Olympus Holdings N.V.

Business Continuity Policy and Disaster Recovery Plan

APRIL 2024
VERSION 1.0 **TABLE OF CONTENTS**

TABLE OF ACRONYMS

GCB	Curacao Gaming Control Board
IT	Information Technology

SBD	Significant Business Disruptions
USD	United States Dollar
VPN	Virtual Private Network

TABLE OF DEFINITIONS AND INTERPRETATIONS

“Board” means the Board of Directors of Olympus Holdings N.V.;

“Company” means Olympus Holdings N.V. which is formed and registered in Curacao with registration number 161166;

"Customer" shall mean the natural person or legal entity being a customer of Olympus Holdings N.V.;

“Employee” means a person employed by Olympus Holdings N.V. at non-executive level;

“Management” comprises of CEO, Human resource Manager, Finance Manager, Operations Manager, Chief Technology Officer, Compliance and Reporting Manager and Sales, Marketing and Business Development Manager

“Officer” means a person employed by Olympus Holdings N.V. at executive level;

“Plan” means Olympus Holdings N.V.’s Disaster Recovery Plan;

“Policy” means Olympus Holdings N.V.’s Business Continuity Policy;

Words importing one gender include all other genders and words importing the singular include the plural and vice versa.

1.0 INTRODUCTION

The Company understands that, it is required to create and maintain a Plan tailored to the size and needs of the firm and reasonably designed to enable the firm to meet its existing obligations to its customers or other counterparties. In accordance with these requirements, the Company has designed the plan to address possible scenarios in efforts to minimize any service impact to our customers. Since the timing and impact of disasters and disruptions is unpredictable, flexibility will be required in responding to actual events as they occur.

2.0 OBJECTIVES

The objective of the plan is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities (*office building*) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

3.0 COMPANY’S BUSINESS CONTINUITY MANAGEMENT PROGRAM

The Company plans to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and property, making a financial and operational assessment, protecting the records of the Company, and allowing our customers to transact business. In short, this Plan is designed to permit the Company to resume operations as quickly as possible, given the scope and severity of the significant business disruption.

In keeping with the regulatory requirements, this Plan is designed to address key areas of concern, including, but not limited to, the following:

i. Data backup and recovery;
ii. Mission critical systems;
iii. Financial and operational assessments;
iv. Alternative communications with customers, employees;
v. Communications with regulators;
vi. Alternate physical location of employees;
vii. Critical supplier, contractor, bank and counter-party impact; and

viii. Regulatory reporting and assuring our customers prompt access to their funds if the Company is unable to continue business.

While every emergency situation poses unique problems based on external factors, such as time of day and the severity of the disruption, the Company has been advised by our platform providers that its objective is to restore its own operations and be able to complete existing transactions and accept new transactions and payments within a short period of time. Customer wagers and requests for funds could be delayed during this period.

4.0 THE POLICY

The Policy sets the principles of emergency response to any interruption and the framework according to which the company shall resume, restore and recover its activities in case of crisis. In short, this Policy guides the development and maintenance of the company's Business continuity plan.

The policy provides guidance for the resumption and recovery of time sensitive business operations in accordance with pre-established timeframes provided in the annexure. It also ensures that adequate arrangements are in place for the less time sensitive business operations.

This Policy and Plan applies to all staff, facilities and systems. The company shall be prepared to deal with extreme scenarios, such as hardware or telecommunication failure, data corruption or power outage as well as natural disasters or other events leading to loss of the company's main operating site.

The Risk Management function of the company is responsible for the Policy and for the development and implementation of the Plan.

In the event that the Company determines that we are unable to continue conducting business, the Company will assure customers prompt access to their funds.

5.0 SIGNIFICANT BUSINESS DISRUPTIONS

SBD can vary in their scope, such as only the Company, a building housing the Company, the location in which the Company is situated.

In a disruption affecting the Company, the Company will transfer its operations to a local site when needed and expect to recover and resume business within a period of approximately six (6) hours. We will identify the recovery site and communicate to the GCB as soon as it's possible.

The Company has established a recovery site approximately a few miles from its headquarters that can be used to restore time sensitive functions as soon as key employees are relocated to the facility.

6.0 PLAN LOCATION AND ACCESS

The Company will maintain copies of its plan and the annual reviews, and the changes that have been made to it for inspection. An electronic copy of the plan will be located on the Company's servers in the cloud.

