CELEBRATING 40 YEARS
OF ENGAGING TREASURERS

GIVING DIRECTION

BRIEFING NOTE:

GUIDANCE FOR PRODUCING TREASURY POLICIES

A TREASURER'S CHECKLIST

OCTOBER 2019

CELEBRATING 40 YEARS
OF ENGAGING TREASURERS

Briefing note

GUIDANCE FOR PRODUCING TREASURY POLICIES

A TREASURER'S CHECKLIST

The Association of Corporate Treasurers

The Association of Corporate Treasurers (ACT) sets the benchmark for international treasury excellence. As the Chartered body for treasury, we lead the profession through our internationally recognised suite of treasury qualifications, by defining standards and championing continuing professional development. We are the authentic voice of the treasury profession representing the interests of the real economy and educating, supporting and leading the treasurers of today and tomorrow.

For further information visit **www.treasurers.org**

Guidelines about our approach to policy and technical matters are available at **www.treasurers.org/technical**

Author: **Gurdip Dhami ACA AMCT**

CONTENTS

EXECUTIVE SUMMARY

A key responsibility of the treasurer of an organisation is to manage financial risks such as foreign exchange risk, interest rate risk, liquidity risk and funding risk. Where a treasury function does not exist (as in smaller or less complex companies) the finance director or accountant is typically responsible. This briefing note sets out one approach to producing treasury policies based on current practice in risk management.

In this briefing note a treasury policy is defined as the response to a treasury risk such as those outlined above and a treasury policy document contains the treasury policy along with the key factors supporting the policy such as the description of the risk, assessment of risk and the risk appetite.

This briefing note should be useful to all practitioners involved in producing and using treasury policies such as treasurers, treasury managers, the finance director/financial controller of smaller firms, as well as Board members. The process described is general and can be applied to companies of all types and size. This briefing note sets out the importance of aligning treasury policies with the organisation's profile, organisation's strategy, and the existing corporate governance and risk management frameworks of the organisation.

The paper recommends a standard and well-established process in risk management to produce treasury policies as set out below:

- **Identify the risks**
  Treasury risks are identified using a variety of methods.

- **Assess the risks**
  Once treasury risks have been identified, the magnitude and likelihood of those risks are ascertained to assess their potential impact on the organisation.

- **Evaluate the risks**
  The evaluation of a risk requires that the organisation's appetite for that risk should be considered and compared with the current and potential risk exposure.

- **Respond to the risks (the 'treasury policy')**
  The response to a treasury risk includes the following options:

  - Avoid the risk (e.g. by adjusting the business strategy although in practice this may not be possible)
  - Transfer the risk (e.g. by insurance)
  - Reduce the risk (e.g. introducing controls or other mitigation)
  - Accept the risk (e.g. if the risk is not material, if the organisation actively seeks this type of risk because it has expertise in the area, or if there are off-setting 'natural hedges' in the organisation).

  Internal controls are used to manage risks and this briefing note describes a common classification which can be used to help create the right mix of controls: directive, preventative, detective and corrective.

- **Report the risks**
  It is important that risks are reported and reassessed on a regular basis to ensure risk exposures are within the risk appetite of the organisation and that internal controls are operating correctly.

A checklist which sets out the main contents of a treasury policy document is provided in section 7.2 along with illustrative examples of treasury policies to show the application of the general process described in this note. However treasurers should produce their own policy document structure and policies based on their organisation's profile and risk management framework. For example, it is likely that the risk definitions and risk terminology used in this paper may not align with those used by many organisations as there is a wide array of models and language used in risk management.

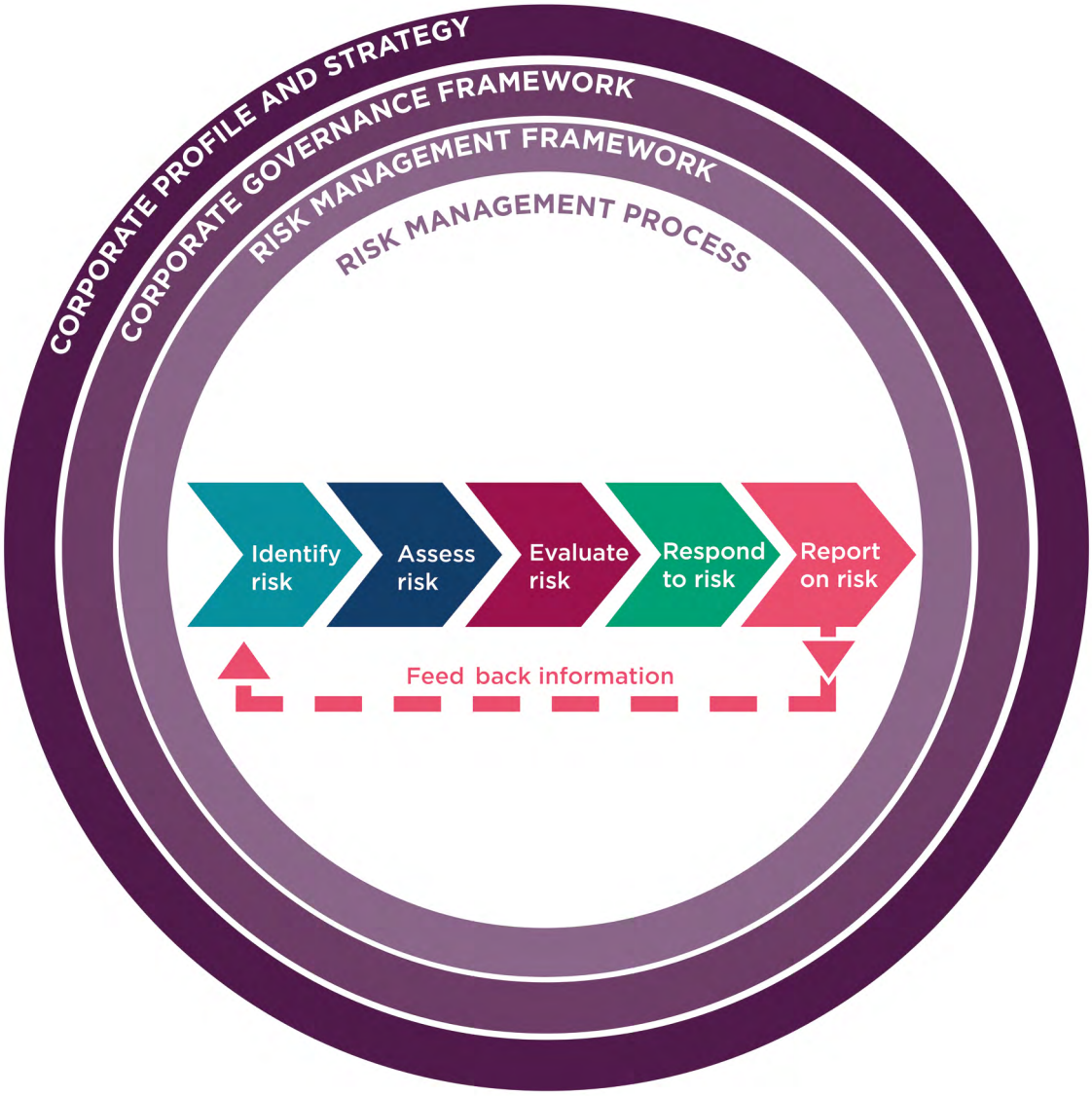
Extracts from the annual reports of companies have been included in this briefing note to illustrate points where possible.

This note provides general guidance on how a treasury policy can be formulated, and examples are provided to illustrate the approach. However, nothing in this paper should be construed as giving specific advice as the circumstances and risk attitude of companies will vary – it is possible that two similar companies may decide on a different response to the same type and size of treasury risk.

1 KEY ELEMENTS IN PRODUCING TREASURY POLICIES

Treasury risks form part of the organisation's overall current and future risk assessment, which helps inform its corporate strategy. The responses to treasury risks as set out in the treasury policy documents should be based on, and included in, the existing corporate governance and risk management frameworks which direct and control the organisation: the process of managing risks is a key part of the governance framework of an organisation – see Figure 1.

Figure 1: Corporate governance and the risk management process



1.1 CORPORATE STRATEGY AND TREASURY OBJECTIVES

Understanding the corporate strategy of the organisation is important when producing risk policies, including treasury policies, for the following reasons:

- The current and future risk exposures will flow from the strategy adopted by the organisation. For example, if a company has a strategy to expand overseas then foreign exchange exposures will arise which will need to be managed. Examining the current and future profile of the company will help to identify the risk exposures that need to be managed
- The Board's attitude to risk is a key part of formulating corporate strategy and in turn an important factor in producing risk policies, for example through the articulation of risk appetite statements.

Treasury objectives should be aligned with the overall organisation strategy and these objectives influence treasury policies because they determine the scope of the risk exposures to be managed by the treasury function. For example, some treasury functions are responsible for managing the credit rating of their organisation and therefore treasury will be responsible for producing the related treasury policy, and managing the resulting risk exposure (e.g. rating downgrade) in conjunction with other departments of the organisation.

The expected contribution of the treasury function to the profits of the organisation needs to be clearly set out as this will determine the attitude to the treasury risk exposures – three common approaches are those of 'cost centre', 'value-added centre' or 'profit centre'.

a. A cost centre is a treasury which acts as a service centre which hedges operational exposures, at a cost. In addition to managing risks, a cost-centre treasury can add value by using techniques such as currency-flow matching or cash-balance aggregation to reduce costs whilst not adding to risks.

b. Treasury value-added centres are a more risk-tolerant variant on a pure cost centre. A value-added centre is a treasury which – like a cost-centre treasury – acts primarily as a service function, but which is allowed a degree of discretion about when to hedge, with a view to adding value to the organisation by reducing net costs. Hence a value-added treasury can add value in a way which is beyond the authority of a cost-centre treasury. However, value-added treasury centres are not allowed to take speculative positions in the financial markets: the only speculation that is allowed is to leave existing commercial exposures unhedged and this discretion is subject to limits on the amount of unhedged exposure that the organisation is prepared to tolerate. Value-added treasury centres are sometimes also known as cost-saving treasury centres.

c. A profit-centre treasury may actively create market positions with a view to earning profits, as well as hedging. Profit-centre treasuries require sophisticated treasury operations and systems with very strong internal controls and management reporting.

The board must fully understand and decide which approach fulfils the objective of aligning the treasury's risk-management policy with the wider strategic objectives and risk propensity of the organisation. The board's appetite for risk will be reflected in the detailed policies covering how the treasury will react to identified financial exposures and the hedging of those exposures. At the same time the importance of performance measurement applies equally whether the treasury operates as a cost centre, value-added centre or profit centre.

1.2 CORPORATE GOVERNANCE – RELEVANCE FOR TREASURY POLICIES

The treasurer should use the existing corporate governance structure within the organisation, including risk management processes, to produce treasury policy documents. Although the risk management framework will vary from organisation to organisation and will depend on the size and complexity of the organisation, key elements usually include:

- Standards for producing risk management policies including the required content (using templates if they exist) and approval process
- Ownership and accountability for risks and policies
- A process to determine the key risks facing the organisation and the organisation's risk appetite
- Mechanisms to monitor and report the effectiveness of risk policies.

The risk management process is a key part of corporate governance and is further described in section 2.

An overview of the UK Corporate Governance Code ('the Code'), which is mandatory for companies with a premium[1] listing on the London Stock Exchange, is provided in Appendix 1, along with extracts from the Code which relate to risk management. The Code can also be a useful guide for companies which do not have to follow it by law.

1. Companies have the choice of three types of listing on the main market of the London Stock Exchange – a Premium (formerly Primary) listing, a Standard (formerly Secondary) listing and an admission via the High Growth Segment. Issuers with a Premium listing are required to meet the UK's super-equivalent rules which are higher than the EU minimum requirements while a company with a Standard listing has to meet EU harmonised standards only rather than the UK 'super-equivalent' requirements.

2 RISK MANAGEMENT FRAMEWORK

A risk management framework provides an organisation with the mechanisms and systems to develop an overall approach to managing risks by creating the means to discuss, compare, evaluate and control substantially different risks.

Risk management frameworks usually include:

- A risk management process
- A risk infrastructure (including reporting, governance and IT tools)
- A risk strategy (philosophy, appetite, attitude etc)
- Risk protocols (procedures, tools, techniques etc).

The terms risk management framework and risk management process are sometimes used interchangeably but we define risk management process as a subset of the risk management framework.

A typical risk management process can be seen as a series of phases, each of which progresses on from the previous phase as shown in Figure 2 below:

Figure 2: Risk management process

RISK IDENTIFICATION:

This is the definition, identification and classification of an organisation's treasury risk exposures and their sources.

RISK ASSESSMENT

This is an assessment of the likelihood of each risk occurring and of its potential impact.

RISK EVALUATION

In this phase, risk exposures are compared against the organisation's appetite for risk.

RISK RESPONSE

Once risks have been evaluated, the responses to them can be planned and implemented. This phase includes the design of treasury policies.

As described in section 3.3, under an 'Enterprise Risk Management' approach, all main risks should be considered together, for example at a risk committee (if one exists) or by the Board so that relationships between the risks, if they exist, can be evaluated: for example, the response to a risk may have to be adjusted if it is negatively correlated to another risk faced by the organisation.

RISK REPORTING

This phase helps to ensure that risks are being managed as agreed, i.e. that methods and processes are being properly applied and carried out, and to check that the responses are having the desired effect.

FEED BACK INFORMATION

The feedback loop – the reviewing of risk management outcomes compared to plan – is vital within the risk management process so that risk management practice evolves to keep pace with developments in the business and in the outside world.

Having a consistent approach to risk management within the organisation helps bring information together in order to deal with risk issues at the overall corporate level.

Figures 3a, 3b, and 3c below show three examples from the annual reports of companies' risk management processes. In each case, even though the terminology varies, the main elements of the process described are: identification, assessment, evaluation, response (management), reporting and feedback (monitoring).

