Cyber Risk Assessment Questionnaire

Introduction

This questionnaire is designed to provide us with a comprehensive view of the effectiveness and maturity of information and data security within your company. 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. Considering this, someone within the company responsible for information security should answer and sign the questionnaire or at least support the person who is answering it by countersigning. If you have no information security resource, then the questionnaire should be completed by a senior representative (owner or board member).

This questionnaire is neither an offering nor binding of an insurance contract (coverage). Furthermore, the completion of this questionnaire does not obligate the insurer to offer coverage to you.

Are any further information or details regarding your information security enclosed by attachment? ☒ Yes ☐ No

Currency used for this questionnaire: ☐ USD ☐ EUR ☐ GBP ☐ Other: **INR**

1 Company / applicant information

Name of applicant	CANARA BANK
Address	**HEAD OFFICE 112, J C ROAD BENGALURU**
Country	India
Email	hoditcsg@canarabank.com
Phone	080-25535277
Subsidiaries	
All web domain names that should be covered by this insurance	There are approximately 8 domains like canarabank.com, canarabank.in etc. hosting various underlying sub-domains/applications

1.1 Industrial sector(s)

Please check the industrial sector(s). Details and assignment are available in the annex on page 12.

- ☐ Business & Professional Services
- ☐ Defense / Military Contractor
- ☐ Education
- ☐ Energy
- ☐ Entertainment & Media
- ☒ Financial Services – Banking
- ☐ Financial Services – Insurance
- ☐ Financial Services – Investment management
- ☐ Food & Agriculture
- ☐ Healthcare
- ☐ Information Technology – Hardware
- ☐ Information Technology – Services
- ☐ Information Technology – Software
- ☐ Manufacturing
- ☐ Mining & Primary Industries
- ☐ Pharmaceuticals
- ☐ Public Authority; NGOs; Non-Profit
- ☐ Real Estate, Property & Construction
- ☐ Retail
- ☐ Telecommunications
- ☐ Tourism & Hospitality
- ☐ Transportation/Aviation/Aerospace
- ☐ Utilities
- ☐ 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 **(₹ In Cr)**	99,353.18	914.49	2,265.98	653.34
Your share of turnover/revenue **created online** for the last fiscal year				

	Last year	Year before last –Mar 22	Last but two years-Mar 21
Your gross profit (or equivalent)	₹ 27716.01 Cr	₹ 23088.98 Cr	₹ 19688.97 Cr

Please state the number of employees	83,824*			
Please state the (estimated) number of individual IT devices deployed	Details cannot be disclosed	Server	Details cannot be disclosed	Desktops
		Laptops		Mobile devices

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)	More than 11 Crores		
☒	Payment Card Information (PCI)	Credit card base = 8,20,319* debit card base = (active card) 5,56,70,877*		
☐	Protectable Health Information (PHI)			
☐	Intellectual property (IP)			

(* As on 31-01-2024)

1.4 Requested cyber insurance

Policy period	From	31-03-2024	To	30-03-2025
Aggregate limit requested	As per RFP & per scope document			
Retroactive date	As per RFP & per scope document			
Territorial scope of insurance cover	As per RFP & per scope document			

Cover modules/elements

Please check all cover modules requested. Details and assignment are available in the annex on page 12.

First party losses	Deductible/SIR for each and every insured event	Sub-limit for each and every insured event and in the aggregate
☐ Breach and privacy event	As per RFP & per scope document	As per RFP & per scope document
☐ Data and software loss		
☐ Business interruption		
☐ Contingent business interruption		
☐ Incident response costs		
☐ Regulatory and defence cover		
☐ Financial theft and fraud		
☐ Cyber extortion		

Third party claims	Deductible/SIR for each and every insured event	Sub-limit for each and every insured event and in the aggregate

☐	Network service failure liability	As per RFP & per scope document	As per RFP & per scope document
☐	Technology E&O		
☐	Multi-media liability		

Internal

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?	☒ Yes ☐ No
2	Has any insurer ever declined or non-renewed a policy that provided the same or similar coverage as the insurance applying for?	☐ Yes ☒ No

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, malware or other incident?	☒ Yes ☐ No
2	Have you experienced an **unplanned business interruption** of longer than four hours caused by a cyber incident?	☐ Yes ☒ No
3	Have you experienced an **extortion attempt or demand** with respect to your computer systems?	☐ Yes ☒ No
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?	☐ Yes ☒ No
5	Are you / Have you been subject to any **government action, investigation or subpoena** regarding any (alleged) violation of any (privacy) law or regulation?	☐ Yes ☒ No
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?	☐ Yes ☒ No
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?	☐ Yes ☒ No

