

## **RISK MANAGEMENT POLICY**

Our risk management approach is a balanced one, recognising that we cannot hope to enjoy a high reputation as a respected firm if we put excessive caveats on the advice that we give. The key elements of our approach are as follows:

- To assess carefully the risks, and thus the desirability of accepting types of work.
- To use competent, knowledgeable and reliable third party assistance.
- To take a professionally sound, but nonetheless commercial, approach to our work.
- To provide appropriate documentation and advice for each of the services that we provide.
- To make adequate provision for consultation and review, particularly in areas of potentially high risk.

KPM have in place a documented practice wide risk assessment that identifies and assesses the risks of Money Laundering and Terrorist Financing to which the practice may be exposed and risks to the operational disruptions that may from time to time occur. These are addressed in our Business Continuity Plan.

As part our Risk Management Policy, KPM updates and maintains:

- A Compliance Plan.
- A Risk Register.
- We have defined the risk management roles and responsibilities.
- We have made arrangements and have put in place training for communicating risk information.

### **Business Continuity Plan**

KPM has adopted a business continuity plan to address the emergencies that might disrupt its operation. Additionally KPM have adopted and use the Law Society Framework for Monitoring, Reviewing and Managing Risks of Non-Compliance in order that we can ensure we have effective systems and controls to enable us to meet our regulatory requirements (see Annex 1H).

The person responsible for the plan is Karen South.

The procedures used to test the plan periodically (but at least once in every two years) to verify its efficacy in the event of business interruption, include:

- A forced "*lock-out*" of the premises to test the continuity plan.
- A mock interruption of business due to power failure and/or terrorist action and/or health and safety disruptions including pandemics or health and safety issues.

The plan includes adequate and progressive back-up routines as recommended by our suppliers of computer software programs; appropriate facilities for the storage of back-up media both on and off site; arrangements for acquiring replacement hardware (where appropriate), and for downloading software and data. Details of the plan have been made available to those staff members who are involved in the recovery procedure. Computer logs detail of:

- The location and cycle of back-ups.
- A duplicate of the records which are stored off-site.

Disaster recovery procedures should be reviewed at least annually to ensure their continued relevance and adequacy. Testing of elements of the plan are regularly carried out.

## Critical Business Functions

We have identified the following critical business functions which it is imperative are maintained or replicated as soon as possible after any incident which threatens our operations: -

- Telephone switchboard/call centre response;
- Physical office space for client, staff and management meetings;
- Ability to contact all personnel 'off site';
- Access to centralised electronic diary;
- Access to client contact records;
- Access to practice management, accounting and case management computer system data;
- Staff records/payroll details held by Kavanaghs Accountants;
- Website maintenance.
- Alterations to static working practices such as pandemics or other health and safety issues.

## Disruptive Hazards

There are many hazards that can disrupt business continuity, we have deduced that the most likely to affect our business are: -

- IT failure/loss of data;
- Utility failure e.g. gas, electricity, water;
- Staffing issues;
- Fire;
- Flooding;
- Extreme weather;
- Loss of premises;
- Temporary loss of access to premises.
- Nationwide or localised lockdowns.

## Risk Matrix

The Risk Matrix enables us to identify higher priority risks for the organisation.

↑ Increasing likelihood	B High Impact Low Likelihood	A High Impact High Likelihood
	D Low Impact Low Likelihood	C Low Impact High Likelihood
	Increasing likelihood ⇒	

## Critical Business Functions - Effects on Service if Unavailable

IT Failure/Loss of Data	
Risk Matrix Score	'A'
Mitigation in place	In respect of client PC failure, we hold one spare PC on site at any one time in case of failure. In respect of main server failure, we have a service level agreement in place with our supplier confirming a 24

	hour turnaround for a replacement machine. All software backups are taken on a daily basis as recommended.
Mitigation possible	KPM has largely moved to the Cloud. The Osprey software management system is on the Cloud and therefore accessible from any working PC. Emails are also held on the Cloud (in secure location) and so operations can continue if we have an office based IT failure.
Personnel Responsible	Jason Jackson & Karen South
Testing procedure(s)	Re-build departmental PC; test restore all backups for integrity (not on principal server but one supplied for testing purposes).

