CONTROL FRAMEWORK

FOR REGULATORY AND TAX REPORTING (SERVICE COMPANY BUSINESS)

User Guide version 3.0

Updated January 2016

KEY CONTACTS

Website: www.lloyds.com/controlframework

General enquiries: controlframework@lloyds.com

CONTENTS

EXECUTIVE SUMMARY

MANAGING AGENTS HAVE A RESPONSIBILITY TO CARRY OUT THEIR OBLIGATIONS IN RELATION TO REGULATORY AND TAX REPORTING, SUPPORTED BY LLOYD'S.

THIS FRAMEWORK SETS OUT THE MEANS THROUGH WHICH MANAGING AGENTS DEMONSTRATE COMPLIANCE AGAINST THE REGULATORY AND TAX INFORMATION REQUIREMENTS SET OUT BY LLOYD'S FOR SERVICE COMPANY BUSINESS.

IT MUST BE IMPLEMENTED BY MANAGING AGENTS IN A TIMEFRAME AGREED INDIVIDUALLY WITH LLOYD'S.

As the supervisory and regulatory environment changes, there is a shift in expectation as to what constitutes adequate evidence that sufficient rigour has been applied to the quality of regulatory and tax reporting.

This control framework is Lloyd's response to ensuring it can satisfy requests for evidence into the future. Managing agents will benefit as Lloyd's will be able to continue to act as the primary respondent to regulatory and tax reporting queries for Lloyd's business.

This framework, while initially piloted with direct reporting companies, is also relevant to those who chose to process service company business via Xchanging. Companies do not relinquish their responsibilities for regulatory and tax requirements by outsourcing to third parties.

Below is a summary of why the framework is necessary, what the framework is, how it will benefit the market and what this means for managing agents.

Drivers for the framework

- A changing supervisory and regulatory environment, e.g. growing number of tax audits, notably in Europe, both in the Lloyd's market and the general insurance market
- Desire from a number of managing agents for choice in operating model
- Increasing regulatory risks associated with sophisticated cross border business being written

What the control framework provides

- A common structure for the assessment of risks and associated controls in the context of data quality for regulatory and tax reporting
- Mechanisms for managing agents to share the confidence that they have, in the appropriateness and operation of the controls, with Lloyd's
- A proportionate approach that allows managing agents to take credit for what they already do and identify any risks where further mitigation is required

Benefits

- Visible and auditable data standards will help protect managing agents from direct regulatory scrutiny
- Minimising the risk to the overall Lloyd's licences from non-compliance by individual managing agents
- Protection and potential improvement of the competitive position of the platform internationally
- Maintaining or enhancing the Lloyd's brand and reputation

What managing agents will need to do

- Board level understanding of the importance and relevance of the framework to protecting the market
- Take ownership and responsibility for compliance. This should involve appropriate governance with senior management involvement
- Analyse and assess readiness for compliance
- Engage with Lloyd's to put the framework into practice

Ultimately, the implemented framework will provide Lloyd's with a body of evidence that will allow Lloyd's to demonstrate the level of rigour applied to compliance with reporting requirements. This will protect the market. Real commitment will be needed from all involved for it to be a success.

INTRODUCTION

THIS FRAMEWORK IS THE MEANS THROUGH WHICH MANAGING AGENTS DEMONSTRATE COMPLIANCE AGAINST THE REGULATORY AND TAX INFORMATION REQUIREMENTS SET OUT BY LLOYD'S.

THIS DOCUMENT DEFINES THE FRAMEWORK, ITS CONSTITUENT COMPONENTS AND OUTLINES HOW IT IS TO BE APPLIED BY THE MANAGING AGENTS.

The document is intended to:

- Provide background and overview guidance
- Explain the risk methodology applied
- Give examples of how the risks apply at both a generic and detailed level
- Illustrate with examples, controls that could be applied to mitigate the risks
- Provide guidance as to the right balance of evidence of control activities that should be maintained
- Provide guidance as to how assurance in controls can be shared by managing agents with Lloyd's

DEVELOPMENT OF THE FRAMEWORK

Rationale for the framework

Lloyd's has developed this control framework to protect and enhance the operating model for regulatory and tax reporting through a period where the industry is seeing a change in the way that regulatory and tax authorities operate as well as increased demand for choice of operating model by managing agents.

The framework is designed to further enhance and demonstrate Lloyd's and managing agents assurance that effective controls are in place. The framework recognises that each managing agent will manage and control their internal processes in different ways.

This framework has been piloted with a selection of market participants. Critical success factors identified from the pilot, and wider consultation, indicate that for the framework to achieve its objectives:

- Responsibility for compliance with regulatory and tax requirements must be acknowledged by appropriate senior management. Ultimately, responsibility should reside with the board and both the Chief Risk Officer and Chief Financial Officer are expected to have a particular interest
- Senior level acceptance of responsibility should be demonstrated by direct involvement in the application of the framework and by signing off on the controls in place. In larger managing agents, sign off may be delegated to appropriate senior staff, for example to the Head of Tax and Head of Compliance
- To successfully understand the risks associated with regulatory and tax reporting and the associated controls, appropriate involvement of stakeholders across disciplines including Operations, Tax, Compliance, Risk, Underwriting, Claims, Internal Audit and Information Technology will be needed

THE SIX STEP APPROACH: OVERVIEW

The control framework comprises an ongoing cycle of:

- Assessing risks associated with the completeness and accuracy of data (for service company business)
- Gathering evidence that appropriate controls are in place
- Ensuring the controls continue to work and that any breakdowns are addressed

The approach is set out below:

Step 1: Information Requirements

- These are the minimum information requirements for regulatory and tax reporting defined by Lloyd's
- These are provided to individual managing agents. Any changes will be communicated if they occur
- These requirements define the scope to which this framework applies

Step 2: Risk Model

- The risk model is the structure for understanding and identifying risks associated with satisfying the information requirements
- The model, and any subsequent changes, is defined by Lloyd's and provided to managing agents

Step 3: Apply Risk model

- In this step, managing agents use the risk model to assess how the risks are relevant to the information requirements in their business
- In order to perform this step, managing agents need to have a thorough understanding of the information requirements and the risk model provided to them in the previous two steps

Step 4: Identify and Document Key Controls

The next step is for managing agents to identify and document the key controls in place to mitigate those risks. This step consists of three main activities and is likely to be the bulk of the effort involved in deploying the framework:

- Identification of controls
- Consideration of whether the controls address the associated risks and whether there is adequate evidence to demonstrate that the controls operate
- Remediation where appropriate

Step 5: Gather Evidence

- In this step, managing agents gather evidence to demonstrate the effective operation of key controls documented in the step above
- The extent of evidence expected is intended to be proportionate to the associated risks

Step 6: Provide Assurance

- Managing agents are to share the confidence they have in the quality of their regulatory and tax reporting data
- In this step, managing agents will provide sign off together with agreed supporting documentation to Lloyd's

The extent of the supporting documentation required will be decided by Lloyd's in consultation with each managing agent and may, for example, include Agreed Upon Procedure reports, internal audit reviews or some form of external attestation.

USING THIS DOCUMENT

The remainder of this document explains each of the six steps in more detail. A common format is used to set out, for each step:

- Objectives of the step
- What managing agents need to do
- Outputs from the step

Supplemented by:

- What managing agents need to know in order to complete the step
- Lessons from the pilot and other tips
- Supplementary guidance
- Example outputs if the optional Lloyd's templates are used

WHAT NEXT?