Figure 3a: Diageo Annual Report 2018, Page 19

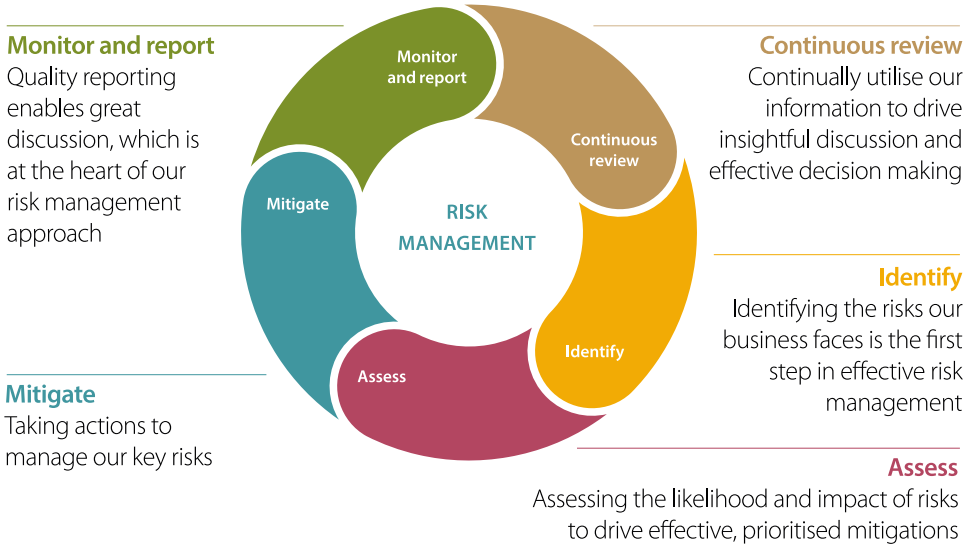


Figure 3b: Johnson Matthey Annual Report 2018, Page 77

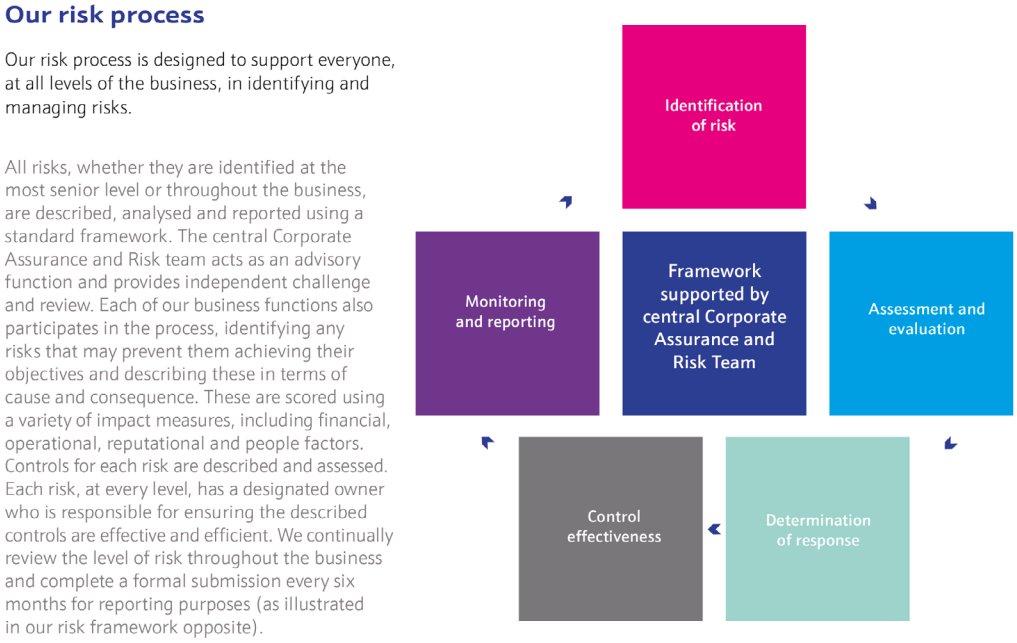
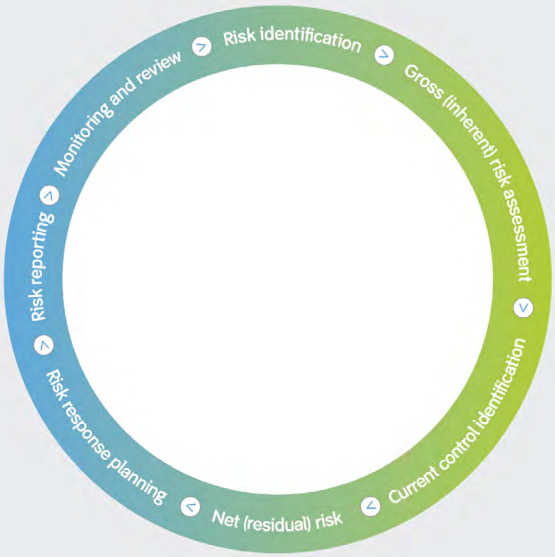


Figure 3c: Smith & Nephew Annual Report 2018, Page 41

Risk management life cycle

Our risk management life cycle was fully refreshed in 2017 and was updated in 2018 to align with our new strategic imperatives which we launched in December.

Our Risk Management Policy, sponsored by our Chief Executive Officer, is supported by an Enterprise Risk Management Manual and the risk team provide regular training to all risk champions throughout the year. As in 2018 risks continue to be managed through a 'bottom up' and 'top down' process, with regular oversight from the Executive Committee and quarterly reports to the Board Committees. An overview of our risk management life cycle can be found below:



1 Risk identification
IDENTIFYING risks associated with the achievement of our objectives by function at the Group level.

2 Gross (inherent) risk assessment
ASSESSING the level of inherent (gross) risk.

3 Current control identification
IDENTIFYING existing controls to mitigate risks.

4 Net (residual) risk
ASSESSING the level of residual (net) risk after mitigation so that risk levels are managed within defined tolerance thresholds without being over-controlled or foregoing desirable opportunities.

5 Risk response planning
IDENTIFYING additional actions required to meet our expected risk tolerance level and **ASSIGNING** risk owners, timeframes and actions for ongoing management and reporting.

6 Risk reporting
REPORTING the status of our most significant risks through the 'bottom up' business area processes and the 'top down' Executive Committee and Board process.

7 Monitoring and review
MONITORING of risks and actions by management, the accountable Executive and Board.

Appendix 2 provides extracts from a guidance note issued by the Financial Reporting Council in September 2014, "Guidance on Risk Management, Internal Control and Related Financial and Business Reporting". The note provides useful information for treasury professionals who are involved in implementing their organisation's risk management processes and describes the key elements of best practice for risk management. The note also includes information on an organisation's reporting requirements relating to risk and going concern which are not covered in this briefing note.

3 IDENTIFICATION AND CLASSIFICATION OF TREASURY RISKS

The first step in risk management is to identify the key risks that an organisation faces. It is also important to capture 'emerging risks' which are potential risks which the organisation does not currently face but which may materialise in the future.

There are various definitions of risk and they usually include some reference to the impact of uncertainty. The ISO 31000 International Standard on Risk Management defines risk as the effect of uncertainty on objectives:

- An effect is a deviation from the expected. It can be positive or negative.
- For an organisation, objectives may include a return on company target (eg. return on equity), minimum profit level or minimum cash flow.
- Examples of uncertainty include potential changes in market rates, regulation or credit quality of counterparties.

3.1 METHODS TO IDENTIFY TREASURY RISKS

The identification of risks should be a continuous process so that new risks are identified on a timely basis. Depending on the company profile and the prevailing economic environment, the frequency could be monthly, quarterly or semi-annually. Common methods used to identify key risks include:

3.1.1 REVIEW OF THE FINANCIAL STATEMENTS AND MANAGEMENT ACCOUNTS

A review of the financial statements and management accounts of an organisation will show those items, such as revenue, costs, assets and liabilities, whose values are directly susceptible to uncertainties such as foreign exchange rates, interest rates, commodity prices and funding costs. The range and size of uncertainties will vary from organisation to organisation.

For example, if a UK company purchases goods from overseas priced in a non-sterling currency then the profit and cash flow of the company will be impacted by changes in the non-sterling currency relative to sterling.

At each period end (e.g. monthly), the management accounts of an organisation should be examined to see whether there are any unexpected variances which have been caused by uncertainties that have not previously been identified.

Although it is a useful starting point, a review of the financial statements will not detect indirect exposures. For example, if a company pays an overseas supplier in sterling, the supplier may over time adjust their prices quoted in sterling to take into account changes in the foreign exchange rate.

3.1.2 RISK ASSESSMENT WORKSHOPS

Workshops can identify risks faced by the organisation by pulling together the knowledge, expertise and experience of people in relevant departments. This is particularly useful in identifying indirect exposures (i.e. those not easily identifiable in the financial statements) and emerging risks. The workshops could also be a useful forum to discuss the response to risks, setting the appropriate parameters for scenario testing, identifying potential contingency plans for stress events and for identifying emerging risks. Although it will probably be efficient to organise the workshops by department (e.g. corporate treasury, finance, tax, sales and marketing, production etc) there should also be some organisation-wide workshops to ensure that the relationship between the risks can also be examined.

It is likely that the workshops will be managed by the risk department (if it exists) or potentially internal audit, and the results will be provided to the Board for review.

Some organisations ensure that their risk process incorporates regular workshop-like discussions at all levels of the organisation including the board, regional teams etc – to ensure risk is at the forefront of people's thinking and is not seen as a bureaucratic paper exercise which is simply a matter of ticking boxes.

3.1.3 REVIEW OF COMPETITOR ANNUAL REPORTS

It is often useful to review the annual reports of competitors for two main reasons:

a. Identification of risks - general

The annual reports may set out the key risks of the competitor, both current and emerging, which could assist in identifying relevant risks in one's own organisation. However, the level of disclosure will vary and, if the organisation is not a listed company, may be limited.

b. Identification of risks caused by the actions of competitors

The way in which a competitor manages its risks may lead to risks in one's own organisation; see example in Figure 4 below. The level of disclosure may be limited.

Figure 4: Example showing the impact of a competitor's FX strategy

A UK-based company sells a product to US customers for $1,000 and has a German competitor which sells a very similar product also for $1,000. Assume that:

- The $1,000 price works for both companies given their cost base and profitability objectives
- The current exchange rates are GBP/USD=1.30 and EUR/USD = 1.15

Changes in both GBP/USD and EUR/USD rates could have an effect on the profitability and competitiveness of the UK-based company; see scenarios below:

	UK Company	German Company
Scenario 1: Initial FX Rates and Sales Price		
Sales Price (USD)	1,000	1,000
Initial FX rate	1.30	1.15
Cash received (GBP and EUR)	769	870
Scenario 2: GBP Strengthens in relation to USD		
Sales Price (USD)	1,000	1,000
FX Rates	1.60	1.15
Cash received (GBP and EUR)	625	870
The UK Company receives less cash if GBP strengthens and sales price remains unchanged		
Scenario 3: GBP Strengthens and UK Company increases sales price in USD		
Sales Price (USD)	1,225	1,000
FX Rates	1.60	1.15
Cash received (GBP and EUR)	766	870
The UK Company receives similar cash as before but is less competitive		
Scenario 4: EUR Weakens and sales price remains as USD 1,000 for both UK and German Companies		
Sales Price (USD)	1,000	1,000
FX Rates	1.60	1.00
Cash received (GBP and EUR)	625	1,000
The German company receives more cash and is more profitable		
Scenario 5: EUR Weakens and sales price is reduced by the German Company to USD 870		
Sales Price (USD)	1,000	870
FX Rates	1.60	1.00
Cash received (GBP and EUR)	625	870
The German company is more competitive than UK Company and receives same EUR cash as scenario 1		

Scenario 2 shows that, as expected, the UK-based company is directly exposed to changes in the GBP/USD rate. Over the short term the company could hedge the exposure using FX forwards.

Scenario 3 shows that the UK company increases its sales price in USD in order to mitigate the effect of GBP strengthening but this makes its product less competitive than that of the German company and over the long term it could lose sales.

Scenario 4 shows that if EUR weakens relative to USD, then even if the sales price of its product remains unchanged, the German company receives more cash from its sales while the cash receipts of the UK company remain the same. The German company could generate more cash to develop its product or increase its marketing campaigns, and thus weaken its UK competitor. In this way the UK company has an indirect exposure to the EUR/USD rate.

Scenario 5 shows that the German company can afford to lower its price if the EUR/USD rate weakens and still receive about the same EUR cash as before from sales. The lower price offered by the German company will make the UK company's product less competitive and reduce its sales. Again, the weakening of the EUR/USD could lead to negative consequences for the UK company even though it doesn't have a direct exposure to EUR.

3.1.4 DISCUSSION WITH STAKEHOLDERS

The organisation's management should consider feedback provided by stakeholders, such as shareholders, bond holders, loan providers, rating agencies and regulators, on the key risks of the organisation and/or competitors.

3.2 RISK REGISTER

Once the key treasury risks have been identified, they can be set out in a 'risk register' along with other risks identified by the organisation's management, such as strategic, compliance, health and safety etc. – an organisation template can be used if one exists. The risk register should describe the risk including the cause of the risk and impact on the organisational objectives (e.g. on cash flow, profits or shareholders' funds). As described later, further information about the risk can be added to the risk register including its assessment and related controls.

An owner should be assigned to each key risk so that it is clear who is responsible for managing that risk.