<b>Data Breaches</b>	
Risk Matrix Score	'A'
Mitigation in place	Data loss can either be client data or software loss. There could be a breach of our files and protections. With regards to the mitigation in place – our software is on the Cloud and we have taken steps to ensure its integrity as far as possible. With regards to the data breaches, our Data Protection Policy covers breaches and reporting of breaches.
Mitigation possible	Keeping the systems up to date via our IT suppliers and training and awareness of data breaches.
Personnel Responsible	Karen South
Testing procedure(s)	We intend to become cyber security accredited.

<b>National Emergencies</b>	
Risk Matrix Score	'A'
Mitigation in place	Remote working and all staff self-isolating. COVID-19 packs on each workstation in the office. COVID-19 measures in place by the landlord of the building to the main front door and contact entrance door. Medical grade hand sanitisation gel available at numerous points. One person at a time in the office.
Mitigation possible	Compliance with social distancing and COVID-19 measures as to masks and handwashing. Undertake and then implement COVID-19 Risk Assessment.
Personnel Responsible	Karen South
Testing procedure(s)	Live in action since 24 March 2020 until lifted in its entirety.

<b>Utility Failure e.g. gas, electricity, water</b>	
Risk Matrix Score	'B'
Mitigation in place	In respect of main computer servers, we have 'uninterruptible power supply' boxes attached to each machine. These give approximately 1 hour of power and are designed to allow orderly shutdown in time of power failure. Loss of power does mean that all IT systems will be rendered inoperative and departments' ability to work will be severely curtailed; however, such interruptions to supply are usually of relatively short duration. In respect of failure to the gas supply, heating and hot water would be affected quickly. During the summer, this has relatively low impact; during the winter it could be more serious. Decisions may have to be made to close the office depending on length of interruption. If water supply is disrupted, this can have an effect on health e.g. operation of bathrooms; any protracted interruption could result in office closure.

Mitigation possible	Consider supplemental electricity generator.
Personnel Responsible	IT Manager, Office Manager, Partners
Testing procedure(s)	Ensure server integrity, cold water tank capacities – carried out by the landlords.

<b>Staffing Issues</b>	
Risk Matrix Score	'A'
Mitigation in place	We now have a telephone answering system in place that picks up all calls if calls remain unanswered for 8 rings. All fee earners/support staff can access their emails over exchange.livemail.co.uk. All fee earners have remote access to their office computers and emails via the Web. All fee earners have the capacity to work remotely from home.
Mitigation possible	Ensure that if reception staff are part-time that they are flexible about additional working; if full-time that there is backup from other departments e.g. that staff other than reception staff are trained in reception/telephone system procedures. Critical accounts department functions e.g. cheque processing and CHAPS receipt/sending procedures are learned by other personnel e.g. IT department staff.
Personnel Responsible	Karen South & Matthew Stubbs
Testing procedure(s)	Release of nominated personnel from regular work on a monthly basis for training/testing of acquired skills.

<b>Fire</b>	
Risk Matrix Score	'B'
Mitigation in place	Internally within the office of KPM, we have fire extinguishers which are serviced annually. Outside the offices of KPM there are fire drills and fire extinguishers. Fire resistant deeds cupboard is in the process of being constructed.
Mitigation possible	With equipment PAT testing. No smoking allowed within building and no flammable substances in building. If a fire is detected, personnel are not to rely only on the central service provider but to also call the fire brigade to make sure they attend.
Personnel Responsible	Richard Max & Co (Tel: 020 7240 2400) & Metro Safety (Tel: 020 7960 3918)
Testing procedure(s)	As normal procedure, the fire alarm system is tested. Staff will be notified if other tests or maintenance are carried out on the alarm system. From time to time fire drills will be carried out and warnings will be given in advance.  The alarm system is linked to a central service provider, details of which are on the main panel as you come in the front door. Alarms are tested by Metro Safety on a Wednesday morning and Jemma Scarry and Ben Mason of Richard Max deal with this when Amanda from Metro Safety attends the building.