Before moving on to the next sections for implementation, individual managing agents should carry out an initial assessment of:

- Who will own the implementation of the framework
- What appropriate governance should be deployed
- The individuals who should engage with Lloyd's on this topic
- The perceived level of confidence in the regulatory and tax reporting processes
- Potential differences between framework implementation responsibilities and day to day operational responsibilities

To do this effectively it is likely that:

- The Board, and potentially the Audit Committee or Risk Committee, will need to be briefed such that they have a good understanding of the overall requirements
- A project manager should be assigned to the framework project to facilitate and coordinate the initial assessment

The Lloyd's team are on hand to answer questions, clarify information and agree checkpoints for review along the way. See Key Contacts at the beginning of the document for detail.

1 INFORMATION REQUIREMENTS

OVERVIEW

This step explains how Lloyd's define the information requirements, and how they affect individual managing agents.

OBJECTIVES

- To ensure managing agents have a thorough understanding of the requirements
- To prepare for the subsequent steps of the framework

WHAT MANAGING AGENTS NEED TO DO

- Go through each requirement in detail
- Raise any queries with Lloyd's

Who should be involved: Initially, the project owner and those with associated governance responsibilities. As the project progresses all those involved with the project should become familiar with the requirements.

OUTPUT

- Managing agents have a thorough understanding of the information requirements as defined by Lloyd's
- Notes of any areas that are challenging to understand and the conclusions drawn

WHAT MANAGING AGENTS NEED TO KNOW

The information requirements for regulatory and tax reporting on service company business are defined by Lloyd's. These can be found in the tables in Appendix 1.

They are described in terms of the following:

- Transaction being reported – for example currency or amount
- Contract – such as dates, risk or coverage
- Losses – for example claims or third party details
- Tax – such as amount, settlement or calculations
- Intermediary – for example role, name and location
- Insured/Reinsured – for example name, address and location

The tables indicate whether the requirements are applicable to reporting premium or claims transactions, or both. They also summarise any additional requirements relating to regulatory and tax liabilities applicable only for specific countries.

All of the requirements are mandatory but have been divided into two categories, 'critical' and 'required'. 'Critical' indicates a high inherent risk of error and/or the implication of an error is more likely to be severe. An example of this would be 'location of risk'. The consequences of getting this wrong could have a significant impact on licences. 'Required' indicates a lower risk of error and the implication associated with an error is expected to be less severe. An example of this would be 'address of direct assured'. This rating will enable Lloyd's and managing agents to focus their attention on key risk areas.

Experience from the pilot

- **The tables in the appendix list the business information which managing agents reporting service company business should have at hand. Depending on the reporting channel and the processing mechanism they choose, they may not have to provide all of them**
- **For example some managing agents report directly to Lloyd's using a flat file or XML format while others report via Xchanging. The base data requirements are the same through each mechanism albeit the format may be different and not all fields are required from managing agents in some circumstances**

Tips for managing agents

- **The information requirements have been defined by Lloyd's. Some of these do not have a single definitive interpretation and in these cases it is for managing agents to determine what the requirements mean in their own context**
- **This requires skills or knowledge and experience from a regulatory and tax background. The risk associated with some managing agents not having tax or regulatory expertise should be specifically highlighted later in the Apply Risk Model step of this framework**

FURTHER CONSIDERATIONS

- Given the focus of the framework is on the data reported to Lloyd's, it is each managing agent's concern as to how they gather and transform that data
- Once the managing agent has understood all the requirements they can start to consider how their current practices are satisfying the requirements

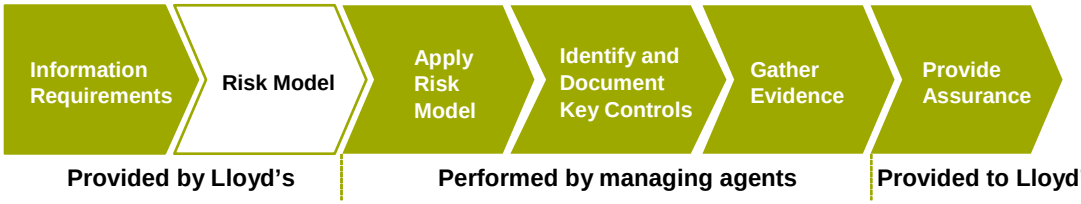
- Automated and manual processes will need to be considered
- Managing agents completed the pilot via a series of workshops. However, each managing agent is better placed to determine the approach themselves

DOCUMENTING THE OUTPUT

During this step managing agents may require further guidance on some of the information requirements. The following example sets out a format managing agents may wish to use to capture the confirmation needed.

Information Requirement	Consideration	Resolution
Intermediary Role, Name and Reference ID	What reference ID is this – is it the internal reference we use or is there a common list of reference IDs that we should be working from?	Confirmed with Lloyd's that this reference can be either our internal reference ID or a market recognised one.

2 THE RISK MODEL



OVERVIEW

This step defines the risk model for this framework. It is integral to strike a balance between being generic enough to apply across all information requirements and businesses while at the same time being specific enough to ensure that key areas of risk are identified.

Managing agents should consider how each of the standard risks is relevant to their business in the next step of the framework – Apply Risk Model.

OBJECTIVES

- To ensure managing agents have a thorough understanding of the risk model
- To prepare for the subsequent steps of the framework

WHAT MANAGING AGENTS NEED TO DO

- Go through and ensure that the risk model is understood

Who should be involved: All those involved in the framework implementation will need to be familiar with the risk model.

OUTPUT

- Managing agents have a thorough understanding of the risk model

WHAT MANAGING AGENTS NEED TO KNOW

The five standard risks used in this framework are defined below. For each, an example of how the risk could apply is also provided, based on experience with pilot managing agents.

Risk 1: Requirements are not understood

Here, 'requirements' refers to the information requirements defined by Lloyd's for service company business in Appendix 1.

There are many reasons why this risk may crystallise. It could be that the individual interpreting the requirements does not have the requisite skills or experience, human error, or the requirements being unclear or ambiguous. Some requirements could still be misinterpreted even when furnished with a detailed explanation. The level of complexity has an impact on the magnitude of the risk that the requirement may be misunderstood.

As an example, a managing agent interpreting the requirement, 'location of (re) insured country' without fully understanding the explanation of the requirement may interpret it incorrectly. The following definition shown here illustrates this point. It is not the most complex but could still easily be misunderstood.

Lloyd's Information Requirement	Description
Location of (Re)Insured (Country)	The country in which the insured is resident, if they are a private individual, or if it is a corporate body, where it has its main operating address. For a reinsurance contract, the country in which the ceding insurer's office is situated. For a global or multi-national policy, the country in which the insured's head or main office is situated. For a master policy, the country in which the master policyholder is situated. It is recommended that the ISO 3166 2 letter country codes are used.

Risk 2: Data capture is inadequate

This may relate to data not being captured, being captured more than once (duplicate) or that the data captured is erroneous. It may also be that data is not refreshed on a timely basis.

For example, if a managing agent insured a chain of petrol stations across the US, they are required to provide the location of each petrol station. It is conceivable that some managing agents may currently only record the address of the head office of the company and as such may not have adequate data to be able to meet the reporting requirements. For example, the requirement below features in the Additional Information Required for US Regulatory and Tax Liabilities section of the information requirements and is a good example of a requirement where this risk may be of heightened relevance.

Lloyd's Information Requirement	Description
Location of Risk (State/Province/Territory)	If applicable, the state / province or territory in which the risk is located.