3.3 ENTERPRISE RISK MANAGEMENT

Splitting risks into categories can lead to a 'silo' approach so that the effects of interaction between risks are missed. Correlations between risks may reduce the overall risk exposures (i.e. natural hedges may exist), or indeed increase them. Therefore it is important that all treasury risks and non-treasury risks are reviewed together on a regular basis in order to assess whether there are any linkages between the them – this is an 'Enterprise Risk Management' approach. This could be carried out at the risk committee (if one exists) or during Board meetings. Some organisations delegate to an audit and risk committee, for example, but good practice is to ensure that risk appears on the Board agenda on a regular basis. It should be noted that the analysis of risk relationships can be a difficult exercise for management and the board of some organisations, given the technical expertise that is required. It would be unusual however nowadays for an organisation of any scale not to have in-house specialist risk management expertise.

3.4 PUBLISHED EXAMPLES OF TREASURY RISKS

Figures 5a and 5b below, show extracts from the annual report of Sainsbury relating to disclosure on treasury risks.

Figure 5a: Sainsbury PLC Annual Report 2018, Page 33

Financial and treasury risk

Risk

The main financial risks are the availability of short and long-term funding to meet business needs and fluctuations in interest, commodity and foreign currency rates. In addition, there remains a risk around pensions as the Group now operates one defined benefit pension arrangement that is subject to risks in relation to liabilities as a result of changes in interest rates, life expectancy and inflation and their alignment to the value of investments and the returns derived from such investments.

Mitigation

The Group Treasury function is responsible for managing the Group's liquid resources, funding requirements, interest rate and currency exposures. The Group Treasury function has clear policies and operating procedures which are regularly reviewed and audited.

Sainsbury's Bank operates an enterprise wide risk management framework. The principal financial risks relating to the Bank and associated mitigations are set out in note 27 to the financial statements on page 148.

With regard to pensions, investment strategies are in place which have been developed by the pension trustees, in consultation with the Company, to manage the volatility risk of liabilities, to diversify investment risk and to manage cash. Both Group defined benefit schemes are closed to future accrual. On 20 March, following the end of the financial year, the two pension schemes have merged.

Figure 5b: Sainsbury PLC Annual Report 2018, Page 130

23 Financial risk management

The principal financial risks faced by the Group relate to liquidity risk, counterparty credit risk, foreign currency risk, interest rate risk, commodity risk and capital risk.

Financial risk management is managed by a central treasury department in accordance with policies and guidelines which are reviewed and approved by the Board of Directors. The risk management policies are designed to minimise potential adverse effects on the Group's financial performance by identifying financial exposures and setting appropriate risk limits and controls. The risk management policies also ensure sufficient liquidity is available to the Group to meet foreseeable financial obligations and that cash assets are invested safely.

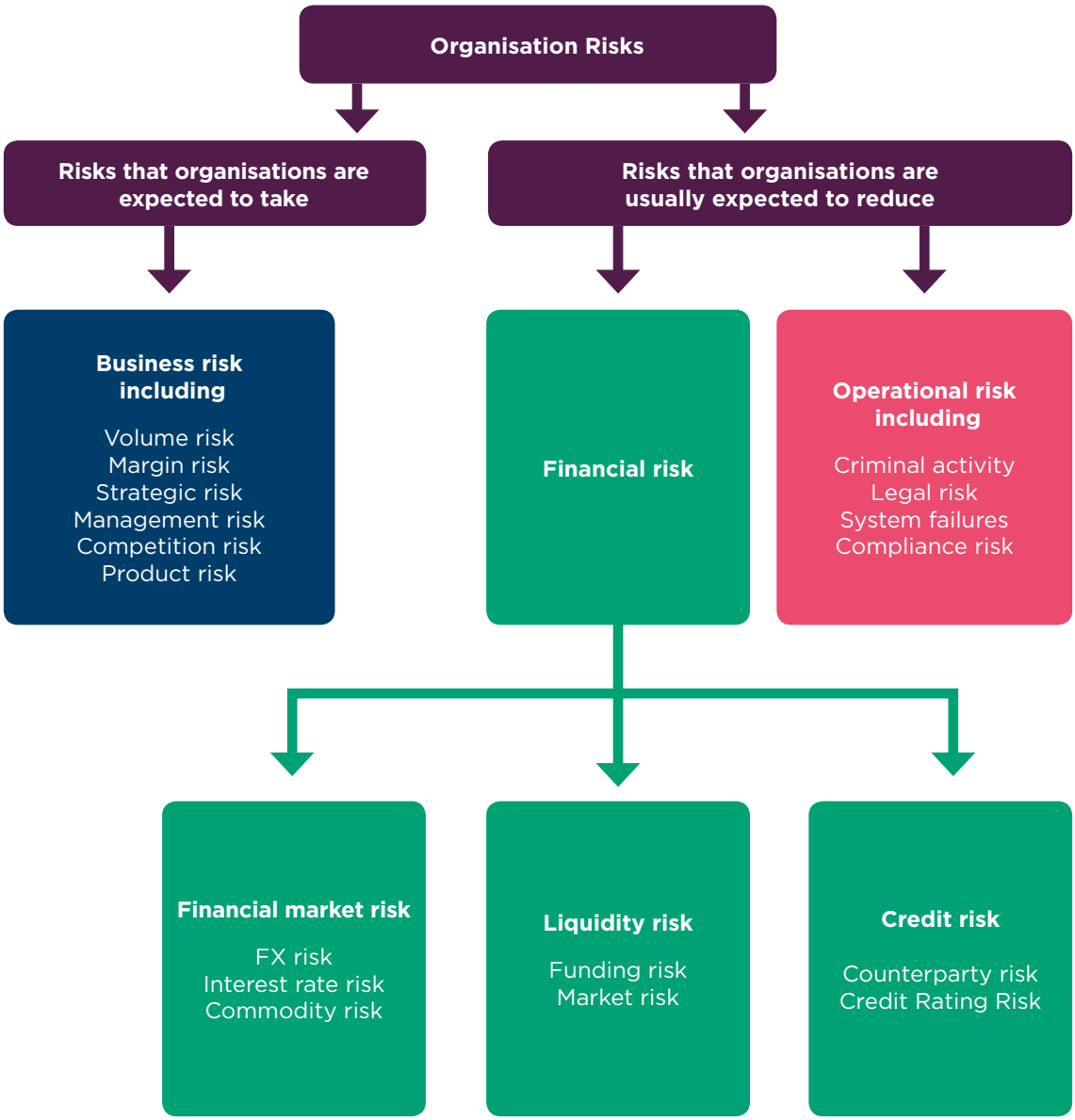
Financial risk management with respect to Financial Services is separately managed within the Financial Services' governance structure. The risks are more fully described in the Financial Services section below.

The Group uses forward contracts to hedge foreign exchange and commodity exposures, and cross currency swap contracts and interest rate swap contracts to hedge interest rate exposures. The use of financial derivatives is governed by Board approved policies which prohibit the use of derivative financial instruments for speculative purposes.

3.5 CLASSIFICATION AND DESCRIPTION OF TREASURY RISKS

Figure 6 below sets out a typical classification of risks in an organisation and shows the risks that the treasury function usually manages – which tend to come under the heading financial risks.

Figure 6: Classification of risks



Financial risk can be divided into financial market risk, liquidity risk and credit risk. Although such categorisation is convenient, usage and definitions vary and boundaries between categories are blurred. For example, liquidity risk magnifies other risks, such as market risk and credit risk and cannot be divorced from them.

3.5.1 FINANCIAL MARKET RISK

Financial market risk is the risk that cash flows, profits and balance sheet values are affected by movements in financial market prices or rates such as those in the interest rate, foreign exchange or commodities markets. Financial market risk may result in a profit or loss, and is the risk that derivatives were designed to manage: an unexpected profit which has occurred as a result of an unhedged position is not necessarily a good thing as it could quite as easily have resulted in a loss.

i. Foreign exchange ('FX') risk

Changes in FX rates will affect a business if it has any unmatched exposures (with respect to FX rates) such as profits, cash flow or net assets. As described in section 3.1.3, even if an organisation doesn't have direct exposures it could still be indirectly affected by FX risk, for example due to the activities of a competitor with a different functional currency.

Foreign exchange exposures are often classified as transaction, pre-transaction, translation and economic. See summary in Table 1 below:

Table 1: Types of FX exposures

Type of FX exposure	Description of exposure
Transaction	Changes in FX rates from the time a foreign currency transaction is entered into until it is settled. For example, the cash inflow from the payment by a customer of a sales invoice denominated in a foreign currency.
Pre-transaction	Potential cash inflows and outflows (with values which vary with changes in FX rates) resulting from the activities of the organisation where the counterparty has not committed yet e.g. the circulation of price lists or the submission of tenders.
Translation	Changes in values of items in the accounting statements (i.e. income, expenses, assets, liabilities) caused by translating items for accounting purposes e.g. using the average exchange rates for the period (for the P&L statement) and closing rate (for the balance sheet). This can cause volatility in the reported profit and shareholders' funds and affect ratios such as debt/EBITDA.
Economic	Changes in FX rates will impact the economic value of the organisation due to the variability of future cash flows. Transaction exposure makes up a part of economic exposure. Indirect exposures, such as those resulting from the actions of competitors, can also impact the value of the organisation and are part of the economic exposure.

ii. Interest rate risk

Changes in interest rates can have favourable or adverse effects, both on the interest charge of floating rate borrowings (which may have associated interest rate swaps) and on the value of fixed and floating rate borrowings or investments such as bonds (see also credit risk below).

iii. Commodity risk

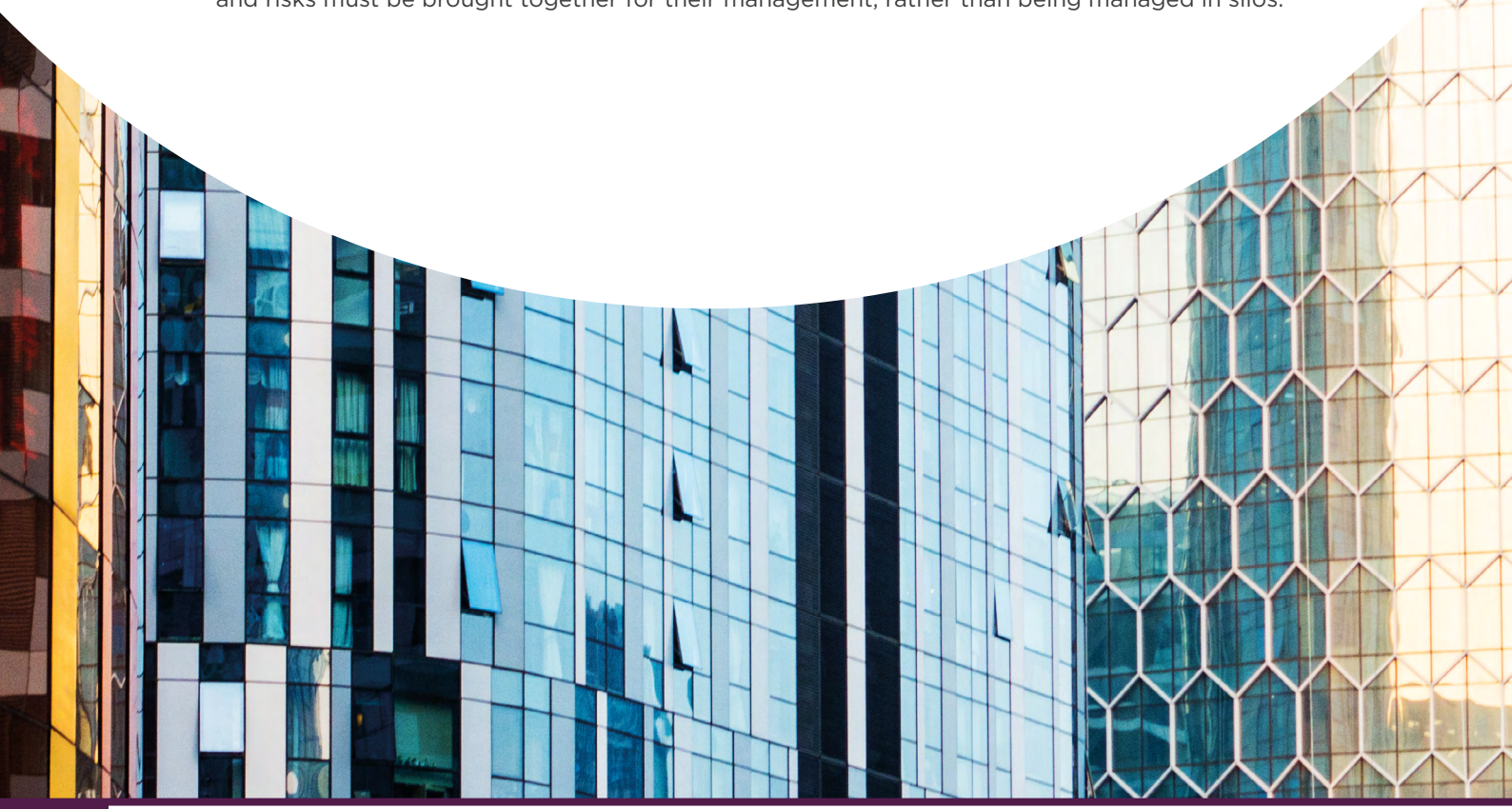
Commodity risk refers to the uncertainties of future market values and income, caused by the fluctuation in the prices of commodities. Commodities often managed by treasurers include grain, metals, fuel (coal, jet fuel, gas) and electricity.

3.5.2 LIQUIDITY RISK

Liquidity is access to cash, and liquidity risk revolves around fluctuations in the ability to access cash when and where it is needed. It is very difficult to find a universally accepted definition of liquidity risk, however it is commonly accepted that it comes in two forms - funding liquidity risk and market liquidity risk.

Funding liquidity risk is defined as an organisation's inability to obtain funds to meet cashflow obligations due to its own issues, whereas market liquidity risk refers to the risk that market transactions will become impossible due to market disruptions or inadequate market depth. The two forms can combine however – for instance, if commercial paper or bond markets dry up that is market risk, which will immediately become funding risk if the borrower has insufficient committed bank facilities to act as a stop gap.