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) *(Applicable for London Branch)*	☐	US Federal Privacy Act
☐	US Health Insurance Portability and Accountability Act (HIPAA) and US Health Information Technology for Economic and Clinical Health (HITECH) Act		

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 27001:2013/2022 Information security management systems	☐	NIST (US National Institute of Standards and Technology) Cybersecurity Framework
☐	Critical Security Controls	☐	Other

☐	COBIT 5 (Control Objectives for Information and Related Technologies)	☐	Information Security Forum (ISF) The Standard of Good Practice for Information Security 2018

If "Other" standard(s) apply, please specify	
Please describe the scope of the certificate	

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.

1 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. ☐ Yes ☒ No

Explanation: The term industrial control system (ICS) embraces several types of control systems and associated instrumentation used for industrial process control. Operational Technology (OT) is defined as a collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process. OT environments usually supervise physical processes such as manufacturing, energy, medicine, building management and ecosystems within other industries. Industrial security in this context encompasses people, processes and technology to secure Operational Technology (OT).

Examples of operational technologies include:

- PLC (programmable logic controller) are physically hardened computers (solid state devices) for the control of industrial assets and processes.
- SCADA (Supervisory control and data acquisition) is a control system architecture for dispersed assets in industrial environments which gathers real-time data from remote locations in order to control equipment and its conditions.
- DCS (distributed control system) is a digital automated industrial control system (ICS) that uses geographically distributed, autonomous controllers that are remotely monitored and supervised.
- IIoT (industrial internet of things) is the use of smart sensors and actuators to enhance manufacturing and industrial processes.

Please only complete this endorsement if your business has a significant reliance on ICS and OT.

2 Do the answers in this questionnaire cover all (co-)insured companies and business units of the policyholder? If no, which companies/business units are covered by the questionnaire? Please provide additional information (e.g. separate questionnaires) for companies/business units that do not fall within the scope of this questionnaire. ☒ Yes ☐ No

_____

_____

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.

1 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? ☒ Yes ☐ No

2 Are your information security policies reviewed (at least annually) and approved by senior management? ☒ Yes ☐ No

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.

1 Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")? ☒ Yes ☐ No

2 Does your IT security responsible person regularly report to senior / C-level management? ☒ Yes ☐ No

3 Do you ensure that there is adequate segregation of duties to reduce the opportunity for accidental or deliberate misuse of IT assets and data? (e.g. employees with payment authorisation should not have access to the bank reconciliation processes) ☒ Yes ☐ No

4 Do you have processes in place to monitor/audit the activity of user accounts with authorisation to bypass implemented rules for segregation of duties? ☒ Yes ☐ No

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?	☒ Yes ☐ No
2	Have you identified specific roles (e.g. privileged users, admins, executives, users of operational technology) and provided them with tailored security awareness training?	☒ Yes ☐ No
3	Do you conduct exercises (e.g. phishing tests) to measure the effectiveness of your awareness training and target additional training to candidates that require improvement?	☒ Yes ☐ No

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?	☒ Yes ☐ No
2	Do you have a comprehensive Configuration Management Database (CMDB) including: all IT assets, public cloud assets, dependencies, criticality, ownership, software and patch versions? Please describe. ITAVM ,Centralised Inventory management tool is in place	☒ Yes ☐ No
3	Do you use a Mobile Device Management (MDM) solution for all laptops and smartphones?	☒ Yes ☐ No
4	Do you ensure that all IT assets (including cloud-based assets) in the inventory are assigned with an owner that is ultimately responsible for the asset?	☒ Yes ☐ No
5	Are asset owners required to ensure that their IT assets are properly classified (based on legal requirements, value, criticality and sensitivity) and protected throughout the entire asset lifecycle?	☒ Yes ☐ No
6	Do asset owners have to follow strict decommissioning processes (including on the cloud), that ensure the secure removal / deletion / destruction of data, update of asset inventories, a log of all related activities, etc.?	☒ Yes ☐ No
7	Do you classify information with regards to confidentiality?	☒ Yes ☐ No
8	Do you classify information with regards to business criticality level (i.e. integrity and availability)?	☒ Yes ☐ No
9	Do you provide guidance on how to handle classified information?	☒ Yes ☐ No
10	Do you regularly review compliance with the guidance on handling of classified information?	☒ Yes ☐ No
11	Do you technically enforce and centrally manage rules that disable media ports and disable or restrict usage to only encrypted removable storage devices (e.g. USB sticks or hard disks)?	☒ Yes ☐ No
12	Is an authorisation required for unencrypted media removed from the organisation and is a record of such removals kept in order to maintain an audit trail?	☒ Yes ☐ No