6.1 OFFICE LOCATION

6.1.1 MAIN OFFICE LOCATION

Our Main office is located at (*to be procured*). Its main telephone number is (*to be procured*). Our employees may travel to that office by means of foot, car, or bus.

6.1.2 ALTERNATIVE PHYSICAL LOCATION(S) OF EMPLOYEES

In the event of an SBD, the Company will move its staff from the affected offices to the closest of our unaffected office locations. If none of our other office locations is available to receive those staff, the Company will move them to another building/office. The principals can be reached on their cell phones at any location and staff may work remotely in the event of a disruption accessing the Company's system via VPN or the internet.

6.2 CUSTOMERS' ACCESS TO FUNDS

The Company takes several measures in order to ensure the maximum protection of the funds that the Company safeguards on behalf of its customers.

The Company will act on behalf of the Customer, following the respective standards:

- Depositing the funds of its customers into special bank accounts in authorized and reliable credit institutions under the name "customers' account" and takes all necessary steps to protect the customer's proprietary rights.

Moreover, in order to safeguard the customers' rights in regard to their wagers, it takes the following measures:

i. Keeps all the necessary records and accounts in order to be in the position, at any given time and with no delay, to distinguish the assets that are kept on behalf of the customer from those that are kept on behalf of any other customer as well as from the Company's assets;

ii. Keeps its records and accounts in a way that ensures that they are true and accurate and that they correspond to the wagers that are kept on behalf of the customers;

iii. Takes all the necessary measures in order to ensure that the customers' assets, deposited at authorized financial institutions, are kept into a separate account or accounts to any other accounts that may be used for assets that do not belong to the Customer; and

iv. Applies all necessary organizational measures in order to minimize the risk of loss or reduction of the customer's assets or rights in regard to these assets, because of asset misappropriation, fraud or negligence.

6.3 DATA BACK-UP AND RECOVERY (*HARD COPY AND ELECTRONIC*)

The Company maintains its electronic records on cloud service providers and gaming and wagering system provider.

These records consist of the Company's internal accounting records, subscription agreements gaming and wagering records etc. If our primary site is inoperable, the Company will continue operations from the back-up site or an alternative location by using new devises and plugging into the Company's online accounts with the cloud service providers.

7.0 TECHNOLOGY, DATA AND CYBERSECURITY

7.1 IT FUNCTION

The relevant IT Department will manage IT functions in-house whereas the company will enter into collaboration agreement with providers in order to ensure the security and Integrity of:

- the network used by the Company;
- the gaming platform which is used by the Company's personnel and customers;
- the servers and personal computers of Company's personnel; and
- In addition, this department with necessary external support shall be responsible to ensure that procedures are in place regarding the following issues: ✓ Information Technology Security, and ✓ Information Technology Backup.

7.2 CONTINUITY OF IT SYSTEMS

The IT Department established procedures to ensure that in situations of an interruption to the Company's systems (*gaming, telephones, etc.*) and procedures, the following are met:

i Preservation of essential data and functions;

ii The maintenance of providing its gaming services and activities; and iii At least the timely recovery of such data and functions and the timely resumption of its gaming services and activities.

The Company identifies specific systems which are considered as core systems required ensuring business continuity. These systems ensure:

a. The continued and uninterrupted access to the internet;
b. The continued and uninterrupted operation of the gaming and wagering platform; and
c. The continued and uninterrupted operation of the digital telephone system which shall be critical to the smooth functioning of the telephone order system. The telephone order placing system shall be an alternative/backup system to the internet based one.

If, due to system or integration failures or the system issue is not resolved immediately and, the user of this document is unable to carry out any tasks then the Company should be contacted and informed immediately.

To reduce the impact to critical systems caused by underlining failures, the system designs these redundant systems which will take into consideration methods and mean to support failover to secondary systems.

In order to ensure that systems continue to operate at appropriate levels of performance system, metrics will be collected and monitored by a centralized monitoring solution. Any breach of performance thresholds will be reported to the technical service team for review with upgrades to be planned where appropriate. The Company's systems will be hosted on the cloud infrastructure which allows for the rapid increase of resource or removal of over allocated resources to manage costs.

