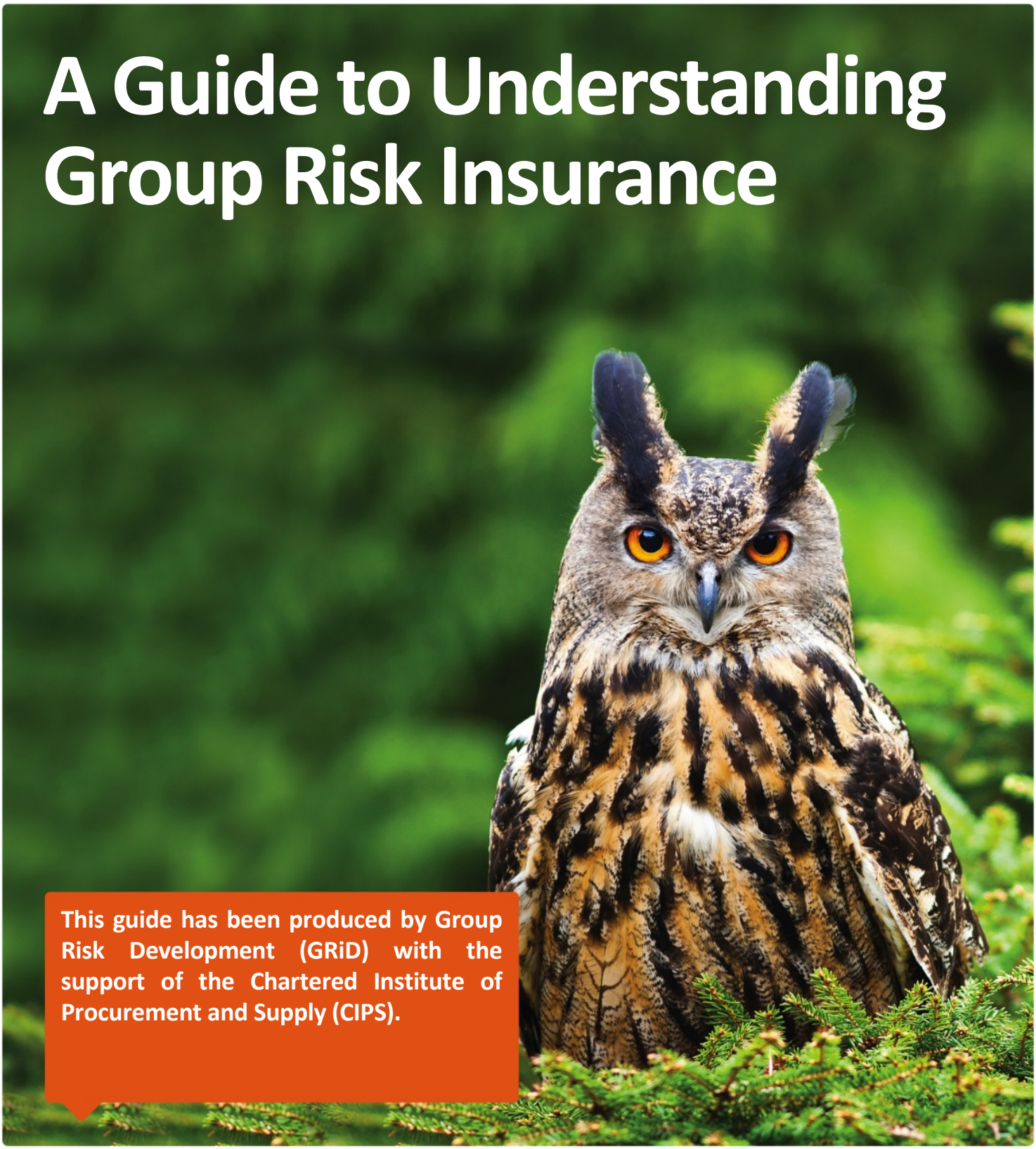
CIPS KNOWLEDGE

A Guide to Understanding Group Risk Insurance



This guide has been produced by Group Risk Development (GRiD) with the support of the Chartered Institute of Procurement and Supply (CIPS).

CPD 1 HOURS

CIPS members can record one CPD hour for reading a CIPS Knowledge download that displays a CIPS CPD icon.