Risk 3: Data is processed incorrectly

Between capture and reporting, data will undergo some form of processing. In some cases this will be about using different

elements of data to compute other information, but it also relates to things such as erroneous report definitions.

Using a straightforward processing example to illustrate this risk, some policy administration systems may be not be able to deal with certain currencies in which business is written. A work-around that may exist is for a managing agent to convert this into a more common currency. Although they know (on source documentation) what the original currency was for the policy, there is a heightened risk of this correct data not being used correctly for reporting as it is recorded in core processing systems incorrectly.

Bringing this example to life, a company that can only process transactions in GBP, EUR and USD, when faced with a premium in SEK, may convert at the point of data entry to EUR. This means that even though the SEK premium data is held by the insurer on the slip, there is a heightened risk that they may not report it correctly because their system does not facilitate this.

Lloyd's Information Requirement	Description
Gross Premium in Original Currency	The premium paid in this transaction before any deductions and before IPT is applied, expressed in original currency. If the transaction is a premium instalment, this should be the gross amount of the instalment.

Risk 4: Data is corrupt

Data may be corrupted accidentally or on purpose. Most obviously, this involves inadvertent or erroneous changes to data when it is being adapted outside of core processing systems, for example in spreadsheets.

For example, this risk could be where the file provided to Lloyd's is a spreadsheet that is compiled as part of a semi-automated process that is subject to manual intervention. The operator could make mistakes, or may submit an incorrect version of the file.

Risk 5: Data is lost and cannot be recovered

This is most likely to crystallise where historic information is not contained in core processing systems that are subject to a robust backup regime, but in end user computing facilities such as spreadsheets or user maintained databases.

This risk is less likely to occur in organisations that have mature IT systems and back up regimes in place. It is more likely to happen where there is a high degree of dependence on spreadsheets and paper based systems. This may be in the managing agent themselves, or at the offices of business partners.

For example, Lloyd's require managing agents to report the date that a claim was first reported by the insured to the first party in the notification chain, as demonstrated below.

Lloyd's Information Requirement	Description
Date Claim Made From	The date that the claim was made by the insured to the first party in the notification chain. This is more commonly used for claims made policies which are a form of insurance that pays claims presented to the underwriters during the term of the contract or within a specific term after its expiration.

If the insured house burns down they may telephone their broker (Intermediary), who records the call on a spreadsheet-based log. If the broker's computer hard drive crashes and the spreadsheet is lost, the data is lost and may not be recovered.

Experience from the pilot

- **In addition to the straightforward business process relevance of this risk, there may be additional risks associated with the behind the scenes operation of the IT systems involved in the processing of data**
- **Some organisations may find that while initially the risk model seems intuitive, this step will likely need to be revisited later on**

Tips for managing agents

- **If those involved with understanding this risk model are having any difficulties they should consult with internal controls specialists, for example, their Internal Audit team**
- **This model applies at the INHERENT RISK level, i.e. before the application of controls. This means that many of the risks may be addressed by existing controls**
- **The purpose of this risk model is to identify the risks that may threaten the completeness or accuracy of the data submitted to Lloyd's for the purpose of regulatory and tax reporting**

FURTHER CONSIDERATIONS

IT specific risks

Risks 3, 4 and 5 could crystallise due to inadequate controls over IT systems. For example systems may process data incorrectly due to inadequate system change controls or data may be lost due to inadequate backup and recovery controls.

To the extent that business process controls are identified in Step 4 of the framework 'Identify and Document Key Controls' which are dependent on IT controls, IT specific risks over the systems relevant to those controls should also be considered.

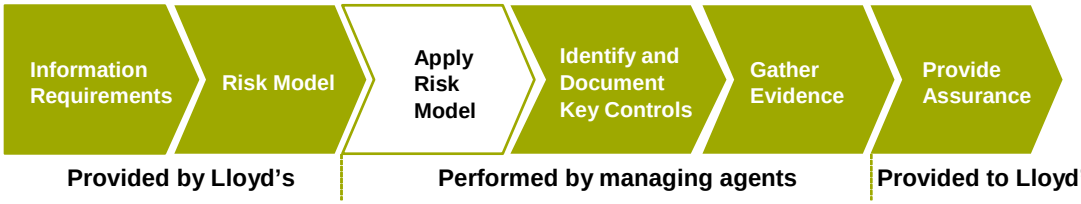
Further guidance in this aspect is provided in Appendix 3.

DOCUMENTING THE OUTPUT

Appendix 2 shows a template which can use to document output as they go through each step of the control framework. Lloyd's will provide managing agents content for the first two columns of the template, namely 'Information Requirement' and 'Applicable Risk'.

The format is not mandatory, but has proved useful with pilot managing agents. Other formats may be used as long as they meet the objectives of the framework.

3 APPLY RISK MODEL



OVERVIEW

This is a process that will need to be thought through by each managing agent. It involves determining where the risks are most likely to crystallise through their processes and management activities.

During this step, each information requirement is risk assessed and prioritised. This will determine the strategy for evidence gathering later on in the framework. Appendix 2 contains an example template that can be used for this step.

As a result of the pilot, it was noted that the most practical way to run this process may be through a series of workshops attended by key stakeholders. This is not the only way to address the activity in this framework. Each managing agent is best placed to decide on the approach.

OBJECTIVES

For managing agents to:

- Identify how the risk model applies over the information requirements on service company business in their individual organisation
- Validate the initial understanding of the requirements and the risk model

WHAT MANAGING AGENTS NEED TO DO

Typically, managing agents may:

- Identify relevant stakeholders within the organisation to participate in the risk assessment
- Plan the approach to break down the activity into manageable components
- Carry out any follow up activities and conclude on the risk assessment

Who should be involved: Participants may include Operations, Tax, Compliance, Internal Audit, Information Technology, Risk, Underwriting and Claims.

OUTPUT

In the course of this step, the following documentation should be produced:

- The risk rating and rationale for how each risk may apply to each information requirement
- Sign-off by a suitably senior member of staff such as the Chief Financial Officer or Chief Risk Officer

WHAT MANAGING AGENTS NEED TO KNOW

Throughout the risk assessment, think about inherent risks, that is, risks that exist BEFORE controls are taken into consideration. This is an important concept and is vital to the success of the process.

In order to make the process as efficient as possible, the following advance information should be considered and should be available:

- The mechanism used to report regulatory and tax data (flat file, XML or via Xchanging)
- The risk model set out in Step 2
- Any existing business process documentation, such as process narratives or risk and control matrices
- Control related documentation such as internal or external audit reports, risk management reports and any other documentation that may assist in the identification of known risks. Note these reports will typically only consider 'net risk' (risk after the application of controls) so these will not be comprehensive for the purpose of identifying inherent risk

Experience from the pilot

- **Techniques such as process mapping can be used during implementation, though no particular approach will be mandated**
- **The examples in this document use a particular risk rating model. However, managing agents may already have an existing alternative methodology in place for this purpose. Alternatives can be used if they yield a proportionate and cost effective response**

Tips for managing agents

- **The risk assessment is something that will need to be updated on a periodic basis or when there are significant changes to scope or process**
- **Because this framework is focused on regulatory and tax information, the accounting concept of materiality does not apply in the way it would for financial reporting relevant to statutory accounts. However, it is reasonable that companies can consider probability and impact of a risk crystallising to determine the extent to which controls should be deployed**

FURTHER CONSIDERATIONS

A small subset of those involved in applying the risk model may wish to consider IT general control in a separate session. As explored in Appendix 3 these relate to some generic risks around the control of IT systems. Note this does not relate to the business process controls operated by the system, it rather covers the 'behind the scenes' aspects of IT such as user access to systems, application maintenance and change control and data backups. There is a relationship, however, between the IT and non-IT considerations so it is important there is some cross-over between the groups involved in the IT and non-IT aspects.

