk management department and then escalated up to senior management. This will typically include qualitative or quantitative measures of risk, depending on the nature of the risk, for example:

- aggregate RDS property damage exposures are typically reported on a quantitative basis, drawing on a range of commercially available modelling tools; and
- operational risk may be typically reported by means of qualitative and quantitative measures.

TOOL 6.3
ROLES & RESPONSIBILITIES

The following examples may assist organisations when **assigning responsibilities** for **risk and control owners**. It is standard risk management practice that each risk and control should be assigned an owner, with clearly defined responsibilities, including escalation of any significant change in levels of risk.

Risk owner roles and responsibilities

- to identify, regularly maintain and communicate up to date risk information
- ongoing monitoring of risks for changes in their impact or likelihood by:
- communication and liaison with control owners to put in place sufficient control activities appropriate to the nature of the risk;
- identifying and assessing the appropriateness and effectiveness of controls and systems being relied on to manage risk;
- sourcing, collating and analysing relevant data indicating movements in impact from or likelihood of the risk;
- reporting information in a regular and timely manner to the appropriate individuals / forums / committees;
- creating and implementing appropriate action driven by the information;
- escalating / immediate reporting to the appropriate individual / forum / committee of any changes in existing, or new risks as well as significant control failings / weaknesses or events that may arise; and
- ensuring effective implementation of risk management action plans.
- accountability for the effective management of owned risks

Control owner roles and responsibilities

- ensuring effective and efficient control design to manage the impact and likelihood of the risk (in conjunction with the risk owner)
- effective performance of control activities as designed
- provision of information / reporting related to the performance of controls
- sourcing and collating relevant data concerning the performance of controls
- analysis of this data – conversion into indicative information
- reporting information on a regular and timely manner to the risk owner and other individuals or committees
- creating and implementing corrective action driven by the risk information
- escalating / immediate reporting to the risk owner and other individuals or committees of any control weaknesses or breakdowns.

LLOYD'S

TOOL 6.4
RISK ASSESSMENT CRITERIA

Risk impact / probability assessment criteria

One possible **example of risk assessment scoring** is provided below:

- **probability,** also known as **likelihood,** is defined as the likelihood that the risk will occur within the next 12 months based on previous history, management experience and intuition; and
- **impact,** also known as **consequence,** is defined as the level or extent to which the risk would affect the ability of the business to deliver its strategy and objectives if it were to occur.

This approach to the scoring of risks can be difficult due to the non-financial nature of the definitions, however, the assessment involves a judgmental assessment of the most appropriate score. The assessments may be done either at an inherent level (before the application of controls) or residual level (after the application of controls). Adopting an inherent and residual level assessment will provide more insight into the nature of the risks and control strategy adopted.

Example parameters for assessing probability and impact are as follows:

Probability – likelihood that the risk will occur within the next 12 months based on the scoring **1 to 4** and your own management experience and intuition	**1**	< 5% likelihood
	2	5% to 25% likelihood
	3	25% to 50% likelihood
	4	> 50% likelihood
Impact – the level to which the risk would affect the ability of the business to deliver its strategy and objectives based on the scoring **A to D**	**A**	No material impact
	B	Material impact, no significant lasting risk to organisation
	C	Significant risk to organisation
	D	Potential organisation failure

TOOL 6.5
CONTROL ASSESSMENT CRITERIA

Control design / performance assessment criteria

One possible example of control assessment scoring is provided below:

- **design** considers how well the control should work in theory if it is always applied in the way it is intended to work. It might well be that the control is not designed to reduce the risk completely for one of the following reasons:
  - alternative or additional controls address the risk entirely;
  - we are prepared to accept the level of risk;
  - it is uneconomical to mitigate the risk entirely; or
  - the control is poorly designed for the particular risk examined.
- **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. If the performance is not rated as good, an explanation should be given and a decision taken as to whether to accept the level of risk or to re-engineer the control to improve the performance.

Example parameters for assessing design and performance are as follows:

Design – how well the control should work in theory, if it is always applied in the way intended	**Green**	designed to reduce risk entirely
	Yellow	designed to reduce most aspects of risk
	Amber	designed to reduce some area of risk
	Red	very limited or badly designed, even where used correctly provides little or no protection
Performance – 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	**Green**	control is always applied as intended
	Yellow	control is generally operational but on occasions is not applied as intended
	Amber	control is sometimes applied correctly
	Red	control is not applied or applied incorrectly

LLOYD'S

TOOL 6.6
RISK ASSESSMENT TEMPLATE

The attached Excel template provides a template for undertaking **a self assessment exercise**. Descriptions of the various fields and rating tables are set out below the template (also see the risk register tool for a further example template).

The attached template is designed to be **completed by risk owners** to reflect their own assessment of risks faced by the business as follows:

- **risk event and components –** a brief description of the risk should be entered, along with a description of its components; and
- **inherent risk assessment –** this requires the risk owner to assess the risk faced, before any mitigating controls are considered.

The assessment is split between impact and likelihood. In completing these columns, the risk owner should consider the impact of the risk occurring (i.e. the financial implication) and the likelihood (i.e. the expected frequency of the risk materialising) based on thresholds. The thresholds given below are for illustrative purposes only.

Impact

Rating	Definition	Monetary Impact
1	Insignificant	< £5k
2	Minor	£5k – £50k
3	Moderate	£50k – £500k
4	High	£500k – £5,000k
5	Very high	> £5,000k

Likelihood

Rating	Definition	Frequency
1	Remote	Once in every 20+ years
2	Unlikely	Once in every 5-20 years
3	Possible	Once in every 1-5 years
4	Likely	Once a year
5	Frequent	More than once per year

Once the initial assessment of risk has been carried out, further assessments should be completed:

- **control –** details of the control activities should be added. All relevant controls should be noted that reduce impact, likelihood or both. Non-control related mitigations, such as insurance, should also be detailed;
- **residual risk –** the risk should be re-assessed following application of the identified control measures using the same impact and likelihood scales as for inherent risk. The ratings should reflect the actual risk faced by the business, given the existing control environment;
- **assessment of risk mitigation / controls –** once the effect of introducing the control measure has been taken into account, the business can assess the effectiveness of the control(s) itself. One example classification is provided below:

Risk mitigation assessment

Rating	Definition	Description
1	Ineffective	Fundamental deficiencies exist in risk mitigation / controls
2	Deficient	Deficiencies exist in risk mitigation / controls
3	Adequate	Minor weaknesses exist in risk mitigation / controls
4	Effective	Risk mitigation / controls are considered sufficient
5	Excessive	Opportunities exist to streamline risk mitigation / controls

It should be noted that it is possible for the mitigation to be classed as “excessive”. In such a situation, the cost of risk control outweighs the benefit of the reduced risk, in which case the measure may be streamlined.

Following this:

- **target –** an indication of the target residual risk (i.e. risk appetite) may be entered, against which the residual risk may be compared;
- **action –** where the risk mitigation measure is assessed as “ineffective” or “deficient”, i.e. in cases where the residual risk is considered too great to be acceptable, an action plan should be devised to address the weakness. This plan should have clear deliverables and target dates.

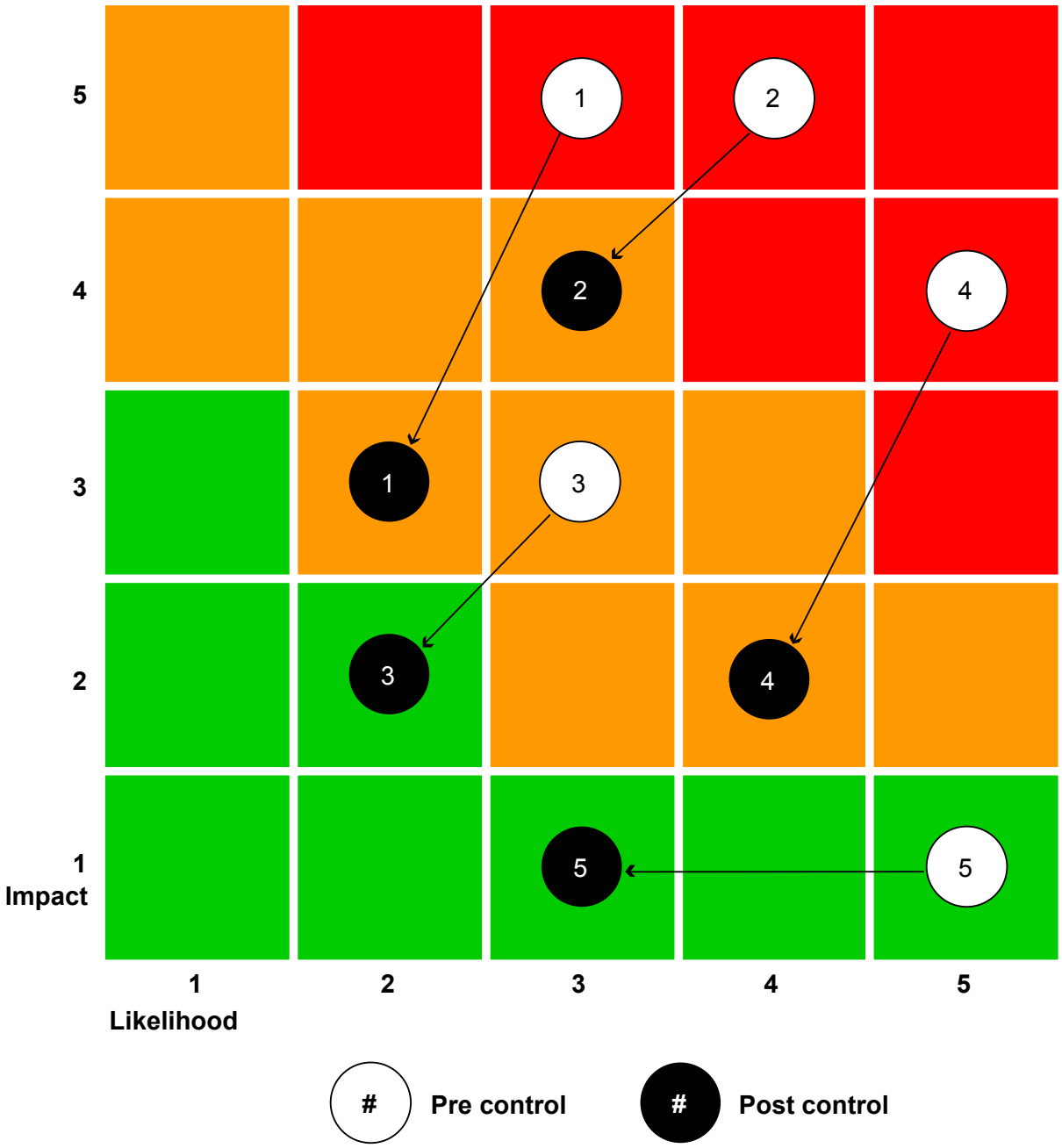
LLOYD'S

TOOL 6.7
EDITABLE RISK ASSESSMENT TEMPLATE

This is an Excel tool that provides a template for undertaking **a self assessment exercise**. This tool can be found in the "Self assessment" section (6) of the toolkit.

Descriptions of the various fields and rating tables are set out below. The attached template is designed to be **completed by risk owners** to reflect their own assessment of risks faced by the business. The data used is illustrative and for example purposes only.

TOOL 6.8
RISK ASSESSMENT OUTPUT



LLOYD'S

TOOL 6.9
RISK PROFILE TOOL

This is an Excel tool that can be used to create heatmap management information for a risk profile. . This tool can be found in the “Self assessment” section (6) of the toolkit.

The data used is illustrative and for example purposes only. As a result, a franchisee could use this tool as a template replacing the example data with their own. The risk profile template provides franchisees with an example risk profile that can be replaced with their own data.

LLOYD'S

TOOL 6.10
RISK REGISTER TOOL

This is an Excel tool that can be used to **create a risk register**. This tool can be found in the "Self assessment" section (6) of the toolkit.

The data used is illustrative and for example purposes only. As a result, a business could use this tool as a template, replacing the example data with their own. It is important to remember that data does not flow through this document.

