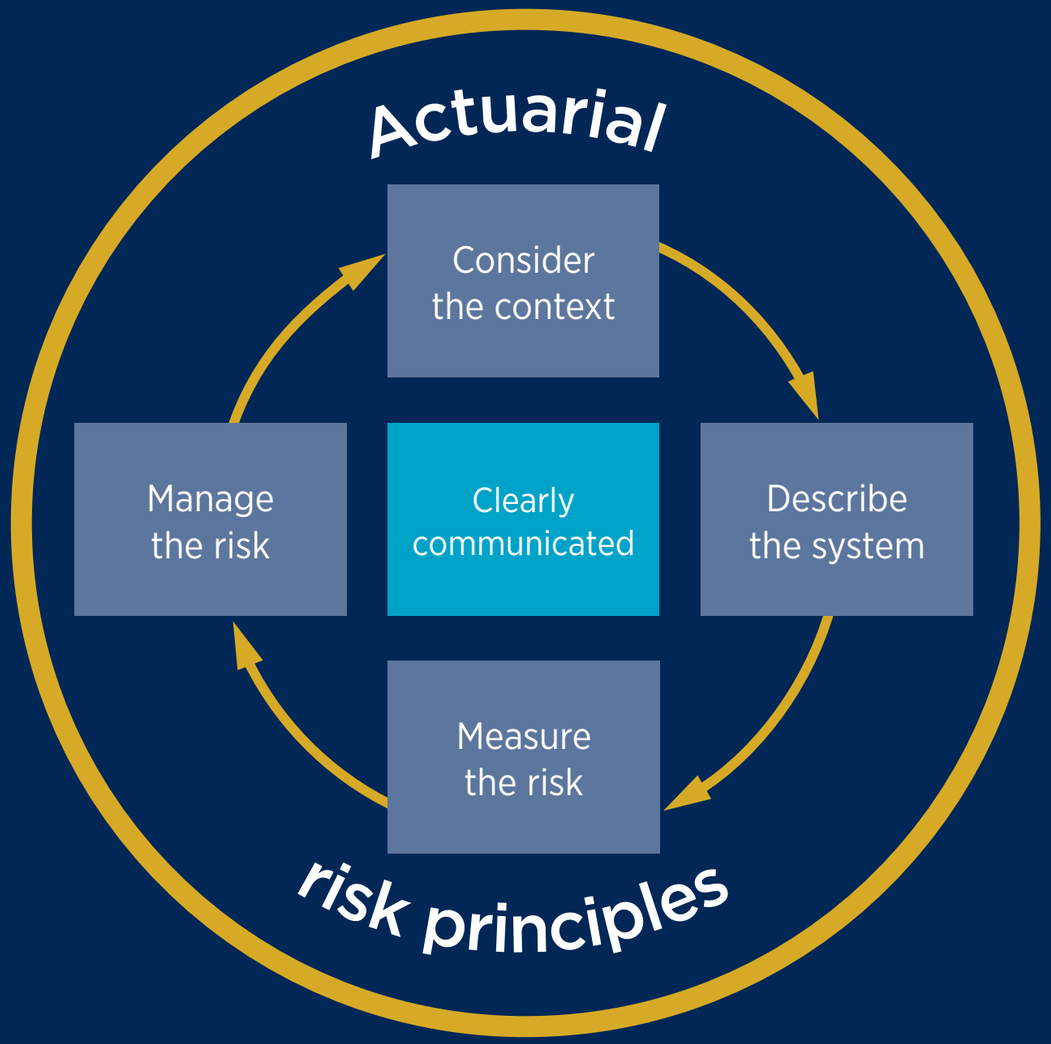
Institute
and Faculty
of Actuaries

Risk management – an actuarial approach

www.actuaries.org.uk

June 2017

Contents



In essence, risk management is an important tool to reduce losses, control uncertainty and optimise decision making to improve performance

Risk management – an actuarial approach

In the increasingly complex world within which we live, risk management is a discipline that is growing in importance for both private and public sector organisations.