Some form of quality assurance activity should take place after the session. This may involve challenge by someone from a risk and control background, for example someone from Internal Audit.

DOCUMENTING THE OUTPUT

During this step, managing agents will complete the third and fourth column of the example document in Appendix 2, namely 'Risk Rating' and 'Rationale for Risk Rating'. This involves completing the risk rating and the rationale to support it.

4 IDENTIFY AND DOCUMENT KEY CONTROLS

OVERVIEW

This step requires managing agents to identify and document the key controls mitigating the risks identified in Step 3. In addition, they should consider the effectiveness of the design of the controls identified to confirm that the design is appropriate to mitigate the risks.

OBJECTIVES

For managing agents to:

- Identify and document the key controls over the risks described in the previous step such that an independent reviewer would be able to understand what each control is seeking to achieve and how it is done
- Assess whether individual or a combination of controls sufficiently mitigate the relevant risks
- Improve (remediate) controls if any relevant risks are not sufficiently mitigated

WHAT MANAGING AGENTS NEED TO DO

Managing agents may typically hold sessions in which they will:

- Understand the way in which relevant data flows through the organisation
- Identify controls that have been deployed that may be relevant to the mitigation of risk
- Determine which controls are most relevant and document them in some form of risk and control matrix that sets out those relevant to the mitigation of each risk, for each of the information requirements
- Evaluate whether the controls associated with each risk adequately mitigate the risk - a step also known as carrying out an assessment of design adequacy
- Determine how to remediate (fix) any controls that are not designed effectively

Who should be involved: People involved with the day to day processes, together with those who understand the information requirements, risk model and risk assessment. In addition, the documentation of key controls is an activity that requires a certain level of skill or experience and therefore it is recommended that specialist support, for example internal controls specialists or internal audit, be sought during this phase.

OUTPUT

At the conclusion of these activities, the following information will have been compiled and should be signed off by Business Senior Management:

- Risk and control matrices
- Design adequacy assessment
- Control deficiency log and improvement plan (if needed)

Who should be involved: It is suggested that the managing agent assigns a suitably senior member of staff to review the output from the control assessment. Sign-off should be carried out by the line manager relevant to the controls being considered with final overall sign-off by the framework owner, appointed by the board.

WHAT MANAGING AGENTS NEED TO KNOW

In order to successfully complete this step, those involved will need:

- Knowledge used during earlier steps
- Knowledge of how relevant data flows from source through to submission to Lloyd's. Where there is a high degree of dependence on reconciliations at the back end to source documentation this data flow mapping can be done at a high level. Otherwise the detailed flow must be understood
- The detail of how controls operate and how the controls address the identified risks

Risks are not expected to be mitigated to zero. The extent to which they need to be mitigated is a matter of judgement, hence the need for senior involvement referred to already in this methodology. For the purpose of regulatory and tax reporting, the extent to which controls should mitigate risk is likely to be similar to that for other statutory tax reporting and for FSA returns.

Experience from the pilot

- **Involve those who actually carry out the activities on a day to day basis. Often the real operation of controls may be different to what others perceive**
- **Try not to make assumptions about what others know. This is particularly the case where there is terminology or classifications unique to Lloyd's**

- **Where processes are highly automated and systemic there may be less risk of control breakdown or management override of controls**

Tips for managing agents

- **Break work up into manageable pieces**
- **If individuals are struggling to understand how they ensure data quality is met, ask about what they do and this will usually reveal controls they are undertaking without realising**
- **Where detective controls, such as reconciliations are used, it is important to ensure that these happen on a timely basis such that they can detect errors, and allow for correction, prior to reporting taking place**

FURTHER CONSIDERATIONS

This section sets out further guidance on the following, which provides assistance to managing agents when documenting and assessing the design of the control environment:

- Good practice documentation of controls
- Assessing design adequacy
- Design adequacy, special considerations

This step involves the main bulk of effort within the framework: there are tips for managing agents and lessons from the pilot for each of the three topics above.

Good practice documentation of controls

Controls can be diverse and include activities such as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Good practice control documentation is such that someone reading the control will understand:

1. What the control is intended to do
2. What the subject matter of the control is
3. What event (or timing) triggers the control
4. Who carries out the control
5. How the control is carried out
6. How the outcome is recorded

A control is simply an activity, or series of activities, intended to ensure that specific circumstances or criteria are met. The following examples use the numbering above to highlight how different aspects of good practice documentation can be used.

- When a slip is passed to them (3), the claims administrator (4) verifies the details of claimant against the policyholder (2) as noted on their record (5) in order to determine if they match (1) before marking the claimant ID as confirmed (6)
- The system (4) reconciles (5) the cash received (2) each night (3) to the debtor balance for the specific policy number in order to ensure it matches (1) and any exceptions are posted to a suspense account (6)
- The system (4) only allows underwriters authorised (1) to write marine business (2) to post marine business (3/5) to their record. Any exceptions are rejected (6)

In some circumstances it is reasonable for some assumptions about knowledge to be made for the sake of avoiding excessive effort and length of control description. This is a matter of judgement. As mentioned already, the documentation of controls is an activity that requires a certain level of skill or experience. It is recommended that specialist support, for example from internal controls specialists or internal audit, be sought during this phase.

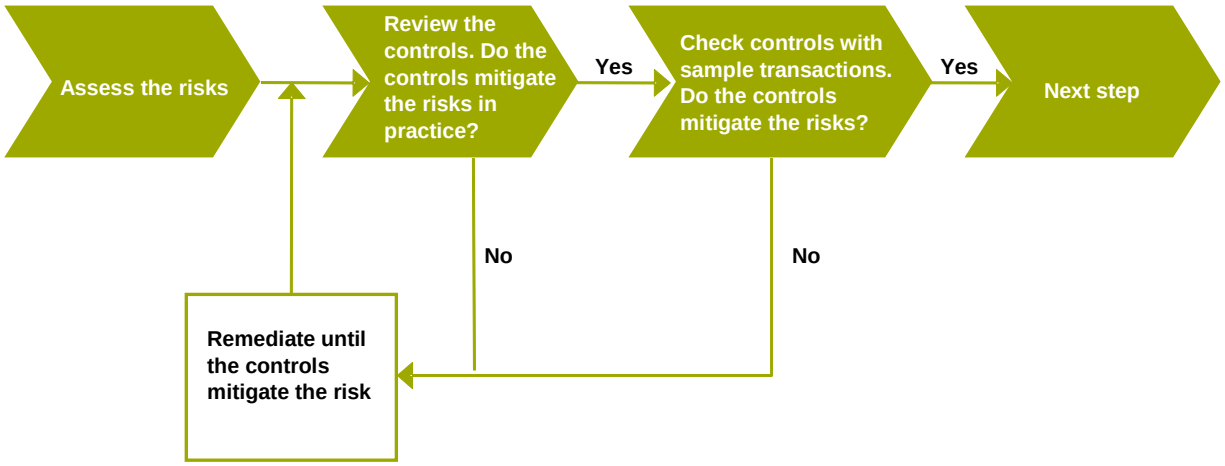
Experience from the pilot

- **Controls exist to mitigate risks - risks can be mitigated by more than one control, equally one control can address multiple risks**
- **Getting the balance right – it is not the number of controls but keeping the right balance that makes the difference. Include a mix of preventative controls, for example segregation of duties and detective controls such as reconciliations. A good balance of preventative and detective controls can reduce the impact if there is a control failure**

Tips for managing agents

- **Use existing documentation. If the business already has documented controls these can be leveraged here. Use existing control deficiency/gap reports to highlight current control gaps**
- **Controls may not exist in the same business process as the risk. They could be downstream in other processes. For example, the risk of booking the wrong premium might be mitigated by a control in finance where cash flows are matched to the outstanding premium**
- **Remember a control can only be demonstrated as operational if there is evidence of it**

ASSESSING DESIGN ADEQUACY



Design adequacy is about ensuring that the relevant risks have been mitigated to an acceptable level. An individual risk may be mitigated by one or more control.