LLOYD'S

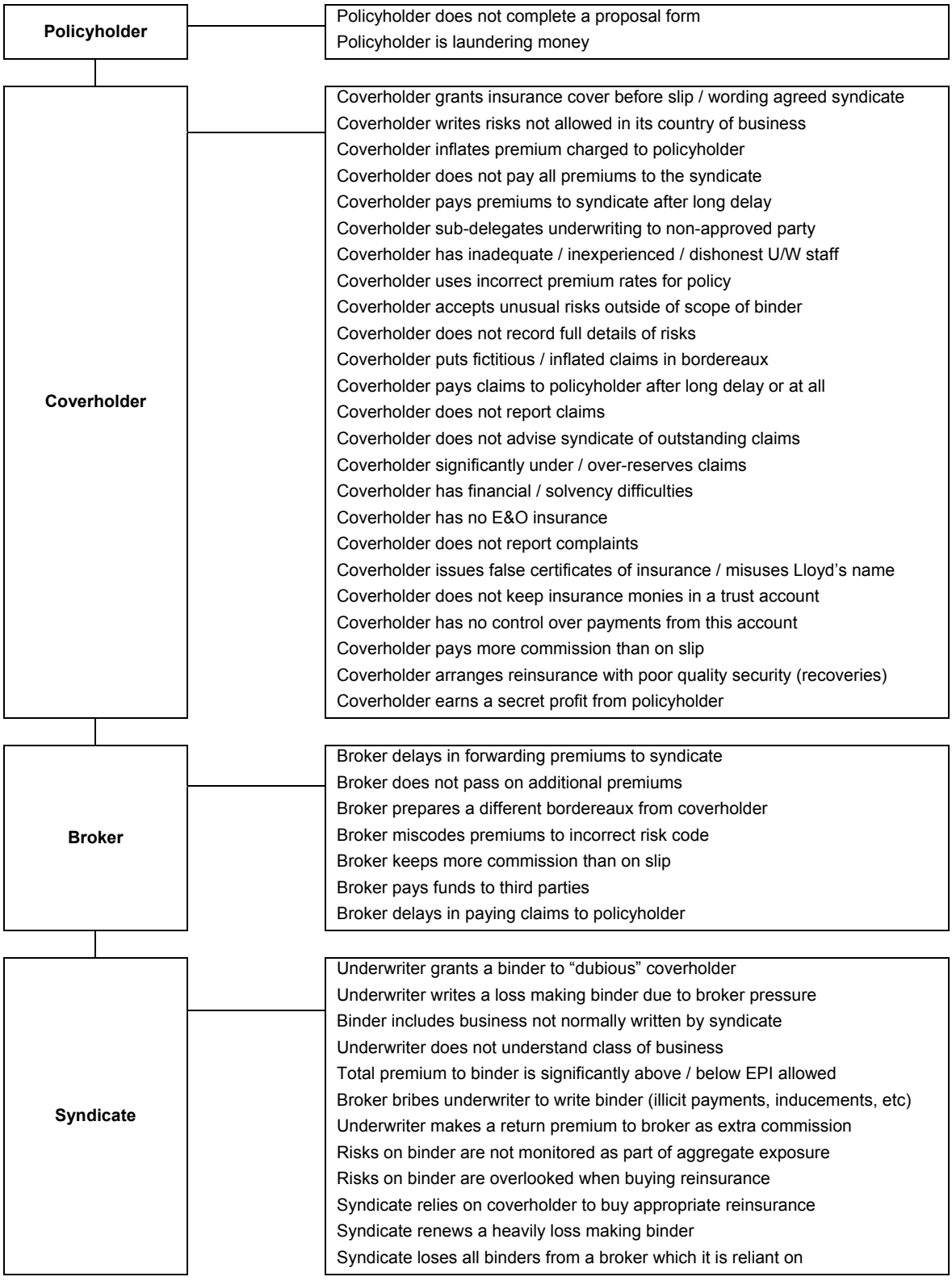
TOOL 6.11
UNDERWRITING PROCESS MAP

Business planning (1)	• detailed plans by division • challenge of business plan assumptions • reasonable maximum line to premium income • communicated to staff
Authority limits (2)	• organisation & reporting lines • defined limits for specific underwriters • risks written within underwriting limits
Underwriting guidelines (3)	• guidelines, rating • broker relationships & remuneration • underwriting objectives clear and understood by staff
Quoting & declining (4)	• handling of quotes, declinatures, promised lines & NTUs • central index. Risks already seen • risk recording, copying, referencing is complete accurate and timely • time limits. Chasing outcome. Updating status
Accepting (5)	• handling of new risks, renewals & endorsements • underwriting stamps & signatures • recording, copying, referencing • history screen. Premium / claim look-up. Action if unclosed
Supervision & review of underwriters / business written (6)	• underwriters registered for all classes & supervised • effective underwriting meetings attended by the active UW • peer review process is detailed, timely and carried out by an experienced person • active U/W adequately supervises and reviews the performance of class underwriters • exception reports are adequate, timely and reviewed • compliance monitoring function • independent review process • board reporting of major issues
Premiums & policies (7)	• terms of trade. Bureaux vs. non-Bureaux • chasing overdue closings • tracking receipt of instalments, APs / RPs for endorsements • policy wordings. Monitoring receipt / signature / issue
Systems & processing (8)	• system adequacy • PC / system security : passwords, lockouts, status controls • data entry, EPI, delays, field adequacy • new brokers, authorisation, setting up, trading status • catastrophe aggregates • filing system: new vs. renewal, availability, destruction

LLOYD'S

TOOL 6.12
BINDING AUTHORITY PROCESS MAP

This illustrates what can go wrong with binding authority.



LLOYD'S

KEY RISK INDICATORS

SECTION 7

TOOLS

Tool 7.1 – Frequently asked questions on KRIs

Tool 7.2 – Illustration of a KRI for staff turnover

Tool 7.3 – Roles and responsibilities for KRIs

Tool 7.4 – Major steps necessary to generate KRIs

Tool 7.5 – Insurance specific operational risk KRIs

Tool 7.6 – Generic operational risk KRIs

Tool 7.7 – A KRI tool

7 KEY RISK INDICATORS

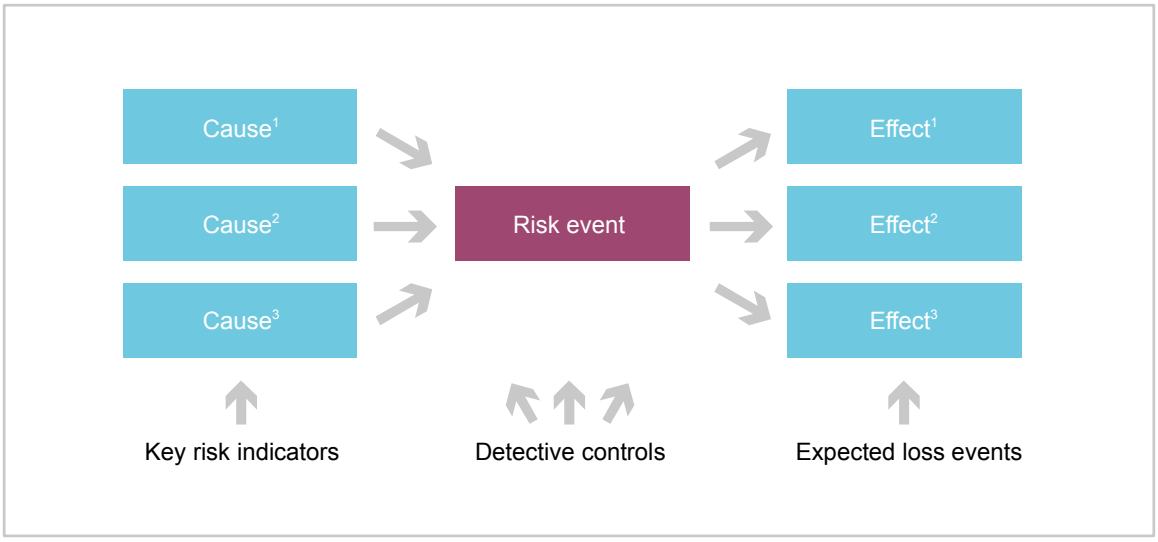
What are key risk indicators (KRIs)?

KRIs are **parameters** which can act as **indicators** and which can be seen to be **predictive** regarding **changes in the risk profile** of a business. This enables **timely action** to be taken to deal with issues arising.

KRIs can include:

- **something observed or calculated –** used to identify a condition or trend;
- **an instrument or gauge –** measures something and registers the measurement; and
- **something such as a "light, sign, or pointer" –** provides information, for example, about which direction to follow, and which serve as "signals".

KRIs then are **measures which indicate the level of and changes in an organisation's risk profile**. This is achieved by focusing KRIs on the root causes of potentially significant risk events and exposures, as illustrated below.



The **key attributes of KRIs** are that they:

- **highlight current risk levels** by providing a measure of the status of an identified risk and the effectiveness of its control. Risk indicators can provide information which gives a useful ongoing view of the underlying behaviour of the risk profile[1];
- **highlight trends and changes in risk level** by monitoring changes in risk between formal risk and control assessments;
- **provide early warning signals** through predictive risk indicators which highlight changes in the risk environment, control effectiveness and potential risk issues, before they crystallise and result in loss or other exposure;

---

[1] Another type of indicator is a **key control indicator (KCI),** which is a measure of the effectiveness (e.g. design and performance) of a specific control. Deterioration in KCIs can show an increase in residual risk impact or likelihood. KCIs are relevant to a particular control activity(s).

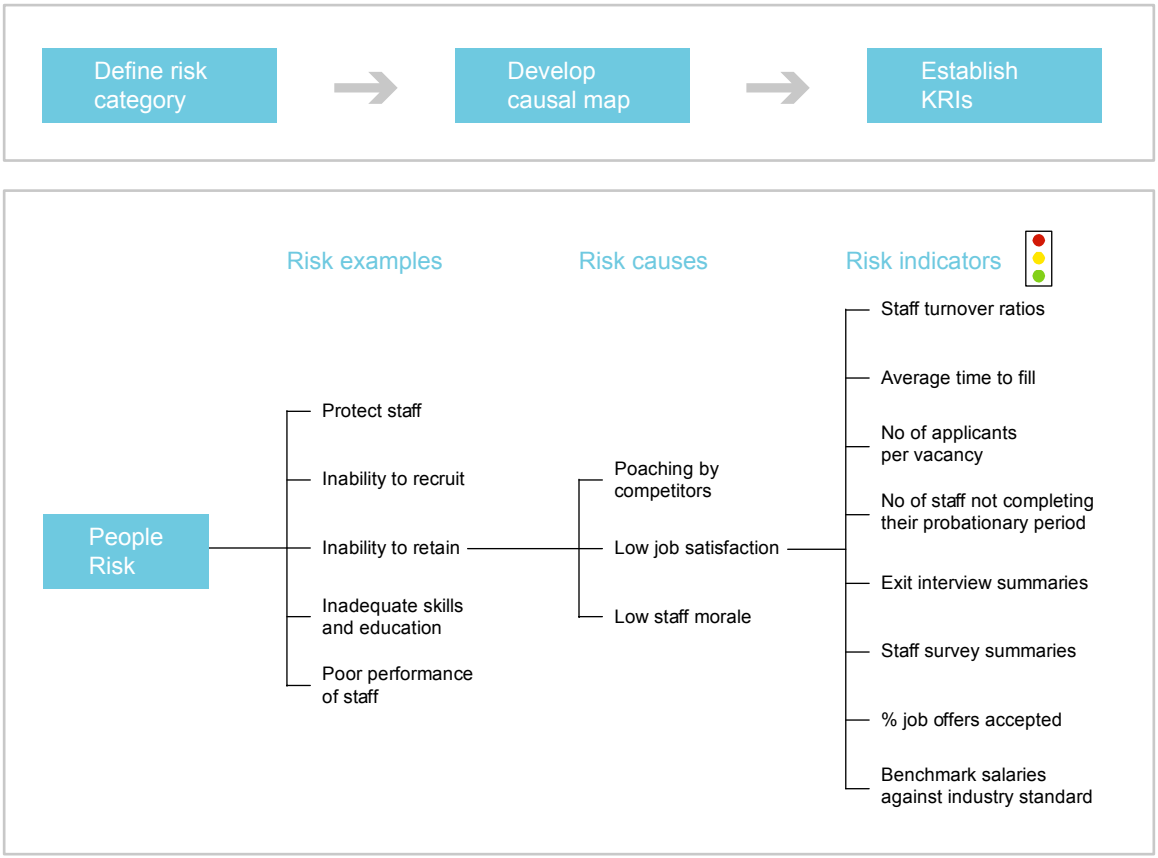
- **enable actions that prevent or minimise material loss or incident** by prompting timely action on early warning signals; and
- **express escalation criteria for risk management** by using thresholds to convert raw indicator data into meaningful risk ratings to aid effective decision making.