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?	☒ Yes ☐ No

Internal

2	Do you maintain audit logs of access management activities (grant, change and revoke access rights)?	☒ Yes ☐ No
3	Do you restrict user access (employees, contractors etc.) on a business need-to-know and least-privilege basis?	☒ Yes ☐ No
4	Do you have a solution for the secure access to a network from a remote location (e.g. VPN, Zero Trust)?	☒ Yes ☐ No
5	Do you have a solution for secure authentication over networks (e.g. IPSec, TLS and WPA2 or WPA3 for wireless access)?	☒ Yes ☐ No
6	Do you have a formal access provisioning process in place for assigning and revoking access rights?	☒ Yes ☐ No
7	Do you have implemented a central Identity and Access Management ("IAM") system for assigning and revoking access rights?	☒ Yes ☐ No
8	Does the asset owner review access rights at least annually?	☒ Yes ☐ No
9	Do you prohibit local admin rights on workstations for users?	☒ Yes ☐ No
10	Do you use Privileged Identity and Account Management ("PIM", "PAM") or dedicated Privileged Access Workstations ("PAW")?	☒ Yes (PIM is in place) ☐ No
11	Do you review and verify the need for privileged access accounts at least annually?	☒ Yes ☐ No
12	Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors or vendors)?	☒ Yes ☐ No
13	Do you remove unnecessary user rights after organisational role changes?	☒ Yes ☐ No
14	Do you have a procedure to report a security event according to a defined escalation process if a potential attempted (e.g. brute force) or successful breach of log-on controls is detected?	☒ Yes ☐ No
15	Do you terminate inactive sessions after period of inactivity of devices and applications?	☒ Yes ☐ No
16	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)?	☒ Yes ☐ No
17	Have you changed all default passwords on all devices on the network (e.g. routers, switches, Internet of Things)?	☒ Yes ☐ No
18	Do you provide an approved password manager to all your users?	☒ Yes ☐ No
19	Do you technically restrict user access to programs that are able to override system and application access controls?	☒ Yes ☐ No
20	Do you log the activity of programs that are able to override system and application access controls?	☒ Yes ☐ No

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)?	☒ Yes(Wireless communication is not applicable) ☐ No
2	Do you enforce the use of encryption of sensitive / confidential information while at rest (e.g. on premise, mobile devices and/or in cloud)?	☒ Yes ☐ No

2.7 Physical and environmental security

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

1	Do you regularly review your physical and environmental security controls around your facilities hosting critical assets?	☒ Yes ☐ No

2	Have you installed advanced entry controls (e.g. biometrics, mantraps, 24-7 closed-circuit television (CCTV), recording of every access)?	☒ Yes (biometrics, CCTV, access logs are in place) ☐ No

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?	☒ Yes ☐ No
2	Does your change management include testing, failback scenarios (rollback strategy) and communication of changes?	☒ Yes ☐ No
3	Do you have provisions for emergency change processes to enable quick and controlled implementation of changes to resolve an incident?	☒ Yes ☐ No
4	Is the IT-environment for development and testing separated from live IT-environment?	☒ Yes ☐ No ☐ Not applicable
5	Do your developers use different accounts for development, testing and day-to-day tasks?	☒ Yes ☐ No ☐ Not applicable
6	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?	☒ Yes(Not applicable to web proxy) ☐ No
7	Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malware?	☐ Yes ☐ No
8	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)?	☒ Yes(Offsite) ☐ No
9	Do you regularly (at least annually) test that data backups are complete and can be restored as quickly as possible with minimal impact to business?	☒ Yes ☐ No
10	Do you create multiple generations of backups and store them separately from production?	☒ Yes ☐ No
11	Do you have a Security Information and Event Management ("SIEM") in place to collect and analyse all events relating to user activity, network activity, exceptions, faults and any other relevant information security events from all your IT assets? Please describe.	☒ Yes ☐ No
12	Do you ensure that event logs containing sensitive data and PII are protected at the same security levels as the production data?	☒ Yes ☐ No
13	Do you have technical controls in place to ensure that system administrator / privilege accounts activity logs are tamper proof?	☒ Yes ☐ No
14	Have you implemented a centralised software installation process?	☒ Yes ☐ No
15	Do you ensure that any end-of-life (legacy) vendor supplied assets (including software, firmware etc.) in use is protected by mitigating controls? Please describe. We don't use any EOL assets	☐ Yes ☐ No ☒ Not applicable
16	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?	☒ Yes ☐ No
17	Do you install critical security patches (CVSS > 9.0) on internet-facing IT systems and applications in a timely manner? Please describe. Critical security patches are applied in an emergency manner.	☒ Yes ☐ No