All major systems within the Company's computing infrastructure are backed up on a regular basis. IT Services have a Backup Strategy which details the frequency of backups. The Company will also strongly advise that all users which in this case is the employees, save their work to their network drive, this drive is backed up and any loss or damage to files can often be rectified by the restoration of the files from an existing backup.

7.3 DATA PROTECTION - CONFIDENTIALITY OF DATA

The company adopts measures in order to implement and maintain systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information. The Company established security mechanisms in order to guarantee the security and authentication of the means of transfer of information, minimize the risk of date corruption and unauthorized access and to prevent information leakage, in order to maintain the confidentiality of the data at all times.

All material non-public information provided by the customers to the Company is held in confidence and is not made known to any other except as follows:

i with the express consent of the customer providing such information; ii
to GCB if the Company is requested or legally required to do so by the GCB; iii
pursuant to a lawful discovery requested;

iv to a counterparty provides clearing services of which such customer is a member or in connection with the clearing of an Instrument;

v subject to appropriate confidentiality requirements, to any person providing services to the Company; vi subject to appropriate confidentiality requirements, to the Company employees, the board, board committees, attorneys, auditors and agents, independent contractors or other persons that have been engaged by the Company, in each case, who require such information in connection with the discharge of their duties to the Company; and

vii All information and data obtained or received by the Company from inspections of accounting and other records will be treated as confidential by the Company.

7.4 CYBERSECURITY

The company will maintain certain personally identifiable information regarding customers in its electronic databases to facilitate the processing of transactions on behalf of its customers to comply with the relevant rules, regulations and laws. The personally identifiable information stored on the Company‘s network is protected from unauthorized access, treated as confidential, and handled according to the terms of the company’s privacy policy. The Company attest that personally identifiable information and customer information stored on its systems will be protected as follows:

- The Company‘s Internet-facing servers will be protected from access through firewalls and/or other security devices.
- The Company's critical servers will reside on isolated networks that will have no direct Internet access.

- The Company's internal systems that store customer personally identifiable information will lock people out of internal systems after a few unsuccessful login attempts.
- Access to shared drives will be restricted to active employees and pre-authorized individuals on a "need to know" basis within the Company through password-protected logins to the network.
- Encryption technology will be employed for data transmissions across public networks and on portable media devices.
- System backups will reside either in secure facilities at the Company or in secure storage provided by a third party specializing in secure information management.
- All end-station computers will use state of the art antivirus software that is regularly updated.
- Operating System security patches will be applied to all systems on a regular basis.
- Employees will be trained on the requirements to protect personal information.
- Reasonably designed to protect personally identifiable information.

The Company further attests that should a breach occur, management will promptly take action to secure information, mitigate the breach, and notify, on a timely basis, any customers whose personally identifiable information could have been compromised.

8.0 CONTINGENCY FUNDS

The Board shall Endeavor at all times to maintain liquid or nearly liquid assets of between USD 50,000 to USD 100,000 to cover for any contingencies or mass redemptions from investors. The shareholder shall have access to the Contingent fund which will only be used if the company runs into financial difficulties

9.0 GOING CONCERN

Should management determine the company to not be a going concern, they must immediately determine whether to put the company under administration or liquidate it. There are certain rules and regulations surrounding company liquidation, many of which focus on the actions as a director. Once a company becomes insolvent, the directors will put creditor interests first by ceasing to trade and safeguarding its assets, with little or no consideration for shareholders, members or directors.

The Board will call in a professional insolvency practitioner to help to avoid inadvertent wrongful business operations. Once liquidation gets underway, all directors will lose control over the company and its assets. In observing their roles and responsibilities during this process the directors shall:

1. Directors to cease operation	The directors shall cease operation as soon as it is clear that the company is insolvent. This is a non-negotiable action which, aimed at limiting damage to the company and shall help prevent of wrongful operations under the relevant legislation pertaining to insolvency.
2. No new borrowing	No new borrowing should be taken on by the company once insolvency is apparent. Additionally, assets must be secured prior to sale by the liquidator.
3. Directors to call Shareholder and creditor meetings	Directors call a meeting of shareholders, during which they need to agree to a 'winding up resolution'. This effectively leads to the closure of the company. Within two weeks of passing the resolution a meeting of creditors will be called, during which directors
	must answer questions relating to the company's situation. A Statement of Affairs will be presented at this meeting, describing the financial position.
4. Appoint a liquidator/administrator	It is at this stage that directors will appoint a liquidator as per the relevant law.
5. Surrender company control	Deliver all business records, paperwork and assets to the liquidator.
6. Directors' loan accounts	Repay any company loans due from directors
7. Cooperate with liquidator/ administrator/receiver	Give the new management cooperation with providing required information and explanations to help secure the interests of customers, investors and creditors.