Key risk indicators can be **classified into two categories**, namely:

- **specific indicators**, which relate to particular processes within a franchisee, such as the number of reconciling items in a given area; and
- **environmental indicators**, which impact the franchisee as a whole, for example, business volume.

How do you identify key risk indicators?

The diagram below illustrates **how key risk indicators may be identified**, using people risk as an example.



The following are **considerations in the selection of KRIs**:

- ideally determined for many of the **significant risks** identified in the risk and control self assessment (self assessment) process;
- can provide **"early warning"** signals to trigger actions that reduce potential risk exposures;
- some indicators are meaningless on their own and need to be combined with other KRIs. In many cases, it is **a group of KRIs** that will provide the best management information for a meaningful assessment;

- can indicate **past, current and projected level of risks** and can be used as a criteria to monitor, escalate and manage risk and related actions; and
- KRIs **relevance and change in importance** over time.

The **appropriate frequency of reporting and monitoring** of each identified indicator is also an important consideration.

The following (non exhaustive list) provides some sources of **information that can help to identify significant risks** and aid in KRI identification:

- historical internal loss events;
- risk and control self assessment results;
- internal / external audit findings;
- regulatory inspection findings; and
- workshops / discussions with business functions e.g. Human resources (including staff turnover statistics).

Why are they important?

An important objective of key risk indicators is to **provide a measure of risk causes in addition to the effects of risk**, so aiding robust risk management and enabling timely action. Key risk indicators play an important role in:

- **Risk management –** namely:
  - the ability of KRIs to predict **potential "risk hotspots"** can help a franchisee avoid or minimise losses;
  - KRIs help identify **process and/or control weaknesses** and thus enable action to be taken to strengthen controls and resolve issues; and
  - targets for KRIs can be set to **drive behaviour** and desired outcomes for the franchisee.
- **Risk appetite setting –** one of the methods to articulate risk appetite, particularly for operational related risk, is through the setting of **tolerance and escalation levels** for key risk indicators;
- **Regulatory compliance –** identification and management of KRIs is an area of regulatory focus; and
- **Capital calculation –** data from established KRIs can be used as one of the inputs into operational risk capital calculations.

What practical steps are necessary for implementation?

From a **practical standpoint**, KRIs need to be built into (rather than bolted onto) operational and business processes:

- "opening up" legacy operational and business processes and supporting systems to retroactively build in KRI requirements is likely to be an **expensive and potentially impractical** proposition for many organisations;
- as a result, for all but a few absolutely vital KRIs, introducing KRIs for most organisations is most practically undertaken as an integral part of **new system development** and **process transformation** initiatives where the cost is likely to be much lower.

Given the above, the following guidance is intended to help organisations understand what is involved from a practical standpoint to implement this **KRI section:**

- **Staff resource and skills**
    - business unit workshops to identify the important key risk indicators, drawing on senior business unit managers and expert staff, facilitated by risk management
    - IT programming resource to develop and integrate KRI reporting
    - briefing of senior management and committees
    - internal auditor or external consultant review to provide technical assistance and support and assurance that KRIs are focussed on key areas and are robustly implemented, such that they support risk monitoring and decision making
- **Enabling technology**
    - MS Excel and/or Access software
    - bespoke operational risk software (developed in house or from third party vendors)
- **Time**
    - initial workshops and IT implementation – 3 to 6 months
    - iteration, refinement and assurance over selected KRIs – 3 months
    - overall expected implementation time – 6 to 12 months
- **Direct / indirect costs**
    - management and staff time – per 2 to 3 hour workshops
    - IT staff time – for programming
    - risk management time – facilitation, documentation and review
    - internal audit / external consultants – for support, quality assurance, technical review and independent assurance

Given the differences in scale, sophistication and resources between franchisees, the capacity to establish KRIs, to monitor and react to KRI information, and the overall number of KRIs will **vary significantly across organisations.**

It is therefore anticipated that this section would be of **relevance to organisations** as follows:

- **Large / composite –** highly relevant: expected to be in use for business unit management reporting;
- **Medium / multi-line –** highly relevant: expected to be generally in use for business unit management information; and
- **Small / mono line –** relevant: but with less extensive KRI reporting.

Relevant toolkit contents

Relevant toolkit contents for key risk indicators include:

- **Tool 7.1 – Frequently asked questions on KRIs:** frequently asked questions and helpful pointers with respect to key risk indicators;
- **Tool 7.2 – Illustration of a KRI for staff turnover:** an example key risk indicator for staff turnover to illustrate the design / use of key risk indicators;
- **Tool 7.3 – Roles and responsibilities for KRIs:** an illustration of principle roles and responsibilities with respect to key risk indicators and the associated reporting structure;
- **Tool 7.4 – Major steps necessary to generate KRIs:** identifies six major steps necessary in establishing key risk indicators, with an illustrated example range of KRI perspectives for LMP slip compliance;
- **Tool 7.5 – Insurance specific operational risk KRIs:** a non-exhaustive list of example insurance specific key risk indicators for operational risk, broken down by people, processes, systems & external events;
- **Tool 7.6 – Generic operational risk KRIs:** a non-exhaustive list of example generic key risk indicators for operational risk, again broken down by people, processes, systems & external events;
- **Tool 7.7 – A KRI tool:** a tool that can be used to create heatmaps, trend analysis and management information for key risk indicators, with illustrated insurance specific KRIs – including supporting dummy data tables (by operational risk category) and working KRI reporting graphics, formats and templates.

LLOYD'S

TOOL 7.1
FREQUENTLY ASKED QUESTIONS

Frequently asked questions & helpful pointers

- How should **KRIs link with risk assessments** and event reporting?
  Focus on indicators which track changes in the risk profile or the effectiveness of the control environment.
- What is the **most practical way of arriving at a set of KRIs?**
  Concentrate on the significant risks and their causes and consider forward looking and historical indicators.
- How should **KRIs** be set **in terms of measurement?**
  Consider absolute values and numbers, ratios, percentages, ageing, etc.
- With what **frequency** should KRIs be captured?
  Data on KRIs should be collated on a systematic and consistent basis in order to be meaningful, e.g. on a monthly basis.
- How should **acceptable ranges and escalation thresholds** be determined for KRIs?
  Consider in detail the risk appetite set by the board and cascaded down to business level when setting thresholds.
- Will KRIs **change over time?**
  Key risk indicators will evolve over time. Analysis of actual losses and near misses will assist in identifying which KRIs are the best at giving early warning and allowing timely action. Periodic review needs to take place of the indicators themselves and their associated thresholds to ensure they remain aligned with the dynamic of the business environment and the significant risks faced by the franchisee at any point in time.
- How can KRIs be linked to **operational risk appetite and tolerance?**
  By defining targets, tolerance ranges and escalation thresholds for risk appetite.
- How should **roles and responsibilities** be assigned for the collection, collation, monitoring and challenge of KRIs?
  Assign KRI owners who are responsible for collection and collation. The risk management function should provide challenge and internal audit, independent validation.

TOOL 7.2
ILLUSTRATION OF A KRI FOR STAFF TURNOVER

A key risk indicator for **monitoring and responding to risk** around the effectiveness and continuity of essential business functions relates to **staff turnover levels.** This is important for all positions and particularly for positions where there is a critical level of dependency. Key risk indicators of this type require;

- **tolerance thresholds** in order to give a meaningful representation of the risk; and
- the resultant ratings which could be used to create **"heat map" reporting** on indicators.

For example, when given thresholds are breached there will be a requirement to escalate to an appropriate level of management:

- **Below 24% – No risk.** The organisation is comfortable with the level of staff turnover. No escalation or treatment required.
- **Above 24% – Potential risk.** The risk is a concern and HR would be expected to monitor actively and establish causes and actions. Escalation required raising awareness but explanatory report not required.
- **Above 28% – Significant risk.** Action and escalation with explanatory report required.

Staff turnover KRI

%	Risk level
0 – 24	
24 – 28	
> 28	

Thresholds can be used alongside targets set by management. These could be flexed over time as objectives / strategy and risk appetite develop. These targets will help drive the desired behaviour and outcomes and improve the organisation's operational risk profile over time.

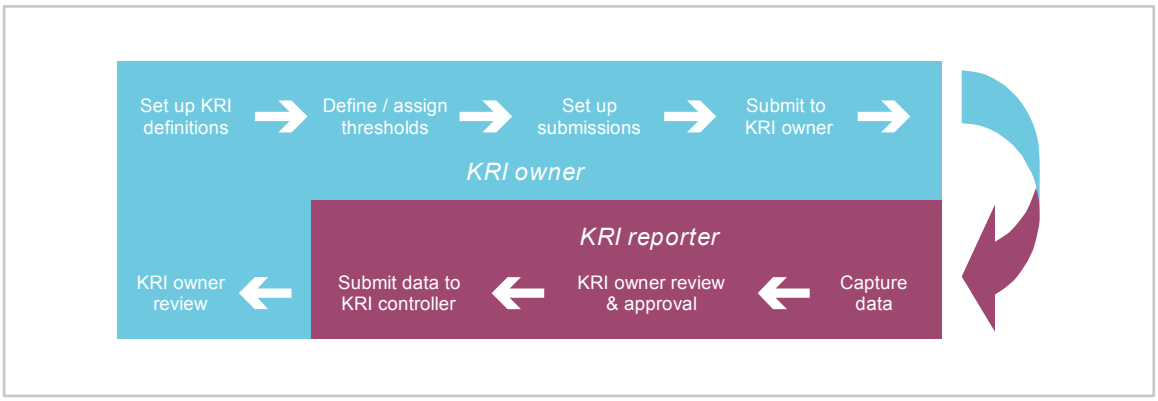
TOOL 7.3
EXAMPLE ROLES AND RESPONSIBILITIES FOR KRIS

The following diagram illustrates **principal roles and responsibilities** in respect of KRIs and the associated reporting structure[2].

Business function	Risk management	Internal audit
Identification of indicators	Provide guidance and challenge the selection of KRIs and thresholds	Provide validation / independent assurance around the KRI process
Setting of thresholds	Monthly reporting on KRI breaches	Incorporate outputs into audit plan
Monitor position against targets and limits	Ad-hoc escalation reporting to Board	
Escalate breaches to operational risk management	Identify trends across the business	

Key risk indicator workflow diagram

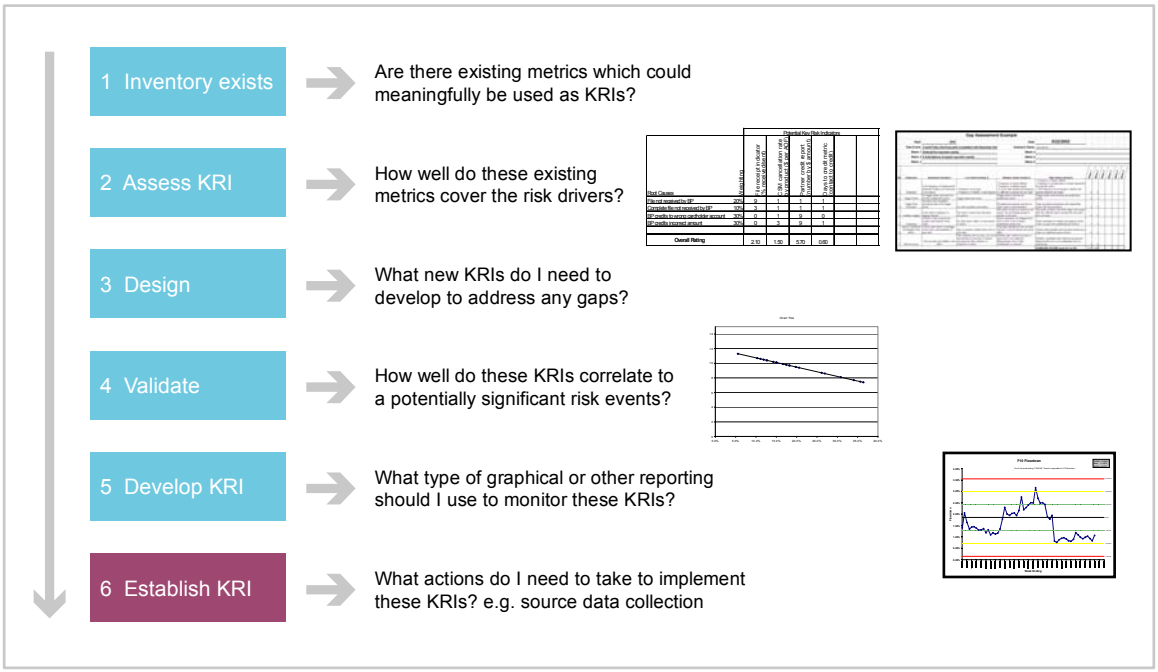
The diagram below illustrates the steps from development to reporting of key risk indicators and could be used to facilitate a franchisee workshop or group discussion on KRIs.



