

SHA^o
risk specialists

STANDARD CYBER RISK ASSESSMENT QUESTIONNAIRE

☎ 011 731 3600 ✉ info@sha.co.za 🌐 www.sha.co.za

📍 The Pavillion, Wanderers Office Park, 52 Corlett Drive, Illovo, 2196

Santam is an authorised financial services provider (FSP 3416), a licensed non-life insurer and controlling company for its group companies.

a division of

**Santam**

INTRODUCTION

This questionnaire is neither an offering nor binding of an insurance contract. Furthermore the completion of this questionnaire does not obligate the insurer to offer coverage to you. It is recommended to use this questionnaire only by companies with a revenue/turnover of up to R1bn (ZAR and USD equivalent value) or a staff headcount of less than 250. The answers to the questions are very important to us for assessing the risk in order to provide cyber insurance to you based on the information we receive. Therefore we rely on your statements made in the questionnaire which are the basis for the insurance contract. If you have no information security resource, then the questionnaire should be completed by a senior representative (owner or board member).

Are any further information or details regarding your information security enclosed by attachment?

NO YES

Currency used for this questionnaire:

ZAR

USD

EUR

GBP

Other

1. COMPANY / APPLICANT INFORMATION

Name of applicant

Address

Country

Email

Phone

Subsidiaries

All web domain names
(covered by this insurance)

1.1 COMPANY / APPLICANT INFORMATION

Please check the industrial sector(s). Details and assignment are available in the annex on page 8.

Business & Professional Services

Information Technology – Software

Defense / Military Contractor

Manufacturing

Education

Pharmaceuticals

Entertainment & Media

Public Authority; NGOs; Non-Profit

Financial Services – Insurance
(Agencies)

Real Estate, Property & Construction

Food & Agriculture

Retail

Healthcare

Telecommunications

Information Technology – Hardware

Tourism & Hospitality

Information Technology – Services

Transportation/Aviation/Aerospace

Financial services - Investment
Management

Financial services - Banking

Other

For “Other” type of industry, please specify

Please specify details of your activities

1.2 TURNOVER/REVENUE AND REGIONAL FOOTPRINT

	Domestic	USA	European Union	Rest of world
Your turnover / revenue for the last fiscal year				
Your share of turnover/revenue created online for the last fiscal year				
		Last year	Year before last	Last but two years
Your gross profit (or equivalent)				
Please state the number of employees				

1.3 TYPE AND QUANTITY OF DATA

Please estimate type and volume of the following categories of sensitive data your company is maintaining/processing to the best of your knowledge.

Type of data	Number of unique records	Number of unique records of US citizens	Number of unique records stored in US data centres
Personally Identifiable Information (PII)			
Payment Card Information (PCI)			
Protectable Health Information (PHI)			
Intellectual Property (IP)			

1.4 REQUESTED CYBER INSURANCE

Policy period	from	to
Aggregate limit requested		
Retroactive date	<input type="text"/>	
Territorial scope of insurance cover	<input type="text"/>	

Cover modules/elements

Please check all cover modules requested. Details and assignment are available in annex 2 on page 8.

First party cover:

Data breach response	Reputational risk sub-limit	Restoration
Business interruption	Cyber extortion	Cyber Crime
PCI-DSS		

Third party claims:

Confidentiality and privacy breach liability	Network security liability	Multimedia
--	----------------------------	------------

1.5 PRIOR CYBER INSURANCE

- | | | |
|---|----|-----|
| 1. Do you currently hold or have ever held cyber insurance providing the same or similar coverage as the insurance sought? | NO | YES |
| 2. Has any insurer ever cancelled or non-renewed a policy that provided the same or similar coverage as the insurance applying for? | NO | YES |

1.6 INFORMATION SECURITY EVENTS AND LOSS HISTORY

Please answer the following questions by considering any time during the past three years

- | | | |
|--|----|-----|
| 1. Have you had any incidents, claims or suits involving unauthorized access or misuse of your network, including embezzlement, fraud, theft of proprietary information, breach of personal information, theft or loss of laptops, denial of service, electronic vandalism or sabotage, computer virus or other incident? | NO | YES |
| 2. Have you experienced an unplanned business interruption of longer than four hours caused by a cyber incident? | NO | YES |
| 3. Have you experienced an extortion attempt or demand with respect to your computer systems? | NO | YES |
| 4. Have you received any claims or complaints with respect to allegations of defamation, invasion or injury of privacy, theft of information, breach of information security, transmission of malware, participation in a denial of service attack, request to notify individuals due to an actual or suspected disclosure of personal information? | NO | YES |
| 5. Are you / Have you been subject to any government action, investigation or subpoena regarding any (alleged) violation of any (privacy) law or regulation? | NO | YES |
| 6. Are you aware of any release, loss or disclosure of personally identifiable information in your care, custody or control, or in the control of anyone holding such information on behalf of you? | NO | YES |
| 7. Are you aware of any actual or alleged fact, circumstance, situation, error or omission, or potential issue which might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for or any similar insurance presently or previously in effect or currently proposed? | NO | YES |