Risk management is used to assist organisations to avoid, reduce the likelihood of, or minimise the impact of, events that might otherwise cause them significant harm, whether that be financial, reputational or any other damage. In essence, risk management is an important tool to reduce losses, control uncertainty and optimise decision making to improve performance.

Actuaries are skilled professionals whose comprehensive training includes the use of statistical analysis to understand risks and uncertainties. They are therefore well placed to support organisations' risk management efforts. There are many useful books and guides written on the subject of risk management. However, an actuarial approach to risk management places a particular focus on measuring and understanding the impact of risks, both positive and negative, on the outcomes experienced and considering how the risks and their impacts may evolve over time. Where appropriate an actuarial approach will place financial values on risk. In particular an actuarial approach considers risks more broadly, seeking to understand the range of potential impacts and the interaction of risks, rather than adopting a distinct impact and probability for each risk separately.

Actuarial risk analysis is not just based on short-term horizons but may extend many decades into the future when necessary. This focus on understanding long term impacts allows decision makers to better understand the typical range within which outcomes are expected to lie, as well as appreciating the potential impacts of more extreme events occurring.

The training and experience actuaries receive provides them with a uniquely broad-based combination of skills suited to risk management, allowing them:

- To explore the full range of risks that might affect an organisation;
- To quantify risks and their implications in the short and long terms;
- To quantify the value of any mitigation versus the cost of undertaking it;
- To illustrate the range of possible outcomes;
- To link financial and non-financial factors, such as the social and environmental impact for example from rising global temperatures;
- To integrate risk analysis into the wider economic business management process; and
- To communicate the risks to decision makers in a balanced and effective way.

Given the complexity of the wide range of events that could affect a business or government, the actuarial approach is highly valued by a range of organisations in growing and protecting their operations.

Set out below are what we see as the key principles adopted in an actuarial approach to risk management. They focus on the identification, quantification, mitigation and control of risks rather than the governance arrangements that might be placed around a risk management framework. Other principles may be added to this framework to address particular issues.

Building on the principles, we intend to illustrate the benefits of this approach through practical case studies on climate change risk and other topics.

It is important to see the framework not as a series of boxes to tick, but as a continuous cycle, as the diagram opposite indicates. The appropriate speed for navigating this cycle depends on the pace of change of the organisation or the wider environment.

Consider the context

1. Define the situation and stakeholder objectives under consideration

Before any analysis or management of risks can occur it is necessary to define what situation is being considered and which stakeholders are of relevance. The impact of risks can vary from party to party, and we therefore need to clarify the perspective and timescale from which risk is being studied.

A part of this is understanding what the potential positive and negative implications of each risk looks like. For example, we often focus on solvency as the ultimate downside risk definition for a business, seeking to identify which risks and which levels of impact would stop the business operating as a going concern. However, when looking at upside potential, and when considering governments as a stakeholder, solvency has limited use whereas other measures, for example the health measure Quality-Adjusted Life-Years (QALYs) may be more relevant[1].

Describe the system

2. Gather knowledge and data to reduce uncertainty

Risk managers cannot be experts in all areas where risks to an organisation may develop. They must discuss risks with the stakeholders and gather other experts' views of known and emerging risks. By gathering as much robust and relevant data/information as possible on the risks that exist, they can build up a more accurate picture of the drivers for risks and their likelihood and potential impact. This then allows for more informed choices about which risks are more or less important to study further. The more we can prioritise the risks that really matter to the stakeholders under consideration, the better the decision making process will be for managing those risks.

3. Understand the connection between risks

Many risks are connected with each other, meaning that events in one system can trigger failures in another. It is necessary, therefore, to study all risks together holistically, so that interactions between risks can be understood as much as possible. For example, 2011 showed how a natural disaster such as a tsunami could trigger a nuclear disaster in Fukushima. That a tsunami could disable the cooling and power supplies of the nuclear reactors had not been fully anticipated before the event.

