Financial Institutions
Insurance application form

CAN

The purpose of this application form is for us to find out more about you. You must provide us with all information which may be material to the cover you wish to purchase and which may influence our decision whether to insure you, what cover we offer you or the premium we charge you.

How to complete this form

The individual who completes this application form should be a senior member of staff at the company and should ensure that they have checked with other senior managers and colleagues responsible for arranging the insurance that the questions are answered accurately and as completely as possible. Once completed, please return this form to your insurance broker.

Section 1: Company Details

1.1 Please state the name and address of the principal company for whom this insurance is required. Cover is also provided for the subsidiaries of the principal company, but only if you include the data from all of these subsidiaries in your answers to all of the questions in this form.

Company name:

Primary Address (Address, Province, Postal Code, Country):

Website Address:

1.2 Date the business was established (DD/MM/YYYY):

1.3 Please state your gross revenue in respect of the following years:

	Last complete FY	Estimate for current FY	Estimate for next FY
Domestic revenue:	$	$	$
US revenue:	$	$	$
Other territory revenue:	$	$	$
Total gross revenue:	$	$	$
Profit (Loss):	$	$	$

1.4 Please provide details for the primary contact for this insurance policy:

Contact name: Position:

Email address: Telephone number:

Section 2: Activities

2.1 Please describe below the services supplied by your business:

2.2 Please provide an approximate breakdown of how your revenue is generated:

	%
	%
	%
	%

2.3 Please complete the following in respect of your 5 largest jobs in the last 3 years:

Client Name	Professional services:	Gross Revenue:
		$
		$
		$
		$
		$

2.4 Do you employee subcontractors? ☐ Yes ☐ No

If "yes", please state:

a) the approximate percentage of your revenue, in your current financial year, that will be paid to subcontractors:

b) whether you sign reciprocal hold harmless agreements: ☐ Yes ☐ No

c) whether you ensure that contractors have their own errors and omissions and general liability insurance: ☐ Yes ☐ No

If you answered "yes" to c) above, what is the limit of liability that subcontractors must purchase? $

Section 3: Management Liability

Only complete this section if you require Management Liability cover

3.1 Have you in the past 3 years, or do you during the next 12 months, have plans to:

a) sell all or part of the company? ☐ Yes ☐ No

b) be involved in any mergers, acquisitions or divestments? ☐ Yes ☐ No

c) change your capital structure? ☐ Yes ☐ No

d) raise any new capital? ☐ Yes ☐ No

If "yes" to any of the above, please provide details:

3.2 Is the company listed on any stock exchange or other securities? ☐ Yes ☐ No

If "yes", please state:

a) the ticker symbol:

b) the number of shareholders or unitholders there are in the company:

c) the total number of shares or units owned by senior executive officers:

d) the number of shares or units outstanding in the company:

Section 4: Cyber Security Risk Management

Only complete this section if you require Cyber cover

4.1 Please describe the type of sensitive information you hold and provide an approximate number of unique records that you store or process:

4.2 Please describe the most valuable data assets you store:

4.3 Please state:

a) who is responsible for IT security within your business (by job title):

b) how many years have they been in this position:

c) whether you comply with any internationally recognized standards for information governance: ☐ Yes ☐ No

If you answered "yes" to c) above, please state the internationally recognized standards with which you comply:

4.4 Please tick all the boxes below that relate to companies or services where you store sensitive data or who you rely upon to provide critical business services:

☐ Adobe	☐ Amazon Web Services	☐ Dropbox	☐ Google Cloud
☐ IBM	☐ Microsoft 365	☐ Microsoft Azure	☐ Oracle Cloud
☐ Salesforce	☐ SAP	☐ Workday	

4.5 Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanation on the final page of this document.

☐ Advanced Endpoint Protection	☐ Application Whitelisting	☐ Asset Inventory	☐ Custom Threat Intelligence
☐ Database Encryption	☐ Data Loss Prevention	☐ DDoS Mitigation	☐ DMARC
☐ DNS Filtering	☐ Employee Awareness Training	☐ Incident Response Plan	☐ Intrusion Detection System
☐ Mobile Device Encryption	☐ Penetration Tests	☐ Perimeter Firewalls	☐ Security Info & Event Management
☐ Two-factor Authentication	☐ Vulnerability Scans	☐ Web Application Firewall	☐ Web Content Filtering

4.6 Please provide the name of the software or service provider that you use for each of the controls highlighted in 4.5:

Section 5: Crime

Only complete this section if you require Crime cover

5.1 Do you have dual control procedures in place for the transfer of assets, funds, investments, disbursements and for the signing of cheques in excess of $2,500? ☐ Yes ☐ No