If one question or more of this section 1.6 is answered with "Yes", please attach a description including complete details (cause, costs, notification, time to discover, recovery time and steps taken to mitigate future exposure) of each event (incident, claim etc.).

1.7 FRAMEWORKS AND STANDARDS

Please check all legal frameworks you have to adhere to.

General Data Protection Regulation (GDPR) of the European Union (EU)	US Federal Privacy Act
Protection of Personal Information Act (PoPIA)	Other

Please check all standards for which you have successfully been audited or hold a valid certificate.

Payment Card Industry Data Security Standard (PCI DSS)			
Merchant level 1	Merchant level 2	Merchant level 3	Merchant level 4
ISO 27001:2013 Information security management systems	NIST (US National Institute of Standards and Technology) Cybersecurity Framework		

If “Other” standard(s) apply, please specify

If “Other” standard(s) apply, please specify

2 INFORMATION SECURITY

The following questions help us to evaluate the maturity of your information security. Please answer all questions and provide evidence where available (e.g. reports, presentations, documents etc.). The questions are structured according to the clauses of the ISO/IEC 27002 standard. Hence questions focussing on one security objective can appear in different sections of this questionnaire. In order to create a better understanding about why we ask the questions, each section starts with the objective(s) of the ISO security control categories.

- Do you operate Industrial Control Systems (ICS) and Operational Technologies (OT) in addition to your ordinary Information Technology? If yes, please answer the following sections with a focus on your IT information security controls and the dedicated “Endorsement ICS and OT” separately. NO YES
Explanation: The term Industrial control system (ICS) embraces several types of control systems and associated instrumentation is used for industrial process control. Operational Technology (OT) is defined as collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process. Industrial Security in this context is used to secure Operational Technology
- Do the answers in this questionnaire cover all (co-)insured companies and business units of the policyholder? Please provide additional information (e.g. separate questionnaires) for companies/business units that do not fall within the scope of this questionnaire. NO YES

2.1 INFORMATION SECURITY POLICIES

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

- Have you developed and implemented a formal information security policy which is entity-wide and permanently available to all group entities, employees and relevant external parties? NO YES

2.2 ORGANIZATION OF INFORMATION SECURITY

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

- Have you assigned a responsible person for information security (e.g. Chief Information Security Officer “CISO”)? NO YES

2.3 HUMAN RESOURCE SECURITY

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. To ensure that employees and contractors are aware of and fulfil their information security responsibilities. To protect the organization's interests as part of the process of changing or terminating employment.

- | | |
|---|----------|
| 1. Do you provide users (employees and contractors) with mandatory information security awareness education covering social engineering (e.g. phishing emails), data privacy and current cyber threats at least annually? | NO YES |
|---|----------|

2.4 ASSET MANAGEMENT

Objective: To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

- | | |
|--|----------|
| 1. Do you keep an up-to-date inventory of software (including operating systems, cloud solutions etc.) and hardware assets connecting to your network? | NO YES |
| 2. Do you classify information with regards to confidentiality? | NO YES |

2.5 ACCESS CONTROL

Objective: To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.

- | | |
|---|----------|
| 1. Have you implemented an access control policy that covers roles, rights and restrictions reflecting the associated information security risks through need-to-know and need-to-use principles? | NO YES |
| 2. Do you restrict user access (employees, contractors etc.) on a business need-to-know and least-privilege basis? | NO YES |
| 3. Do you prohibit local admin rights on workstations for users? | NO YES |
| 4. Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors or vendors)? | NO YES |
| 5. Do you make use of strong (long and complex) passwords and enforce MFA (multi-factor authentication) based on criticality (e.g. for remote or privileged access)? | NO YES |

2.6 CRYPTOGRAPHY

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

- | | |
|--|----------|
| 1. Do you enforce the use of encryption over all external communication lines (e.g. website / email / wireless)? | NO YES |
|--|----------|

2.7 PHYSICAL AND ENVIRONMENTAL SECURITY

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

2.8 OPERATIONS SECURITY

Objective: To ensure correct and secure operations of information processing facilities. To ensure that information and information processing facilities are protected against malware. To protect against loss of data. To record events and generate evidence. To ensure the integrity of operational systems. To prevent exploitation of technical vulnerabilities. To minimise the impact of audit activities on operational systems.