To illustrate, in this example more than one control is needed to adequately address the risk that data capture is inadequate (Risk 2 from the risk model) in relation to 'intermediary location (country)':

The managing agent policy capture system may contain a predefined list of valid countries. If users can still process a policy and associate a different country (i.e. the field is a free text field), there may be a validation check built into the system that produces an automatic exception report which is reviewed by management when an invalid country is used.

In this situation, the control to ensure that the 'intermediary location (country)' is captured adequately has multiple controls involved with mitigating the one risk:

- *The policy capture system contains a list of valid countries for the intermediary field. Access to edit this list is restricted*
- *The policy administration system produces a weekly exception report which details any invalid countries*
- *The exception report is reviewed by management who investigate any issues and resolve them*

All three of these controls are needed to adequately address the risk.

The design adequacy assessment occurs during the documentation of controls and is finalised by sign-off by appropriate management after the documentation is substantially complete. Ultimate sign-off should be by the person responsible for the framework, appointed by the board.

For the purpose of regulatory and tax reporting the extent to which controls should mitigate risk are likely to be similar to that for other statutory tax reporting and audits.

Experience from the pilot

- **At this stage controls will either be confirmed as being design effective, or considered design ineffective. If they are ineffective, some form of prioritisation should take place based on their importance and they should be remediated. A deficiency log can be a useful way of tracking such items**
- **Those responsible for collating and submitting data for reporting should work with those responsible for individual processes and controls to ensure that those documented are a true and fair representation of actual activity**
- **It can also be helpful to have people available by telephone who can explain individual controls more fully than they are documented**

Tips for managing agents

In order to carry out the design adequacy assessment it is likely a separate session will be needed, though a limited number of participants should be involved, generally the more senior people who have been involved in the previous steps. Useful documents to have to hand during this process include:

- **The completed risk assessment**
- **Control documentation**
- **Supporting process documentation (not mandatory)**
- **Findings of past reviews of controls (not mandatory)**

Make sure someone has considered the true execution activity of the controls (for example by walking through the process using a real transaction) to validate the control as documented. This will ensure that any issues are picked up early rather than in the next step of evidence gathering.

Design adequacy, special considerations

Some controls can be difficult to assess and concluding on them may have to be carried out separately for later ratification, e.g. system based controls or complex manual controls which have not been documented at the time of carrying out this exercise.

Automated (systems based) controls

There are controls businesses rely on that are automated or significantly dependent on information systems and technology. Some form of testing of system functionality for these controls should be considered. This may be historic testing, the evidence for which has been retained and can be examined, or new testing carried out to prove a particular function.

Judgement is required to determine the appropriate level of testing for the individual situation. It may be that some system based information can be corroborated against independent sources of information.

Automated controls are unique in that in the next step of the framework for gathering evidence, less frequent evidence collection will be needed. This is because, so long as the system operates in a well controlled environment from a 'behind the scenes' IT perspective, confidence can be gained from the fact that well controlled systems operate in a consistent way.

Information Technology general controls and end user computing controls

These are considered in Appendix 3. To ensure correct coverage, it is important that all relevant systems and spreadsheets are identified during the main business process focused sessions and that it is agreed with those focusing on control of systems and end user computing facilities, such as spreadsheets.

Experience from the pilot

- **Additional people will need to be engaged in conversations around automated and IT controls from those involved in the sessions around main controls. Automated controls, however, should not be considered in a silo as, to understand these well, typically business and IT input is needed**
- **Remember that spreadsheets are inherently risky but that they can be properly controlled. Understand why and how a spreadsheet is used to determine the relative importance of it. For example a spreadsheet used for analytical review and monitoring may be less risky than one that is part of a significant process**

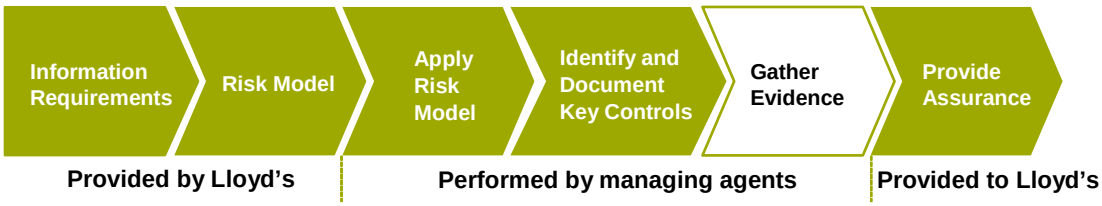
Tips for managing agents

- **If IT general controls or end user computing controls are not effective, it will likely mean that the business process controls dependent on them will, by default, be ineffective also. For this reason these controls should not be left until last**
- **It is likely that IT general controls may address risks for multiple information requirements. For example Risk 5 relating to data loss may be addressed by controls over system backups for all information requirements**

DOCUMENTING THE OUTPUT

During this step, managing agents will complete the fifth and sixth column of the example document in Appendix 2, namely 'Controls' and 'Control Gaps Detail'. This provides detail of the controls in place to mitigate the risks, and allows the follow up of controls gaps (i.e. risk is not mitigated by current control practices).

5 GATHER EVIDENCE



OVERVIEW

This step sets out the expected requirements from managing agents in retaining and providing evidence to support the control activities documented in the previous step. This evidence should be retained to support activities in the next step of this framework - Provide Assurance.

OBJECTIVES

- To confirm the extent of evidence to be maintained over the operation of the controls identified in the previous step

WHAT MANAGING AGENTS NEED TO DO

- Document the required degree of evidence needed for each control

This is judgemental and should be linked to the relative importance of each risk (determined in Step 3). Common sense should also be applied to ensure the evidence required does actually provide evidence that the control, as described, is operational.

Who should be involved: The main driver of this process should be the individual or team tasked with documenting the output, with input from the individual who operates or owns each control.

OUTPUT

At the conclusion of these activities, the following information will have been compiled:

- Evidence retention plan (detailed for each control)

The following provides guidance on how to practically determine how much evidence should be retained.

WHAT MANAGING AGENTS NEED TO KNOW

Managing agents should maintain evidence that controls operate. The extent of evidence required will depend on the overall assessment of risk associated with each information requirement and a summary of the expected evidence requirements is set out below:

Overall Risk Assessment Score	Evidence Requirements
High	Managing agents are expected to retain evidence to support the operation of the controls to the degree that an independent person could perform the control activity again.
Medium	Management should document sufficient evidence that the control occurred.
Low	Managing agents should document the symptoms that would arise if the control failed and how management would be aware of this control breakdown.

Managing agents should determine what is appropriate for them. Lloyd's expect that for requirements they have classified as critical, the overall risk assessment will never be less than medium.