5.2 Do you have facilities to transfer funds without using a third party financial institution? ☐ Yes ☐ No

If "yes", please give details:

5.3 Are bank statements independently reconciled at least every 30 days by staff who are not authorised to make payments? ☐ Yes ☐ No

5.4 Are transactions only permitted to be made via internally approved counterparties? ☐ Yes ☐ No

5.5 Are the trading systems adequately controlled to ensure that only authorised personnel are able to trade on the system? ☐ Yes ☐ No

5.6 Are all key source documents maintained in a secure environment prior to being entered onto the computer system, in order to prevent unauthorised modifications or inappropriate use of this data? ☐ Yes ☐ No

If you answered above, please explain below:

5.7 Are there adequate controls to ensure fraudulent instructions are not given to any financial institution by any employee or any other person who does not have authority to give genuine instructions? ☐ Yes ☐ No

5.8 Are telephone instructions confirmed in writing? ☐ Yes ☐ No

5.9 Are all banks required to confirm fund transfer transactions within 24 hours? ☐ Yes ☐ No

5.10 Do you have procedures in place for the use of passwords for your computer systems and is authorization automatically withdrawn at cessation of employment? ☐ Yes ☐ No

5.11 Are the finance, accounts and treasury department employees required to take two weeks of consecutive holiday each year? ☐ Yes ☐ No

If you answered above, please explain below:

Section 6: Kidnap and Ransom

Only complete this section if you require Kidnap and Ransom cover

6.1 Please provide the following information in respect of each planned foreign trip in the coming 12 months by your employees:

Country of destination:	Number of employees travelling:	Duration of visit:

If you have more than 10 trips planned in the coming 12 months, please provide an itinerary

6.2 Please state any special security precautions taken prior to and during foreign travel:

Section 7: Compliance

7.1 Please state whether your company has an:

Internal Audit Department ☐ Yes ☐ No

Compliance Department ☐ Yes ☐ No

EDP Audit Department ☐ Yes ☐ No

Data Security Department ☐ Yes ☐ No

Audit Committee ☐ Yes ☐ No

7.2 Please state:

a) how regular audits are performed:

b) the date of the most recent audit performed (DD/MM/YYYY):

c) whether all recommendations from the most recent audit have been completed? ☐ Yes ☐ No

If "no", please explain:

7.3 Has there been any examination conducted on you by the SEC, any government regulatory agency or any self-regulatory organisation in the past three years or you have received notice of a future examination? ☐ Yes ☐ No

If "yes", please state:

a) the date of completion of examination (DD/MM/YYYY):

b) whether all cited deficiencies have been corrected? ☐ Yes ☐ No

Please attach copies of any letters received as a result of the inspection and a copy of management's responses to all letters and comments received.

Section 8: Insurance Requirements

Please provide details of the cover you require:

	Limit:	Prior and pending dates:
Professional indemnity:		
Management liability:		
Cyber security risk management:		
Crime:		
Kidnap and ransom:		

Section 9: Claims Experience

9.1 Please state whether you are aware of any incident:

a) which may result in a claim under any of the insurance for which you are applying to purchase in this application form: ☐ Yes ☐ No

b) which resulted in legal action being made against any of the companies to be insured within the last 5 years: ☐ Yes ☐ No

c) which resulted in anyone working for the companies to be insured, experienced any kidnap, extortion, highjack, wrongful detention or a political threat: ☐ Yes ☐ No

If you have answered "yes" to any of the above then please describe the incident, including the monetary amount of the potential claim or the monetary amount of any claim paid or reserved for payment by you or by an insurer. Please include all relevant dates, including a description of the status of any current claim which has been made but has not been settled or otherwise resolved.

Section 10: Additional Information

Please provide the following information when you send the application form to us.

- The organizations latest financial report;
- Directors or principals resumes if the company has been trading for less than 3 years;
- Directors or principals percentage of ownership;
- List of professional societies and organizations in which you belong to;
- Advertisements, brochures and descriptive literature on your business; and
- The standard form of contract, end user license agreement or terms of use issued by the company.

Name:	Date of Acquisition:	Country of Domicile:	Percentage of ownership:

Please provide this space below to provide us with any other relevant information:

Important notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. CFC Underwriting will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on our privacy policy please visit ***www.cfcunderwriting.com/privacy***

Contact Name: Position:

Signature: Date (DD/MM/YYYY):

Cyber security controls explained

Advanced endpoint protection

Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

Application whitelisting

A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any non-whitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organizations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Employee awareness

Training programs designed to increase employees' security awareness. For example, programs can focus on how to identify potential phishing emails.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Penetration tests

Authorized simulated attacks against an organization to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Two-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organization. For example, known malicious websites are typically blocked through some form of web content filtering.