Given the potential for risks to magnify and interact, it is essential to carry out careful analysis and interpretation of the factors that can cause and exacerbate risk events. Building mathematical models is part of this, but not necessarily as a way to forecast outcomes. They are more often used as a tool for exploring the dynamics between the various risks, as well as particular scenarios in which a number of risks materialise together (see principle 8), and providing an indication of the potential consequence of such interactions.

4. Develop an initial model

A clear initial model of the system subject to the risk needs to be developed. This model can help us to explore the consequences of changing inputs to the system; and to identify the most important interactions within it.

The model should include key assumptions and drivers, and these should be easily communicated along with a clear description of the system. The model development process requires as much real-world data as possible, but often this can be limited either because the system has little history or very few examples have been sufficiently studied. Expert judgement, from actuaries and/or subject specialists, is needed to interpret this limited data.

The model outputs should be chosen to align with the risk perspectives of key stakeholders (see principle 1). A balance must be struck to ensure that the model is not too complicated to allow the outputs to be interpreted, but also not too simple to be useful in exploring the system.

Risk managers should develop an awareness of their own skills and experience, and a realistic assessment of when they can add value and when they must decline an assignment.

1 | See, e.g., this definition from the National Institute for Health and Care Excellence (NICE): **https://www.nice.org.uk/Glossary?letter=Q**

It is important to be aware that all models have limitations: for example, they may include assumptions which are inaccurate or oversimplified; use flawed or incomplete data; or fail to adapt to changes in the external environment they are seeking to encapsulate. The following section, Measure the risk, describes practical ways to ensure that models remain a relevant risk management tool despite these limitations.

Measure the risk

5. Consider the full range of possible outcomes

The initial model will usually be set up to provide information about the range of most likely outcomes from a given set of inputs into a system. However, it is also important to recognise and understand extreme outcomes at the "tails" of the range of possible outcomes. This is particularly the case where the extreme outcomes may represent catastrophic results. Even if the probability of an extreme event is currently estimated to be low, our estimate could increase once we have a better understanding of causation factors which have not yet been recognised.

Actuaries are experienced in producing and using models to examine both the expected outcome as well as those that lie in the "tails". In particular, their training to consider the risk analysis required for insurance companies focusses on ensuring financial reserves are sufficient to cover more extreme outcomes.

For those inputs to the model where there is a degree of uncertainty, it is important to conduct a sensitivity analysis by completing the modelling using other plausible inputs to understand the implications for the likely outcomes. This is different to scenario testing and stress testing, which are described further in principle 8.

6. Allow for possible effects over the full time horizon of interest

The level of uncertainty in a particular risk – and the assessment of its impact – may change depending on the time horizon. Different factors may be more prominent over different time scales. To take an example, a significant shift in the real price of fuel would be more likely to affect driving mileage, and impact on related issues such as pressure on road infrastructure, accident rates and environmental requirements, if it was expected to be a long term development rather than a temporary one.

Uncertainty about outcomes may increase over time – the far future is sometimes more uncertain than the near future. It is therefore important to clarify which time horizon is most important for the stakeholder, so that we can focus on considering the right system drivers for that period. Furthermore, it may be important to try to understand the longer term development of a system, particularly where changes to the system take a long time to evolve, since these changes could affect the time horizon of interest.

7. Identify and adapt to changes to the underlying system

It is important to challenge prior assumptions about the way a system will run, and to see whether they still hold. When system dynamics change, the previous measurement approach may no longer be valid.

Sometimes the system provides a clear signal to review our approach, such as the Global Financial Crisis, though this may be a symptom of an earlier change (in this case the dynamic of mortgage lending and securitisation). However, it is not always the case that there is a clear signal, and there may be room for valid disagreement about whether a decisive change has taken place, particularly if a high threshold of evidence is required to acknowledge a change. In order to build an accurate and nuanced view, it is important to gather a wide range of interpretations of historic data and to consult a number of experts about the possible patterns of future experience.