[2] This structure follows the 'Three lines of defence' approach used in the governance section of the toolkit with respect to roles and responsibilities within a risk management function.

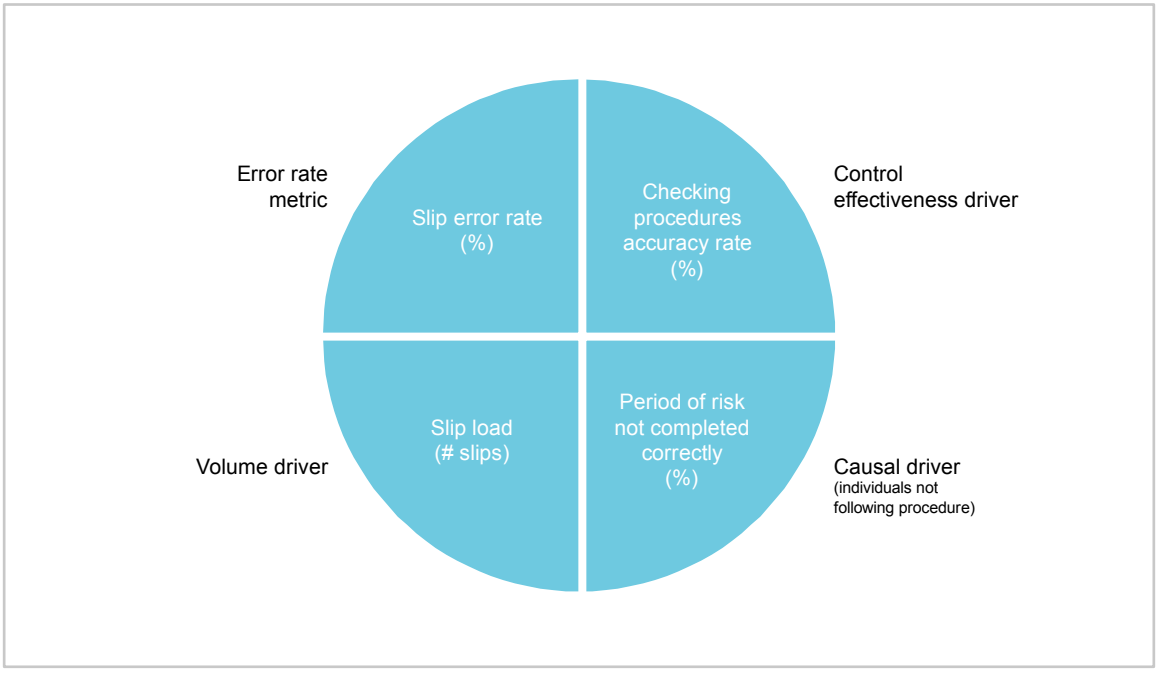
TOOL 7.4
MAJOR STEPS NECESSARY TO GENERATE KRIS

This example illustrates **6 major steps for establishing key risk indicators.**



The following diagram illustrates the need for a **balanced range of KRI perspectives** in order to monitor a significant risk, for example, LMP slip compliance.

Risk event – LMP slip standards are not adhered to.



LLOYD'S

TOOL 7.5
INSURANCE SPECIFIC OPERATIONAL RISK KRIS

Risk category	Example key risk indicator
People	• staff turnover rates • sickness rates per division per month / year • number of contract staff • percentage referral rates • number of complaints referred to ombudsman per month / year
Processes	**Basic underwriting process** • percentage slips recorded within 24 hours • percentage slip entry error rate • percentage endorsements recorded • percentage aggregates (or proxy for max aggregate) recorded within 24 hours • percentage of slips underwritten within authority • percentage referral where appropriate • percentage underwriting guidelines to be followed, subject to referral **Underwriting review** • percentage of slips with greater than £1m premium or £10m exposure to be peer reviewed within 10 days **Monitoring of underwriting** • number of premium and reinsurance debt greater than 90 days outstanding • number of claims greater than £10m to be reviewed • number of non-moving claims to be reviewed every 6 months • number of contracts greater than 110% loss ratio to be investigated, (subject to de-minims £1m premium) • number of exposures not recorded within 1 month of underwriting • number of less than 100 binders not written, with minimum income £100k • number of outstanding wordings greater than 1 month **Agency level underwriting controls** • percentage of major contracts to be independently reviewed within 1 month of underwriting **Placement of reinsurance programme** • percentage of reinsurance order forms and cover notes reviewed against requirements per month • percentage accuracy on reinsurance orders and cover notes per month

Risk category	Example key risk indicator
	Agency level reinsurance purchase controls • percentage set limits on exposures to reinsurers (e.g. less than 10% premium to be placed with 1 reinsurer) • elapsed days since security ratings for reinsurers last measured • number of material exposures / recoveries from reinsurers / erosion of reinsurance per month / year **Claims processes** • percentage material claims / disputes / complaints reported to senior management / Board per month • number of second adjustor review for material claims greater than £10m per month / year • number of monthly reconciliation breaks of claims reserves • percentage of claims advices reviewed within 2 days • percentage of collection notes issued within 30 days • percentage of outstanding debts chased after 90 days • number of ongoing disputes with syndicate actuaries or accountants per month / year **Liquidity processes** • percentage contingency plans for potential or expected cash shortfalls **Generic process failures** • percentage manual input errors per month • number underwriting staff with access to accounting system • percentage of management information and exception reporting produced and reviewed within 2 days of month end • percentage of IT system queries responded to within 24 hours • percentage of complaints resolved within 1 month of receipt • number of adverse press comment(s) per month / year • number of outstanding external and internal audit / compliance / regulatory report points
Systems	• number of IT system outages per month • number of IT security breaches per month / year • number of IT virus caused outage per month / year • number of IT supplier failure incidents per month / year • number of 1 day server failures per month / year • number of tested IT disaster recovery procedures and systems per year
External events	• number of incidents of third party provider failure, from outsource providers per month / year • number of successful external fraud incidents per month / year • number of IT system security breaches per month / year • number of regulator action / concerns per month / year • number of outstanding Lloyd's operational risk review points raised

LLOYD'S

TOOL 7.6
GENERIC OPERATIONAL RISK KRIS

Risk category	Example key risk indicator
People	• diversity stats by ethnicity / sex / age / disability • number of staff disciplinaries / dismissals • percentage of staff appraisals below "satisfactory" • number of staff grievances • results of staff surveys • staff turnover rates • percentage of joiners leaving within the first 6 months • actual versus budgeted FTE • proportion of permanent versus temporary staff • average length of service per member of staff • average time to fill vacant positions • staff absenteeism / sickness rates • overtime • actual versus budgeted training costs • average number of days training per member of staff • percentage of staff who have attended health and safety training • percentage of staff who have attended financial crime / anti money laundering training • percentage of staff who have not had two weeks consecutive leave • proportion of permanent versus temporary staff • average length of service per member of staff
Processes	• number / percentage of accounts with outstanding / incomplete customer documentation • number / percentage of unauthorised customer accounts opened • number / percentage of customer accounts with significant change in volume / value of transactions • number of incidents reported to the Money Laundering Reporting Officer • number / percentage of customer accounts with unusual transactions • number and nature of limit breaches • number of new products • market share by product • customer intake / retention / churn by product versus budget • significant revenue variance by product • number of new products / new products awaiting approval / unapproved products • projected transaction processing volumes versus capacity • percentage change in transaction volumes • percentage of total transactions handled • number / value / age of processing exceptions • processing exceptions as a percentage of transaction volumes • number of customer complaints • number of compliance / regulatory breaches

Risk category	Example key risk indicator
	• budgeted versus actual FTE within customer & account servicing / moving money / collections • supplier performance versus SLA • number of unreconciled accounts • number / value / age of unreconciled items
Systems	• number and type of security violations • number of virus incidents • systems usage versus capacity • systems downtime • number, type and severity of system incidents / SLA breaches • number of system upgrades / version releases • number of open system change requests • number of help desk calls • virus incidents • number of outstanding business continuity plans • utility performance statistics
External events	• number of overdue tests / maintenance of detection & suppression mechanisms • number of outstanding disaster recovery plans • number of overdue disaster recovery plan tests • number and nature of physical security incidents

LLOYD'S

TOOL 7.7
A KRI TOOL

This is an Excel tool that can be used to create heatmaps, trend analysis and management information for key risk indicators. This tool can be found in key risk indicator section of the toolkit.

The data in this template is illustrative and for example purposes only. The pie charts and graphs are plotted using data contained within the tool. As a result, an organisation could use this tool as a template replacing the example data with their own. It is important to remember that as it stands, this tool will not automatically update cell colour.

LLOYD'S

INTERNAL LOSS EVENT DATA

SECTION 8

TOOLS

Tool 8.1 – Internal loss event data requirements

Tool 8.2 – Basel II framework detailed loss event type classification for operational risk

Tool 8.3 – Internal loss event data collection template

Tool 8.4 – Internal loss event database tool

8 INTERNAL LOSS EVENTS

What are internal loss events?

Internal loss events may be viewed as actual loss, potential loss and "near miss" events experienced by an organisation[1]:

- **Actual loss** – an incident that has resulted in a negative financial impact for the business;
- **Potential loss** – an incident that has been discovered, that may or may not ultimately result in a financial loss; and
- **Near miss** – an incident discovered through means other than standard operating practices and through good fortune or focused management action which has resulted in nil or a positive financial impact (it should be noted that a near miss could potentially result in a financial gain).

Sources of loss events can be considered in two ways:

- as a result of a **new risk** to the organisation, leading to a loss event; or
- as a result of a **lack of control or control failure** surrounding an already identified risk.

Why are they important?

The tracking of internal loss event data is a **key component** of robust risk management and contributes to the assessment and monitoring of risk. By capturing risk event information in a consistent manner, organisations are able to:

- **measure risk exposure** more accurately;
- **justify the cost of new or improved controls** and compare the effectiveness of controls;
- **identify trends** and lessons to be learned over time; and
- use loss data as a **potential input for capital calculation.**

Robust risk management relies on a sufficient volume and quality of data if analysis is to be meaningful and decision making effective, therefore, the **integrity of data is important** in any loss event database.