A Guide to Understanding Group Risk Insurance

Contents

Part 1: Introduction to this Guide

1. Learning outcomes

For purchasing and supply specialists, the learning outcomes are to develop a better understanding of the following:

- What is Group Risk insurance?
- How Group Risk insurance works.
- Group Risk and UK legislation and regulation.
- Information handling by the Group Risk insurer.
- The contractual nature of Group Risk insurance.
- How a 'scheme' providing group risk benefits works.
- Purchasing a Group Risk policy and considerations for:
    - Non-Disclosure agreements (confidentiality agreements),
    - Supplier agreements,
    - Data processing agreements,
    - Service level agreements,
    - IT Security and audits,
    - Internal procedures.

2. About this guide

This guide has been produced by Group Risk Development (GRiD) with the support of the Chartered Institute of Procurement and Supply (CIPS). This guide is not designed to provide guidance on procuring insurance. Instead it is designed to provide purchasing and supply specialists with a better understanding of:

- Group Risk insurance.
- How Group Risk insurers are regulated.
- The responsibilities of Group Risk insurers to protect their customers' employee data.
- Why some common procurement solutions aren't suitable for Group Risk insurance.

This guide will be of interest to Procurement Professionals, Insurance & Risk Managers and others with a responsibility for defining Group Risk insurance requirements and selecting Group Risk insurers. In particular it aims at enhancing an understanding of Group Risk insurers' contractual and regulatory obligations. This can prevent delays through the expensive use of your firm's legal resources and ensure that an appropriate assessment of the insurer takes place.

Part 2: What is Group Risk insurance?

Group Risk is an umbrella term for three types of company sponsored employee benefits:

Group Life Insurance

This provides a benefit on an employee's death while in service. This can be a lump sum payable to nominated beneficiaries or a taxable pension payable to the employee's spouse, civil partner and/or other financial dependants, or both. A Group Life Insurance policy can be put in place by the trustees of a pension scheme to cover the scheme's liabilities for death in service benefits or by an employer to cover a contractual promise outside of a pension scheme to pay a benefit on an employee's death in service.

Group Income Protection

This provides a continuing income for employees if illness or injury prevents them from working for a prolonged period of time. It can also replace lost income where an employee has to take a part-time or lower paid position because of illness or injury. A Group Income Protection policy is used by an employer to cover a contractual promise of long-term sick pay to employees.

Critical Illness cover

This pays a tax free lump sum to an employee on the diagnosis of one of a defined list of serious conditions or on undergoing one of a defined list of surgical procedures. There is usually a choice of base or core cover (which insures against some of the most serious critical illnesses) or base/core plus additional cover (which insures against a number of additional serious conditions too).

Group Risk benefits are often (but not always) fully insured. Provided in isolation or as part of a wider benefits package, these employer sponsored products can give employees access to insured protection cover either at a reduced rate or free of charge as they are covered under one "group" policy. This is often more readily available than individual cover since most employees do not generally need to provide medical details before cover is granted.

Group Risk benefits are highly valued as they provide financial protection for employees and their families, yet they are relatively inexpensive for employers compared with some other components of the typical benefits package.

In the UK all insurers are subject to financial regulation and are required to be authorised by the Prudential Regulation Authority (PRA) and are regulated by the Financial Conduct Authority (FCA) and the PRA.

Group Risk benefits are usually (but not always) bought through employee benefit consultants or insurance brokers. These intermediaries are also required to be authorised and regulated. The only exceptions are exempt professional firms (e.g. a firm of consulting actuaries) who don't have to be authorised by the UK regulators but will be regulated by their own designated professional body.

Part 3: How Group Risk insurance works

Group Risk insurers provide insurance for employers or trustees. The process operates as follows:

i) The insurer is provided with appropriate information about the employer and its employees, usually via an intermediary, in order that it can provide a quotation for the group risk cover required. It is the responsibility of the employer or trustees to provide accurate information and disclose all material facts relevant to the risk.

ii) The insurer issues a quotation for the cover. This includes the insurer's terms and conditions. The basis of the quotation may be subject to negotiation, and any changes must be agreed by the insurer.

iii) The client does not have to accept the quotation, but if they do, once the insurer has agreed risk, the client will complete a proposal form confirming their requirement for cover and agreeing to pay the premium for the cover. This is the basis of the contract.

iv) The insurer then issues the insurance policy, which is evidence of the contract between the insurer and the client. The insurance policy describes the responsibilities of both the insurer and the client, and gives the client clear details of:

- who must be included for cover, from when and for what benefits,
- any exclusions in respect of the cover,
- what premiums are payable by the employer / trustees and when,
- how and when the basis of the Policy can be changed,
- when and how the employer / trustees can make a claim.