Liquidity risk can occur if the liquidity obtained from either the asset (e.g. lower than expected receivables) or the liability (e.g. lower external funding than planned) side of the balance sheet is less than expected, income is not converted to cash or liquidity needs are more than anticipated. This suggests that liquidity risk may result from any or all of the other categories of risk. It is important for treasurers to recognise the overlap that exists between and amongst these different types of risk. It could be argued that all risks eventually result in liquidity risk, and risks must be brought together for their management, rather than being managed in silos.



3.5.3 CREDIT RISK

Businesses are potentially exposed to credit risk in a number of ways.

a. If a borrower or counterparty fails to honour its obligation to pay under a contract because it hasn't the capacity to pay. Examples include:

   i. **Bank deposits/credit extension**
   A business could lose money if it places cash with a bank which fails or if it extends credit to a customer which becomes bankrupt.

   ii. **Derivative counterparty**
   If a business has a derivative contract with a bank (e.g. interest rate swap) and the bank fails, it could lose money if the contract is 'in the money' and not fully collateralised.

   iii. **Insurance**
   If an insurer fails while it is processing an insurance claim for a business customer then that customer could face a loss.

b. If the credit ratings of investments (e.g. corporate bonds) are downgraded.

   A business may invest in corporate bonds or funds which have a credit rating. Rating downgrades may lead to a 'mark-to-market' loss in the financial statements depending on the accounting policies adopted by the business. In any case there will be an economic loss which may or may not be reversed over the longer term.

3.5.4 OPERATIONAL RISK

Treasury professionals also have to manage operational risk that results from treasury activities, for example missed payments, unmatched positions not identified, and mis-reporting. The Basel Committee on Banking Supervision provides one definition of operational risk: "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk".

Operational risks include mistakes by staff, criminal activities, litigation, processing and system failures as well as failures in compliance. There is no upside to operational risk: things can only go wrong. Operational risks may arise from procedural and internal control related issues, and are often unrewarded risks, i.e. risks which investors expect to be controlled and where there is no reward for taking them.

3.5.5 PENSION RISK

Businesses are often exposed to pension risk, which refers to the uncertainty in the value of the organisation's pension fund due to changes in the values of investment assets and pension fund liabilities. The value of the pension fund assets and liabilities are affected by actual and projected changes in interest rates, inflation rates and asset prices (equities, commodities etc) as well as longevity. Some treasurers may contribute to or be responsible, from the organisation's perspective, for managing this risk.

4 RISK ASSESSMENT

Once the key risks have been identified, they need to be assessed in order to measure the size of the risk.

4.1 PROBABILITY/IMPACT MATRIX

A useful way of measuring risks systematically is with a probability/impact matrix, also known as a risk map. Each identified risk is recorded on a diagram or grid according to its probability of occurrence and its potential impact. The range of values may be qualitative only (as in Figure 7 below) or appropriately quantified. The financial consequences should be measured on a consistent basis, for example by their possible or expected effect on consolidated profit, EPS or cash flow, should the event happen.

Figure 7: Probability/impact matrix

		Likelihood or Frequency				
		Very unlikely	**Low**	**Medium**	**High**	**Certain/ very probable**
Severity of Consequence	Catastrophic	**C**	**B**	**B**	**A**	**A**
	High	**D**	**C**	**B**	**B**	**A**
	Medium	**D**	**D**	**C**	**B**	**B**
	Low	**E**	**D**	**D**	**C**	**B**
	Insignificant	**E**	**E**	**D**	**D**	**C**

A	**Extreme:** Very high probability or impact; top priority for mitigating action
B	**Major:** High probability and/or impact; 2nd priority for mitigating action
C	**Medium:** Medium probability and/or impact; 3rd priority for mitigating action
D	**Low:** Low probability and/or impact; 4th priority for mitigating action
E	**Negligible:** Minimal probability and impact; lowest priority for mitigating action

On the probability/impact matrix, both the probability and the impact combine to form the assessment. One aim of the risk assessment process is to prioritise those risks, with most potential to damage the organisation, for further analysis, evaluation and management. Using the risk map as a guide, risks can be tackled in priority order, from top right (high impact, high probability) to bottom left (low impact, low probability).

The 'impact' of risks should initially be on a gross basis – that is, before the benefit of any controls, hedging or any other mitigating action. This is also referred to as the 'inherent' level of risk. By using inherent risk as part of the risk measure, risks can be compared in a consistent manner. 'Residual' or 'net' risk is often used to describe the level of risk after risk mitigants such as controls have been put in place.

We can also start to quantify the risks by being more specific in what we mean by the likelihood of frequency (probability) and the severity of the consequences (impact) by adding in a financial amount at risk and an appropriate time horizon for the expected frequency. The financial amount at risk and its banding need to be relevant to the organisation and consistently applied to risks in a particular risk map as is shown in the example below; see Figure 8

Figure 8: Quantifying risk – an example of the probability/impact matrix

		Likelihood or Frequency (at least one occurrence expected in...)				
		Very unlikely > 5yrs	**Low 3-5 yrs**	**Medium 2-3 yrs**	**High 1-2 yrs**	**Certain/ very probable Annual**
Severity of consequence: Effect on profit (% reduction)	Catastrophic >50%*					
	High 20-50%*					1
	Medium 10-20%*			3	2	4
	Low 2%-10%*	5				
	Insignificant < 2%*					

1	Increases in raw material and energy costs could affect future financial results. **Top priority.**
2	A key customer may experience financial problems which could lead to delayed customer receipts
3	Market demand for new and existing products could decline.
4	Currency fluctuations could significantly impact cash flows and reported results.
5	Changes in national or international laws and regulations could increase costs and liabilities or adversely affect demand for products. **Lowest priority**

**The percentage reduction in profits*

In the above matrix, five potential events have a probability and impact assigned to them based on history and management's experience. For example, the probability of event 1 (increase in material and energy costs) is considered 'very probable' and, given the profile of the company, the impact is classified as high since it could lead to a reduction in profits of up to 50%. To calculate the impact amount, management will have considered the potential increase in material and energy costs e.g. in this case management may have concluded that it is very probable that these costs could increase by up to 20% (say) during the year which leads to up to 50% reduction in profits. On the risk map, this event would be classified as a 'top priority' for management and action will need to be taken to manage this risk, such as fixing

costs with suppliers or using derivatives if there is a market. Event 5 has been classified by management as 'very unlikely' and 'low severity' and therefore lowest priority and, depending on the 'risk appetite' (see section 5) management may decide to take no further action in managing this risk.

In this example, although there has been a focus on the downside, it could be that changes in market prices and regulations (events 1, 4 and 5) could be positive for the company, i.e. profits increase. As will be discussed in section 6, by managing the potential downside through risk transfer and avoidance, opportunities may be missed and management will have to weigh up the costs and benefits of responding to risks in this way. The type of organisation and its risk appetite will influence the approach – for instance, a charity will tend to mitigate its risks wherever possible, (e.g. by hedging) and may miss opportunities but cannot for various reasons leave itself open to the possible downsides.

The probability/impact matrix is not static and should be regularly reviewed and updated. It should be a 'living' document, and the discussion and thought behind it is what is critical to the overall success of the organisation. Both risks and probability will change over time and in some instances the change may be quite significant, for example if the company makes an acquisition.

Risk velocity

In addition to measuring risk using probability and impact, there is another emerging concept called 'risk velocity' which is a measure of the time taken for a risk event to affect the position of an organisation. For example, a change in FX rates has a risk velocity which is greater than a proposed change in an accounting standard - the former could take seconds to impact an organisation while the latter could take months or years. Although risk management standards have traditionally tended to focus on probability and impact when describing risks and risk assessment, risk velocity is starting to become prominent in risk analysis given the rise of social media (which helps spread reputational damage) and the increasing reliance on technology (which makes organisations vulnerable to a high velocity risk such as cyberattack).

There is no standard methodology for measuring and using risk velocity, however most methods involve adjusting the probability/impact matrix (see Figure 8). For example, a risk velocity score can be given to each risk and the font size or colour of the probability/impact score could be adjusted (e.g. high risk velocity = red colour, medium = black, low = green). In this way two risks which have the same probability/impact but different risk velocities can be easily distinguished and then prioritised accordingly.

The Treasury Policy document checklist shown on page 40, can be adjusted to include another row for risk velocity and a score added. This will provide further risk data for discussion. As stated earlier, this is a relatively new concept and it will be interesting to see how it develops and is adopted by standard setters and organisations.

4.2 MEASURES OF PROBABILITY AND IMPACT

4.2.1 MARKET BASED VARIABLES

For example, a UK based company may be exposed to variations in a foreign currency because it is has to pay 100,000 denominated in the foreign currency in one week - if the foreign currency increases in value then the GBP equivalent payable will be more in one week than today.

One simple way to obtain the likelihood (probability) that the foreign currency will change by a certain percentage in one week is to look at the past changes in the foreign currency. Consider the following illustrative example – the historical data for the last 20 years (say) shows that the foreign currency has the following weekly changes (both increases and decreases) in value compared to GBP:

	Decrease	Increase	Increase	Increase
Change in value of currency relative to GBP over one week	All negative values (see note 1)	0% to 5% (see note 2)	5% to 10%	Greater than 10%
% number of weeks out of 1040 weeks (20 years) showing weekly changes in the stated range	50%	25%	20%	5%

Notes:

(1) The number of times (expressed as a %) that the value of the foreign currency has decreased over one week over the last 20 years.

(2) In this case, the value of the foreign currency has increased between 0% to 5% for 25% total number of the weeks in the last 20 years.

If it is assumed that the past data provides a basis for the probability (or likelihood) of future weekly changes, then we can assume that there is a 5% probability that the currency will increase by more than 10% over the next week – and a 95% probability (cumulative) that the currency will change at most by +10% over the next week (this includes decreases in currency). This is referred to as a '95% confidence level' or 1 in 20 stress.

Management will have to decide which level of probability (i.e. confidence level) to use from the table and this will depend on their view of the probability (e.g. are the figures in the table reliable) and their risk appetite (see section 5). Management could choose to manage this exposure by assuming that the foreign currency will increase by a maximum of 10% over the next week (which is a 95% probability) in order to calculate the potential impact.

In addition management could consider adjusting the probabilities (which are based on historical data) to take into account the current economic and political environment. The impact of the change in currency can be calculated once the confidence level has been chosen. For example, if the total exposure in the foreign currency is 100,000, and 95% confidence level is used, then the maximum adverse impact of the change is 10% of 100,000 over the next week (using the above table) which is 10,000. This would have to be translated into GBP using the prevailing foreign exchange rate.

A similar approach can be applied to other financial risks such as interest rates. Consider a company which has floating rate debt of 1 million in a particular currency. Market forecasts provided by external advisors calculate the probability of interest rate changes over the next year are as follows:

	Decrease	Increase	Increase	Increase
Change in interest rates over the next year		0% to 0.49%	0.5% to 0.99%	1.0% or greater
Probability of change	30%	60%	9%	1%

The above table shows there is a 1% probability that the change in interest rate is 1.0% or greater i.e. changes in interest rate below 1.0% (including decreases in interest rates) have a probability of 99%.

In this case management may be comfortable with the 0.49% interest rate increase (because this covers a 90% probability) as the level to assess the interest rate exposure (i.e. 90% confidence level). The maximum negative impact over the next year will 0.49% of 1,000,000 which equals 4,999. Thus, using the data above and based on a 90% confidence level, the worst impact of a rise in interest rates is 4,999.

Note that in this example, external advisors have provided the probability table but as in the previous foreign exchange example, historical data could also be examined if a large enough data set exists.

4.2.2 CREDIT RISK

For credit exposures that have a rating from an external rating agency, it will be possible to get a probability measure from the credit rating agency website using their historical data on default statistics. For example, Standard & Poor's publishes annually the level of historic defaults by rating (i.e. AAA, AA, A, etc) over specific time periods and the probability of default for a particular rating could be derived from that. Note that these are not forecasts.

For credit exposures that are not publicly rated by the main rating agencies, management could use an external advisor or ratings provider (e.g. Dun and Bradstreet) or, will have to form a view on the probability of default using both quantitative (e.g. financial ratios) and qualitative (e.g. strategy, experience of management) analysis. In this case and for other risk exposures it won't be easy to derive an exact probability of a risk event and instead a range may be more realistic. In any case the objective is to rank the key risks so that the response can be prioritised.

The impact of a credit default (e.g. failure of a customer or derivative counterparty) will be based on the credit exposure at the time of default but may be lower if the amount outstanding is protected by credit insurance or collateral.