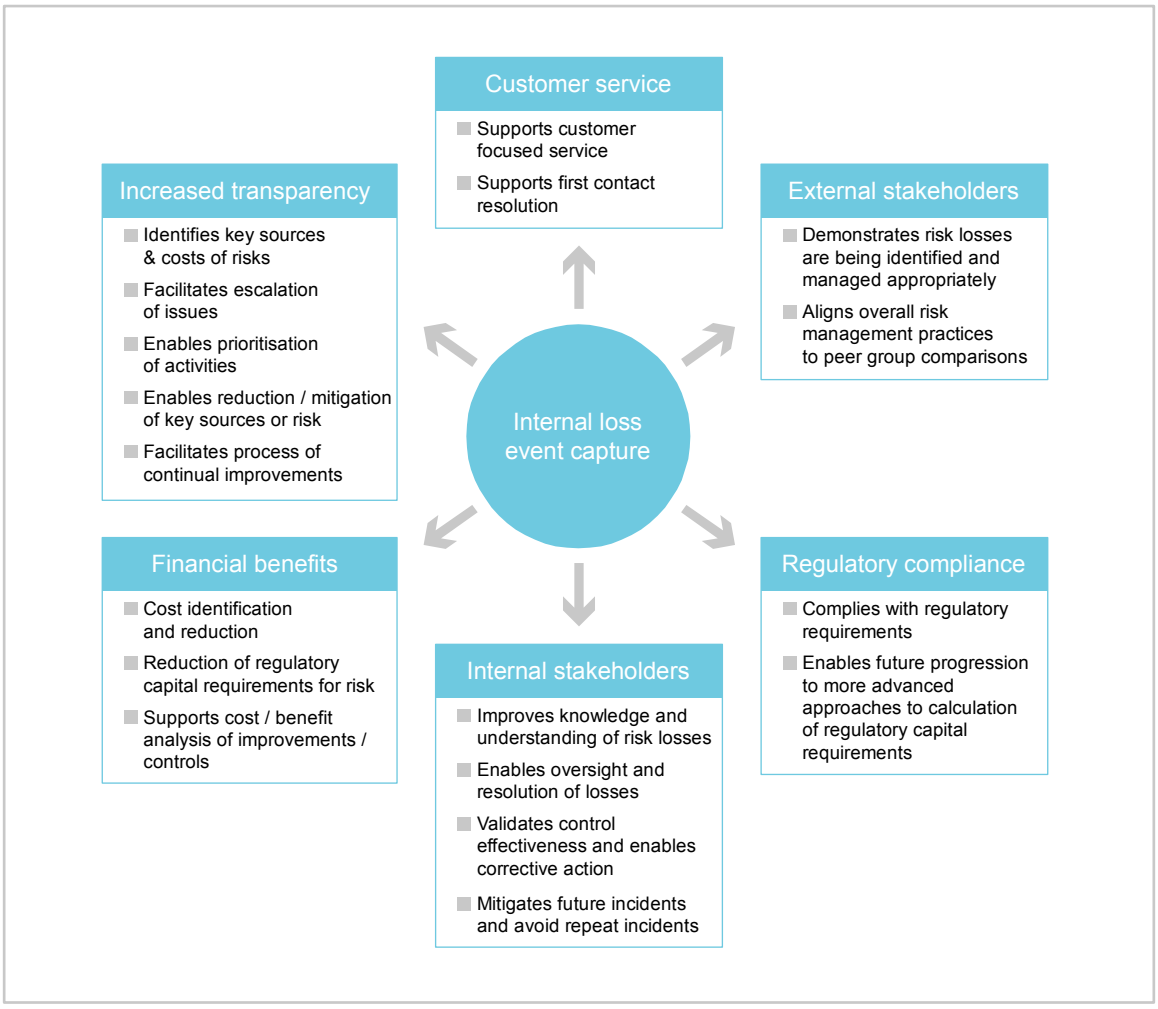
As a first step, **loss event thresholds** should be assigned to actual, potential and near miss loss events. Loss events exceeding these thresholds may then be tracked and recorded in an internal loss event database.

A download from the General Ledger can provide a means of **reconciling losses** on a periodic basis e.g. monthly.

---

[1] Please refer to "External loss data" section of the toolkit (9) for use of external loss database information and suppliers.

Benefits of internal loss event collection



What practical steps are necessary for implementation?

The following guidance is intended to help organisations understand what is involved from a **practical standpoint** to implement this **internal loss event data section**:

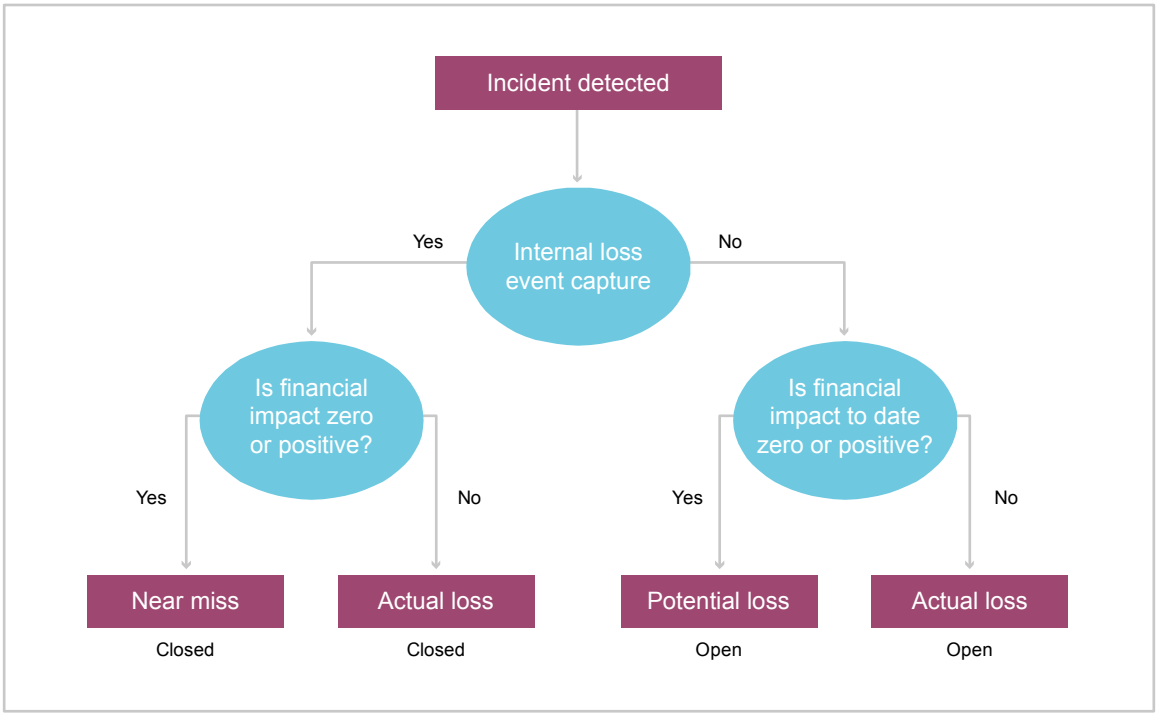
- **Staff resource and skills**
  - business unit workshops to identify relevant and expected loss data to be collected, drawing on senior business unit managers and expert staff, facilitated by risk management
  - IT programming resource to develop and integrate loss data recording and reporting
  - briefing of senior management and committees
  - internal auditor or external consultant review to provide technical assistance and support and assurance that loss data collection is focussed on key risk events and is robustly implemented, such that it supports risk monitoring and decision making
- **Enabling technology**
  - MS Excel and/or Access software
  - bespoke operational risk software (developed in house or from third party vendors)
- **Time**
  - initial requirements workshop(s) and IT implementation – 3 to 6 months
  - iteration, refinement and assurance of loss data and supporting process – 3 months
  - overall expected implementation time – 6 to 9 months, then ongoing
- **Direct / indirect costs**
  - management and staff time
  - IT staff time for programming
  - risk management time for facilitation, documentation and review
  - internal audit / external consultants for support, quality assurance, technical review and independent assurance

In view of the wide range in size and sophistication of businesses, it is anticipated that this section would be of relevance to organisations in the following manner:

- **large / composite (highly relevant)** – expected to be in use for business unit management reporting
- **medium / multi-line (relevant)** – depending on contract volume, expected to be in use for business unit management reporting
- **small / mono line (potentially)** – less relevant depending on contract volume

How to classify a new loss event

The table below illustrates the **process of determining the loss type of a new event**.



Relevant toolkit contents

Relevant risk toolkit content for internal loss events include:

- **Tool 8.1 – Internal loss event data requirements:** an example breakdown of typical information captured in internal loss event data;
- **Tool 8.2 – Basel II framework detailed loss event type classification for operational risk[2]:** this sets out the Basel II loss event categorisation for operational risk;
- **Tool 8.3 – Internal loss event data collection template:** a template organisations can use to capture internal loss event data;
- **Tool 8.4 – Operational risk internal loss event database tool:** a tool to help create an internal loss event database and associated management information using operational risk as a basis.

[2] This tool replicates tool 2.4. A breakdown of potential causes of operational risk by category can be found in the "Risk definition and language" section of the toolkit.

LLOYD'S

TOOL 8.1
INTERNAL LOSS EVENT DATA REQUIREMENTS

A robust operational risk framework requires development of a **franchise database to capture loss events** attributable to the different categories of operational risk (people, processes, systems and external events).

The table below provides an **example breakdown of data fields** that an organisation could apply when collating internal loss data. An organisation may consider initiating the collection of operational risk loss data using the key fields below and develop the fields of data further as the process matures[3].

Data fields	Description
Reported by	Name of person reporting the incident
Incident owner	Name of person who has overall accountability for the management of the incident
Class of business / risk code	Product type in which the loss occurred (e.g. aviation, marine)
Date of incident DD/MM/YY	Date the incident occurred or was first noticed
Reporting month MMM/YY	Month and year the incident occurred
Incident end date DD/MM/YY	Date the incident ceased to occur (if applicable)
Method of detection	How the incident was identified (a free text field)
Incident type	Risk type (actual loss, potential loss or near miss)
Incident open / closed	Open or closed
Total cost to date £	Total costs incurred to date (once closed this should be total cost of the incident)
Maximum potential loss £	Maximum potential amount that could be lost if the incident had or were to occur
Expected loss £	Expected amount that will be lost
Incident description	Description of the incident
Incident cause	Cause of the incident (new risk, control failure, other)
Incident cause categorisation	People, processes, systems or external events
Actions	Remedial actions taken (or to be taken) since incident occurred. NB: should include actions to be taken to recover lost funds as well as actions to be taken to enhance the control environment
Action due date DD/MM/YY	Due dates for the action listed in previous column to be completed
Actions complete? Yes / no	Whether actions are complete

[3] The example internal loss database and management information ("Worked example 2") detailed in this section considers only the key fields of data, for illustrative purposes.

LLOYD'S

TOOL 8.2
BASEL II FRAMEWORK DETAILED LOSS EVENT TYPE CLASSIFICATION FOR OPERATIONAL RISK

Basel II framework – Detailed loss event type classification (operational risk)

The following table sets out the Basel II loss event categorisation for operational risk in order to provide a helpful point of reference.

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity / discrimination events, which involves at least one internal party	Unauthorised activity	• transactions not reported (intentional) • transaction type unauthorised (w/ monetary loss) • mismarking of position (intentional)
		Theft and fraud	• fraud / credit fraud / worthless deposits • theft / extortion / embezzlement / robbery • misappropriation of assets, malicious destruction of assets, forgery, check kiting, smuggling, account take-over / impersonation / etc. • tax non-compliance / evasion (wilful), bribes / kickbacks, Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and fraud	• theft / robbery • forgery • check kiting
		Systems security	• hacking damage • theft of information (w/ monetary loss)

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee relations	• compensation, benefit, termination issues • organised labour activity
		Safe environment	• general liability (slip and fall, etc.) • employee health and safety rules events • workers compensation
		Diversity and discrimination	• all discrimination types
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product	Suitability, disclosure and fiduciary	• fiduciary breaches / guideline violations • suitability / disclosure issues (KYC, etc.) • retail consumer disclosure violations • breach of privacy • aggressive sales • account churning • misuse of confidential information • lender liability
		Improper business or market practices	• antitrust • improper trade / market practices • market manipulation • insider trading (on firm's account) • unlicensed activity • money laundering
		Product flaws	• product defects (unauthorised, etc.) • model errors

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
		Selection, sponsorship and exposure	• failure to investigate client per guidelines • exceeding client exposure limits
		Advisory activities	• disputes over performance of advisory activities
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events	Disasters and other events	• natural disaster losses • human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	• hardware • software • telecommunications • utility outage / disruptions
Execution, delivery and process management	Loss from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction capture, execution and maintenance	• miscommunication • data entry, maintenance or loading error • missed deadline or responsibility • accounting error / entity attribution error • model / system misoperation • other task misperformance • delivery failure • collateral management failure • reference data maintenance
		Monitoring and reporting	• failed mandatory reporting obligation • inaccurate external report (loss incurred)
		Customer intake and documentation	• client permissions / disclaimers missing • legal documents missing / incomplete

Event type category (level 1)	Definition	Categories (level 2)	Activity examples (level 3)
		Customer / client account management	• unapproved access given to accounts • incorrect client records (loss incurred) • negligent loss or damage of client assets
		Trade counterparties	• non-client counterparty misperformance • misc. non-client counterparty disputes
		Vendors and suppliers	• outsourcing • vendor disputes

LLOYD'S

TOOL 8.3
INTERNAL LOSS DATA COLLECTION TEMPLATE

This is an Excel tool that can be used to capture internal loss event data. This tool can be found in the "Internal loss event data" section (8) of the toolkit.

The data used is illustrative and for example purposes only. This template is designed to guide organisations in what they should aim to capture in terms of internal loss event data. Organisations can tailor the template to include or exclude various elements of data.