8. Use stress testing and scenario analysis to test resilience

Scenario analysis is an assessment of a range of scenarios, including extreme ones, to help test the resilience of the stakeholder's strategy. It asks the question "What would we do if this scenario occurred?" and is a crucial method for organisations to understand their resilience to particular risks, and the connectedness of the risks they are exposed to. Studying possible future scenarios is often a more powerful method than studying the risk of specific events in isolation, which does not pick up the possibility of several events happening together in a particular set of circumstances.

Stress testing significantly varies the core planning scenarios to the upside or downside to see the financial impact on the organisation. Reverse stress testing aims to find the situations that cause existential threats for an organisation; for example helping understand where the organisation is at risk of failure or catastrophic loss.

Scenario analysis and stress testing help challenge model outputs to ensure that decision making does not just mechanistically follow the central result of the modelling. From a risk management perspective, these approaches are easy to explain and can therefore help in communicating the impact of risk.

9. Be alert to personal biases

Humans sometimes have personal biases that may cause them to think, act or make assumptions in unexpected or unjustified ways. Such biases may cause model inputs to be distorted and outputs to be misinterpreted, which may result in the level of risk being misconstrued or the priorities being confused. It is important to be aware of the existence of such biases and develop methods, such as cross-checking with others and with actual prior experience, to reduce their impact on the decision making process.

Actuarial research suggests that there are different outlooks among decision makers in terms of their belief in the value of models and their degree of confidence in model results.[2] In cases where confidence is low, reports to decision-makers should avoid putting too much reliance on the quantitative results obtained from modelling, and supplement them by a full discussion of the risks in qualitative terms.

Manage the risk

10. Develop a clear risk strategy

It is often necessary to the success of a business, product or policy to take risks in order to obtain suitable rewards. It is important therefore to manage risks whilst being aware of the impact on any potential rewards. An effective risk strategy for an organisation should:

- identify the main risks to the desired outcome;
- determine whether there are any quantifiable limits to the risks to be retained.
- clarify the extent to which the relevant stakeholders are willing to surrender potential rewards in order to reduce the negative effects of risks materialising – their 'risk appetite';
- determine which risks the relevant stakeholders are comfortable to retain and which they want to mitigate and control ;
- understand the cost and resource available to manage risks;
- decide which risk mitigation options will be most cost effective; and
- study any secondary risks resulting from the risk mitigation options which will be adopted.

11. Control the risk on an ongoing basis

Specific mitigations or controls can be used to reduce ongoing risks, provided that the value placed on this risk reduction is more than the cost of the mitigations and controls. This cost includes not just the direct costs, but also the indirect costs from adverse consequences and lost opportunities. For example, a construction company may opt to avoid the risk to its reputation from carrying out construction in an area with particularly vocal opposition, but would then miss out on the potential profits it might otherwise have achieved in this area.

12. Monitor the risk

Continuing studies of occurrences and other data may indicate increasing levels of risk, though careful analysis and comparison with other data sources is necessary to distinguish these from random or temporary variations. Conversely, monitoring can also highlight falling risk levels, which will sometimes, but not always, reduce the need for mitigation. As well as monitoring changes to existing risks, regular horizon scanning can be undertaken to identify potential new risks as soon as they emerge, while there is still time to do something about them.

Where the monitoring process leads to awareness of significant changes in the risk environment, whether from existing or new risks, this prompts reconsideration of the context and stakeholder perspectives, i.e. revisiting Principle 1 and emphasising the cyclical nature of the Principles as a whole, whilst possibly revising the model and its assumptions, inputs and outputs.

2 | Model Risk Working Party, Sessional paper 'Daring to open up the black box', December 2015

Actuarial risk principles case study:

Climate change

In addition to their obvious human costs, climate change and adapting to it may generate significant financial losses for organisations.