- | | | |
|--|----|-----|
| 1. Have you implemented change management procedures for business processes, IT and information security systems? | NO | YES |
| 2. Is there continually up-to-date malware protection in place on all web-proxies, email-gateways, workstations, laptops and any other applicable systems across your IT/OT-infrastructure? | NO | YES |
| 3. Is there a process for taking regular (at least weekly) backups of all data and storing it on a separate environment from production (e.g. offsite or in a cloud)? | NO | YES |
| 4. Is there a patch management process in place for all IT assets that includes criticality assessment, verification, testing of patches and deployment within one month of release or less? | NO | YES |
| 5. Do you technically prohibit users from installing unauthorised software on their devices? | NO | YES |

2.9 COMMUNICATIONS SECURITY

Objective: To ensure the protection of information in networks and its supporting information processing facilities. To maintain the security of information transferred within an organization and with any external entity.

- | | | |
|---|----|-----|
| 1. Are all internet access points secured by appropriately configured firewalls? | NO | YES |
| 2. Have you implemented a Network Access Control (“NAC”) technology to access your corporate wireless networks? | NO | YES |
| 3. Are all internet-accessible systems (e.g. web / email servers) physically or logically segregated from your trusted network? | NO | YES |

2.10 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. To ensure that information security is designed and implemented within the development lifecycle of information systems. To ensure the protection of data used for testing.

- | | | |
|---|----|-----|
| 1. Do you harden all your systems (servers, clients, networking equipment, databases, mail servers, etc) in accordance with industry standards or manufacturer recommendations? | NO | YES |
|---|----|-----|

2.11 SUPPLIER RELATIONSHIPS

Objective: To ensure protection of the organization’s assets that is accessible by suppliers. To maintain an agreed level of information security and service delivery in line with supplier agreements.

- | | | |
|---|----|-----|
| 1. Do you have an established process so that suppliers are identified, categorised, and a relevant information security assessment is performed at due diligence stage and findings are addressed? | NO | YES |
| 2. Do agreements with suppliers require levels of security commensurate with your own information security standard? | NO | YES |

2.12 INFORMATION SECURITY INCIDENT MANAGEMENT

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

1. Do you have an information security incident response plan that is reviewed and tested at least annually? NO YES
-

2.13 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Objective: Information security continuity should be embedded in the organization's business continuity management systems. To ensure availability of information processing facilities.

1. Do you review and update the validity of your information security continuity plans (Business Continuity Management and Disaster Recovery) at least annually? NO YES
2. Are your information processing facilities (i.e. any system, service or infrastructure, or physical location housing it) implemented with redundancy? NO YES

Please describe

2.14 COMPLIANCE

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

1. Have you assigned a responsible person (e.g. a Data Privacy Officer, DPO) for ensuring compliance with relevant privacy legislation and regulation? NO YES
2. Do you perform vulnerability assessment and penetration testing (VAPT) of critical systems (i.e. applications and networks), internally or by an independent third party, both regularly and after system changes? NO YES
-

3 ADDITIONAL COMMENTS AND SIGNATURE(S)

Would you like to share further information or details regarding your information security?

Herewith, by undersigning this document (must be signed by officer, owner or manager), I confirm that I am a duly authorized representative of the company with sufficient technical skills to provide – to my best knowledge – accurate and comprehensive answers regarding the questions within this questionnaire on behalf of the company. The completed questionnaire and optional attachments are basis for the coverage and will therefore become part of the insurance contract.

Date

Date

Name

Name

Position, task

Position, task

Email

Email

Signature

Signature

ANNEX 1: OVERVIEW – INDUSTRIAL SECTORS

Source: Cyber Insurance exposure data schema v1.0 by Cambridge Centre for Risk Studies