LLOYD'S

TOOL 8.4
INTERNAL LOSS EVENT DATABASE TOOL

This is an Excel tool that can be used to aid the design of an internal loss event database to capture internal loss event data. This tool can be found in the "Internal loss event data" section (8) of the toolkit.

This tool can be used to create an internal loss database and associated management information for operational risk. The data used is illustrative and for example purposes only. The pie charts and graphs are plotted using data contained within the tool. As a result, a business could use this tool as a template replacing the example data with their own.

SECTION BREAK

LLOYD'S

EXTERNAL LOSS DATA

SECTION 9

9 EXTERNAL LOSS DATA

What is external loss data?

External loss data is information relating to the **loss experiences** of other institutions. External loss data can provide an indication of the **size**, **frequency and sources of losses** experienced by others and thus can provide a wider frame of reference when assessing potential risk exposures.

Typically an **external loss database** will consist of:

- large volumes of actual loss data specifying amount, frequency and classification of loss events collated from an industry group; and/or
- specifics of particular large loss events collected from publicly available information.

Why is it important?

External vs. internal loss data

While **internal loss data** will help an organisation to understand its risk exposures by looking at its historic loss experience, this data is unlikely to be wholly indicative of potential future losses. This is because the organisation faces potential exposures and losses which have not previously been experienced, and thus by definition, for which no internal data is available.

An organisation may therefore consider using **external loss data** so that it can understand the types of losses that it could incur in the future.

Benefits of using external loss data

External loss data can add value to an organisation in three main ways, namely to:

- test the **responsiveness of its control environment** against the external loss events in order to assess control effectiveness in helping to avoid, or mitigate against such events;
- assist in the creation of **realistic scenario tests** for the purposes of assessing capital requirements; and
- provide additional data which may potentially assist with the **modelling of capital requirements**. However, careful judgement is needed on the relevance of such data, in view of different industry or industrial sector data sources, differences in operational scale, control systems, cultures and the likely completeness of the data.

At present, the **most directly relevant** external loss data sources are provided by the data consortia being established by **ORX** and the **ABI** (see below).

Relevant tools

Sources of external loss data for operational risk

- **Operational Risk data eXchange association (ORX)**
  - this database uses the **Basel loss event categories** to collect, cleanse, process and report **operational risk loss data** for members
  - founding members are from the **banking sector** and the database is expected to meet FSA regulatory requirements for external data
  - data held in the database is **anonymous**, and records loss events with a **threshold set at €25,000**
  - data is collated, held and distributed by a **third party** for security purposes
  - **reports** on the consortium dataset are made available to all members
  - current database is banking focussed, but ORX are developing an **insurance version**
- **ABI Operational Loss Consortium (OLC)**
  - ABI use **Basel loss event type categorisation** within their database and provide a robust / secure data repository for users
  - database aims "to provide an industry database of quality operational loss event information to enhance both quantitative and qualitative understanding of **operational risk for insurers**"
  - **ABI's objectives** include:
    - providing a quantifiable input into ICA modelling;
    - challenge to internal risk identification;
    - identification of risk areas; and
    - provision of benchmarks.
  - **ABI collate, host and distribute reporting**. A reporting suite enables members to access pre-defined reports, create reports in a secure environment, and benchmark themselves against other consortium members
- **The Fitch first database**
  - has around **5000 loss events** recorded on it and is categorised in the following way:
    - Corporate Finance
      - **Corporate Finance – Underwriting**
      - Corporate Finance – Mergers & Acquisitions
    - Trading & Sales
      - Trading & Sales – Equities
      - Trading & Sales – Fixed Income
      - Trading & Sales – Foreign Exchange
      - Trading & Sales – Commodities

    - Retail Banking
        - Commercial Banking
        - Payment & Settlement
        - Agency Services
    - Asset Management
        - Asset Management – Retail Brokerage
        - Asset Management – Private Banking
    - **Other – Insurance**
    - Other – Accounting
- one of the key limitations of this database is that it is populated with **"public" events** rather than data sharing via a consortium
- as a result **little is known about each organisation involved**. This in turn makes the process of testing, in terms of relevance, scale and completeness, more difficult

For further information on the data consortia outlined here, please contact Andrew Gurney, Lloyd's Risk Analysis at andrew.s.gurney@lloyds.com or 020 7327 6194.

LLOYD'S

MANAGEMENT INFORMATION

SECTION 10

TOOLS

Tool 10.1 – Example reporting matrix

Tool 10.2 – Example management information reporting tool

10 MANAGEMENT INFORMATION

What is management information?

Every business identifies and captures a **wide range of information** relating to external, as well as internal, events and activities which is **relevant to managing the business.** This information is delivered to management and staff in a form and timeframe that enables them to carry out their risk management, measurement and other responsibilities[1].

It is an **ongoing challenge** to provide sufficiently detailed and appropriate information to the different levels of management such that the key issues may be quickly understood, but not so detailed that the issues are obscured.

Typical risk management information

Typical risk management information includes **regular reporting** of:

- actual losses, potential losses and near miss events;
- the business risk profile, including new and changed exposures to key risks;
- significant control weaknesses (which affect significant risks);
- key risk indicators, including trend analysis; and
- progress on action plans to deal with significant risks or control weaknesses.

Besides routine reporting, an **escalation process** to alert senior management of significant issues is also important, for example, in respect of breaches of authorities, limits, thresholds, risk policy or risk appetite.

Why is it important?

Providing the right information to the right people at the right time leads to better identification and prioritisation of **risks and opportunities,** which in turn leads to **better**, **more informed decision making.** This makes it more likely that the business will achieve its objectives.

Timely, accurate and complete management information assists managers to:

- understand the significant risks which make up the **risk profile** of the business and how it is changing over time;
- determine whether the business **risk exposures** are being managed in accordance with the risk appetite and policy set by the Board;
- identify **opportunities** to exploit the upside of risk taking; and
- monitor **actions being taken** to deal with the downside unacceptable exposures and known control failures.

Organisations may therefore consider it important that the **timeliness, accuracy and completeness** of management information be subject to routine quality assurance and periodic independent review, for example by internal audit.

---

[1] COSO Framework, "Enterprise Risk Management – Integrated Framework", p 67 commentary on Information and Communication

What practical steps are necessary for implementation?

From a **practical standpoint**, different parties require different risk management information, about different risk issues and with a different frequency. The attached table provides some guidance which may help organisations think more about their own reporting structure and needs.

In order to assist organisations, each of the toolkit example reports contains an explanation of:

- the **purpose** of the report;
- who the **recipients** of any given report might be;
- **how often** such reports, ideally would be produced; and
- what they should **do with the report** (i.e. from a practical standpoint, they would use the operational risk information to run the business better).

It is important to note that for small businesses, not all of the attached reporting examples may be practical and affordable to systematically produce.

Relevant toolkit contents

The relevant toolkit contents for management information is summarised below:

- **Tool 10.1 – Example reporting matrix:** contains suggested content, recipients and frequency for risk management reporting;
- **Tool 10.2 – Example management information reporting tool:** an illustrative management information pack, which sets out a range of example reporting formats for operational risk, which businesses may draw upon where applicable to their business, including:
    - summary reporting;
    - risk profile reporting;
    - loss event reporting and graphs;
    - key risk indicator reporting; and
    - control assessment reporting.

LLOYD'S

TOOL 10.1
EXAMPLE REPORTING MATRIX – CONTENT, RECIPIENT AND FREQUENCY

	Role	Monthly	Quarterly	Semi Annual / Annual
Board	• ultimate accountability and oversight for business risk and controls • receive assurance that RM within policy		• "top 10" risk list • summary dashboard • pending litigation • major internal and external events	• audit assurance
"Risk Committee"	• oversees development implementation maintenance of RM across the business	• "top 10" risk dashboard • internal & external events • exposure analysis • regulatory update • hot topics (ad-hoc)	• risk profile • self assessment • loss event data • stress testing • key risk indicators • pending litigation	• audit assurance • effectiveness of RM • cost / value of RM • benchmarking RM
Business heads	• own risks • design and own controls • run the business	• "dashboards" • internal and external events • exposure analysis	• risk profile • self assessment • loss event data • stress testing • key risk indicators • pending litigation	

LLOYD'S

TOOL 10.2
EXAMPLE MANAGEMENT INFORMATION REPORTING TOOL

This is an Excel tool that can be used to create monthly management information. This tool can be found in management information section of the toolkit.

The data used is illustrative and for example purposes only. Operational risk has been used as an example risk class to illustrate the different parts of the reporting suite and is aligned to the different sections within the toolkit (i.e. snap shots have been taken from the internal loss data, KRI and risk and control self assessment sections of the toolkit). The raw data behind these graphics and tables is not stored or held within this report.

LLOYD'S

STRESS & SCENARIO TESTING

SECTION 11

TOOLS

Tool 11.1 – Key steps in stress and scenario testing

Tool 11.2 – Suggested workshop participants

Tool 11.3 – Scenario generation

Tool 11.4 – Potential stress and scenario tests

Tool 11.5 – Example template for stress and scenario tests

Tool 11.6 – Example template for use in a stress and scenario workshop

Tool 11.7 – Aggregation tool method for standardising and aggregating

11 STRESS & SCENARIO TESTING

What are stress and scenario tests?

Stress tests and scenario analyses are intended to enable an organisation to gain a better understanding of the significant risks that it potentially faces under extreme conditions and to provide important input to the determination of related regulatory and economic capital requirements[1]:

- **stress testing** typically refers to shifting the values of individual parameters that affect the financial position of an organisation and determining the effect on the business (for example, a doubling of staff turnover in a key, high dependence business function);
- **scenario analysis** typically refers to a wider range of parameters being varied at the same time. Scenario analyses often examine the impact of **catastrophic** or so called "**tail event"** on an organisation's financial position and/or operational position (for example, a terrorist attack in the city), but could also involve **changes to business plans, shock changes in business cycles** and the **reputational fallout** from, say, large scale fraudulent financial reporting or fraud.

Why are they important?

Stress testing and scenario analysis provides:

- help in evaluating the financial and non financial impact of extreme, unexpected but plausible, large loss events;
- help in determining the overall risk profile and setting the risk appetite of an organisation given the capacity to bear or take on risk;
- an additional valuable source of input to the calculation of capital requirements; and
- validation of stochastic modelling and analysis to confirm the reasonableness of results and calibration of model assumptions.

Stress testing and scenario analysis are therefore integral elements of an organisation's risk management framework. Potential scenarios may be derived in a variety of ways, drawing on **stochastic models**; analysis or repetition of **historic events**; or **hypothetical events.**

FSA requirements

It is important to note that the **FSA has imposed requirements on insurers**[2] to carry out stress testing and scenario analysis for each major source of risk (i.e. each risk group) appropriate to the nature of those sources of risk (PRU 1.2.34-36G), in particular:

- "taking reasonable steps to identify an appropriate range of **realistic adverse circumstances** and events in which the risk identified crystallises";
- "estimate the **financial resources** the firm would need in each of the circumstances and events considered in order to be able to meet its liabilities as they fall due"; and
- "tests should be carried out **at least annually**" (or potentially more often if appropriate).

---

[1] This section draws on the GIRO Working Party 'Quantifying Operational Risk in General Insurance Companies'.

[2] The FSA issued DP05/2 'Stress Testing' in May 2005 which provides feedback in respect of stress testing and scenario analysis from a recent survey of 'large and more complex firms'. The toolkit is consistent with DP05/02.

Practical steps for implementation

How is it done?