Below we outline an approach to developing a coherent response to these risks, using the IFoA's actuarial risk principles. This approach divides climate change risks for an institution into three categories that broadly cover physical damage, potential future claims and failure to adapt to climate change. Within each category, the risk principles are a guide to assessing the risk exposure, modelling possible outcomes, and putting a risk management strategy in place.

Consider the context

There is an overwhelming body of evidence that greenhouse gases emitted by human activity are leading to climate change and increasing evidence that this will lead to damage to many parts of the global economy. So compelling is this evidence that governments around the world signed up to the Paris agreement in 2015 to reduce emissions of greenhouse gases with the aim of keeping global average temperature rises to below two degrees centigrade above pre-industrial levels. This forms the "two degree" scenario central to planning for climate change. This degree of warming would still represent a changed climate but one in which some of the risk of extreme changes are reduced. To achieve only two degrees of warming greenhouse gas emissions will need to be cut dramatically resulting in an economy emitting no greenhouse gases by the middle of this century. Current national commitments to reduce emissions are unlikely to achieve this target. We should expect a steady ratcheting up of political and civil pressure to move from a high-carbon to a low-carbon economy.

Describe the system

The Earth's climate is a highly complex system with hard to predict consequences stemming from a given level of greenhouse gases in the atmosphere. However, in terms of understanding the likely effects of climate change on an institution, some relatively simple steps can be taken to categorise the risks. The following risk categories were described by Mark Carney in his "Tragedy of the horizons" speech given at Lloyds of London in September 2015:

- **Physical risks** – the risk of damage to property stemming from extreme weather or long-term changes in climate.
- **Liability risks** – the risk of claims been made by those suffering losses against institutions perceived as being responsible for climate change. In a professional context this may also include claims being made against fiduciaries and advisors who failed in their duties to protect stakeholders from the effects of climate change.
- **Transition risks** – the risk of either holding the assets of the old, high-carbon economy and finding that their value becomes impaired as they are retired quicker than their planned lives ("Stranded assets"); or of failing to invest in the assets required in the future, low-carbon economy (a form of "opportunity cost").

As the two degree scenario is a clear policy aim, calibration of these risks can proceed with reference to this scenario.

Measure the risk

Each institution should consider their exposure to the risk categories above in a two degree scenario. This means:

- Understanding the likely impacts of extreme weather and a warmer climate on your physical assets. This includes assessment of the exposure of assets to flooding, heatwave and drought, wind-storms and rising sea levels. This may extend beyond for example for example a factory in isolation but may additionally incorporate key infrastructure such as bridges or other vital transport links. It may also be germane to consider your supply chain's exposure.
- Assessing the level of greenhouse gases emitted within your business or portfolio of assets and the plans in place to reduce these emissions in line with the two degree scenario.
- Assessing the exposure of the business or assets to changes in technology linked to a movement from a high-carbon to a low-carbon economy.

These risk exposures should be researched and documented even if the risks are only considered material in the longer term. The Taskforce for Climate-related Financial Disclosures (TCFD) set up by the Financial Stability Board has recently consulted on global standards to help institutions disclose their risks publicly in their financial statements.

Manage the risk

Given an understanding of the current exposure to climate risks, the next step is to make a plan to manage these risks over an appropriate time-frame:

- To manage physical risks there should be plans in place to reduce the impact of extreme weather. This could include moving assets away from areas likely to become more exposed; redesigning infrastructure to make it more resilient for future weather conditions; insuring business disruption or other risks; or replanning business activities to remove exposures altogether.
- To manage liability risks these should be plans to reduce emissions consistent with achieving the two degree scenario. Third party claims are likely to improve in their capacity to attribute losses suffered to a specific organisation's greenhouse gas emissions; but stakeholder claims may be avoided if an institution can give evidence that it accepted the need, planned for and implemented a reduction of greenhouse gas emissions.
- To manage transition risks, the business should be actively planning around the technology it and its suppliers use. If low-carbon alternatives can be developed they are potentially highly valuable in the transition period, replacing some of the lost revenue and reduced capital from policy decisions relating to high-carbon technology.