Business & Professional Services	Occupations providing specialist business advice and services. Some professional services require holding professional licenses such as architects, auditors, engineers, doctors and lawyers.
Defense / Military Contractor	Defense industry comprises government and commercial industry involved in research, development, production, and service of military materiel, equipment and facilities
Education	Colleges and universities, independent and unified school districts, student loans and tuition companies
Energy	Companies involved in the exploration, extraction and development of oil or gas reserves, oil and gas drilling, or integrated power firms.
Entertainment & Media	Enterprises involved in providing news, information, and entertainment: radio, television, films, theatre
Financial Services – Banking	Companies engaged in commercial banking, savings institutions, credit unions, credit card issuing, sales financing, mortgage and loan companies and brokers, financial transaction processing, reserve and clearinghouse activities, and central banking.
Financial Services – Insurance	Direct insurance carriers, reinsurance carriers, and insurance agencies and brokerages.
Financial Services – Investment management	Companies engaged in investment banking, securities dealing and brokerage, commodity contracts dealing and brokerage, securities and commodity exchanges, investment clubs and venture capital, portfolio management, investment advice, and legal entity funds and trusts
Food & Agriculture	Those involved in the food industry, including production, processing, distribution, and wholesale supply
Healthcare	Companies providing goods and services to treat patients with curative, preventive, rehabilitative, and palliative care.
Information Technology – Hardware	Companies engaged in manufacturing and/or assembling computers (mainframes, personal computers, workstations, laptops, and computer servers) and peripheral equipment (e.g. storage devices, printers, monitors etc.)
Information Technology – Services	Companies providing hosting or data processing services (incl. cloud and streaming services); internet publishing and broadcasting content (incl. social media); internet search portals; services relating to computer systems design, computer facilities management, computer programming services, and computer hardware or software consulting.
Information Technology – Software	Companies involved in the design, development, documentation, and publishing of computer software
Manufacturing	Companies making or process goods, especially in large quantities and by means of industrial machines
Mining & Primary Industries	Companies involved in the mining, quarrying, and processing of extracting minerals, coal, ores, main commodities, and natural resources.
Pharmaceuticals	Pharmaceutical industry develops, produces, and markets drugs or pharmaceuticals for use as medications. Pharmaceutical companies may deal in generic or brand medications and medical devices.
Public Authority; NGOs; Non-Profit	National or local government agencies, non-governmental and non-profit organizations
Real Estate, Property & Construction	Companies managing, developing, and transacting property consisting of land and buildings, along with its natural resources such as crops, minerals, or water
Retail	Retailers to general public, sellers of goods and services both in retail stores and online, wholesalers and distributors.
Telecommunications	Companies facilitating exchange of information over significant distances by electronic means.
Tourism & Hospitality	Companies providing services for tourism, travel, accommodation, catering and hospitality
Transportation/ Aviation/ Aerospace	Companies facilitating the transportation of goods or customers. The transportation sector is made up of airlines, railroads and trucking companies.
Utilities	The utilities sector contains companies such as electric, gas and water firms and integrated providers

ANNEX 2: OVERVIEW – COVERAGE MODULES/ELEMENTS

Data breach response (1 st party)	We will pay on the insured's behalf any reasonable and necessary costs resulting from an actual or suspected data breach.
Restoration (1 st party)	We will pay on the insured's behalf any reasonable and necessary costs to restore their data and software after a data breach, to the closest possible condition in which they were immediately before the data breach.
Business interruption (1 st party)	We will pay the insured for the reduction of net profit during the interrupted period which has been directly caused by a cyber-incident.
Cyber extortion (1 st party)	We will reimburse the insured for any ransom they pay (where legally permissible and subject to our prior written consent) and any reasonable and necessary costs to resolve cyber extortion.
Cyber crime (1 st party)	We will reimburse the insured for any money illegally taken from them as a direct result of cyber crime.
PCI-DSS (1 st party - optional)	We will reimburse the insured for any monetary fines and penalties levied against them by a Payment Card Brand due to their breach of PCI-DSS which is directly caused by a cyber-incident.
Confidentiality and privacy (3 rd party)	We will reimburse and semi the insured is under legal liability to pay arising from a third party claim or a claim against them by an employee for a data breach relating to confidential information or personal data of a third party, or for infringement for your respective data protection laws and the insured's legal defence costs incurred with our consent.
Network security (3 rd party)	We will reimburse any sums the insured is under legal liability to pay arising if a third party claim is made for a data breach, theft of data or a DoS attack on a third party's computer systems which is directly caused by a malicious act or malware on the insured's computer systems that the insured failed to prevent as well as the insured's legal defence costs incurred with our consent.
Multimedia (3 rd party - optional)	We will reimburse any sums the insured is under a legal liability to pay arising from a third party claim for: defamation, breach of copyright, title, slogan, trademark, trade name, service mark, service name or domain name or breach or interference of privacy rights, resulting from the insured's online media activities and your legal defence costs incurred with our consent.