18	Do you regularly carry out vulnerability scans, analyse the identified vulnerabilities and associated risks as well as take appropriate actions? Please describe.	☒ Yes ☐ No
19	Do you technically prohibit users from installing unauthorised software on their devices?	☒ Yes ☐ No
20	Do have a whitelist of software that users and system administrators are permitted to install?	☒ Yes ☐ No

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?	~~☐ Yes ☐ No~~(Not applicable as we don't have Internet access points)
2	Do you regularly (at least annually and as part of system change management) review or audit the configuration of your firewalls?	☒ Yes ☐ No
3	Do you ensure that business changes are supported by risk related adjustments or updates of firewall rules?	☒ Yes ☐ No
4	Have you implemented a Network Access Control ("NAC") technology to access your corporate wireless networks?	~~☐ Yes ☐ No~~(Not applicable as corporate wireless network is not in place)
5	Are all internet-accessible systems (e.g. web / email servers) physically or logically segregated from your trusted network?	☒ Yes ☐ No
6	Are all high risk network segments (e.g. point of sales (PoS) systems, sensitive data processing, office and operational technology (OT) production networks etc.) segregated?	☒ Yes ☐ No
8	Do you enforce the use of authentication and integrity methods for email such SPF, DKIM, DMARC?	☒ Yes ☐ No
9	Do you use data loss prevention (DLP) software?	☒ Yes ☐ No
10	Do you have appropriate protection (e.g. by sandboxing) from malicious attachments through the use of incoming electronic messages?	☒ Yes ☐ No

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 have a process in place to document and review the requirements for system acquisitions, changes or developments to ensure that they include adequate information security controls?	☒ Yes ☐ No ☐ Not applicable
2	Does your process also include a requirement to inform all operators (e.g. users and SOC) of their new duties and responsibilities following the acquisitions, changes or developments?	☐ Yes ☐ No ☒ Not applicable
3	Do you ensure that data in transit over a public network (e.g. for web applications, file transfer, instant messaging etc.) is secured thus ensuring confidentiality, integrity and authentication of parties as applicable?	☒ Yes ☐ No
4	Do you protect your web-servers against denial of service ("DDoS") attacks (e.g. by utilising a content delivery network provider)?	☒ Yes ☐ No ☐ Not applicable

Internal

5	Do you harden all your systems (servers, clients, networking equipment, databases, mail servers, etc) in accordance with industry standards or manufacturer recommendations?	☒ Yes ☐ No
6	Do you have a secure coding baseline in place that details the requirements during planning, coding, reviews and maintenance of software?	☒ Yes ☐ No ☐ Not applicable
7	Are your developers regularly trained in secure programming techniques and code reviews?	☒ Yes ☐ No ☐ Not applicable
8	Do you conduct security tests or code analysis during system development, before go-live and after system changes take place?	☒ Yes ☐ No ☐ Not applicable
9	Do you ensure that any test data that is confidential is afforded the same security controls as confidential data on production systems?	☒ Yes ☐ No

2.11 Supplier relationships

Objective: To ensure protection of the organization's assets that are accessible by suppliers (goods, products and services including IT and cloud providers). 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?	☒ Yes ☐ No
2	Have you identified and mandated information security controls to specifically address supplier access to your information in a policy?	☒ Yes ☐ No
3	Do agreements with suppliers require levels of security commensurate with your own information security standard?	☒ Yes ☐ No
4	Do you periodically review and update agreements with your business critical suppliers?	☒ Yes ☐ No
5	Do you stipulate the right for third party audits within your contractual agreements?	☒ Yes ☐ No
6	Do you have a process for ongoing monitoring of suppliers for security events (e.g. data breaches, new vulnerabilities, cyber attacks) to manage your current exposure from suppliers?	☒ Yes ☐ No
7	Do you conduct information security assessments or review independent security audit reports / certificates (e.g. SOC 2) to obtain assurance about the security posture of suppliers?	☒ Yes ☐ No
8	Do your written and signed contracts with suppliers include a hold harmless agreement or waiver of liability in your favour in case such suppliers fail to protect your sensitive data or do not comply with the mutually agreed security level?	☒ Yes ☐ No