4.2.3 LIQUIDITY RISK

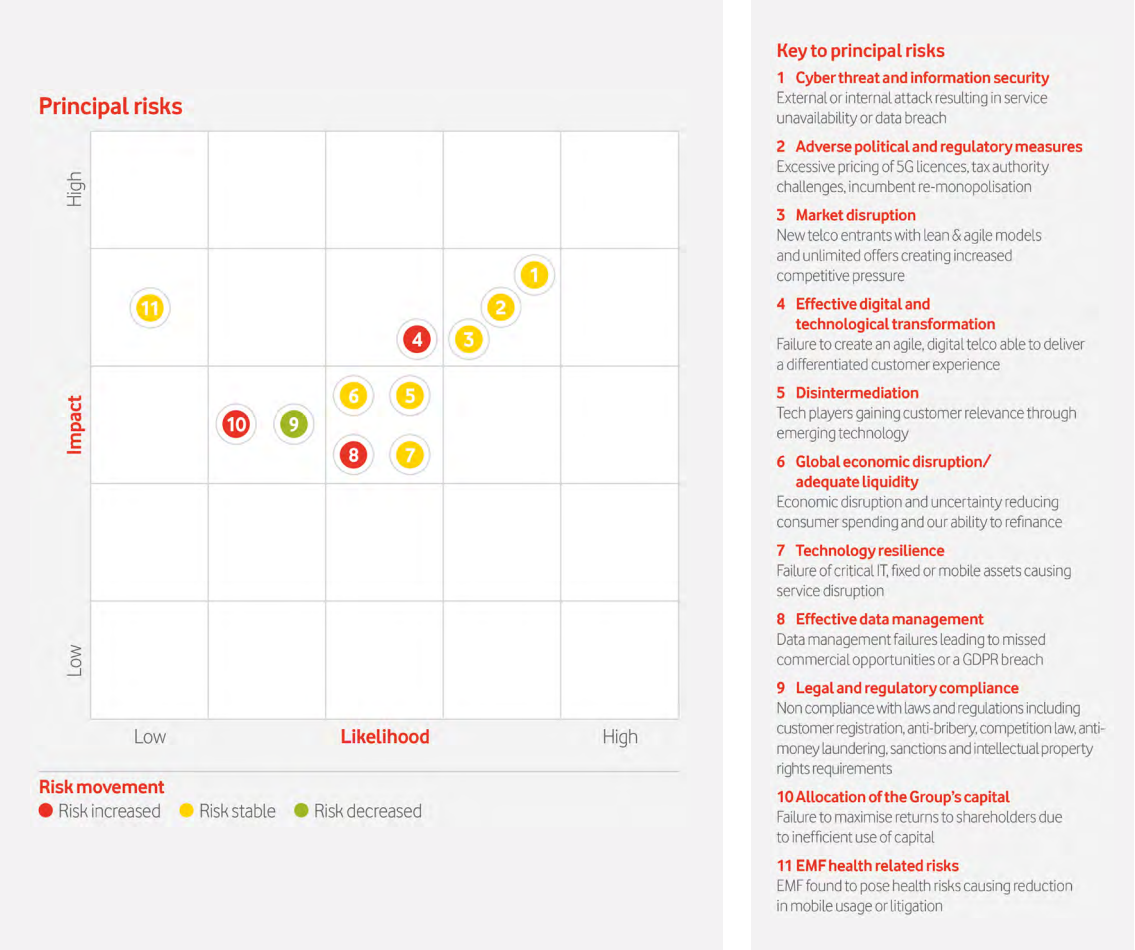
Liquidity risk is the risk that a business will not be able to meet current or future cashflow requirements, thereby putting its existence at risk. Liquidity risk can be reduced by having sufficient cash and other liquid assets, as well as other access to liquidity such as a committed bank facility. The amount of liquidity required by an organisation will depend on many factors including its profile (e.g. current leverage), strategy (e.g. growth), sector and regulatory requirements (if applicable). A common way to measure liquidity is to compare the amount of liquidity available to the company with the net cash outflows in order to calculate how long a company can survive without further external cash injections (e.g. through loans or equity issuance) both in a 'business as usual' scenario or 'stress scenario' (e.g. a large customer defaults or profits decline significantly) - i.e. the company can survive for 'x' months without recourse to new external sources of liquidity.

It is very difficult to calculate the probability that an organisation will have liquidity difficulties because the factors which could cause a reduction in net cash inflow are potentially many e.g. loss in sales due to weak economic conditions or new competitors, default of customers or suppliers, default of counterparties, change in regulation, product problems, labour action etc. However, an attempt should be made to assign a probability to liquidity stress so that this risk can be compared with other risks. Furthermore this exercise may be beneficial in producing a 'contingency funding plan', i.e. what would management do if the company faced a liquidity crisis?

4.3 PUBLISHED EXAMPLE OF RISK ASSESSMENT

Figure 9 below shows extracts from Vodafone's 2018 Annual Report in which the likelihood and impact of the principal risks are shown.

Figure 9: Vodafone Group PLC Annual Report 2018, Pages 38 and 39



4.4 OTHER TREASURY RISKS

As previously described each key treasury risk should be reviewed and a probability and impact assigned to the relevant risk event e.g. rise in commodity prices, rating downgrade of the organisation, missed loan payments due to operational errors, etc.

Although it may not be possible to provide a precise quantification of probability and impact, the best attempt should be made so that treasury risks can be ranked and the appropriate focus given to each as shown in the examples at the beginning of this section.

The impact measure that is used for each risk should ideally be the same (e.g. profit, cash flow etc) so that the risks can be compared on a consistent basis. Also ensuring risks are compared within the same timeframe is relevant to the analysis.

4.5 TOOLS FOR QUANTIFYING RISK

Tools to quantify the impact and likelihood of risk include the following:

Statistics: statistics use assumed patterns of occurrences of events and are meant to describe what might happen in the future, thereby giving an estimate of the risk (the expected value) at different points in the future. As described earlier, they are particularly useful for assigning probabilities to market risk because of the large amount of historical data available for analysis.

Sensitivity analysis: sensitivity analysis measures the change in value of an exposure for a given change in, for example, market prices. Sometimes the sensitivities to two variables will be tabulated. Sensitivity analysis can be used to show, for example, that a given bond portfolio worth $1 million now, will gain or lose value of $10,000 for every 10 basis-point move in five-year interest rates. However, while this technique is useful in showing the impact of a change, it does not show the probability of the change.

Scenario analysis: scenarios attempt to indicate what might happen under identified circumstances by answering a series of 'what if' questions. Scenario analysis should attempt to answer all possible 'what if' questions, from probable but low impact events, to unlikely but disastrous events. A stress test is a type of scenario analysis which aims to determine how resilient an organisation is to large changes in a variable such as FX rate or commodity price. For example, a UK-based organisation which has significant USD revenues and EUR costs could model the impact on profit and shareholders' funds of large changes in the GBP/USD and GBP/EUR exchange rates over the next year.

Simulation: simulation combines a model, such as that used in sensitivity analysis, with data about the size, probability and correlation of the inputs to that model. Combining these inputs with the model derives predictions about likely outputs and their associated probabilities. The most common form of simulation is known as Monte Carlo simulation.

Value at Risk (VaR): VaR aims to quantify the worst loss that might be expected over a given period of time, given a specified level of probability (known as a confidence level). See Appendix 3.

Maximum loss: maximum loss expresses the maximum loss that might occur. The measure takes the maximum loss that might occur from a series of scenario shocks, ignoring any benefits of correlation. So, for instance, the effect of an adverse FX move would be added to the effect of an adverse interest rate move, ignoring the possibility that adverse interest rates might actually cause FX rates to move favourably.

Once the likelihood and impact of each risk has been produced, these values can be added to the risk register.

In summary, the objective of the risk assessment phase of the risk management process is to quantify the impact and likelihood of risks so that they can be compared and an appropriate risk response for each can be considered.

5 RISK EVALUATION

In the risk evaluation phase, a 'risk appetite' is assigned to each treasury risk which has been identified and assessed in the previous phases of the risk management process. The risk appetite is the amount and type of risk that the organisation is willing to bear given its circumstances at a particular time. This differs from the previous step of risk assessment which is the process of quantifying risks.

5.1 RISK APPETITE

The setting of risk appetite involves creating boundaries and placing limits on the risk exposures faced by the organisation.

Articulation of a risk appetite statement for each risk is required before a suitable risk response can be formulated. For example, a UK-based company may decide that it is willing to have an exposure to USD costs each year of up to $10 million but when USD costs exceed $10million it will then hedge the costs exceeding $10million using FX forwards. Sections 5.2 and 5.3 provide guidance on how an organisation can set the risk appetite for a risk.

The actual risk exposure should be managed so that it is less than the risk appetite for that risk. However, depending on the risk, if the risk exposure is much lower than the agreed risk appetite then this could indicate that the business is not taking enough risk to achieve its corporate objectives.

In practice it is difficult to have one universal measure for risk appetite for all the identified risks in an organisation because usually the measure for the underlying risks also differs e.g. the risk appetite for credit risk could be expressed as 'the maximum amount of BBB investments in an investment portfolio', while the risk appetite for liquidity risk may be expressed as 'the minimum amount of cash required to be available at all times to ensure the organisation can survive for six months without recourse to external funding sources'. Management will have to decide which risk appetite measures should be used in the organisation.

Common methods for expressing risk appetite include:

1. Economic capital measures (e.g. £x of capital to cover FX exposures)
2. Changes in credit ratings (e.g. maximum of two-notch downgrade for an investment exposure)
3. Profit and cashflow measures (e.g. level of annual accounting loss)
4. Limits/targets or thresholds for key indicators (e.g. +/- 5% variation in profit or 1 -2.5% variation in revenue)
5. Qualitative statements (e.g. zero tolerance for compliance or operational control breaches)

Examples of risk appetite statements are provided later in this section. Where possible risk appetite should be stated in such a way that it is measurable and not a high-level general statement.

Risk appetite statements should be reviewed regularly, when the organisation profile changes or if there are significant changes in the economic or competitive environment. For example, if the company makes a large acquisition resulting in the level of sales denominated in USD significantly increasing, then the risk appetite statement related to USD receivables may need to be reviewed.

5.2 RISK CAPACITY, RISK APPETITE AND RISK TRIGGERS

The risk appetite for identified risks will depend on the 'risk capacity' of the organisation which is the maximum amount of risk an organisation can bear. For example, a company may breach a bank loan covenant if it makes an accounting loss of £10m so, given a certain level of confidence (e.g. 99%), management may decide to ensure that risks are managed such that the company doesn't make a loss of £10m. Taking into account other risks in the company, management could direct the treasurer to ensure that the treasury risks that are being managed should not exceed a pre-approved level (the risk appetite or risk limit) so that the loan covenant is not breached: for example, in this case the treasurer may be given a risk limit of £1m for all FX exposures using a confidence level of 99%.

In addition to risk capacity, the following factors should be considered when setting a risk appetite for treasury risks:

1. **The risk attitude of the Board**

   Some boards may be naturally more cautious than others in which case more conservative risk appetite statements may be appropriate. See section 1.1 on cost centres and profit centres.

2. **Stakeholder views**

   Stakeholders such as shareholders and bondholders may have a preference on the levels of risk appetite for risks.

3. **Financial profile of the organisation**

   Lower risk appetite for treasury risks may be appropriate for a highly leveraged organisation.

4. **Volatility of business operations**

   High volatility of cash flows may necessitate a lower risk for some risks to ensure overall volatility doesn't endanger the organisation.

5. **Links between risks**

   As described in section 3.3, an Enterprise Risk Management approach will identify the relationship between risks such as the existence of natural hedges. If some risks are negatively correlated, it may be possible to increase the risk appetite for some risks and still maintain an overall level of risk appetite that satisfies the board.

   For example, management may have observed in the past that increases in interest rate costs faced by their organisation (associated with growth in the economy) are offset by increased profits due to increased turnover. In this case, management may decide that this is a natural hedge and no further action is required to manage the interest rate risk.

   However, variables can change, and the natural hedge relationship can break down very rapidly. Management should regularly review and question whether the natural hedge continues to exist.

6. **Stability of business profile**

   If a business has made a large acquisition or is planning to expand abroad, it may decide to lower the risk appetite for treasury risks while it manages the increased risks due to the significant changes in its operations.

To be prudent, a 'risk trigger' could be used in addition to a risk appetite. This could be set at a level below the risk appetite and acts as a warning that the risk exposure is approaching the risk appetite. Once the risk trigger is breached the treasurer can take appropriate action e.g. increase the level of hedging. For example, the risk appetite and risk trigger for exposure to USD receivables may be set at USD 1m and USD 0.5m, respectively, based on the profile and circumstances of the company. If the amount of USD receivables exceeds the trigger of USD 0.5 million, the treasurer may be required to inform the Finance Director and recommend an action such as hedging the amount of USD receivables in excess of USD 0.5m.

5.3 PROCESS TO PRODUCE RISK APPETITE STATEMENTS

Initially, the risk appetite for treasury risks could be derived using either a 'top-down' or a 'bottom-up' approach.

5.3.1 TOP-DOWN APPROACH

In this approach, the Board or risk committee allocates a risk appetite for treasury risks by taking into account the total risk exposures of the company. The treasurer can then allocate a risk appetite to each identified treasury risk. For many companies this may be a new concept and the Board will need educating before this can be effective.

For example, the Board could inform the treasurer that given the position of the company, if possible, all treasury risks should be hedged so that the uncertainty in the accounting profit is minimised. However, it is unlikely that all treasury risks can be hedged and the treasurer will have to produce a risk appetite for some risks e.g. liquidity risk (the risk that the company runs out of cash) or that the credit rating of the company could be downgraded (assuming the treasurer is responsible for managing the credit rating). Alternatively, the board could state that the risk appetite for market risks (such as FX and interest-rate risk) should be such that, given a 90% confidence level, the maximum loss resulting from risk exposures should not exceed a certain level (e.g. £5million) over the next year. To calculate the confidence level, historical data for market prices can be examined: for example, for a particular currency a 90% confidence level may equate to a maximum reduction in the value of the currency by 12% over 12 months based on historical data i.e. 10% of the time the annual reduction of the currency has been greater than 12%. The choice of the confidence level (e.g. 90%, 95%, 99%) by management will depend on a number of factors such as the company's 'risk capacity', as described in section 5.2.

After the treasurer has allocated the risk appetite for all treasury risks, they will need to consider the correlation between treasury risks when they are determining a risk appetite for individual risks. For example, if the treasurer manages FX for two currencies that are not correlated then the risk appetite for each currency risk could be higher than if both currencies are highly correlated.

5.3.2 BOTTOM-UP APPROACH

In this approach, the individual departments or functions of a company (including treasury) produce risk appetite statements for the risks that they manage. Both the actual risk exposures and the risk appetite statements for each risk are then aggregated at the company level to produce an overall risk exposure and risk appetite. There is potential here for conflicting needs, opportunities and interpretation across different business lines which can result in much inter-departmental discussion. This is not a bad thing. The combined results are reviewed by the board or risk committee so that they can be approved or action taken; for example, if the board considers that overall risk appetite is too high or if the risk appetite for a particular risk is too high, then the relevant department(s) can be asked to change the risk appetite.