The following steps are necessary when conducting stress and scenario tests:

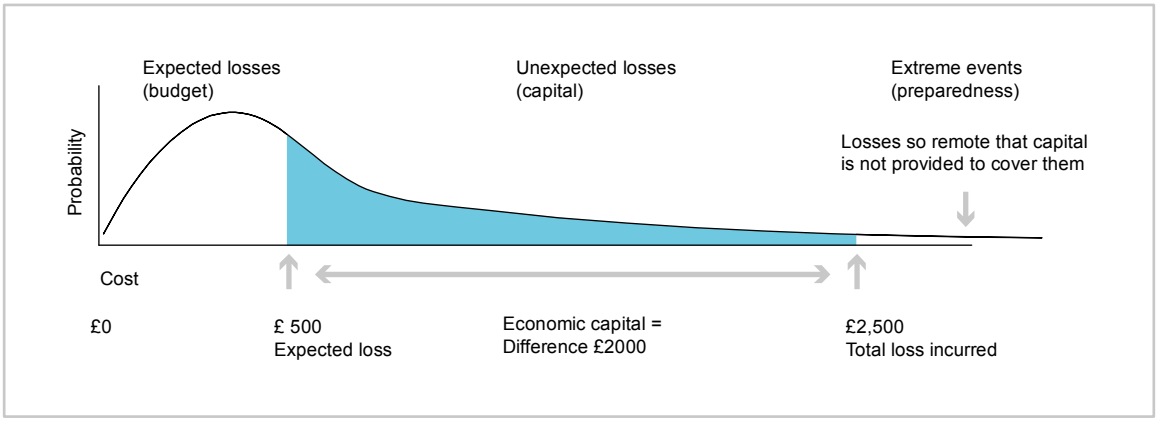
- **clarify the risk categorisation to be used** – because of the FSA's requirements, this will need to be mapped to the FSA risk groups for ICA purposes;
- **identify** a "reasonable set" of **realistic possible events** which reflect the dynamics of the business, drawing on the risk management framework, risk register, executive management and subject matter expert views;
- **assess the impact and probability** of the various scenarios, including direct and indirect effects and the impact of control failures, typically via facilitated workshops;
- **consider wider "ripple effects"** when quantifying the overall effects of each scenario (e.g. a large loss event which leads to reinsurer failure);
- **aggregate the results** of the stress and scenario tests for a given risk group, where appropriate, in order to deal with correlation effects between the scenarios;
- **typically this is done with a correlation matrix –** under this approach, scenario testing is considered and quantified in isolation and a correlation matrix is then specified between scenarios (for example, senior management judgementally allocating a high / medium / low correlation). The results are then aggregated to help derive an overall capital figure for the risk group (e.g. operational risk);
- as a separate exercise, **aggregate the overall results for each risk group** via a second correlation matrix, to help derive an overall capital assessment number.

What events need to be considered?

It is important to understand the nature of the events which need to be quantified by stress and scenario testing, as illustrated below:

- **expected losses –** events that could reasonably be expected to occur within the next 12 months, for which a budget should be held;
- **unexpected losses –** events that are unlikely and therefore not budgeted and for which economic capital is held. Stress tests and scenario analysis focuses on the measurement and quantification of unexpected losses and looks at related reputational damage that might arise;
- **extreme losses –** events that are very remote in likelihood (e.g. one in a 1000 year events) for which capital requirements cannot be meaningfully calculated and capital is therefore not held. In the case of these events the state of preparedness to respond, rather than the amount of capital buffer is more important, for example, by means of business continuity planning.

The nature of these losses is illustrated below:



It should be noted that:

- **economic capital** is held to cover unexpected losses to a specified level of confidence (e.g. to support an "A" rating); and
- **regulatory capital** is the minimum level of capital required by the FSA to cover unexpected losses to a 200 year level of confidence (i.e. to support the ICA).

Relevant toolkit contents

Relevant toolkit contents for stress and scenario testing include:

- **Tool 11.1 – Key steps in stress and scenario testing:** an illustration of a possible approach to stress and scenario testing using operational risk examples;
- **Tool 11.2 – Suggested workshop participants:** highlights some key participants typically involved in workshops at various stages in the stress and scenario development process;
- **Tool 11.3 – Scenario generation:** an illustration of the scenario generation process with some operational risk example events and concerns;
- **Tool 11.4 – Potential stress and scenario tests:** examples of operational risk scenarios that may assist agents when assessing operational risk;
- **Tool 11.5 – Example template for stress and scenario tests:** an example template that an organisation can use during workshops to consider and capture a range of data with regards to scenarios;
- **Tool 11.6 – Example template for use in a stress and scenario workshop:** a template that may help organisations complete a stress and scenario testing workshop;
- **Tool 11.7 – Aggregation tool method for standardising and aggregating:** a tool to standardise the return periods of different scenarios and correlates the scenario results.

It is important to note that guidance in this section is intended to help organisations understand and undertake stress and scenario testing. It is not intended to contradict or add to the requirements set out in the 2006 ICA guidance document or provide guidance on stochastic modelling approaches

LLOYD'S

TOOL 11.1
KEY STEPS IN STRESS & SCENARIO TESTING

The following key steps illustrate one possible approach to stress and scenario testing, using operational risk examples.

Step 1: Initial planning

Hold an **initial planning workshop** to:

- review operational risks within the organisation's risk register and **identify a range of potential 'straw men', extreme scenarios** as a starting point for scenario development;
- **identify key subject matter experts,** who should participate in workshops to develop and confirm the scenarios, and an appropriate **facilitator** for each workshop, and arrange the workshops;
- **prepare a standard template to guide scenario development** for use in the workshop**,** with a standard scoring method to assess the impact and probability of the scenarios;
- obtain **executive management's view** on major and extreme events which could affect the organisation, prior to the workshops; and
- collate other **useful sources of material** for use in the workshops, for example, the operational risk register, Basel II operational risk loss event categorisation, the ICA guidance document and FSA guidance on operational risk.

Step 2: Hold the workshops

Hold **scenario workshops, to challenge and develop** the scenarios:

- **debate** the **proposed scenarios** and modify as appropriate, for example, where the scenario is generally not seen as being extreme, or does not cover sufficient risks, or is otherwise felt to not be applicable;
- scenarios are intended to be **significant, rare or extreme 1 in 200 year events**, which may be brought to life by asking "could you see this event happening in your lifetime";
- **complete a scenario template** for each agreed scenario, which includes the following fields:
    - test name;
    - attendees;
    - FSA risk group;
    - detailed description of the event;
    - the inherent and residual event impact – qualitative rating (e.g. high, medium, or low);
    - the subjective probability of the event (rare, extreme, etc.);
    - controls assumed to be operating – all listed;
    - total quantified impact – all expected impacts listed, split by risk group (if appropriate), with an explanation of the relationship between causes and consequences;

  - dependencies and ripple effects – an assessment of any possible interrelationships between the various scenarios; and
  - sensitivity to key factors in the scenario test.
- **assign a "scenario owner"** to each to complete and document the scenario.

The following are six examples of completed operational risk scenarios:

  - damage to physical assets and denial of physical and logical access due to a terrorist bomb;
  - failure of a key outsource provider to perform;
  - organisation business practice or product flaws – flawed wording in document;
  - improper business or market practice – e.g. failure to execute strategy or deliver essential process change on a timely basis;
  - financial crime – significant internal or external crime; and
  - pension fund deficit caused by incorrect mortality assumptions and adverse market movement.

Step 3: Aggregation of scenarios

Finally, aggregate the results of the above scenarios:

- initially, **convert the scenario results to the desired return period** (e.g. 200 years for an ICA) by means of an assumed underlying distribution;
- use a **correlation matrix** to assign a level of correlation between the scenarios (as agreed at the workshop) and then calculate a **diversification credit** to be subtracted from the sum of the individual stress and scenario stress test results.

LLOYD'S

TOOL 11.2
SUGGESTED WORKSHOP PARTICIPANTS

Workshops held to develop, discuss and challenge risk scenarios should ideally contain participants from across the business in order to:

- provide a **broad understanding** of the significant, extreme risks faced by the business, the **potential consequences or impact** of the risks and the related control environment; and
- provide an **understanding of potential cost** and **reputational impacts** that are relevant to the business.

Individuals from the following areas may be considered as **key participants**:

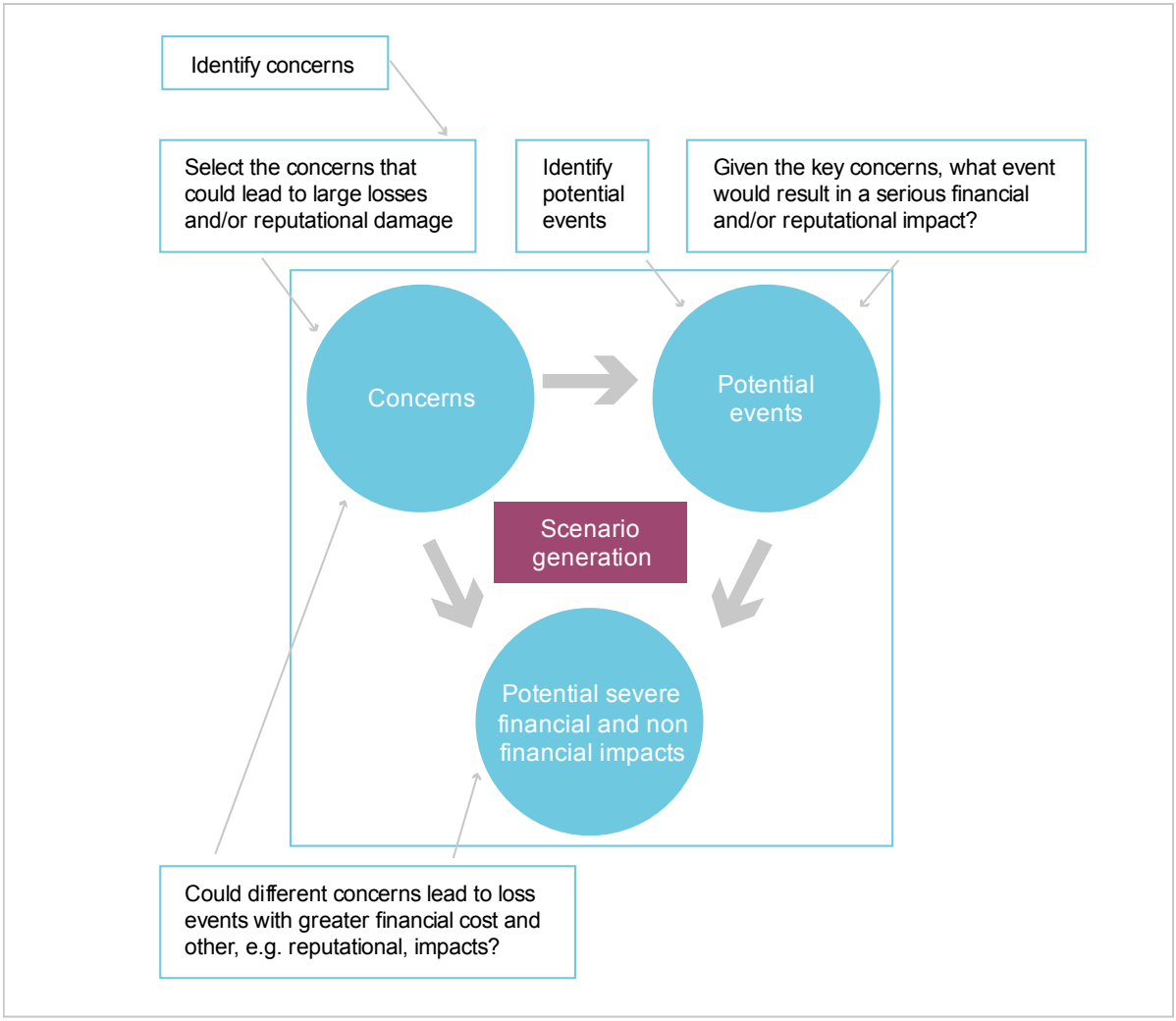
- **risk owners** – individuals who perform risk self assessments and who are responsible for identified risks;
- **senior management** representation – providing a big picture view of potential operational risk scenarios;
- **human resources** representation – where people / staff related scenarios have been identified, e.g. internal fraud;
- **IT** representation;
- **business continuity planning** representation – applicable if a separate function exists; and
- **finance** representation.

Consideration could be given to **segmenting workshops** into **"scenario generation"** and **"scenario evaluation"** making better use of time and adding most value for each of the relevant participants.

TOOL 11.3
SCENARIO GENERATION – AN ILLUSTRATION & EXAMPLES

The diagram below illustrates the scenario generation process and could be used to facilitate a workshop to discuss, challenge and develop scenarios.

Workshop members can generate a realistic extreme scenario by considering which combination of identified concerns and events would lead to the most severe financial cost and/or reputational impact.



Example concerns for operational risk may include:

- potential **control failures** – control can fail over time, even when rated highly in the risk and control self assessment (self assessment) process;
- changes in the **performance** of the business processes (including controls), systems, staffing or infrastructure;
- changes in the business **processes**, systems, staffing or infrastructure contained in business plans;

- changes in the **type of business** undertaken; and
- changes in the **business environment**.