Experience from the pilot

- **Evidence may also be electronic. For example, if one of the controls relied upon is that access to systems and databases is restricted to appropriate individuals, then the evidence to support this could be a system generated access list. This list might be reviewed by business management (i.e. application and data owners) on a periodic basis, such as quarterly or semi-annually**

Tips for managing agents

In relation to the Risk Assessment Scoring:

- **High – for those areas rated high, it is important to ensure that the control can be performed again. If the control in question is a management review of data and judgements have been made, then these judgements should be documented**
- **Medium – to ensure evidence exists to support that the control has occurred, management should retain items such as sign-offs, meeting minutes, approvals within emails etc. It may not include the requirement to document all judgments and decisions, but crucial evidence around the control operating should be retained**
- **Low – this rating requires consideration to be given to the symptoms that exist should a control fail. This might be a non-reconciling item, a threshold exceeded on a report, consistent errors on data quality reports or any other mechanism that would trigger management to suspect a**

control might not be working

FURTHER CONSIDERATIONS

Gathering Evidence – being proportionate

This section presents an approach that assumes the suggested risk assessment model has been used. If an alternate model has been used by a managing agent, for example to be consistent with a wider corporate framework, the same principle should apply.

The following methodology is used to define this:

1. A risk assessment score for each information requirement is defined and documented by Lloyd's (this is the 'critical and required' categorisation referred to in Step 1 of the framework), based on the overall risk of that information requirement being incomplete, inaccurate or inappropriate
2. A risk assessment score is applied to each of the five risks within the risk model by the managing agent, based on the risk within their business processes of providing incomplete, inaccurate or inappropriate data to satisfy the requirement

Weighting is given to Lloyd's risk assessment (the allocation of critical or required) as this assessment is more directly related to the individual data and consequences of that data being incomplete, inaccurate or inappropriate. An overall score is then assigned (which is the addition of both the Lloyd's score and the managing agent's score), which is then used as a basis to determine the degree of evidence required to support the control activity, which the managing agent has defined in their control assessment.

An illustration of the scoring template is shown below:

Lloyd's Information Requirement Rating	**Managing Agent Data Risk Assessment**		
	Low (1)	Medium (2)	High (3)
Critical (6)	7	8	9
Required (3)	4	5	6

Those areas scoring an 8-9 will be categorised as 'High', 5-7 will score 'Medium' and 4 will score 'Low'.

The table under 'What Managing Agents Need to Know' for this step sets out the minimum evidence requirements for each type of score.

DOCUMENTING THE OUTPUT

At the end of this step, managing agents will complete the seventh column of the example document in Appendix 2, i.e. 'Evidence of Control'. Part of the implementation may require these controls to be tested and shared with Lloyd's.

Column eight, entitled 'Remediation Plan', provides managing agents with an opportunity to address the control gaps (i.e. the implementation of a new control or enhancement of an existing one). Ideally there will be no items for remediation, but if there are it is good to be able to demonstrate the plan to mitigate the risk, together with any current controls or context that may reduce the risk.

6 PROVIDE ASSURANCE

OVERVIEW

As set out in the Introduction, Lloyd's may be required to share the confidence they have in the controls in place over the data supplied to meet the information requirements within managing agents with other regulatory and tax authorities. For Lloyd's to do this, they in turn will require managing agents to share their confidence with Lloyd's by providing evidence based assurance.

This step describes how this assurance will be provided by managing agents.

OBJECTIVES

- To determine the extent of sharing assurance in controls that each managing agent will need to undertake. This may change as demands on Lloyd's by others will change over time
- For the sharing to take place when due

WHAT MANAGING AGENTS NEED TO DO

- Discuss and agree with Lloyd's the extent of documentation to be shared
- Prepare suitable documentation to share with Lloyd's. This may involve self prepared documents or documents prepared by independent third parties

OUTPUT

- Report on design effectiveness
- Report on operational effectiveness

Who should be involved: It is expected that responsibility and ownership of this output should be those tasked with 'senior level acceptance of responsibility' as defined in the Introduction of this document.

WHAT MANAGING AGENTS NEED TO KNOW

The amount of assurance to be shared between Lloyd's and the managing agent should be proportionate. This means that there are a range of options available, which have been assessed by Lloyd's with the objective to strike a balance between cost and granularity of the assurance provided. The mechanisms that are suggested may change over time in response to external pressures.

At this stage it is important to consider the two types of assurance that will be shared:

1. Assurance over the design of the controls to mitigate the risks
2. Assurance over the operation of the control

Experience from the pilot

- **Each managing agent is unique and therefore the mechanisms used to provide assurance over controls with Lloyd's will vary**
- **The information provided in the design and operating effectiveness assessment will influence the level of evidence Lloyd's will wish to see**

Tips for managing agents

- **Managing agents should present to Lloyd's their proposals for assurance sharing, but the decision as to whether this is adequate will remain with Lloyd's**
- **Mechanisms may change year on year in response to a changing environment**

FURTHER CONSIDERATIONS

Assurance over design effectiveness

For those areas where management have documented a control, providing assurance in the first instance is for a design assessment to be performed.

In the first year and in future years of significant change, it is expected that the design assessment will be completed by an agreed independent team, such as a suitably skilled internal audit team, or by a firm of auditors. Once the framework is embedded, annual refresh may involve self assessment or a further independent review, supplemented by discussions with Lloyd's.

The exact mechanism used to share assurance will be discussed between managing agents and Lloyd's. Lloyd's will decide on the most appropriate mechanism to achieve the objectives of the framework in an effective and efficient way.

Assurance over operational effectiveness

Operational effectiveness refers to the 'working' effectiveness of a control against a risk, so it measures whether or not a control is working as documented.

It is expected that Agreed Upon Procedures (AUPs) performed by an independent party would be the most suitable option for the assessment of operational effectiveness. However there may be situations where other options are acceptable. In some circumstances the level of rigour required to opine on operating effectiveness may be toned up or down depending on changes within the control environment.

The table below shows some mechanisms by which operational effectiveness can be measured:

Assurance Mechanism	Additional Information
Reporting Accountant's Report with an external opinion	Managing agents may choose to use this mechanism for assessing operating effectiveness. Lloyd's do not currently envisage an audit at this level being necessary. However, this could change based on requirements of regulators and tax authorities.
AUPs (Agreed Upon Procedures) – performed by external or internal parties	AUPs can be used and carried out by external parties, or by suitable internal parties. AUPs can be agreed with Lloyd's so that testing procedures are vetted as appropriate.
Managing Agent Internal Audit	Could be used to test the operating effectiveness of the controls, also using AUP or other tools.
Self Certification	Self Certification of the operating of controls can be performed; however this provides the lowest level of assurance and may only be acceptable in subsequent years when controls are embedded with a low history of control deficiencies.

In both cases, when the reports on both design and operational effectiveness are prepared by management, detail on the nature, timing and extent of the testing should be included and detail on who performed the testing. This will allow Lloyd's to assess the competency and objectivity of the work that has been carried out and will be used to determine the extent of any further actions, if required.

To the extent that there are any control design or operating deficiencies identified, managing agents should set out their response as to how they have or will mitigate the associated risks. This should be reviewed by Lloyd's and Lloyd's may ask for further evidence to support this response.