In practice a combination of the top-down and bottom-up approaches is usually taken, and the board should review and approve the treasury risk appetite statements. A board level review will help to highlight if any risks are linked so that the benefits of diversification can be used to calculate the risk appetite: for example, if interest-rate changes are found to be negatively correlated with sales, then management may decide to apply a higher risk appetite for interest-rate exposure.

5.4 PUBLISHED EXAMPLE OF RISK APPETITE STATEMENTS

Figure 10 below shows an example of a risk appetite statement published in Network Rail's Annual Accounts

Figure 10: Network Rail Ltd Annual Report 2018, Page 39

Network Rail has defined its risk appetite as follows:

Network Rail has no appetite for safety, health or environmental risk exposure that could result in injury or loss of life to public, passengers and workforce or irreversible environmental damage. Safety drives all major decisions in the organisation. Network Rail will consider options to reduce safety risk where the business case goes substantially beyond our legal obligation to reduce risk so far as is reasonably practicable.

In the pursuit of its objectives, Network Rail is willing to accept, in some circumstances, risks that may result in some financial loss or exposure including a small chance of breach of the loan limit. It will not pursue additional income generating or cost saving initiatives unless returns are probable (85 % CI for income and 60 % CI for cost reductions where potential returns are high).

The company will only tolerate low to moderate gross exposure to delivery of operational performance targets including network reliability and capacity and asset condition, disaster recovery and succession planning, breakdown in information systems or information integrity.

The company wants to be seen as best in class and respected across industry. It will only tolerate low to moderate exposure that may result in short term negative impact on reputation and stakeholder relationships and is easily recoverable, i.e. minimal negative local or industry media coverage, and/or minor employee experience and political impact. This will continue to be balanced by regular positive media coverage at national and local level.

6 RISK RESPONSE

6.1 FACTORS IN CHOOSING A RESPONSE

Following the elements of the risk management process previously described (identify, assess, evaluate), the treasurer will now be in a position to consider the appropriate response to the risk. The factors to consider include:

a. **Size, frequency and nature of the risk**
If the risk is not significant relative to the size of the organisation or the likelihood of the risk materialising is extremely low then the treasurer may choose not to respond to the risk. Note that for compliance risks the materiality threshold for ensuring the risk is managed and reporting the exposure to the board could be lower than other risks due to sensitivity surrounding non-adherence.

b. **Risk appetite**
Treasury's response to risk will be guided by the risk appetite for the risks which the treasury is required to manage (see previous section). If risk exposure is greater than the risk appetite then treasury should reduce the risk or re-evaluate the risk appetite in conjunction with the board and/or risk committee (if one exists).

c. **Competitor behaviour**
The treasurer can review practices in comparable companies as a guide although this should not be considered a main reason for choosing a response. Note the disclosure by competitors on risk policies and practices may be limited.

d. **The cost of the risk response**
The cost of a risk response (e.g. new control or buying insurance) has to be weighed up against the benefit (e.g. reduction in risk) to ascertain if it is worthwhile. The accounting and tax treatment of the risk response should be taken into account when evaluating the impact on cash flow and profit. Depending on the product chosen there may also be an opportunity cost of hedging.

e. **Secondary risks**
The costs of managing any secondary risks which may be introduced by the risk response should be assessed. For example, using an interest-rate swap may introduce counterparty risk, liquidity risk or operational risk, depending on its structure.

6.2 RISK RESPONSE STRATEGIES

There are four types of risk response as set out below:

Table 2: Types of risk responses

Response to a risk	Description
Avoid	Eliminate cause of risk
Transfer*	Have a third party take responsibility for the risk for example via insurance or derivative contract
Reduce the risk - the impact and/or likelihood of the risk	Reduce the risk by actions such as implementing controls or diversification
Accept the risk	Accept the risk, without further action

***Note: Hedging** *is the process of trying to neutralise or smooth the impact of fluctuations in market variables on the organisation's cash flows.*

For treasury professionals, managing risk is often discussed in terms of 'hedging' but, as noted above, hedging is just one of several possible risk responses. Hedging may either take the form of 'insuring' against adverse events, or of 'fixing' the outcome of an uncertain event, or the price of a market variable. Neither approach will prevent a negative event from happening, but if it does happen and the business is properly hedged, the impact of the event is reduced or eliminated.

6.2.1 AVOID THE RISK

A risk can be avoided by an organisation if it chooses not to take that risk. For example, a direct foreign exchange risk (e.g. US Dollars, Euros etc) can be avoided if an organisation chooses not to conduct business (i.e. incur costs or generate sales) directly in that currency – although, as previously discussed, a business may be indirectly exposed to foreign exchange risk. In some cases it may not be possible to avoid particular risks if the organisation decides to implement a particular strategy, in which case the risks will need to be managed.

It is essential that all significant risks, especially for new products, geographies and customer types, are identified, assessed and evaluated prior to the implementation of an organisation's strategy so that appropriate risk responses can be developed/agreed. If the risk exposure resulting from a new initiative such as a product or company acquisition is higher than the corporate risk appetite then management will need to consider whether the initiative should go ahead.

6.2.2 TRANSFER THE RISK

Some risks can be transferred to a third party. Traditionally risks could be transferred through insurance, for example property risk. Market risks (such as foreign-exchange risk and interest-rate risk) and credit risk can sometimes be transferred to counterparties such as banks using derivatives, assuming a relevant market exists – this process is also called hedging. Risk transfer usually gives rise to other risks such as counterparty risk, liquidity risk and operational risk. For example, if a company decides to hedge an interest-rate risk using an interest-rate swap with a bank on an uncollateralised basis then there will be a counterparty risk because if the bank fails it will not be able to fulfil its contract with the company. If the swap is collateralised then there will be liquidity risk because the organisation may have to provide liquidity to support the swap and the amount of liquidity required will vary with market rates. The secondary risks that arise from hedging will have to be assessed and evaluated to determine whether they are within the risk appetite of the organisation. If they are not, then the risk transfer will not be a viable option and alternative solutions will have to be found.

6.2.3 REDUCE RISK

The severity of risks and their frequency can be reduced by putting in place controls or reducing the underlying exposure. Operational risks usually can't be transferred to third parties and therefore these risks are often managed via internal controls. For example, the risk of misdirecting large payments to the wrong party could be reduced by having the payment instructions reviewed by a second person or by breaking down any large payment into a series of smaller ones and checking that each payment is received before the next one is sent (i.e. a reduction of the exposure).

6.2.4 ACCEPT THE RISK WITHOUT MITIGATION OR REDUCTION

Risk acceptance without action is appropriate if the risk is not material or is associated with a core competency and strategy of the business. For example, a mining company may retain commodity risk rather than hedging it if it has expertise in how to react to changes in commodity prices and remain profitable, or skills in forecasting commodity prices and has clearly communicated this as a strategy to its investors who will have full knowledge that they are taking on this risk via their investment in the company.

6.3 PUBLISHED EXAMPLES OF RISK RESPONSES

Figures 11a, 11b and 11c below show published examples of risk responses.

Figure 11a: Associated British Foods plc Annual Report 2018, Page 61

RISK TREND	MITIGATION	CHANGES SINCE 2017
UNCHANGED MOVEMENT IN EXCHANGE RATES AND INFLATION **Context and potential impact** **Associated British Foods is a multinational group with operations and transactions in many currencies.** **Changes in exchange rates give rise to transactional exposures within the businesses and to translation exposures when the assets, liabilities and results of overseas entities are translated into sterling upon consolidation.**	Our businesses which are impacted by exchange rate volatility and currency depreciation constantly review their currency-related exposures. Board-approved policies require businesses to hedge all transactional currency exposures and long-term supply or purchase contracts which give rise to currency exposures, using foreign exchange forward contracts. Cash balances and borrowings are largely maintained in the functional currency of the local operations. Cross-currency swaps are used to align borrowings with the underlying currencies of the group's net assets (refer to note 24 to the financial statements for more information).	Sterling has strengthened against most of our major trading currencies this year, other than the euro, resulting in a loss on translation this year of £22m. Although Primark covers its currency exposure on purchases of merchandise denominated in foreign currencies when orders are placed, this hedging activity typically covers a period of only six months. US dollar weakness against the euro has had a favourable transactional effect on Primark's largely dollar denominated purchases, particularly in the second half.
UNCHANGED FLUCTUATIONS IN COMMODITY AND ENERGY PRICES **Context and potential impact** **Changes in commodity and energy prices can have a material impact on the group's operating results, asset values and cash flows.**	We constantly monitor the markets in which we operate and manage certain of these exposures with exchange traded contracts and hedging instruments. The commercial implications of commodity price movements are continuously assessed and, where appropriate, are reflected in the pricing of our products. We operate a diverse portfolio of commodities across a number of geographies.	EU and world sugar prices were lower than last year which had a negative effect on Sugar profitability. Wheat prices have increased significantly during the year in the UK. Failure to recover these increases would adversely affect the future profitability of our bakery businesses.

Figure 11b: Johnson Matthey Annual Report 2018, Page 74
(Note comment that treasury is run as a service centre).

TREASURY POLICIES AND FINANCIAL RISK MANAGEMENT

Group Treasury is a centralised function within Johnson Matthey based in the UK and US. The role of Group Treasury is to secure funding for the group, manage financial risks and provide treasury services to the group's operating businesses. Group Treasury is run as a service centre rather than a profit centre. The group does not undertake any speculative trading activity in financial instruments.

INTEREST RATE RISK

At 31st March 2018 the group had net borrowings of £679 million of which 99% was at fixed rates with an average interest rate of 3.1%. The remaining 1% of the group's net borrowings was funded on a floating rate basis. A 1% change in all interest rates would have an immaterial impact on underlying profit before tax.

CREDIT RISK

The group is exposed to credit risk on its commercial and treasury activities. In both cases counterparties are assessed against the appropriate credit ratings, trading experience and market position. Credit limits are then defined and exposures monitored against these limits. In treasury and precious metal management, these exposures include the mark to market of outstanding transactions and potential settlement risks.

Figure 11c: Severn Trent PLC Annual Report 2018, Page 55

OUR POLICY FOR THE MANAGEMENT OF INTEREST RATES IS THAT AT LEAST 40% OF OUR BORROWINGS IN AMP6* SHOULD BE AT FIXED INTEREST RATES, OR HEDGED THROUGH THE USE OF INTEREST RATE SWAPS OR FORWARD RATE AGREEMENTS. AT 31 MARCH 2018, INTEREST RATES FOR 48% (2017: 51%) OF OUR NET DEBT OF £5,356.6 MILLION WERE FIXED.

*From Severn Trent website, explanation of AMP6 in above extract: "Our regulated water and waste water business works within five-year planning cycles that are determined by our economic regulator, Ofwat. Each of these periods is called an Asset Management Plan ('AMP') and allows us to fund our investment programme and cover our operating costs. This was the first year of AMP6."

6.4 INTERNAL CONTROLS

Internal controls can be used to avoid and reduce risk exposures. Internal controls can be classified as directive, preventative, detective and corrective and it is important for treasury professionals to consider the best mix of controls when managing risk exposures, taking into account the costs and benefits of each type of control; see Table 3 on following page:

Table 3: Classifications of internal controls

Control type	Description	Examples
Directive	These controls are broad based and designed to ensure that particular outcomes (e.g. risk exposure levels) are achieved – they usually require individuals to behave in a particular way.	Staff training, written policies and procedures, job descriptions, contingency plans
Preventative	These controls prevent an undesirable event occurring	Segregation of duties, authorisation limits, 'four eyes' check
Detective	These controls detect when an error has occurred	Reconciliation, audit, financial analysis
Corrective	These controls help mitigate the impact of an adverse event or error	Credit insurance, contingency plans

As further described below, there can be an overlap in the control classifications (e.g. a contingency plan could be described as both a directive and corrective control) and therefore these classifications should be seen as a starting point for formulating the appropriate controls to manage risk exposures. If implemented correctly preventative controls should be the most effective control, as directive controls rely on individuals following instructions and detective and corrective are 'after the event'. Detective and corrective controls in their nature don't prevent errors or 'out of appetite' risk exposures occurring.

6.4.1 DIRECTIVE CONTROLS

These controls (in a treasury context) set out how individuals should conduct themselves within the treasury department so that risk exposures are managed to agreed levels and/or potential risk exposures that are foreseeable do not materialise. For example, there could be instructions that bank debt should always be in fixed rate form and that if liquidity limits are breached contingency plans are implemented. Some directive controls rely on individuals to act as required and therefore can be weaker than preventative controls which often require two or more individuals.

6.4.2 PREVENTATIVE CONTROLS

These are the most important controls, which help to stop a risk exposure from exceeding risk appetite or to avoid a risk exposure entirely. For example, if there are agreed policies on the investment of surplus company funds, preventative controls such as segregation of duties and authorisation limits should ensure that credit limits and liquidity limits are not breached.

6.4.3 DETECTIVE CONTROLS

These types of controls identify when a treasury policy has been breached i.e. after the error has occurred. As an example, a month-end review of the 'value at risk' measure of foreign exchange exposures can be compared to risk appetite and if one or more exposures exceed appetite then a suitable response can be implemented.

6.4.4 CORRECTIVE CONTROLS

If the risk exposure exceeds the risk appetite then corrective controls are used to reduce the exposure as set out in the treasury policy. Any plan to adjust a risk exposure to agreed levels can be considered a corrective control. For example, a company may have a pre-approved plan to raise funds if the company's liquidity is below the treasury policy.