10.0 RISK ASSESSMENT AND RISK MITIGATION

During the course of its activities the Company may face various external risks which may have a certain effect on some or all of the critical functions; potential hazards of such risks may influence the functioning of the Company in general.

Although the origins and existence of such risks may lie outside the reasonable expectations and, therefore, they may not be treated as completely unavoidable, the company has concentrated on detection of such risks, assessment of their quantitative and qualitative impacts and implementation of measures aimed at mitigation of their negative effect.

The Risk Analysis Policy reviews the possible risk factors, possible impact of hazards and the likelihood and degree of impact of these events and the means of mitigation of these risks which is provided in the annexure.. However, in case the procedures for risk mitigation would not be sufficient for elimination of a certain risk factor consequences, the Company is capable of using additional means of decrease of hazards impact.

It must be noted that it is impossible to eliminate all of the existing risks, therefore the Company has developed different approaches to the risk consequences basing on the grade of underlying risks - some cases prescribe an immediate action on the side of the Company, while other cases might be tolerated in absence of instantaneous remedial measures.

Each risk factor is assigned a grade on the basis of the factors of its likelihood and impact:

1 = HIGH Likelihood and HIGH Impact;

2 = LOW (or MEDIUM) Likelihood and HIGH Impact;

3 = HIGH Likelihood and LOW (or MEDIUM) Impact; and

4 = LOW (or MEDIUM) Likelihood and LOW (or MEDIUM) Impact.

The analysis shows that currently the Company, in general, does not face the high risks (*grade 1 and 2*), and it has in place the necessary procedures for mitigation of the risk hazards that may happen.

10.1 RISK MITIGATION MEASURES

The Company has addressed the possible risk hazards and has implemented the risk mitigation facilities providing that the additional measures might be put in place in the event of the emergency. Depending on the covered critical functions, the existing risk mitigation measures could be grouped as follows:

Technical Measures addressing the operation of computer hardware and software and performance of business communications:

- In case of any disruption of functioning of Company's servers, the switching to reserve facilities takes place automatically and immediately.

The reserve servers are situated in a location different from the business premises of the Company. In addition, the Company maintains cloud servers to safeguard continuity and maintenance of data. Switching back to the main servers is affected automatically upon the resumption of their functioning:

a) Recovery of data that might be lost or corrupted is affected within the business day of the event that might lead to such loss or corruption;
b) There is a duplicate backup server which is situated in a location different from the business premises of the Company; We will clarify the location to the Authority Asap.
c) Remote access to the business software and hardware of the Company by the members of its staff might be established from any location;
d) Remote access to the software might be established from any personal computer, including the home personal computers of the Employees and Officers of the Company;
e) In case of unavailability of business premises, fully operational functioning of the Company might be established from the home premises of one of the members of the Board within one (1) business day and without any significant interruption of the Company's activities;
f) In case of any disruption to the functioning of the telephone lines, the switching to reserve dedicated telephone lines takes place automatically;
g) In case of any significant disruptions, the relevant employees of the Company shall use the alternative means for communication with its customers, counterparties and the GCB, including the mobile devices, laptop computers, remote access to the corporate electronic mail using any available internet connections, public and/ or commercial telephone and internet facilities.

Administrative Measures Addressing the Performance of the Members of Staff:

a) In case of unavailability of any member or members of staff their functions may be performed by any of the Executive Directors of the Company or by the members of the Board; the specific provisions for replacement of employees are stated in the Employees Replacement Policy;
b) Following the procedures stated in the Company's Internal Operational Manual, the functions of unavailable employees might be performed by other members of staff;
c) In case of such unavailability the Management of the Company takes the decision on its seriousness and possible duration, considering all relevant circumstances;
d) Where deemed applicable, in case of continuing unavailability of the Employee or the Officer, the Management of the Company might initiate the search for substitute, additional and/ or

new employees following the procedures determined by the GCB and informing it accordingly without delays.

Where the existing measures might be not valuable enough for the sufficient mitigation of hazard effect in the particular event of an emergency, the Company may use other available measures, including the applying for assistance to other members of business community and to competent supervisory authorities.