The strategy for adapting to climate change risks will still need to be dynamic as climate science will improve our understanding of the future damage climate change is likely to cause, and governments will change their targets in response. These may challenge some of the assumptions within a climate risk strategy, so there will need to be a regular process to monitor how the risks are changing over time.

Actuarial risk principles case study:

Cyber risk

Cyber risk relates to the failure of an organisation's IT systems, and it could therefore be seen as the preserve of technical IT specialists. However, such events can generate significant financial losses, and in order to manage the risks, organisations need robust analysis of what could occur and what their options would be.

Below we outline how the IFoA's actuarial risk principles can provide a structured approach to developing a strategy for controlling the risk. This approach includes building a detailed picture of the risk exposure, modelling possible outcomes, addressing resource allocation choices and using new information to refine the strategy.

Consider the context

Cyber risk is relevant to a very wide range of organisations and individuals. In the traditional areas where actuaries advise on risk, the key stakeholder is likely to be an insurer or pension fund, but actuaries increasingly practice in 'wider fields', advising other financial firms as well as non-financial ones.

Whoever the key stakeholder may be, it is important to clarify its degree of concern about cyber risk (which may also be related to the stakeholder's awareness of potential cyber risk exposure). If it is very confident that it can avoid this risk then it is unlikely to invest much in controlling it – and vice versa.

It is also important to consider how the risks might manifest. For example, when a cyber risk materialises an organisation could face:

- Direct costs, such as hiring consultants or paying Government fines.
- Indirect costs, such as in-house investigations, or a slowdown in the rate of acquiring new customers.
- Opportunity costs, such as reduced customer trust and reputational damage.

Risk managers need to understand the stakeholder's business and which of these costs will be of most concern.

Describe the system

Having sketched a picture of the stakeholder and its risk attitudes and susceptibilities, the risk manager can begin to prepare the ground for analysing and measuring cyber risk. The first stage is to talk to experts in the organisation to build an accurate picture of its cyber risk exposure. These experts should represent disparate areas of the business, such as governance, IT, sales and outsourcing. Cyber risks can arise from a variety of sources, both internal and external, so it is also essential to monitor external sources of information on potential risks, especially as this is an area in which the risks are evolving rapidly. This detailed information gathering enables the risk manager to identify the priority risks to be analysed.

Some cyber risks could have a bigger impact in combination than on their own, and it is important to understand these connections.

Knowing the key cyber risks and how they interact will help risk managers to build an initial model of the risks. If it is available, industry loss data can be used to benchmark the model, taking account of important factors that affect the risk, such as location, revenue size, and sector. However, in some cases lack of data - in what is a relatively new area - may restrict the scope for modelling.

Measure the risk

Adaptability is particularly important for measuring cyber risk, which is changing rapidly and affects different organisations in different ways. This rapid development of the risk means that greater reliance is placed on human judgement, rather than available data, to determine appropriate modelling assumptions. This brings a danger that personal biases may lead to a failure to assess risk levels appropriately. With this in mind, working with more than one model may be a valid approach to generate helpful cyber risk narratives.

Risk managers can identify key cyber risk processes, study how they occur and develop scenarios – including extreme ones – to create a broad understanding of plausible situations. As the quantity and availability of data improves and the scenarios modelled become more detailed, it may be possible to place greater reliance on the modelling to forecast probable losses.

An effective cyber risk model should not only highlight the most likely outcomes but also the 'tails', more extreme outcomes which could nevertheless represent very large losses.