7 RISK POLICY DOCUMENTS

Risk policies are the risk responses for each identified key risk (such as FX risk, interest-rate risk etc) and are detailed in a broader 'treasury risk policy document' (also referred to as 'treasury policy document') which as a minimum should include the following elements for each risk:

- What is the risk and why is it being managed, taking into account the organisation's risk appetite?
- The risk response
- Risk measures to be used in measuring the risk and risk management performance
- Procedures for the day-to-day management of the risk, including:
  - The delegation of responsibility for managing the risks
  - Procedures and controls to be followed
  - Risk targets and limits based on an acceptable level of risk
- Performance reporting/feedback mechanisms
- Process to update the policy

Many treasury policies will require co-operation with other departments and a prime example is the FX risk policy where the risk may arise from trading with overseas parties. Strong liaison with sales, marketing and procurement departments would be required.

It should be noted that treasury policy documents (along with other risk policy documents such as IT or health and safety) are usually updated annually or when there is a major change in the organisation's profile, however the actual risk management process is more fluid and occurs throughout the year i.e. risks are often assessed monthly. Hence the risk assessment as stated in the treasury policy document is typically the level of the risk exposure when the policy document was written (or last updated) and is used to set the risk appetite for the rest of the year until it is next updated.

Treasury policy documents are internal documents and are not published. Some treasury risks and associated policies may however be published – see examples from the annual reports of companies earlier in this briefing note.

A description of the roles and responsibilities of the staff in the treasury department is often attached to the departmental risk policy document which contains all the treasury policies for the treasury risks as described above.

7.1 GENERAL GUIDANCE FOR PRODUCING A TREASURY RISK POLICY DOCUMENT

As previously described, prior to producing detailed treasury policies, treasury professionals should apply the following general guidance:

a. Use existing risk management frameworks and systems in the organisation, including risk terminology, risk measures (for example, Value at Risk – VaR) and policy templates (if they exist), to ensure policies are produced on a consistent basis across the organisation

b. Take into account the organisation's business profile, financial position, corporate strategy and economic environment to identify the key risks, identify potential offsetting risks ('natural hedges'), set the risk appetite and set the risk response.

c. Adopt a standard risk management process for each risk, for example: identify, assess, evaluate, respond and report.

d. Assign ownership and accountability for the management of each treasury risk and associated treasury policy.

e. Key performance indicators (KPIs) are used by the board and senior management to manage and control all aspects of the organisation including financial performance, compliance with laws and regulations, health and safety, safeguarding assets etc. KPIs should also be used to ensure that treasury policies are being implemented as planned. For example, to ensure that a treasury policy relating to the management of an FX exposure is being adhered to, the relevant KPIs could include the gross FX exposure, net FX exposure (i.e. after hedging), cumulative FX revaluation profit/loss to date, current FX volatility etc. The type of KPIs will vary according to the type of risk and the business model of the organisation; for example, a KPI relating to liquidity risk could be the amount of liquidity available as a percentage of forecast cash outgoings in the next 12 months

f. Review the risk management process at least annually or when there are major changes in the business profile, corporate strategy or economic environment. Additionally, there should be a process to identify 'emerging risks', which may not be an immediate threat, but could be more significant in future, for example climate change and automation.

7.2 TREASURY POLICY DOCUMENT CHECKLIST

The following table sets out a checklist of key items to include within a treasury policy document:

Treasury policy headings	Notes	Risk management process	Briefing note section reference
Policy name	Each policy should be given a name		
Risk exposure description	What is the risk and how does it arises	**IDENTIFY**	**3**
Size of risk (unhedged) for different levels of stress	What is the size of the exposure before risk management? The risk measurement will vary by type of risk. Use appropriate benchmark (e.g. SONIA, EURIBOR) where appropriate The level of stress could vary by risk	**ASSESS**	**4**
What are the other risks in the organisation which could potentially reduce the impact of this risk?	Review whether there are any 'natural hedges' in the business which could mitigate the risk exposure	**ASSESS**	**4**

Treasury policy headings	Notes	Risk management process	Briefing note section reference
Risk appetite	The risk appetite for each risk should be determined and approved	**EVALUATE**	**5**
Risk response (the policy objective)	The risk response should clearly define what treasury is expected to achieve. List authorised instruments and if necessary, hedging strategies (if not specified elsewhere) List authorised counterparties with risk limits (if not specified elsewhere).	**RESPOND** *(avoid, transfer, reduce, accept)*	**6**
Risk owner	Should set out which decisions are delegated to the treasurer including when treasurer should report back to the board or other person in the organisation List authority limits (if not specified elsewhere)	**RESPOND**	**6**
Risk limit/risk trigger	The risk limit and risk trigger (if set) for each risk should be determined and approved	**CONTROL**	**6**
Potential actions if risk trigger and risk limit reached?	An action plan should be in place in case risk triggers and risk limits are breached. For example, there should be a reporting system for escalating the breaches to senior management with recommendations to manage the risk exposure such as reducing the underlying risk or mitigating the exposure.	**CONTROL**	**6**
Key risk controls	Risk controls which are used to manage the risk should be described	**CONTROL** *(directive, preventative, detective, corrective)*	**6**
Key performance indicators("KPIs")	KPIs should be chosen which measure the risk exposure and related hedges (if relevant)	**REPORT & MONITOR**	**8**

Treasury policy headings	Notes	Risk management process	Briefing note section reference
Reporting	The system for reporting the risk exposures should be established so that senior management can monitor and control the key risks in the organisation	**REPORT & MONITOR**	**8**
Update of policy	The process for updating the policy should be described including the frequency of update and approval process.	**FEED BACK**	**8**

7.3 TREASURY POLICY DOCUMENT CHECKLIST EXAMPLES

7.3.1 EXAMPLE 1: FOREIGN EXCHANGE TRANSLATION RISK (For illustrative purposes only)

Treasury policy	Description
Policy name	US$ FX structural exposure
Risk exposure description	The net value of the investment in company X, an overseas subsidiary in USA, rises/falls as the GBP/USD exchange rate weakens/strengthens
Size of risk (unhedged) for different levels of stress	Current value is $280m (approx. £200m at GBP/USD of 1.4), Assume there is a 90% probability of up to 15% strengthening of GBP i.e. rate goes from 1.4 to 1.61 over one year. Cash flow: nil. Accounting profit/loss: nil Shareholders' funds: reduction of £26m
What are the other risks in the organisation which could potentially reduce the impact of this risk through negative correlation?	None identified
Risk appetite	Assuming a maximum foreign exchange rate change, which has a probability of 90% of occurring based on historical data, then for each FX structural exposure, no exposure should lead to a P&L loss of more than £30m in a single year Total FX structural exposure (US$, Euros, Yen etc) cannot be more than £300m equivalent after hedging

Treasury policy	Description
Risk response (the policy objective)	Consider hedging 50% of the exposure using foreign exchange forward contracts when risk trigger reached. Hedge 100% of the exposure when risk limit reached
Risk owner	Treasurer is responsible for managing the risk exposure in line with the risk response. Finance department will provide the gross and net exposure each month to the treasurer and the board of directors The treasurer has the authority to hedge up to 50% of the risk exposure using FX forwards with pre-approved counterparties Any variation from the risk policy has to be agreed by the Board
Risk limit/risk trigger	Risk limit =£30m P&L loss Risk trigger = £15m P&L loss
Potential actions if risk trigger and risk limit reached?	Risk trigger breached: treasurer to inform the finance director immediately and discuss appropriateness of risk limit and risk appetite given the forecast volatility of FX markets and the prevailing risk capacity of the organisation. Consider hedging 50% of the exposure Risk trigger breaches and actions taken are reported to the board as part of the regular monthly treasury report Risk limit breached: Board to be informed immediately. 100% of the exposure to be hedged immediately
Key risk controls	Treasury team to review FX exposures against risk triggers and risk limits each month but move to weekly monitoring if volatility of FX rates increases Treasury can manage the FX risk through FX forwards only using approved counterparties FX forward contracts are subject to counterparty limits provided by the risk department.
Key performance indicators("KPIs")	Gross FX exposure, value of FX forwards, net FX exposure, P&L gain/loss each month and cumulatively during each financial year, FX rates, volatility of FX rates both actual and forecast
Reporting	The risk exposure and financial impact (P&L, change in shareholders' funds) to be reported to risk committee and Board each month

Treasury policy	Description
Update of policy	Annual update or when there is a major change in corporate profile (e.g. M&A) or corporate strategy

7.3.2 EXAMPLE 2: INTEREST RATE RISK (For illustrative purposes only)

Treasury policy	Description
Policy name	Interest rate risk exposure
Risk exposure description	Interest costs due to net debt will increase/ decrease as interest rates rise/fall
Size of risk (unhedged) for different levels of stress	£200m of debt and £50m of cash (average balance). £100m of debt is fixed rate (5% rate) and £100m of debt is floating rate (3-month SONIA + 4%). Overall there is a £50m net debt exposure to changes in interest rates. If SONIA increases by 0.5% this will lead to £0.25m loss which equates to a 10% probability based on external forecasts. If SONIA increases by 1% this will lead to £0.5m loss which equates to a 1% probability based on external forecasts
Other risks in the organisation which could potentially reduce the impact of this risk	Rising interest rate environment could indicate a stronger economy which could lead to higher revenues and profits which would offset higher interest costs
Risk appetite	Maximum adverse pre-tax impact caused by increase in SONIA: Cash flow: £0.5m Accounting P&L: £0.5m Shareholders' funds: £0.5m Equivalent to 1% increase in SONIA
Risk response (the policy objective)	Keep fixed/floating mix of 50%/50% unless interest rates go up by 1% or more in which case change debt to 100% fixed rate. Confirm if profit is forecast to increase due to a stronger economy
Risk owner	Treasurer is responsible for managing the risk exposure in line with the risk response. Finance department will provide the gross and net exposure each month to the treasurer and the Board of directors The treasurer has the authority to hedge up to 100% of the risk exposure using interest rate swaps with pre-approved counterparties. Any variation from the risk policy has to be agreed by the Board

Treasury policy	Description
Risk limit/risk trigger	Variance from budget due to increase in rates of 1% and 0.5% respectively Risk limit =£0.5m loss, risk trigger = £0.25m loss
Potential actions if risk trigger and risk limit reached	Risk trigger breached: treasurer to inform the finance director immediately and discuss appropriateness of risk limit and risk appetite given forecast interest rates, the prevailing risk capacity of the organisation and management's view on potential off-setting factors such as increased revenues. Consider whether debt mix should be changed to 75% fixed and 25% floating using interest rate swaps. Assess whether risk trigger level is still appropriate. Board to be informed of breach and potential actions for approval Risk limit breached: board to be informed immediately and consider changing debt to 100% fixed – however review if there are off-setting factors such as increased revenues in which case fixed/floating mix could be maintained Note: risks of using interest-rate swaps to be evaluated i.e. increased liquidity risk and counterparty risk (if not collateralised).
Key risk controls	Treasury team to review interest rate exposures against risk triggers and risk limits each month Treasury can only use approved counterparties to manage the interest-rate risk through interest-rate swaps Interest-rate swap contracts are subject to counterparty limits provided by the risk department and have to be collateralised
Key performance indicators (KPIs)	Fixed/floating mix, P&L gain/loss each month and cumulatively during each financial year, impact of 0.5% rise in interest rates on cash, P&L and balance sheet, and interest-rate forecasts
Reporting	The risk exposure and financial impact (P&L, change in shareholders' funds) to be reported to risk committee and board each month
Update of policy	Annual update or when there is a major change in corporate profile (e.g. M&A) or corporate strategy

8 RISK REPORTING

A system to report on the risk management process is required to ensure that it operates as expected, emerging risks are identified, and control failures are dealt with in a timely and effective manner – for example, the reporting system should alert senior management if a risk exposure exceeds policy. However, risk reporting systems will vary from organisation to organisation and will depend on its size, type and complexity. They are likely to include the following type of documents:

a. Risk register

As described in section 3.2, a risk register is used to document the key risks faced by the organisation once they have been identified so that ownership can be assigned and management of the risk can be facilitated. For each risk, the register should contain:

- A description of the risk including the source and potential impact of the risk
- Which individual and department is responsible for managing the risk
- The size of the risk (likelihood and magnitude) both before and net of mitigants (such as derivative hedges)
- The risk appetite
- The risk response and related controls
- Risk triggers/risk limits

The risk register provides senior management with a snapshot of the key identified risks facing the organisation. It is important that the register is regularly updated to ensure that it doesn't become out of date, especially when a major change in the organisation's profile has occurred e.g. major acquisition. Moreover, it should be a living document, with management continually asking the question: what keeps me awake at night?

b. Treasury policy documents

There should be a treasury policy document for each key risk as described in section 7.

c. Risk assessment report

Key risks should be assessed on a regular basis to ensure that risk exposures are within risk appetite. This is also an opportunity to identify new risks.

d. Risk control reports

After controls have been put in place, they should be tested on a regular basis to ensure they are working as expected and failures should be reported to senior management immediately.

e. Breaches of policy and control failures

Breaches of risk policy and control failures should be reported to senior management – if the impact is significant enough, they should be reported immediately. In any case, action (including new controls if required) should be taken.

f. Emerging risks report

A process to identify emerging risks should be put in place including discussion with senior management so that any appropriate action can be considered. For each identified emerging risk, an estimate of the size of the risk along with the timing of the potential impact should be assessed. Examples of emerging risks relating to treasury could include significant changes in market rates due to economic or political events or proposed legislation relating to the capital markets. For smaller corporates this process may be more to inform.

g. External reporting

Listed companies are required to report on risk management in their annual reports and the UK Corporate Governance Code sets out the requirements along with other legislation; see Appendix 1.