11.0 EMERGENCY RECOVERY PLANS

The Company must always remain flexible reacting to the external and internal events, therefore it has developed a list of steps, which might be appropriate in case an emergency occurs.

One of the most useful tools in determining of the priorities of actions and decision making upon the possible emergency is the following Priority List of critical functions, which is formulated on the basis of the above assessments. This List is designed for immediate addressing of the critical function which must be resumed in a first place.

Table 1.0: Priority List of Critical Functions

PRIORITY	CRITICAL FUNCTION
1.	Ability by the key Officers and Employees to perform their functions
2.	Access to the business premises by the staff members
3.	Ability to organize the effective Information Technology Team
4.	Functioning of the personal computers of Officers and Employees
5.	Operation of servers
6.	Functioning of data storage and backup facilities
7.	Operation of electronic mail and internet connections and other data exchange means
8.	Functioning of telephone and facsimile lines
9.	Operation of remote access facilities
10.	Operation of business software
11.	Access to the Company’s payment methods, including bank accounts

The steps that might be undertaken by the Company in emergency cases are the following:

I. Where necessary, immediate contacts with emergency services;
II. Identification of damage;
III. Identification of disrupted critical functions;
IV. Assembling of the Information Technology Team;
V. Provision of information to Officers and Employees regarding the situation;
VI. Decision on the course of actions;
VII. Communication of this decision to the members of staff and parties concerned;
VIII. Provision of public information;
IX. Maintenance of the log of events and of the actions taken;
X. Calling of a general meeting of staff of the Company for analysis of the situation;
XI. Where necessary, the revision of the Policy;
XII. Organization and update of the Key Contacts list that is used in the emergency event.

12.0 TESTING

In order to assess the effectiveness of the Plan, the soundness of the relevant procedures must be tested and verified, which is achieved by the following:

a) Each Officer and Employee of the company is familiarized with the Policy, which is attested by his/her signature on the Documents Distribution List;
b) Each member of staff is welcome to express his recommendations and remarks in order for the Management to gain the most efficient business continuity procedures;
c) The Company convenes, on a regular basis, tests of the emergency procedures acting on a different scenario; and
d) Basing on the result of each test, the Management of the Company and the Information Technology Team analyze the procedures and the Policy in order to address any possible deficiencies.

It must be stressed that Plan is a recurring process, which assumes the realization of practical steps, the main of which are stated in the current Policy. In order for this Plan to be up to date and effective on a continuous basis, the Management of the company performs, at least annually, its periodical reviews basing on the results of the business continuity tests, input from Officers and

Employees of the company, changes in the business and organizational environment and other applicable considerations.

APPENDIX 1 TO THE POLICY

BUSINESS IMPACT ANALYSIS

CRITICAL FUNCTION	OPERATION OF COMPUTER HARDWARE AND SOFTWARE / PERFORMANCE OF BUSINESS COMMUNICATIONS

RECOVERY RESOURCE REQUIREMENTS

DURATION OF DISRUPTION	NUMBER OF STAFF	POSSIBILITY OF RELOCATION	REQUIRED RESOURCES
1 HOUR	1	Not practicable	▪ Contacts with IT service providers
1 – 6 HOURS	2	Not practicable	▪ Contacts with IT service providers
6 HOURS – 1 DAY	2	Possible	▪ Contacts with IT service providers ▪ Establishment of remote access facilities ▪ Relocation of business to other premises (home premises of one of the Directors)
1 DAY – 1 WEEK	4	Possible	▪ Contacts with IT service providers ▪ Establishment of remote access facilities

			▪ Use of alternative means of communication (mobile telephones, paper documents, external internet facilities)
1 WEEK – 1 MONTH	4	Possible	▪ Assistance of partners
MORE THAN 1 MONTH	4	Possible	▪ Establishment of the new operational framework