Throughout, the Lloyd's objective is to:

- Protect managing agents from direct regulatory investigations/scrutiny by applying a visible and auditable data standard
- Minimise the risk to the overall Lloyd's licences from non-compliance by individual managing agents
- Protect and potentially improve the competitive position of the platform internationally
- Maintain or enhance the Lloyd's brand and reputation
- To achieve these in an effective and efficient way

APPENDIX 1: THE LLOYD'S INFORMATION REQUIREMENTS

Update January 2016: Please refer to the Lloyd's Direct Reporting requirements for up-to-date tax and regulatory information requirements:

http://www.lloyds.com/the-market/operating-at-lloyds/direct-reporting

APPENDIX 2: ANALYSING RISK

Below is a template that managing agents might find as a useful aid in performing the risk assessment described in Phase 3:

RISK ASSESSMENT TEMPLATE

INFORMATION REQUIREMENT	APPLICABLE RISK	RISK RATING	RATIONALE FOR RISK RATING	CONTROLS	CONTROL GAPS DETAIL	EVIDENCE OF CONTROL	REMEDIATION PLAN
Location of Risk	R1 - Requirements are not understood	High	Location of Risk requirements are complex and may not be fully understood, e.g. the requirement to distinguish between Worldwide/Europe and individual countries for example. It is possible that U/W's do not understand the downstream effects of the classification decision.	U/W's code location of risk based on their experience and judgement and enters onto U/W slip, which is reviewed and signed off by XXX.	N/A	U/W slip, signed by XXX.	N/A
				GAP	Training is not provided to U/Ws to facilitate the understanding of the information requirements and how location of risk is required to be country specific.	N/A	Training to be provided to U/Ws and data entry staff to ensure they understand the importance for regulatory and tax reporting of capturing the location of risk field accurately.
	R2 - Data capture is inadequate	Medium	Slips completed by U/Ws are freeform allowing for judgement when completing the location of risk field. This can provide the ability to avoid specific answers (e.g. using 'Europe' and not specific countries within Europe). System provides a series of drop downs in the field for location of risk, making it impossible to enter non-standard data.	GAP	Location of Risk is not challenged if ambiguous (e.g. Worldwide/Europe).	N/A	Implementation of a new control, U/W team to challenge all ambiguous entries before entry into system (clarification of unacceptable entries to be provided). Evidence of review of Location of Risk by U/W team maintained (e.g. sign off).
				GAP	System does not provide the ability to record multiple locations of risks for multiple insured items on single policies.	N/A	Maintenance to allow system to process multiple locations of risks on a single policy.
				GAP	No spot check performed on data entry to ensure data is entered in-line with U/W documentation.	N/A	Periodic (Monthly) check of system data to U/W documentation to ensure accurate capture of location of risk. Check to be signed off by XXX.

RISK ASSESSMENT TEMPLATE (CONTINUED)

INFORMATION REQUIREMENT	APPLICABLE RISK	RISK RATING	RATIONALE FOR RISK RATING	CONTROLS	CONTROL GAPS DETAIL	EVIDENCE OF CONTROL	REMEDIATION PLAN
Location of Risk	R3 - Data is processed incorrectly	Low	Once location of risk is entered into the main U/W system is it not subject to further processing (e.g. data field is not amended/processed further before download into an XL spreadsheet)	Data in the Data Requirements spreadsheet is reconciled back to U/W systems to ensure complete and accurate capture. Reconciliation is signed off by XXXX when complete.	N/A	Completed reconciliation, signed by XXX	N/A
				Access to the Data Requirements spreadsheet is restricted to XXX.	N/A	Access rights over the folder in which the spreadsheet is stored.	N/A
	R4 - Data is corrupted	Low	Risk is low. Data is not subject to complex processing or regular 'movement' between systems.	ITGCs controls are in place over key systems that protect the integrity of data. The key controls are (but not limited to) : > Access to applications and databases is restricted to appropriate personnel > Anti-Virus software is run on all servers > Firewalls are in place to protect unauthorised external entry to the network > Changes to systems and data are subject to a defined change control process.	N/A	Examples are: > Access control lists for applications and database > Anti-virus running on key servers > Firewall configuration > Change control tickets	N/A
	R5 - Data is lost and cannot be recovered	Low	IT back up procedures are routine and non-complex. Documentation is retained and can be relied on if IT records are lost.	Back up procedures are in place. Key systems and data are backed up on a daily basis and stored off site. Evidence of the backup is retained on the daily checklist, which is signed off by the IT manager.	N/A	A daily checklist is completed by the IT operations team (including sign off by the IT manager) that shows the status of backups for the day.	N/A
				A yearly DR plan is performed, which includes testing of the recovery of backup tapes on which critical business data is stored.	N/A	Yearly DR tests are performed to ensure backed up data can be restored. Evidence of the test outcome is maintained and any issues recorded in a remediation plan.	N/A

APPENDIX 3: INFORMATION TECHNOLOGY CONSIDERATIONS

As mentioned in the framework, Risks 3, 4 and 5 could crystallise due to inadequate controls over IT systems and similarly end user computing facilities (such as spreadsheets) present similar challenges. These are considered here in this appendix. However, it is anticipated that many organisations will already have frameworks specific to these areas which are likely to be of relevance.

To the extent that business process controls are described in Step 4 of the framework 'Identify and Document Key Controls' which are dependent on IT controls, IT specific risks over the systems relevant to those controls should also be considered. Similar considerations are relevant to spreadsheets and other end user computing facilities.

Information Technology General Controls

Some simple examples of the relevance of IT general controls is the risk that systems may process data incorrectly due to inadequate IT system change controls or data may be lost due to inadequate backup and recovery controls.

IT general controls are relevant where there are automated controls identified as part of the main control identification process, or where a manual control activity is heavily dependent on an input such as a system generated report.

Automated controls are those within computer applications and are dependent on the application performing as expected in order for them to be effective. For example, a system may restrict access to a particular function, or it may apply individual limits to a particular type of transaction based on access rights given within the system. When these controls are relied on to mitigate risks, the IT general controls are important as they underpin these automated controls and provide comfort that access to influence how an automated control performs is appropriate and changes to automated controls are made in an approved manner.

If a managing agent chooses to rely on automated controls and once the population of applications in which those controls operate has been determined, then the managing agent should understand what IT general controls are in place to support the in-scope applications.

This is a topic that is well documented elsewhere. Below are links to website that may be useful when determining how to consider IT general controls:

ICAEW IT Faculty
http://www.icaew.com/index.cfm/route/158987/icaew_ga/en/Faculties/IT/IT_Faculty_home_page/Information_Technology_Faculty

COBIT
http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Online.aspx

The following outlines generic IT general control risk and controls which are based on the ISA (International Standards on Auditing) principals, although this is a concept most managing agents will be aware of and may have their own framework that addresses these points.

End User Computing

End user computing facilities are IT tools developed by end users that perform limited processing activities where the use of a system may not be relevant. They are typically spreadsheets or databases and are controlled by the user community. As end user computing tools can perform important calculations and processing, companies are placing more emphasis on understanding and controlling the risk associated with using them.

Where managing agent's data is maintained or processed through such tools, they should consider the risk associated with this and document the mitigating controls in place. This section gives an example of some of the typical end user computer controls that might be relevant to managing agents during their assessment.

Most managing agents will already be considering the topic of spreadsheet control in the context of their Solvency II programme. The principles considered by such activity are also relevant where spreadsheets are being used as part of processes such as direct reporting.

As an illustration, the following controls are some of the typical controls seen over such facilities.