9 MONITORING

The risk management process, treasury policies and internal controls can be reviewed and monitored by non-treasury personnel in order to provide an independent check.

a. Reviews by the risk department

If a risk department exists in the organisation, risk specialists can carry out regular reviews to ensure that the treasury policies are being adhered to. Given their specialist knowledge, risk personnel can also provide more detailed advice on risk methodologies and measurement of risk.

b. Internal audit reviews

The treasury department will likely be reviewed by the internal audit department, if one exists in the organisation, although the review may not be annual depending on the size of the internal audit department. As part of the review process, the internal audit team is likely to review the treasury policy process along with other treasury procedures and controls.

c. External audit/preparation of financial statements

Depending on the scope of the external audit, treasury policies may be examined, but in any case the financial impact of the policies will be reviewed, - for example, the result of hedging using derivatives, the cost of insurance, the profit or loss relating to foreign exchange and other market risks. As with internal audit, control weaknesses which are picked up by external auditors will be reported internally to senior management.

APPENDIX 1: OVERVIEW OF THE UK CORPORATE GOVERNANCE CODE ('THE UK CODE')

The separation of ownership and management in large companies can lead to the non-alignment of the interests of shareholders and directors (commonly known as the 'agency' problem). Good corporate governance can help address this by ensuring that there is a system in place by which a company can be directed, monitored and controlled by its stakeholders. There is no single, universally accepted definition of corporate governance, however in practice it can be observed that corporate governance structures usually include, inter alia:

- A process that sets out the roles and responsibilities of the board of directors, managers and auditors so that their respective powers and accountabilities are defined
- A process by which corporate objectives are set and implemented given the resources available to the company and taking into account the prevailing economic, competitive and regulatory environment
- Appropriate decision-making rules, procedures and controls for running the company
- Mechanisms which monitor and report on the actions, policies and priorities of all stakeholders so that their interests can be balanced.

In the UK, good corporate governance has been codified in The UK Corporate Governance Code (the 'UK Code') which is produced by the Financial Reporting Council.

On 16 July 2018, the Financial Reporting Council (FRC) published an updated version of The UK Corporate Governance Code (the Code), along with the revised Guidance on Board Effectiveness, which provides further details and guidance on the Code, including questions for boards to consider. A supporting document, Revised UK Corporate Governance Code 2018 Highlights, was also released, which provides a broad overview of the Code.

The Code applies to all companies with a premium[1] listing and for accounting periods commencing on or after 1 January 2019, although some companies may have chosen to adopt certain parts early. As the Code contains best practice for corporate governance, non-premium listed or unlisted companies may wish to adopt the Code in whole or in part.

A BRIEF OVERVIEW OF THE CODE

The purpose of this section is to provide a brief overview of the Code and to highlight the sections on risk management, since these are likely to be more relevant to treasury professionals in their day-to-day activities.

It has been more than 25 years since The UK Corporate Governance Code was published in 1992 by the Cadbury Committee. It defined corporate governance as 'the system by which companies are directed and controlled'. The updated Code is shorter and more concise than the previous one and includes changes or additions in the following areas: the concept of company purpose, stakeholder engagement (including workforce), corporate culture, diversity, succession planning and remuneration.

Additionally, as discussed overleaf, the concept of 'emerging risks' has been introduced.

The Code is composed of 18 Principles and 41 more detailed Provisions grouped into five sections:

1. Board leadership and company purpose
2. Division of responsibilities
3. Composition, succession and evaluation

1. Companies have the choice of three types of listing on the main market of the London Stock Exchange – a Premium (formerly Primary) listing, a Standard (formerly Secondary) listing and an admission via the High Growth Segment. Issuers with a Premium listing are required to meet the UK's super-equivalent rules which are higher than the EU minimum requirements while a company with a Standard listing has to meet EU harmonised standards only rather than the UK 'super-equivalent' requirements.

4. Audit, risk and internal control

5. Remuneration

The application of the Code Principles and Provisions is publicly reported by the company – the Provisions operate on a 'comply or explain' basis, providing companies with flexibility.

The fourth section of the Code, 'Audit, risk and internal control', is likely to be of most relevance to treasury professionals because part of it relates to risk management. Relevant extracts are reproduced below:

- **Principle O:** "The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives."

- **Provision 28:** "The board should carry out a robust assessment of the company's emerging and principal risks. The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated."

- **Provision 29:** "The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls."

  The FRC defines principal risks in the following way: "Principal risks should include, but are not necessarily limited to, those risks that could result in events or circumstances that might threaten the entity's business model, future performance, solvency or liquidity. In determining which risks are the principal risks, entities should consider the potential impact and probability of the related events or circumstances arising, and the timescale over which they may occur."

HOW TREASURERS CAN ASSIST THE BOARD

Although the Code is directed at the Board of directors, it is likely that the treasury function will assist the board in its application in some of the following ways:

- As required by Provision 28, treasury risks, such as liquidity, interest rate, funding, FX, counterparty, etc will need to be identified and assessed. Treasury risks that are deemed to be 'principal risks' will be reported by the company along with the principal risks identified and managed by other parts of the company

- Assess emerging risks as required by Provision 28. This is an addition to the Code, and some treasury functions may need to set up new processes to comply

- Address the requirement stated in Principle O to "determine the nature and extent of the principal risks the company is willing to take". This is also commonly known as risk appetite. For example, it would usually be the responsibility of the treasury function to recommend the level of liquidity risk and interest rate risk that is acceptable given the company profile, strategy and external environment of the company. The recommendation would ultimately be approved by the board

- As required by Provision 28, explain how treasury risks are managed or mitigated. If relevant, this would include a description of hedging strategies

- Carry out a review at least annually of the effectiveness of the risk management and internal control systems within treasury as required by Provision 29. In practice, it is likely that most companies and their treasury functions will carry out a more frequent review (for example, quarterly) and this would include a review of the effectiveness of key controls used to manage treasury risks

APPENDIX 2: "GUIDANCE ON RISK MANAGEMENT, INTERNAL CONTROL AND RELATED FINANCIAL AND BUSINESS REPORTING" FROM THE FRC, SEPTEMBER 2014 ('FRC GUIDANCE ON RISK MANAGEMENT')

The FRC Guidance on Risk Management paper provides high level guidance on the factors that boards should consider when designing and monitoring risk management and internal control systems. The paper will be useful for treasury professionals who are involved in implementing their company's risk management processes including the design of treasury policies. It doesn't set out detailed procedures or examples but describes the key elements of best practice for risk management. The paper also includes information on a company's reporting requirements relating to risk and going concern which are not covered in this overview.

BOARD RESPONSIBILITY

The paper states that the board of a company has the following responsibilities with respect to risk management and internal control:

- Design and implement systems that identify risks facing the company and making an assessment of the principal risks
- Determine the company's risk appetite
- Ensure an appropriate culture and reward system
- Agree how principal risks should be managed or mitigated
- Monitor and review:
  - The risk management and internal control systems and
  - Management's process of reviewing
- Satisfy itself that corrective action is taken where necessary
- Ensure sound internal and external information and communication processes on risk management and control

The above list can be a useful general starting point for treasury professionals designing risk management systems in the treasury department, although it is likely that there will be an organisation-wide approach which includes standard methods and templates for risk assessment and reporting.

EXERCISING RESPONSIBILITY

The paper suggests that the following should be considered to enable the Board to meet its responsibilities:

- The culture it wishes to embed in the company
- How to ensure adequate discussion at the Board
- The skills, knowledge and experience of the Board and management

- The flow of information to and from the board and the quality of that information
- The use of delegation
- What assurance the board requires and how this is to be obtained

The factors listed above may be a useful checklist for those treasury professionals who are involved in the establishment and running of committees or steering groups.

ESTABLISHING THE RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The paper sets out the objectives of a risk management system which include the identification of emerging risks and reducing the likelihood of taking risks above levels agreed by the Board. It states the key elements of the system are:

- Risk assessment
- Management or mitigation of risks including use of controls
- Information and communication systems
- Processes for monitoring and reviewing effectiveness

The paper also states that the board should consider the following when looking at risk:

- The nature and extent of the risks faced or taken by the company
- The likelihood of risks materialising and the potential impact
- The company's ability to reduce the likelihood and impact of risks
- The exposure to risks before and after management or mitigation
- The operation of relevant controls
- The costs and benefits of controls
- The impact on values and culture of the company including use of incentives

Treasury professionals may find the list above useful when drawing up treasury policies and procedures for risks which treasury manages.

MONITORING AND REVIEW OF RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The paper states that ongoing monitoring and review is an essential component of a risk management system. The UK Code requires that the board conduct an annual review of the effectiveness of the company's risk management and internal control systems and therefore those treasury professionals in companies which are subject to the UK Code may have to contribute to this review. The FRC guidance states that the review should consider:

- The company's risk appetite, the desired culture and whether the culture has been embedded
- The operation of the risk management system
- The integration of risk management with strategy and business model, and business planning processes
- Changes in principal risks and the company's ability to respond to changes in its business model and external environment

- Communication to the board on management's monitoring
- Issues dealt with in reports reviewed by the board such as significant control failures
- The effectiveness of the public reporting processes

APPENDIX 3: VALUE AT RISK ("VAR")

VaR is sometimes used in larger companies as a measure of risk and aims to quantify the worst loss that might be expected over a given period of time, given a specified level of probability (known as a confidence level). In addition to understanding the inputs and methodology it is important that senior management and the board fully understand and can interpret the VaR output, which may require some education.

The calculation of VaR for an exposure requires the following inputs:

1. **The amount and type of exposure**

   VaR is particularly useful for market and credit risks which often have large sets of historical data for related market prices. For example, VaR can be calculated for foreign currency denominated assets (e.g. USD sales receivable), interest rate liabilities (e.g. floating rate loans) or counterparty exposures (i.e. credit risk of financial counterparties).

2. **The variable which causes the uncertainty in exposure value**

   The relevant variable will depend on the underlying exposure. For example, for a foreign exchange exposure it will be a foreign exchange rate because the change in exchange rate causes the base currency value of the exposure to increase or decrease in value.

   To calculate VaR, both the current value of the variable and historical or estimated changes in the variable are required e.g. changes in the GBP/USD over 1 day.

3. **The confidence level**

   This is the probability that is used to obtain the 'worst loss' that could be expected and is often based on a 95% or 99% confidence level – in other words there is a 5% or 1% probability that the actual loss will be greater than the expected worst loss as calculated by the VAR method.

4. **Timeframe**

   This is the period associated with the stated VaR e.g. the expected worst loss during one day, one month or one year.

There are two common methods used to calculate VaR:

1. **Use historical data**

   The actual recorded changes in the relevant variable (e.g. foreign exchange rate, interest rate, equity price) over a time period are first ordered from high to low and then the value corresponding to the 95th (or 99th) percentile of the total number of values is used for the VaR calculation; see example below. The advantage of this method is that it is relatively simple and easy to understand, however disadvantages include:

   i. The results depend on the quality of the data

   ii. Data points are usually weighted equally so effects such as seasonality are not taken

into account. If it is believed that recent data is more relevant then a sub-set of the data could be used

iii. This method assumes that the future volatility will be the same as in the past

iv. The VaR result may underestimate the actual number of extreme events especially if the historical data set only has a few outliers. It is therefore good practice to produce a histogram of the data to get a sense of the potential 'tail risk'

Another useful measure is the "expected shortfall" which quantifies the "tail risk". It is the average of all the losses above the confidence level e.g. if VaR is calculated at a 95% confidence level then the expected shortfall is the average of the worst 5% of results.

For example, consider the case of a UK-based company which has a receivable of USD 100,000 and is therefore exposed to a strengthening in the GBP/USD rate (e.g. from the current rate of 1.3 to 1.5). Let's assume that we know the daily changes in GBP/USD over the last 10 years – approximately 2,500 data points assuming each year has 250 trading days. The process for calculating the VaR for this exposure is:

a. Order the daily changes in GBP/USD from the lowest to the highest. For example, in this sample the lowest figure could be -12% (i.e. GBP/USD falls by 12%) while the highest daily change could be +5% (i.e. GBP/USD increases by 5%)

b. Decide on a confidence level e.g. 95%

c. Find the value of GBP/USD such that 95% of the actual daily changes in GBP/USD are below this value – that is 95% of the 2500 rate changes are less than the worst expected rate. Let's assume this is 1% for this example.

d. The VaR is therefore the USD exposure using today's GBP rate (e.g. 1.30) less the exposure using worst expected rate (1.30 plus 1% change= 1.31). This results in a VaR of £587 i.e. the USD 100,000 receivable could decrease by up to £587 over one day assuming an expected loss in line with a 95% confidence level based on historical data. Of course, the actual loss could be much greater because firstly we are assuming a 95% confidence level and secondly the past is not always an indicator of future changes in exchange rates.

2. Assume the changes in market prices follow a normal distribution

In this method the VaR is calculated using the properties of a normal distribution and the standard deviation of the variable. Consider the example of a company which expects to receive USD100,000 from a customer. The method for calculating VaR using the normal distribution is:

a. Calculate (or assume) the standard deviation for the daily changes in the GBP/USD rate. For this example, assume it is 0.5% based on a data set and the current GBP/USD rate is 1.30.

b. Given the shape of the normal distribution, it can be shown that 95% (or 99%) of data fall within a value which is 1.645 (or 2.33) times the standard deviation from the mean value of that data set – assuming the data follows a normal distribution.

In our example, using a standard deviation of 0.5%, the GBP/USD rate which corresponds to a 95% confidence level is obtained by adding the result of 1.645 multiplied by 0.5% of 1.30 to the current exchange rate of 1.30, which gives 1.31.

c. The VaR is the GBP value of the USD 100,000 at the current exchange rate of 1.30 less the GBP value at 1.31 (the 95% confidence level) which is £587 i.e. this is the worst expected loss over one day based on a 95% confidence level.

The advantage of this method is that it is easy to use but it assumes that the variable follows a normal distribution which may not be the case. It may be more appropriate to use a different distribution based on historical data.

NOTES

THE ACT WELCOMES COMMENTS ON THIS REPORT

Please send your comments to
technical@treasurers.org

The Association of Corporate Treasurers
69 Leadenhall Street, London EC3A 2BG **t** +44 (0)20 7847 2540
A body established in England by Royal Charter. Registration Number RC000859