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?	☒ Yes ☐ No
2	Have you appointed a responsible person or team for incident response?	☒ Yes ☐ No
3	Do you have an incident response or digital forensic outsourcing retainer agreement to support in the case of a major incident?	☒ Yes ☐ No
3	Are your employees and contractors trained to help identify security events and how to report them in a timely manner?	☒ Yes ☐ No
4	Do you document, follow up and report all information security events in a centrally organised solution (e.g. via your Security Information and Event Management (SIEM))?	☒ Yes ☐ No
5	Have you established an escalation procedure (e.g. as part of Security Operations Centre, SOC responsibilities) for information security incidents?	☒ Yes ☐ No
6	Do you collect evidence as soon as an incident is noted and maintain it within tamper-proof environment?	☒ Yes ☐ No

Internal

7	Do you regularly inform management about critical incidents?	☒ Yes ☐ No
8	Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future incidents?	☒ Yes ☐ No
9	Do you quantify and monitor types, volumes and costs of information security incidents?	☒ Yes ☐ No

Internal

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 regularly (at least annually) review the potential cyber scenarios that can impact business continuity (e.g. in a Business Impact Analysis, BIA)?	☒ Yes ☐ No
2	Does your BIA include an analysis of the time it takes before an outage affecting a critical system(s) has a material impact on revenue? Please describe.	☒ Yes ☐ No
3	Are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined based on the level of criticality of the system / application?	☒ Yes ☐ No(RTO and RPO is defined for individual applications based on its complexity, inter-dependency, functioning and criticality.)
4	Do you have both Business Continuity Management (BCM) and Disaster Recovery (DR) plans in place that include cyber scenarios?	☒ Yes ☐ No
5	Have you nominated personnel with the necessary responsibility, authority and competence to manage incidents and maintain information security?	☒ Yes ☐ No
5	Do you review and update the validity of your information security continuity plans (Business Continuity Management and Disaster Recovery) at least annually?	☒ Yes ☐ No
6	Do you exercise and test the processes and content documented in the plans (e.g., Table-Top or Red Teaming) at least annually?	☒ Yes ☐ No
7	Are the results of the continuity test activities reviewed, documented, reported to management and are the plans revised based on lessons learned?	☒ Yes ☐ No
8	Are your information processing facilities (i.e. any system, service or infrastructure, or physical location housing it) implemented with redundancy? Please describe. Redundancy is ensured through the presence of DR site and NDR with High Availability	☒ Yes ☐ No
9	Do you conduct redundancy testing at least annually to ensure that failover works as intended?	☒ Yes ☐ No

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 implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements?	☒ Yes ☐ No
2	Do you have a compliance function in place with the authority to report to "C"-level management or equivalent?	☒ Yes ☐ No
3	Have you implemented processes and procedures for the retention, storage, handling and disposal of records and information?	☒ Yes ☐ No
4	Do you have a documented schedule to identify records and the period of time for which they should be retained and safely disposed?	☒ Yes ☐ No
5	Have you assigned a responsible person (e.g. a Data Privacy Officer, DPO) for ensuring compliance with relevant privacy legislation and regulation?	☒ Yes ☐ No
6	Do you have a policy for the privacy and protection of personally identifiable information developed and implemented?	☒ Yes ☐ No
7	Do you ensure that Personal Identifiable Information (PII) is only handled as authorised by the data subject?	☒ Yes ☐ No
8	Are your cryptographic controls maintained up-to-date and in-line with any relevant agreements and/or laws/regulations?	☒ Yes ☐ No
9	Do you perform regular reviews (or audits) to evaluate compliance with relevant information security policies, standards and/or laws or regulations?	☒ Yes ☐ No
10	Are asset owners (systems/data) assigned with the responsibility to ensure that findings from compliance reviews are remediated?	☒ Yes ☐ No
11	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?	☒ Yes ☐ No
12	Do you perform information security audits in alignment with information security frameworks (e.g. ISO 27001, NIST 800-53, ISF etc.) at least annually?	☒ Yes ☐ No

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 the basis for the coverage and will therefore become part of the insurance contract.

Date	_____	Date	_____
Signature	_____	Signature	_____
Name	_____	Name	_____
Position, task	_____	Position, task	_____
Email	_____	Email	_____

Internal