End User Computing (EUC) – Example Controls

- Change control – maintaining a controlled process for requesting changes to an EUC, making changes and then testing the EUC and obtaining formal sign-off from an independent individual that the change is functioning as intended
- Version control – ensuring only current and approved versions of EUCs are being used by creating naming conventions and directory structures
- Access control (e.g. create, read, update, delete) – limiting access to EUCs and assigning appropriate rights. EUCs can also be password protected to restrict access
- Input control – ensuring that reconciliations occur to make sure that data is inputted completely and accurately. Data may be inputted into EUCs manually or systematically through downloads
- Security and integrity of data – implementing a process to ensure that data embedded in EUCs is current and secure. In spreadsheets, this can be done by 'locking' or protecting cells to prevent inadvertent or intentional changes to standing data. In addition, the EUCs themselves should be stored in protected directories
- Documentation – ensuring that the appropriate level of EUC documentation is maintained and kept up-to-date to understand the business objective and specific functions of the EUC
- Development lifecycle – applying a standard software development life cycle to the development process of the more critical and complex EUCs covering standard phases: requirements specification, design, building, testing and maintenance. Testing is a critical control to ensure that the EUC is producing accurate and complete results
- Back-ups – implementing a process to back up EUCs on a regular basis so that complete and accurate information is available for financial reporting
- Archiving – maintaining historical files no longer available for update in a segregated drive and locking them as 'read only'
- Logic inspection – inspecting the logic in critical EUCs by someone other than the user or developer of the EUC. This review should be formally documented
- Segregation of duties/roles and procedures – defining and implementing roles, authorities, responsibilities and procedures for issues such as ownership, sign-off, segregation of duties and usage
- Overall analytics – implementing analytics as a detective control to find errors in EUCs used for calculations

Examples of Information Technology General Control Considerations

ITGC Risks	Example Controls
COMPUTER OPERATIONS	
Inappropriate manual intervention or unreported/unresolved failures in automated batch processes may result in incomplete or inaccurate recording of transaction data.	Only approved and tested changes are made to the batch scheduler. Errors in production processing are identified and resolved.
Systems failure (such as network outages or hardware faults) may result in loss of transaction records or inability to access them as required for financial reporting.	Errors in production processing are identified and resolved. Data is appropriately backed up and recoverable.
ACCESS TO PROGRAMS AND DATA (COVERING ACCESS CONTROL AND SECURITY)	
Normal user accounts (i.e. business users) may be used to bypass authorisation or segregation of duties controls, leading to invalid transactions.	Passwords to applications are utilised in an effective manner. Passwords to the operating system/network are utilised in an effective manner. Access requests to the application are properly reviewed and authorised by management. Access requests to the operating system/network are properly reviewed and authorised by management. Terminated application user access rights are removed on a timely basis. Terminated operating system/network user access rights are removed on a timely basis. Access rights to applications are periodically monitored for appropriateness. Access rights to the operating system/network are periodically monitored for appropriateness.
Privileged users (i.e. IT personnel such as systems administrators) may bypass authorisation or segregation of duties controls, leading to invalid transactions.	Policies are maintained for segregation of duties within IT. Super-user/administrative application transactions and activities are monitored. Super-user/administrative database/data file transactions and activities are monitored. Super-user/administrative operating system/network

	transactions and activities are monitored.
Database administrators (or other users with direct edit access to production data stores) may make improper (i.e. inaccurate or invalid) changes to transaction records or master files.	Access requests to the database/data file are properly reviewed and authorised by management. Terminated database/data file user access rights are removed on a timely basis. Super-user/administrative database/data file transactions and activities are monitored. Access rights to the database/data file are periodically monitored for appropriateness. Passwords to the database/data file are utilised in an effective manner.
PROGRAM DEVELOPMENT (COVERING APPLICATION SYSTEM ACQUISITION AND DEVELOPMENT)	
Errors in the build or configuration of new applications (including associated interfaces, batch processes, data stores, etc.), may lead to inaccurate processing or reporting of transactions.	New systems/major enhancements are adequately tested and authorised. Only properly approved new systems/major enhancements are migrated into production. Problems during program development are monitored and resolved. Errors in production processing are identified and resolved.
Transaction records and/or master files may not be completely and accurately migrated during an application replacement or upgrade, leading to processing or reporting of inaccurate data.	Data is properly migrated or converted.
PROGRAM CHANGE CONTROLS (COVERING APPLICATION SYSTEM MAINTENANCE AND SYSTEM SOFTWARE ACQUISITION/MAINTENANCE)	
Changes that are necessary for accurate financial reporting (e.g. to reflect new regulations or accounting standards) may not be made (e.g. due to failure to identify, understand or prioritise these changes)	Changes processed to application programs are periodically monitored for appropriateness. Changes processed to application configurations are periodically monitored for appropriateness.
Changes may introduce errors to the code or configuration of existing applications (including associated interfaces, batch processes, data stores, etc.), leading to inaccurate processing or reporting of transactions.	Changes processed to application programs are periodically monitored for appropriateness. Changes to application programs are adequately tested. Changes to application configurations are adequately tested. Only properly approved changes to application programs are migrated into production. Only properly approved changes to application configurations are migrated into production. Development, testing and production environments are segregated for changes to application programs. Development, testing and production environments are segregated for changes to application configurations. Errors in production processing are identified and resolved.
Developers or support teams may directly access the production environment and make unauthorised changes to application code or configuration, leading to invalid transactions or errors in transaction processing or reporting.	Policies are maintained for segregation of duties within IT Access requests to the operating system/network are properly reviewed and authorised by management. Terminated operating system/network user access rights are removed on a timely basis. Access rights to the operating system/network are periodically monitored for appropriateness. Emergency changes to application programs are adequately tested and authorised after implementation. Emergency changes to application configurations are adequately tested and authorised after implementation.
Updates to system software (i.e. operating systems, middleware and utilities) may result in existing applications inaccurately processing or reporting transactions.	Changes to the operating system/network are adequately tested. Only properly approved changes to operating system/network are migrated into production. Changes processed to the operating system/network are periodically monitored for appropriateness. Emergency changes to the operating system/network are adequately tested and authorised after implementation.

APPENDIX 4: POTENTIAL CHALLENGES

Here are some of the challenges that may be of particular relevance to managing agents as they strive to implement the framework. This is based on experience from pilot organisations and wider discussions.

These items were noted during the discussions with managing agents. However these may not be a complete listing of all the challenges that a managing agent might face:

- Systems being able to deal with multiple characteristics, e.g. risks with multiple locations of risks or premiums with multiple currencies
- Limitation in systems meant there may be a need for manual workarounds to source and input data to meet the requirements
- Understanding and interpretation of the meaning of location of risk
- Variable levels of formality and robustness of processes mean providing evidence for some key controls may be a challenge
- General lack of tax expertise within smaller managing agents
- Different managing agents apply controls in very different ways; for example some apply data quality controls on data entry while others have processing centres of excellence that are trained to highlight anomalies. Others have informal processes where there is a high degree of reliance on back-end, detective highlighting of issues. This has a significant impact on an organisation's ability to demonstrate the robustness of the controls employed

Managing agents will have different approaches to implementing the framework. Below are some indicative estimates for time and costs that might be required to address some of the challenges:

Activity	Potential Impact
System enhancements	Circa £50,000 for small managing agents For larger client this could run upwards of £1,000,000
System implementation	£200,000 - £1,000,000 plus
Employing dedicated tax resource (IPT specialist/Head of Tax)	£60,000 - £150,000 p.a.
Internal workshops and project to respond to the requirements	Objective – to perform and document risk assessment, document controls, identify control gaps, plan for remediation, documentation evidence retention plan and plan attestation activities. Ultimately the time required depends on the robustness of the current processes and procedures. This may take anywhere from 3 to 6 months
Consultancy support	Similar to the option above, although specialist risk and controls resource support may reduce the total number of hours required. Average rates of approximately £200-£300 per hour