It is a requirement of the FCA, under the Insurance Conduct of Business Sourcebook (ICOBS) that the insurer issues a policy document.

v) Insurers will only share information about the client or individual employees with third parties that are directly concerned with the provision of the requested insurance. For example, information may be shared with reinsurers.

Part 4: Group Risk and UK legislation and regulation

There is a high degree of protection in the UK via legislation and regulation that applies to the insurance sector.

Supplier agreements and confidentiality agreements which are designed for use with companies that provide services to clients in connection with their business are not appropriate in connection with insurance. These could conflict with the insurance policy that outlines the

cover, make it difficult for the insurer to carry out its normal procedures in connection with the insurance, and also conflict with the insurer's regulatory and legal responsibilities under UK legislation and regulations.

Insurers regulated by the PRA and FCA are authorised to provide insurance cover. They are not providing professional services, are not suppliers of services and are not authorised to provide these services.

The PRA and FCA set out 11 principles of business that are a general statement of the fundamental obligations of all authorised firms:

1. **Integrity**. A firm must conduct its business with integrity.

2. **Skill, care and diligence**. A firm must conduct its business with due skill, care and diligence.

3. **Management and control**. A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

4. **Financial prudence**. A firm must maintain adequate financial resources.

5. **Market conduct**. A firm must observe proper standards of market conduct.

6. **Customers' interests**. A firm must pay due regard to the interests of its customers and treat them fairly.

7. **Communications with clients**. A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading.

8. **Conflicts of interest**. A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.

9. **Customers: relationship of trust**. A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely on its judgment.

10. **Clients' assets**. A firm must arrange adequate protection for clients' assets when it is responsible for them.

11. **Relations with regulators**. A firm must deal with its regulators in an open and co-operative way, and must disclose to the FCA anything relating to the firm of which the FCA would reasonably expect notice.

The PRA and FCA requirements for Systems and Controls covers some of the main issues which a firm is expected to consider in establishing and maintaining the systems and controls appropriate to its business. These include:

1. **Organisation.** A firm should have clear and appropriate reporting lines.

2. **Compliance, financial crime and money laundering.** A firm must establish and maintain effective systems and controls for compliance with applicable requirements and standards, including having a Money Laundering Reporting Officer and a Compliance Function.

3. **Employees and agents.** A firm should be able to satisfy itself of the suitability of anyone who acts for it.

4. **Business strategy**. A firm should plan its business appropriately so that it is able to identify, measure, manage and control risks of regulatory concern.

5. **Business continuity**. A firm should have in place appropriate arrangements, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption.

6. **Records**. A firm must make and retain adequate records of matters and dealings (including accounting records) which are the subject of requirements and standards under the regulatory system.

The PRA and FCA do not set down specific rules on how firms must meet these principles, systems and controls and firms will have their own policies and procedures in place to meet these principles, that they are satisfied meet the FCA and PRA requirements.

The PRA and FCA require firms to report compliance with the above principles and controls and firms will be audited by the PRA or FCA to confirm their compliance.

Part 5: Information handling by the Group Risk insurer

The insurer requires information to be able to:

- Assess the insurance risk.
- Calculate the premiums to charge for the cover.
- Issue any necessary documentation.
- Assess and pay claims.

This will include:

- Membership data, which, where an individual can be identified, is classed as personal information and is protected by the Data Protection Act 1998 (DPA).
- General information, for example, the location of the workforce, the nature of their occupations, and details of their employee benefits which will be in the public domain.

Insurers do not seek confidential information that might involve, for example, commercially sensitive information about a client's products and operations.

Therefore, suitable protection is provided for the information required by the insurer via the DPA, PRA and FCA regulations, so it should not be necessary to enter into any non-disclosure agreements which could conflict with the insurer's responsibilities under this regulation and legislation.