When a cyber risk takes place, the impact can occur in distinct phases. For example, straight after a cyber attack the affected company may close down a compromised application and hire more staff to deal with queries; later on, the focus could be to manage the impact by adjusting premiums and improving cybersecurity; still later, the company may need to alter strategic decisions, for example stepping back from an acquisition because the cyber event led to a lower credit rating. It is therefore important to clarify which time horizon matters most for the stakeholder in order to fully assess the potential implications of a risk occurring.

Manage the risk

The process of describing and then measuring and modelling cyber risk should give an organisation a realistic picture of its cyber risk exposure, together with plausible scenarios and their impacts. To turn this information into a plan of action to manage cyber risk, the company must now interpret this evidence in the context of its risk appetite. One key issue will be to find an appropriate balance between investing in actions to mitigate the risk, and buying cyber insurance.

An organisation will often have scope to introduce new practices or improve internal processes in order to mitigate aspects of cyber risk. Examples include communicating the seriousness of cyber risk at Board level; implementing IT controls; ranking internal data by the level of potential damage if it was compromised; or reducing ties to suppliers seen as high-risk.

Where the company is considering cyber insurance, the nature of the insurance coverage is likely to be an important factor – not only the range of financial losses covered, but also whether the policy terms include advice on risk solutions to help mitigate future risks.

Rapid innovations in information technology mean that new and unforeseen forms of cyber risk are inevitable. This makes it all the more important for organisations to carry out continuous horizon scanning of potential cyber threats and to ensure new intelligence is fed back into their risk modelling, thus enabling the cyber risk strategy to remain up-to-date and fit for purpose.

Actuarial risk principles case study:

Automated vehicles

The pace of development of automated vehicles has increased in recent years, with intensive vehicle testing in increasingly real-world settings.

Automated vehicles offer the prospect of major benefits, such as reducing the number of accidents based on human error, and increasing mobility for the elderly population and others. At the same time, there are many unknowns, and therefore many risks that need to be assessed. Below we outline some of these risks, and how the IFoA's actuarial risk principles can provide a framework to develop an effective risk management strategy.

The context

In relation to emerging risks from automated vehicles, it will be critical to consider stakeholders' perspectives ranging from drivers, passengers, car manufacturers, governments, industrial users, software providers, other road users, the general public, highway agencies and insurers. In the examples that follow we are just considering a potential insurer's perspective and the risks they would wish to understand and minimise.

The system

The approach might involve gathering key findings from prototype tests already undertaken and sponsoring further prototype initiatives through industry body / government initiatives or partnering with particular motor manufacturers. As more test miles are completed by prototype cars, greater understanding should develop regarding the nature of the risks of collisions, initially with non-automated vehicles which currently form the bulk of the traffic, but moving on to consider the risk of accidents involving a network of automated vehicles.

Any model will need to capture such interactions as the relationship between the speed of design developments, speed of legislative change, the number of automated cars and other vehicles in use, the diversity of different systems that are subsequently involved and the emerging cultural changes in society at large with regard to the use and ownership of automated vehicles. These interactions may create a more complex environment for such vehicles to operate within, therefore impacting the risk of accidents occurring. There may be other factors such as the risk of bad weather or light leading to particular issues for automated vehicles and hence higher numbers, or more severe accidents. Conversely the vehicles themselves may help to further reduce accidents over time as they share data between themselves and continue to improve as more and more data is gathered with increasing miles driven by the fleet of cars as a whole.

Insurers are likely to be most focussed on the frequency of accidents involving automated vehicles and the likely costs involved. They will then focus on who pays those costs which requires an understanding of where liability will sit. It may be that manufacturers' product liability insurance will cover the costs. Modelling may therefore include a focus on automated car numbers and the extent of different automation systems. However the legislative environment may force a different perspective which would require the insurer to initially meet the cost of any claim and then seek recovery from the manufacturer (or their insurer).