Example operational risk events may include:

- **specific events** that could have a significant impact on the organisation (e.g. system outage, fire, flood), including consideration of the most likely underlying causes of these events (e.g. a system upgrade could be a potential cause of an IT system failure / outage);
- **relevant trends** in business plans which may add to / detract from concerns;
- use and challenge of any available **internal / external databases** where applicable; and
- **media articles** reflecting on the “blockbuster” loss event experiences of other financial institutions.

LLOYD'S

TOOL 11.4
POTENTIAL STRESS & SCENARIO TESTS

The following are some **examples of operational risk scenarios** that may assist agents when assessing operational risk. These examples are not exhaustive and organisations will need to consider scenarios which are appropriate to their business:

- loss of the largest underwriting team to a competitor, resulting in additional recruitment and training costs and loss of business;
- a major loss is notified late, controls do not catch it promptly and many additional policies are written with cumulating losses;
- a coverholder breaches US licences with the subsequent loss of the licence in the largest US state;
- loss of the syndicate's largest broker through regulatory action;
- error or omission leads to voiding / mismatch of a significant part of the syndicate's reinsurance programme;
- a major claim is conceded due to lack of agreed policy wording;
- terrorist attack in the City of London, with the total loss of the office, documents, IT and central processing at Lloyd's, requiring relocation and full Disaster Recovery Programme (DRP) and Business Continuity Plan (BCP);
- losses arising from accounting valuation errors and misinterpretation of accounting standards and misrepresentation of financial reports; losses resulting from lack of completeness or accuracy in financial data;
- losses stemming from accepting money that stems from criminal activity, corruption or the misappropriation of public funds (money laundering);
- losses resulting from incomplete documentation (company and policyholder records);
- losses resulting from mishandling of client, employee and company data;
- losses resulting from unauthorised activities such as transactions not reported (intentional), unauthorised transaction types or mis-marking of positions (intentional);
- product mis-selling. Losses resulting from any sale of products to clients who later are able to reasonably claim that the product was not suitable for them; and
- losses arising from a protracted breakdown(s) of central IT systems and networks.

LLOYD'S

TOOL 11.5
EXAMPLE TEMPLATE FOR STRESS & SCENARIO TESTS

This **template** may be used in a stress and scenario workshop to help consider the full physical and other effects of potential scenarios, as illustrated for one operational risk scenario.

Event	Scenario options	Physical effects	Other effects	Potentially relevant reference event	Risk register reference
Damage to physical assets Lloyd's building plus 500m environment destroyed / damaged / denial of access	• terrorism bomb in City – conventional or "dirty"	• Lloyd's building damaged beyond repair	• loss of "key man" figures, resulting in leadership "void" and loss of confidence in Markets operation	• 1992/3 IRA bombs	**Primary risk –** failure / loss of key infrastructure **Secondary risks –** failure of core processing / ineffective management of IT / failure of key service providers / ineffective governance / failure of strategy
	• major water supply contamination	• site "out of action" for prolonged period	• potential death / injury to staff and ensuing compensation claims	• both occurred during weekend period and City was re-opened by Monday morning	
	• Thames surge	• damage to organisations' offices	• claims on Lloyd's policies for damage / injury within environment	• cost of repairs from 1993 Bishopsgate bomb estimated £1bn	
		• relocation of "Underwriting Room"	• loss of business to Lloyd's Market	• 9/11 WTC disaster	
		• relocation of key staff to alternative sites	• cashflow difficulties for organisations	• Cantor Fitzgerald	

Event	Scenario options	Physical effects	Other effects	Potentially relevant reference event	Risk register reference
		• loss of physical assets (e.g. PCs) and operational assets (e.g. IT systems / processes / data / documentation)	• pressure on capital e.g. CIL difficulties		
		• financial cost of rebuild / repair over and above insurance provision	• pressure on syndicate reserves		
		• extensive data / document recovery process required	• pressure on Lloyd's solvency		
		• casualties e.g. employees / Market staff / visitors	• pressure on Lloyd's security rating		
		• loss of intellectual assets and underwriting talent	• reputational damage / loss of market place / industry credibility		
		• inability to underwrite due to lack of skilled people and appropriate systems			
		• delayed / reduced capability to provide key processing functions to Market			
		• prolonged operational inefficiencies			

LLOYD'S

TOOL 11.6
EXAMPLE TEMPLATE FOR USE IN A STRESS & SCENARIO WORKSHOP

This is an Excel tool that can be used to help an organisation complete a stress and scenario test workshop. This tool can be found in the "Stress and scenario testing" section (11) of the toolkit.

The data in this template is illustrative and for example purposes only. The tool has been designed to highlight the areas of information deemed important when designing stress and scenario tests.

LLOYD'S

TOOL 11.7
AGGREGATION TOOL METHOD FOR STANDARDISING AND AGGREGATING

This is an Excel tool that can be used to standardise the return periods of different scenarios and correlate the scenario results. This tool can be found in “Stress and scenario testing” section (11) of the toolkit.

SECTION BREAK

LLOYD'S

RISK CULTURE

SECTION 12

12 RISK CULTURE

What is risk culture?

The FSA defines risk culture as the following:

> **"a firm's risk culture encompasses the general awareness, attitude and behaviour of its employees to risk and the management of risk within the organisation"**

Why is it important?

Embedding risk management in an organisation

Bringing about fully effective risk management, and embedding risk management into the minds, behaviours and activities of all staff, require a significant cultural change

What sort of risk culture should I be aiming for?

The following are typical characteristics of a strong risk culture:

- **positive and accepting** – people consider risk naturally, without being told to do so;
- **open and transparent** – everyone feels free to talk about risk honestly without creating a blame culture. This must however be supported by actions that don't conflict with the policy otherwise people will perceive it as merely rhetoric;
- **acknowledging** – risk is acknowledged as being part of everyone's daily activities, strategic & business planning and projects;
- **risk closely linked to performance and development –** risk forms part of departmental and personal objectives, performance development and appraisal processes; and is therefore reflected in reward structures;
- **awareness of expectations** – everyone knows their responsibilities and their freedom to act in respect of risk.

Questions to consider before implementation

- To what extent are all employees able to **articulate the expectations of them** and their **scope of freedom to act** with respect to risk?
- To what extent does the **high level sponsorship of risk management** encourage the timely sharing of significant risk information?
- Does the **attitude and do the actions of management** encourage the open and honest discussion of risk?
- To what extent has the organisation developed **consistent training, development, tools and techniques** for risk management that are used throughout the business?
- Are **rewards structured** in such a way as to encourage risk management activities as part of everyone's job?
- Are the **benefits of risk management** understood by all, so that people do risk management because they want to, rather than because they have to?

Where do I start?

Context-setting

- What sort of organisation is it?
- What are the main types of risk faced?
- What magnitude are the most significant risks likely to be?

Objectives

- What are the objectives of the organisation? Make sure these are clearly agreed and articulated.
- What are the objectives of risk management in the organisation? Are you doing it for the business benefit, as a result of regulatory requirements, or pressure from other stakeholders?

Stakeholders

- Who are the significant stakeholders?
- What are their needs?
- What sort of relationship do you have with them?
- How do you want to manage those relationships?

What's already done?

- Don't re-invent the wheel. A large part of many peoples' jobs is managing risks… but it is likely that it will be called something else.
- Speak to people. Ask them what they do and why.

Who's going to do it?

- Risk management is the responsibility of everyone, but the risk management co-ordination and support function is likely to be done by an individual (risk manager) or team (risk management department).

Where do you start? 3 vital stages:

- **convince yourself –** make sure that you understand what you intend, test it locally;
- **convince supporters –** e.g. consultation, participation, information, pilot more widely (some of these need to be within the senior management team); and
- **convince adversaries –** look for gaps, overlaps, easy wins, long term projects and have a staged roll out. This is very difficult to embed (rather than impose) in one go in an organisation of any size.

And lastly, but most importantly, **PERSEVERE** – it will take time!

Tips for embedding and implementing risk culture

High level sponsorship a "must"

Why?

- it sets the tone across the organisation, and enables appropriate resource and importance to be given to risk management
- to develop the positive and aware attitude to risk amongst senior managers, which then filters down

What do you need?

- active support of the Managing Director / Chief Executive Officer
- risk champions amongst the senior management group
- support for the embedding initiative from the senior management group

What happens if you don't have it?

- lack of understanding and enthusiasm will be the norm
- threatened feeling as a department / practice
- lack of buy-in at the top makes embedding impossible

Practical tips on how to develop and maintain it:

- clear, concise, and early individual briefings and consultation with directors and senior managers;
- clear, strong, repeated messages using common terminology coming from the senior management team, particularly the Chief Executive Officer, are extremely powerful and work particularly well when combined with repeats of the messages later. To this end, the provision of suitable messages and sound bites for the Chief Executive Officer to use is an extremely effective tool;
- explain the benefits to be gained from risk management;
- emphasise the benefits that will appeal to them (better / easier decision making, more effective meetings, better measurement);
- show them the benefits that others are enjoying, especially competitors;
- build on what already exists. Enhancement and adaptation of what already exists is almost always more palatable and easier to buy in to than wholesale change. Be prepared to recommend such change if that is the right thing to do;
- make appropriate staff accountable for risks, for controls, for action plans and link it to performance appraisal and reward; and
- get risk management mentioned in the organisation business plan, and annual report and accounts as something the company supports and does.

Involve all staff

- promote an organisational culture that says everyone is a risk manager;
- explain how risk management helps:
    - deliver results;
    - promote innovation;
    - improve resource allocation;
    - reduce failure or inability to cope with crises. People must be able to see "what's in it for me?"
- involve lots of people at all stages of the risk management cycle, including objective-setting, risk identification and risk and control self assessment;
- risk must become part of day to day activities and core processes. Every project, business plan and workstream must include considerations of the risks involved and the risks they are addressing;
- risk management is not something that can be done effectively by the risk manager or risk management department in isolation. The risk manager should identify, harness and build on the expertise that exists within the organisation. There is a dual benefit to be utilised:
    - people in the organisation (rather than the risk manager) know the business best. They are therefore in the strongest position to have the appropriate answers, therefore benefiting risk management;
    - those people in the organisation therefore feel involved and have a better understanding of what risk management is and how it is part of their responsibility.
- encourage people to manage their own risks, with risk managers acting as a support mechanism;
- document and communicate risk management roles and responsibilities;
- include risk management in personal objectives;
- develop risk-based recognition and reward initiatives;
- recruit on attitude as well as experience;
- written code of ethics to reinforce values.

Training and awareness

Key aims:

- all relevant staff in the organisation understand the basic concepts and benefits of risk management;
- all staff are aware of and understand the organisation's approach to risk management; and
- all staff apply the organisation's risk management principles in day to day operations.

Failure to achieve these will result in people acting against the stated aims of the organisation, confusion, wasted effort and unnecessary conflicts. It is important that everyone is pointing in the same direction, and that the direction is the right direction.

Practical tips on how to develop and maintain training and awareness:

- include risk management objectives in department and personal objectives, appraisal, pay & rewards;
- questionnaires can be used to assess level of awareness and understanding, and also act as an advertisement, raising the profile of risk management;
- training is tailored to specific needs of departments, teams, individuals. Training must be ongoing, not just one-off. There is a need to keep training programs up to date with developments (and new recruits);
- encourage, and create opportunities for, training and development;
- reference sources (library, bulletins / newsletters, briefing notes, risk champions, etc.). Not only should some or all of these be in place, but everyone should know where to find it and who they can turn to for advice and support;
- if appropriate, develop risk management pages on the local intranet;
- encourage the use of role models as ambassadors for risk management and culture change;
- recognise that there is a wide range of perceptions about risk. Individual psychology, past experience, individual risk appetite, organisational roles and group dynamics influence peoples' perceptions and decision-making with respect to risk;
- user groups, and local experts or "risk champions" may be helpful; and
- develop a dedicated risk management helpline, as this may also be useful.

Communications

- regular communications keep everyone informed of developments, but also serve as a gentle reminder, keeping risk management from slipping to the back of peoples' minds;
- encourage and facilitate meetings, seminars, workshops;
- ensure that risk is an integral part of Board agendas;
- communicate expectations of individuals and departments with respect to risk;
- agree and publish a risk assessment and reporting timetable;
- develop and communicate escalation procedures for risk issues;
- commonly agreed and understood terminology and language should be published, communicated, publicised and readily accessible. This facilitates clear communications and helps to minimise confusion and misunderstanding;
- ensure constancy and consistency of approach, i.e. it is seen and experienced over and over again; and
- a risk manager can help draft communications for other individuals and departments that include key messages on risk.