APPENDIX 2 TO THE POLICY

BUSINESS IMPACT ANALYSIS

CRITICAL FUNCTION	**PERFORMANCE OF THE MEMBERS OF STAFF**

RECOVERY RESOURCE REQUIREMENTS

DURATION OF DISRUPTION	**NUMBER OF STAFF**	**POSSIBILITY OF RELOCATION**	**REQUIRED RESOURCES**
1 HOUR	1	Possible	▪ Substitution of unavailable members of staff
1 – 6 HOURS	1	Possible	Establishment of remote access facilities Substitution of unavailable members of staff
6 HOURS – 1 DAY	2	Possible	▪ Use of alternative means of communication (mobile telephones, paper documents, external internet facilities)
1 DAY – 1 WEEK	3	Possible	Relocation of business to other premises (home premises of one of the Directors) Additional personnel
1 WEEK – 1 MONTH	4	Possible	▪ Assistance of partners
MORE THAN 1 MONTH	4	Possible	▪ Establishment of the new operational framework

APPENDIX 3 TO THE POLICY

RISK ANALYSIS

POTENTIAL HAZARD	**HAZARD EFFECT**	**LIKELIHOOD**	**IMPACT**	**RISK GRADE**	**MEANS OF MITIGATION IN PLACE**	**POSSIBLE MEANS MITIGATION (WHERE APPLICABLE)**	**RISK GRADE AFTER MITIGATION**
Earthquake	Inability to access premises Possible injuries to members of staff Possible loss of data Time and other resources required for recovery Time and other resources to organize remote access Significant financial losses	MEDIUM	HIGH	**2**	Immediate automatic switching of servers to the backup facilities Immediate automatic switching to reserve telephone lines Automatic data recovery Remote access to the business hardware and software from any location Use of non-office personal computers	Applying for assistance to other companies Possible use of alternative means of communication	**3**

Fire / Flood	Inability to access premises Possible loss of data Time and other resources to organize remote access Significant financial losses	LOW	HIGH	**2**	Immediate automatic switching of servers to the backup facilities Immediate automatic switching to reserve telephone lines Automatic data recovery Remote access to the business hardware and software from any location Use of non-office personal computers	Applying for assistance to other companies Possible use of alternative means of communication	**3**
Collapsing of Office Building	inability to access premises possible loss of data Significant financial losses	LOW	HIGH	**2**	Immediate automatic switching of servers to the backup facilities Immediate automatic switching to reserve telephone lines Automatic data recovery Remote access to the business hardware and software from any location Use of non-office personal computers	Applying for assistance to other companies Possible use of alternative means of communication	**3**

Unavailabilit y of Premises	Significant time losses	LOW	LOW	**4**	Remote access to the business hardware and software from any location Use of non-office personal computers	Applying for assistance to other companies Possible use of alternative means of communication	**4**
Electricity Failure	Losses of time and resources	MEDIUM	MEDIUM	**4**	Immediate automatic switching of servers to the backup facilities Immediate automatic switching to reserve telephone lines Automatic data recovery	Possible use of alternative means of communication	**4**
Failure of Internet Service Provider	Losses of time and resources	HIGH	MEDIUM	**3**	Remote access to the business hardware and software from any location Use of non-office personal computers Possible use of alternative means of communication		**3**
POTENTIAL HAZARD	**HAZARD EFFECT**	**LIKELIH OOD**	**IMPACT**	**RISK GRADE**	**MEANS OF MITIGATION IN PLACE**	**POSSIBLE MEANS MITIGATION**	**RISK GRADE AFTER**

						(WHERE APPLICABLE)	MITIGATIO N
Computers Malfunction	Losses of time and resources	LOW	HIGH	**2**	Remote access to the business hardware and software from any location Use of non-office personal computers Highly qualified and reliable IT providers		**3**
Data Loss or Corruption	Losses of time and resources	LOW	HIGH	**2**	Immediate automatic switching of servers to the backup facilities Automatic data recovery Highly qualified and reliable IT providers		**3**

Unauthorized Data Access	Losses of time and resources	LOW	LOW	**4**	Immediate automatic switching of servers to the backup facilities Automatic data recovery Use of non-office personal computers Highly qualified and reliable IT providers		**4**
Legal Sanctions	Reputation losses Possible financial sanctions Possible suspension or withdrawal of license	LOW	HIGH	**2**	Highly qualified staff Long-standing reputation Up to date analysis of legislative requirements on a continuous basis Sufficient resources for maintaining compliance	Hiring of additional personnel	**3**
Non-Availability of Personnel	Time and resources required to organize remote access Possible financial losses	MEDIUM	MEDIUM	**4**	Performance of functions by the Executive Directors and members of the Board Performance of functions by other employees Search for and hiring of new personnel		**4**