The following outlines how the DPA applies to the insurer and the employer / trustees:

Under the DPA, both the client and the insurer are Data Controllers in respect of any personal information in connection with the scheme. The insurer will be registered with the Information Commissioner's Office (the body that is responsible for the DPA) as a Data Controller. As a Data Controller, the insurer is directly responsible to the Information Commissioner for handling any personal data in accordance with the DPA. The insurer does not act as a Data Processor on behalf of the client. It is therefore not appropriate to have an agreement between the client and the insurer on how personal information will be processed, as a Data Controller is directly responsible for the way in which information is processed.

Data Controllers are required to adhere to the following 8 key principles of the DPA:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The insurer's proposal form outlines how personal information will be processed, as required by the DPA, and the client gives their consent for any personal information to be processed in this way. The client also confirms that they have the necessary consents from employees to pass their personal information to the insurer. If the insurer asks for any sensitive personal information directly from an individual, for example, to medically underwrite them, they will obtain consent from the individual. The DPA statement outlines:

- How the information will be used. This will be used to set up and administer the insurance cover provided as well as carrying out any other activity related to the insurance cover that is necessary.
- Who information may be provided to. This could include other companies in the insurer's organisation, their service providers, their reinsurers, other insurers and the client.

The information is not used in any other way or shared with other third parties without the specific consent of the client or individual employee.

Insurers do not require access to a client's premises or their computer systems or allow clients to have access to their premises or systems for audit purposes, in order to verify the accuracy of any data provided.

Part 6: The contractual nature of Group Risk insurance

The contractual nature of the relationships between the parties involved in a group risk contract is not the same as other types of insurance.

The employee

Any group risk benefits are promised to the employee by their employer via their contract of employment. The employee has no direct relationship with the insurer and generally any Third Party rights that an employee could have under the Contracts (Rights of Third Parties) Act 1999 are excluded from the insurance contract.

The employer

The employer initially establishes a scheme and funds it. For group income protection and group critical illness schemes, the employer is responsible for managing the scheme and can insure part or all of the benefits if required and if they do they will be the policyholder of the group contract and have a direct contractual relationship with the insurer.

For group death in service cover, the 'scheme' is established by the employer using a discretionary trust. However, the employer has no direct responsibility for managing the scheme. That rests with the trustees. The employer is likely to be a trustee and has responsibility for the operation of the scheme in his capacity as a trustee. The employer has no direct relationship with the insurer.

The trustees (group death in service cover)

The trustees are responsible for the management of the scheme and providing the benefits promised to employees. The trustees do not have to insure any of the benefits, but if they do they will be the policyholder of the group contract and have a direct contractual relationship with the insurer.

The insurer

The insurer provides group risk cover for the employer or trustees, who are the policyholder. The insurer can only deal with the employer / trustees or persons appointed to act on their behalf.

Part 7: How a 'scheme' providing Group Risk benefits works

Group income protection and group critical illness

For group income protection and group critical illness, the employer will usually set out some rules for employees outlining the benefits they are entitled to and when they are eligible for these benefits. The employer can insure all or part of these benefit promises.

Group death in service

Death in service benefits can be provided for employees as part of a pension scheme, which also provides retirement pensions, or via a 'stand-alone' group life scheme. Both these arrangements are set up using a discretionary trust. This is referred to as the scheme. There are greater regulatory controls on pension schemes.

Most schemes are registered with HM Revenue & Customs (HMRC), but it is also possible to have schemes that are not registered. Both types are established via a discretionary trust.

An employer establishes the scheme by 'executing' a trust deed. The trust deed:

- Appoints the first trustees of the scheme.
- Explains how trustees can be appointed and removed, and how they can resign.
- Sets out the key trustee responsibilities including:
    - setting out any discretionary powers they have and how / when these can be used;
    - accountability for any tax due to HMRC;
    - any reporting responsibilities.
    - Identifying any time limits within which the trustees must act.
- For schemes registered with HM Revenue and Customs (HMRC) the trust will clarify the scheme administrator's role and responsibilities and will also adopt the scheme rules. The rules themselves will set out:
    - the benefit structure
    - who is eligible to join the scheme
    - the range of beneficiaries and dependants the trustees can take into consideration in exercising their discretion to pay out benefits.
- For schemes not registered with HMRC, which generally have no scheme rules, the trust will also explain the trustees' administrative powers, i.e. what they can/can't do under the terms of the trust.