<b>Extreme Weather</b>	
Risk Matrix Score	'D'
Mitigation in place	A spare set of keys is held at Gough Square Chambers which will only be released to KPM personnel to ensure that all personnel will be able to access the office in emergencies. All personnel have up-to-date

	contact telephone numbers of all members of staff. There is a telephone answering system in place that picks up all calls if calls remain unanswered for 8 rings. All fee earners/support staff can access their emails over exchange.livemail.co.uk. All fee earners have remote access to their office computers.
Mitigation possible	As above to ensure continuity if possible in the office running.
Personnel Responsible	Karen South & Matthew Stubbs
Testing procedure(s)	Tested in the winter of 2015 under actual conditions.

<b>Loss of Premises</b>	
Risk Matrix Score	'A'
Mitigation in place	All fee earners have access to their emails remotely from computers and can take over their office computers. The partners have available space for temporary offices together with an arrangement for using colleagues' office space in London.
Mitigation possible	Access to the computers and server remotely.
Personnel Responsible	Jason Jackson of Apnet Limited.
Testing procedure(s)	Mock forced lock-out.

<b>Temporary Loss of Access to Premises</b>	
Risk Matrix Score	'B'
Mitigation in place	All fee earners have access to their emails remotely from computers and can take over their office computers. The partners have available space for temporary offices if required but can now facilitate client meetings via secure access to video conferencing sites. All telephone calls are diverted to a remote dedicated reception service.
Mitigation possible	Access to the computers and server remotely.
Personnel Responsible	Jason Jackson of Apnet Limited.
Testing procedure(s)	Mock and real forced lock-out.

Risk analysis is broadly decided to include:

- Risk assessment;
- Risk characterisation;
- Risk communication;
- Risk management;
- Policy relating to risk.

We are exposed to many types of risks:

- Reputational;
- Operational;
- Strategic;
- Economic;
- Competitive;
- Regulatory;
- Risks to human health and the environment both built and natural.

The amount of risk we face within KPM will depend on the quality of our management skills and internal systems and procedures.

KPM have been reviewing and overhauling both internal systems and procedures and individual working practices.

By working independently and adhering to your own individual ways of working leads to, for example, variations of service level delivered by different lawyers.

Traditionally we have been reactive in our approach to risk management but we must now become pro-active.

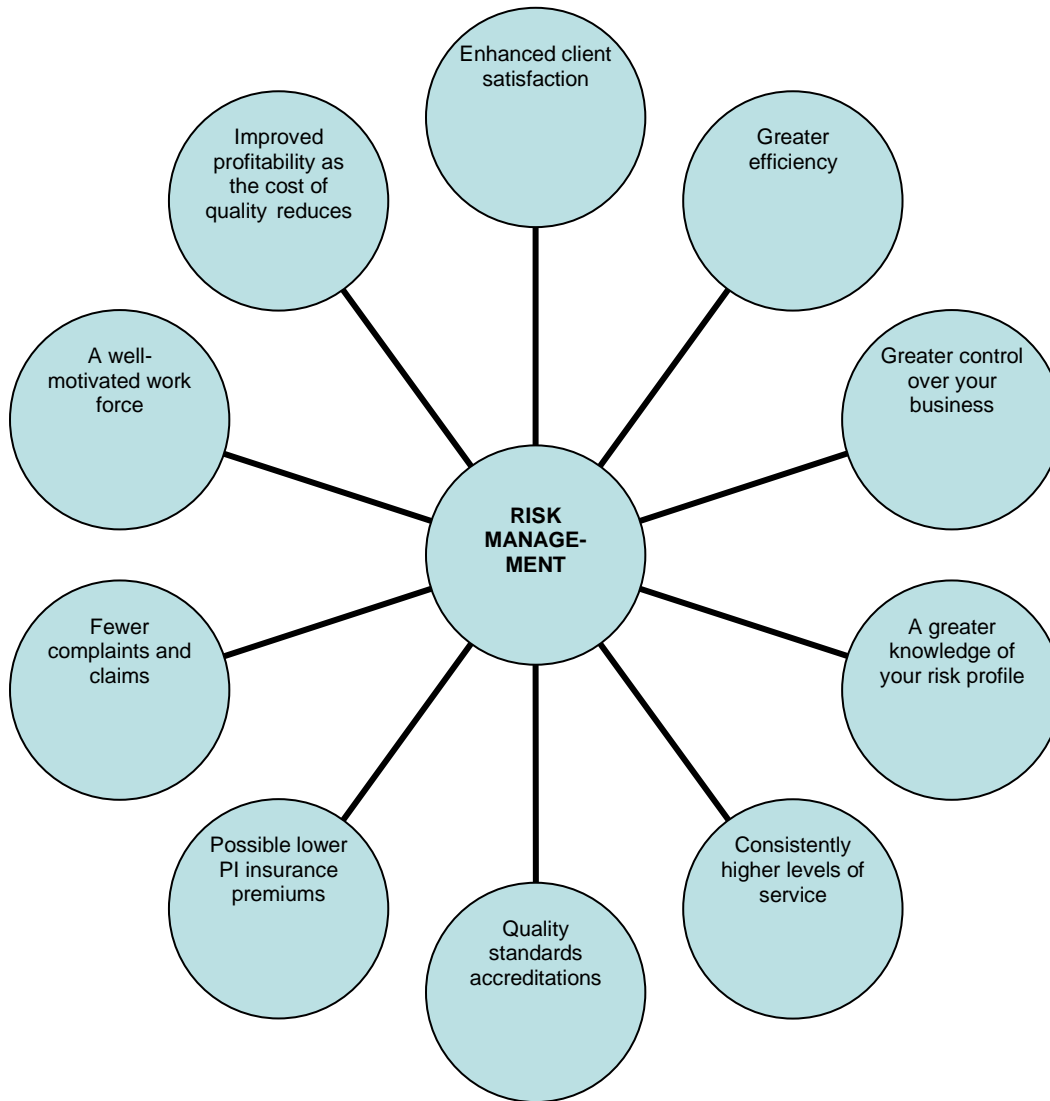
Risk management involves being in control of our business by:

- Utilising planning;
- Firm wide policies;
- Harnessing technology;
- Training;
- Training to reduce or eliminate risk.

Risk management involves three fundamental concepts which are:

- Identification of the risk;
- Analysis and assessment of the risk;
- Reduction and elimination of the risk.

Simply because a procedure is written down does not mean that it will be followed. Management is essential to ensure that the procedures we put in place are as follows:



## Operational Risk

Lexcel encourages lawyers to think about each new matter in terms of the individual risks it presents to the firm.

Operational risk must be considered and recorded in all matters before, during and after the processing of instructions. Before the matter is undertaken, the fee earners must:

- Consider if a new client and/or matter, is accepted by the practice, in accordance with the below.
- Assess the risk profile of all new instructions and notify the supervisor, in accordance with KPM procedures of any unusual or high risk considerations in order that appropriate action may be taken.

During the retainer the fee earner must:

- Consider any change to the risk profile of the matter and report and advise on such circumstances without delay, informing the supervisor if appropriate.
- Inform the client in all cases where an adverse costs order is made against KPM in relation to the matter in question.

There are many generic risks within the practice of solicitors. Generic risks are common across the whole of the firm regardless of the practice area.

These can be eradicated and hopefully eliminated by setting up generic procedures and protocols.

The KPM procedures and protocols are in standardised format and can be accessed on the KPM central folder.

These procedures are:

- Conflict of interest check;
- New client opening forms with risk category;
- Anti-Money Laundering procedures;
- File closure letters bringing important dates to client's attention;
- Email, fax, and attendance note protocols;
- Undertakings protocol;
- Complaints procedures.

### **Looking After Your People**

All colleagues, whatever their job description, are an integral part of any firm. The work that our colleagues do with us and for us reflects on how our practice is perceived by the outside world.

Well developed HR processes are a vital part of any firm's risk management strategy and help to eliminate avoidable risk.

KPM have the following procedures in place to manage their HR processes:

- A documented recruitment process understood by all those involved in recruitment.
- A standard induction process for all people joining the firm.
- An employment file held by accounts that contains:
  - A contract of employment incorporating the terms and conditions and disciplinary and grievance procedures;
  - An accurate and up to date job description;
  - A copy of the signed and completed induction sheets;
  - An appraisal process and copies of appraisal forms and reports;
  - Individual training agreed at appraisals.