Risk measurement

For insurers, it is critical that the potential impacts of more extreme levels of accident are considered and what might give rise to these. As an example, it is important that an analysis considers both the potential for a greater frequency of accidents or an increase in the severity of accident events. A possibility to be considered is that extreme weather over a wide area might cause an unexpectedly large number of vehicle malfunctions and accidents to arise simultaneously. There could be other reasons for a sudden surge in accidents such as a software malfunction or hacking of the software.

Based on the current rate of change, it is likely that it will take a number of years, possibly a decade or more, until society is dealing with easily accessible automated vehicles and there will be a number of transition stages until we get there. This leads to a wide range of possible scenarios/developments that could happen and it is important that these multiple pathways are considered in any analysis.

Models may be constructed allowing for specific types of automation and volumes of traffic. Manufacturing developments, population changes and other external factors could alter the system and the hence the risks an insurer is exposed to.

An example of a stress test scenario could be considering the outcome of all cars going offline at the same time, with limited manual intervention, leading to mass accidents and global chaos.

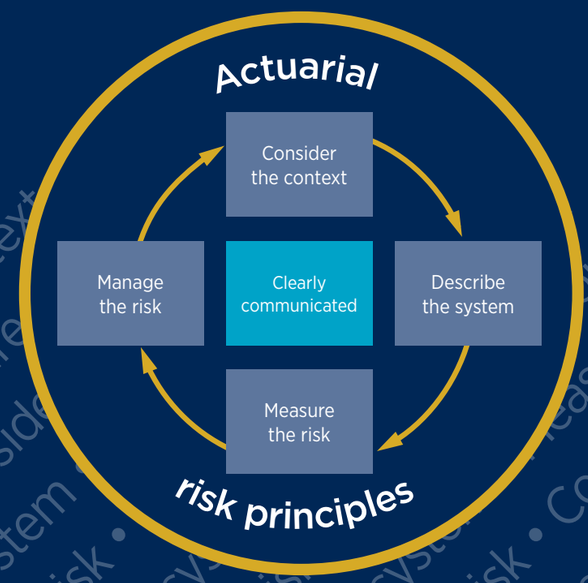
Manufacturers, insurers or users may make an unjustified assumption that later designs will be no riskier than previous ones, because they incorporate additional safety features and new technology. The converse may instead be that newer models have software which has undergone less testing than that which has been used on the road for some time.

Risk management

Risk management scenarios could have wider consequences which need to be thought through and reflected in any modelling or understanding of their impact.

An example might be that by limiting speeds to reduce the risk of collisions this could increase traffic jams and extensive delays. This may in turn reduce future car ownership and hence the demand for insurance.

An alternative example might be certain insurers including clauses in policy wording making it clear that drivers still have responsibility for their vehicles as new technologies are introduced and articulating where policies will not provide cover. This would leave such policyholders reliant on the manufacturer and their product liability insurance. The claims costs for insurers of these drivers might be reduced, but there may be a growing reluctance for people to take out insurance with them.



Institute and Faculty of Actuaries

Beijing
14F China World Office 1 · 1 Jianwai Avenue · Beijing · China 100004
Tel: +86 (10) 6535 0248

Edinburgh
Level 2 · Exchange Crescent · 7 Conference Square · Edinburgh · EH3 8RA
Tel: +44 (0) 131 240 1300 · **Fax:** +44 (0) 131 240 1313

Hong Kong
1803 Tower One · Lippo Centre · 89 Queensway · Hong Kong
Tel: +852 2147 9418

London (registered office)
7th Floor · Holborn Gate · 326-330 High Holborn · London · WC1V 7PP
Tel: +44 (0) 20 7632 2100 · **Fax:** +44 (0) 20 7632 2111

Oxford
1st Floor · Park Central · 40/41 Park End Street · Oxford · OX1 1JD
Tel: +44 (0) 1865 268 200 · **Fax:** +44 (0) 1865 268 211

Singapore
163 Tras Street · #07-05 Lian Huat Building · Singapore 079024
Tel: +65 6717 2955

www.actuaries.org.uk