The trustees must act in accordance with the trust (and rules if applicable) in making all decisions about the scheme. They also have a fiduciary duty to act in the best interest of the scheme member and all the beneficiaries of the scheme.

Although the trustees will take account of any wishes a scheme member may have notified them of before their death, the final decision as to how the scheme benefits are distributed rests with the trustees. This makes sure that the scheme benefits do not form part of the deceased's estate for inheritance tax purposes.

The rationale for using this approach is that it provides protection for employees and provides the most beneficial tax treatment for benefits and premiums. Most UK insurers only offer

group death in service cover in association with schemes that are established under a discretionary trust. There can be individually appointed trustees, or in certain circumstances, the employer can be the sole trustee, but the important point is that the trustee or trustees are the custodians of the scheme. When dealing with the scheme, the employer as a trustee (or more correctly, authorised officials of the employer) will not be acting in a corporate capacity, they will be acting in their capacity as an appointed trustee of the scheme.

If any work is required in connection with the scheme, the trustees or the scheme administrator must formally request a person or organisation to undertake work on their behalf. For example, a purchasing department of the employer would only be able to act on the scheme's behalf, if they had been formally requested to do so by the trustees or the scheme administrator.

Part 8: Purchasing a Group Risk policy

When you buy a Group Risk policy, you'll want to make sure that you are dealing with a reputable company that acts to the highest standards and you are protected if problems arise. Many companies ask Group Risk insurers to provide information to help reassure them of this. You'll usually find that Group Risk insurers and intermediaries are happy to provide information to help you.

However, many companies are often unfamiliar with the way that Group Risk insurance operates in the UK, or the protection that is provided, and this can lead to a number of areas of misunderstanding. The following are examples that you may not be aware of:

- When a company accepts an insurer's quotation they enter into an insurance contract. This is evidenced by the insurance policy so there shouldn't be a need for a separate contract.
- Insurers provide insurance, which is a product, not a service as such.
- Firms (insurers, intermediaries and reinsurers) must comply with UK laws and regulations. They cannot operate in a way which conflicts with these obligations.
- Firms who operate in the UK are not required to comply with legislation and regulation in other countries.
- Agreements which may be necessary between a company and their suppliers in a 'non-regulated' environment are not appropriate in the context of insurance in the UK, which is closely regulated.
- The 'service' which a firm provides in managing the insurance provided is a high priority for all firms, but making this a contractual obligation for group risk cover is not appropriate.

Within this part of the document, you will find some points to consider when purchasing a Group Risk policy and why some current approaches to procurement aren't necessary or indeed, suitable.

1. Non-disclosure agreements (confidentiality agreements)

Protection for customers is already provided by PRA and FCA regulations and the Data Protection Act 1998 (DPA). Non-disclosure agreements can conflict with an insurer's responsibilities under this UK legislation and regulations and can also conflict with the insurance terms and conditions. Group Risk insurers do not require confidential information from a client that might involve, for example, commercially sensitive information about a client's products and operations.

As a Data Controller under the DPA, Group Risk insurers and intermediaries have registered with the Information Commissioner in respect of personal data they may handle and as such they are obliged to follow the eight key principles of the DPA. For this reason, non-disclosure agreements shouldn't be needed.

However, if despite this, a non-disclosure agreement is required in order to provide a quotation for group risk insurance, most insurers can provide a draft agreement that is suitable for group risk insurance. Using this template can save time as the insurer won't need to refer any company specific agreement to its Legal department before entering into an agreement.

2. Supplier agreements

Supplier agreements are not appropriate or relevant to Group Risk business and it is very unlikely that an insurer will enter into one.

Group Risk insurers are authorised by the PRA and regulated by FCA and the PRA. The insurers are only authorised to provide insurance, they are not authorised to provide services. They are also required by the FCA to issue a policy, which details the basis of the cover provided and forms the basis of the contract between the client and the insurer.

Supplier agreements usually conflict with and can over-ride:

- The quotation terms.
- The policy terms.
- The insurer's responsibilities under relevant UK legislation and regulation including the Data Protection Act and PRA / FCA rules.
- Company policy in areas like security and disaster recovery, where the insurer is required to have 'suitable systems and controls in place'.