KPM are committed to training their colleagues to implement the individual training and development plan and relevant training courses are essential to ensure that all staff reach a level of competence appropriate to their position.

### **Departmental Risk Procedure**



Each department has a documented list of procedures that are audited and reviewed by the department head. They include:

- Standard client care letter for the relevant department.
- Standard terms of business and conditions of acting.
- Anti-Money Laundering procedures.
- Supervision procedures by department head with those below the department head being supervised.
- File management procedures.
- Procedures for new file vetting and risk assessment.
- Diary systems and method of recording critical dates.
- Listing critical dates which fall within a standard procedure for the work type by use of authorised checklists.
- Check on fee earner level of workload.
- The importance of training.

Fee earners must judge whether the matter is ordinary or high risk, attributing the case to the latter category of high risk if:

- There is a novel or unusual aspect of law involved.
- A foreign jurisdiction is to be involved.
- A value of a potential claim is unusually high.
- The client has transferred this matter to the firm in circumstances where they were dissatisfied with the advice or service provided by their previous advisors.
- The matter is outside the expertise or knowledge of the individual fee earner.
- When the client is in a high risk country;
- When the client is a politically exposed person (PEP).
- When the transaction is unusually large and has no apparent economic or legal purpose.

When placing a risk assessment on a file, fee earners should consider a traffic light approach:

- Red – stop;
- Amber – further consideration;
- Green – go.

KPM can and will refuse instructions. Such clients are saved within P:\LEXCEL\Anti-Money Laundering\Experian\Clients requiring higher authority.

### **Client Care Agreement and Scope of Engagement Letter**

KPM have documented procedures for receiving client's instructions and confirming to the client terms and conditions as well as ensuring that the client is informed at every stage of its case.

The agreement is contained in two documents and there are two copies, one for the client and one kept on the client file. The agreement contains:

- Client instructions;
- The advice given;
- The full requirements of Chapter 1 of the SRA Handbook 2011;
- Details of a case plan if appropriate;
- Name and status of the person dealing with the matter;
- Complaints procedure;
- Costs, merits, justification if necessary.

Within our documented procedure and our standard terms of business KPM ensures that the client is fully informed on all aspects of their matter as it progresses. KPM have included within the terms and conditions the following:

- Agreement with the client as to agreed minimum frequency for regular communication of progress.
- Timely response to telephone calls and correspondence.

### **File Closing Procedures**

A report is made to the client at the conclusion of the matter on the outcome of the matter or why the matter was concluded.

KPM will then close a file according to the file closing form at Annex 8M which includes:

- Report to the client on the outcome of the matter.
- Account to the client for any outstanding money.
- Return to the client any original documentation or advise the client as to storage of documentation.
- Advise the client if the matter needs to be reviewed.
- Carry out a concluding risk assessment as to the outcome against the client's expectation and objectives.
- Carry out administrative checks.
- Ensure all undertakings are discharged.
- Scan and shred ID in accordance with data protection.
- Notify the supervisor of all such circumstances in accordance with documented procedures.
- KPM have procedures to manage instructions, which may be undertaken even though they have a higher risk profile, including unusual supervisory and reporting requirements or contingency planning.

### **Business Continuity**

The KPM computer system is held on a central server. There are back-ups of the system done each evening. Two sets of back-up tapes are taken of the system.

That then ensures that all client files are backed up, allowing instant access to all KPM data.

In respect of client PC failure, we hold one spare PC on site at any one time in case of failure. In respect of main server failure, we have a service level agreement in place with our supplier confirming a 24 hour turnaround for a replacement machine. All software backups are taken on a daily basis as recommended.

In respect of main computer servers, we have 'uninterruptible power supply' boxes attached to each machine. These give approximately 1 hour of power and are designed to allow orderly shutdown in time of power failure. Loss of power does mean that all IT systems will be rendered inoperative and departments' ability to work will be severely curtailed; however, such interruptions to supply are usually of relatively short duration. In respect of failure to the gas supply, heating and hot water would be affected quickly. During the summer, this has relatively low impact; during the winter it could be more serious. Decisions may have to be made to close the office depending on length of interruption. If water supply is disrupted, this can have an effect on health e.g. operation of bathrooms; any protracted interruption could result in office closure.

All KPM personnel have keys to ensure that all personnel will be able to access the office in emergencies. All personnel have up-to-date contact telephone numbers of all members of staff.

We now have a dedicated reception service in place that picks up all calls if calls remain unanswered for 8 rings. All fee earners/support staff can access their emails over exchange.livemail.co.uk. All fee earners have remote access to their office computers and our case management system.

Our case management system is on the Cloud and accessible via the Web. The important documents are stored on the Cloud.

### **Client Files**

KPM appreciate their responsibilities towards client files and their obligations to retain the file in a complete and usable condition, allowing access by the client or the Law Society at any given time up to the destruction date.

KPM archive files onto disk with Microeye Services Limited of Unit 2, Howbury House, Thames Road, Dartford, Kent, DA1 4RQ. The files on disk are readily accessible by providing Microeye Services Limited with the unique file reference number. The files are downloaded onto three separate hard drives. KPM has one, Microeye have one and one is kept off-site. Once committed to digital archiving, the paper file is securely shredded.

### **Strategic Risk Management Policy**

KPM have the following business planning documentation:

- Business plan which is reviewed six monthly or as needs be.
- In November of each year the Partnership holds an AGM at which the documentation set out on the Annual Review Form at Annex 6H is considered:

#### **Review**

To review and consider:-

- Objectives for the next 12 months.
- External developments and relevant general trends;
- KPM's position and pressures including competition; and
- The effectiveness or otherwise of action taken during the preceding 12 months and evaluation of those actions.

#### **Objectives**

To document and formulate or re-formulate short, medium and long-term objectives in relation to each of the following areas:-

- Office management and resources;
- Finances;
- Personnel/staff;
- Quality management;
- Accommodation;
- Services offered and delivery;
- Clients;
- Marketing;
- Fee-earner charge out rates.
- Health and safety issues.

## **Detailed Plans**

The detailed plan for the year incorporates the resources which will be required to meet the objectives in respect of: finances, staff, training, marketing, equipment, office systems and procedures, management, quality control and safety of clients and colleagues.

## **Forward Planning And Service Plan**

KPM's Forward Plan and Service Plan are set out in separate documents, which are available for consultation, by all members of staff. Staff members wishing to consult the latest draft of the Plans should contact a Partner.

The strategic plan is reviewed as necessary but at least every six months.

Furthermore, the Partners hold a bimonthly Partners' meeting at which management, strategic and personnel issues are discussed, recommendations and decisions made which are then implemented ahead of the next Partners' meeting.

KPM hold quarterly Lexcel meetings with all KPM colleagues or as is necessary.

In November of each year the Partnership sets primary objectives for the year following which are reviewed at the Partners' meetings according to the following:

- KPM has obtained the Lexcel accreditation.
- The Partners consider the overarching policy documentation, business documents, personnel requirements and strategic decisions to be considered by the Partnership.

## **Reputation Risk Management**

KPM are aware that their reputation is only good as the service they provide and the people they have to provide the service. With that in mind, KPM operates a structure within the firm which is governed by the KPM personnel policy documentation, the employee handbook and the Lexcel kite mark.

KPM appraises its employees at least annually and carries out at least quarterly supervision and periodic file reviews of both partners and fee earners. There is therefore appraisal sideways on partner and appraisal down as well as monthly reviews.

Additionally at the Partners AGM there is a risk assessment carried out of complaints and complaints handling, with a view to spotting trends and with a view to avoiding repetition of complaints made.

## **Regulatory Risks**

KPM is aware of its responsibilities towards its clients and colleagues and to its professional bodies and accordingly KPM adheres to the following regulatory rules:

- Money laundering regulations
- Solicitors Regulation Authority Code of Conduct
- Council of Mortgage Lenders regulations
- Health and Safety rules and regulations
- Professional Indemnity Insurers rules and regulations.

Within the bimonthly Partners' meetings any breach of the above or any suggestion of non-compliance is dealt with on a Partner to Partner basis with the matter being discussed and action taken and corrective action noted at the Partners' meetings.

The persons responsible for the policy are both Matthew Stubbs and Karen South.. This policy is reviewed annually by the Partners as part of its Lexcel annual review process.