If there is a particular topic that you wish to have an agreement on, then if it agreeable to both parties, it is more appropriate to make it part of the insurance agreement. Some insurers are happy to issue a side letter to the insurance policy for such items.

3. Data processing agreements

Insurers are Data Controllers. For this reason they are unlikely to enter into Data Processing agreements. Insurers determine the purposes for which and the manner in which any personal data are, or are to be, processed, which means they are Data Controllers. Insurers do not process personal data on behalf of their customers in the provision of insurance, so the insurer does not act as a Data Processor on behalf of the customer. It is therefore not appropriate to have an agreement between the client and the insurer on how personal information will be processed, as a Data Controller is directly responsible to the Information Commissioner for the way in which personal information is processed. This principle applies to situations where an insurer provides an insurance quotation as well as when an insurance policy starts.

4. Service level agreements

When a firm is supplied a service on which it depends to operate its business, if that service is not supplied to a suitable standard, the firms' business could suffer financially. It is therefore common practice to agree service standards as part of the contract to provide services. If the standards are not met, the agreement will stipulate the financial penalties that might apply and what remedial action can or will be taken if the service standards are not met, to the extent that the firm can cancel the contract early without incurring a penalty to enable it to find an alternative supplier.

Most Group Risk insurers have a set of minimum service standards. These could be agreed as a statement of principle, but it is not appropriate for them to form part of a legally binding agreement and they are not outlined in the insurance policy. The provision of Group Risk insurance is a product, rather than a service. Under a Group Risk policy, the insurer can only cancel the cover if the client fails to meet its commitments under the policy, for example, paying the premium on time. The client can cancel the cover at any time without any penalty, enabling them to obtain cover from another insurer, if they are unhappy in any way with the insurer or are able to obtain better terms.

For this reason it is unusual for insurers to enter into contractual service level agreements, although these may be agreed as a statement of principle.

5. IT security and audits

It is very unlikely that a Group Risk insurer will agree to meet another company's IT security procedures and controls as this may conflict with their own internal procedures. The insurer will already have robust systems and controls for IT security which will have been designed to meet their obligations under PRA and FCA regulations and those of the DPA. It is also very unlikely that the insurer will agree to an audit of their systems and controls as this may undermine the security that is in place or is simply not practical for a large organisation to agree to. However an insurer may, if requested, provide information to their customers in relation to IT security. Due to the confidential nature of the subject matter, the insurer may insist on a non-disclosure agreement being in place between the two parties before disclosing such information.

6. Internal procedures

Just as it is unlikely that a Group Risk insurer will agree to meet another company's IT security procedures, it's also very unlikely that the insurer will contractually agree to comply with your company's internal procedures. Most Group Risk insurers are large corporate entities and are likely to have their own policies freely available to highlight their commitments to high ethical standards.

Disclaimer

To find out more about GRiD visit http://www.grouprisk.org.uk/

To find out more about Chartered Institute of Procurement & Supply visit
http://www.cips.org/ or call +44 (0)1780 756777 or email info@cips.org
Easton House, Church Street, Easton on the Hill, Stamford, Lincolnshire, PE9 3NZ.

CIPS Group Easton House, Easton on the Hill, Stamford, Lincolnshire, PE9 3NZ, United Kingdom
T +44 (0)1780 756777 F +44 (0)1780 751610 E info@cips.org

CIPS Africa Ground Floor, Building B, 48 Sovereign Drive, Route 21 Corporate Park, Irene X30, Centurion, Pretoria, South Africa
T +27 (0)12 345 6177 F +27 (0)12 345 3309 E infosa@cips.org.za

CIPS Australasia Level 8, 520 Collins Street, Melbourne, Victoria 3000, Australia
T 1300 765 142/+61 (0)3 9629 6000 F 1300 765 143/+61 (0)3 9620 5488 E info@cipsa.com.au

CIPS Middle East & North Africa Office 1703, The Fairmont Hotel, Sheikh Zayed Road, PO Box 49042, Dubai, United Arab Emirates
T +971 (0)4 327 7348 F +971 (0)4 332 5541 E mena.enquiries@cips.org