GND Advisory

BUSINESS CONTINUITY PLAN

Approved by:	GND Advisory Management
Updated on:	July 2021
References to external policies:	Principles for the Sound Management of Operational Risk European Securities and Markets Authority (ESMA) Guidance Luxembourg's Financial Sector Supervisory Authority (CSSF) Guidance
References to internal policies:	Business Code of Conduct Risk and Compliance Policy Operational Risk Management Plan

Contents

1. The Firm

GND Advisory is an autonomous investment advisory firm registered in the Republic of Lithuania. The records of GND Advisory are kept at the State Enterprise Centre of Registers.[1] GND Advisory ("GND") and each of its majority-owned subsidiaries (together with GND, the "Firm") conducts its operations in compliance with the EU and Lithuanian Law, Regulations, and its internal Code of Conduct.

2. General provisions

Operational Resilience is a high priority for GND. Our goal is to ensure our continued ability to serve our clients and to protect their assets as well as protecting the people and assets of our firm. Our Business Resilience Program (“program”) has been developed to provide reasonable assurance of business continuity in the event there are disruptions of normal operations, and continues to evolve the concepts of Operational Resilience.

The Firm has established a global, structured approach to ensure that the firm is prepared in the event of an operational disruption. Our business resilience plans address operational disruptions of varying scope, including, but not limited to, GND-only disruptions, medium to large scale events involving the disruption of operations which may include displaced personnel or a significant reduction in our workforce due to illness, injury or death, and disruptions to critical third parties that the firm depends on. Operational disruptions caused by cyber-security incidents impacting the confidentiality, availability, or integrity of our systems and the systems of critical third parties are also in scope. Non-GND specific disruption such as a pandemic is also contemplated.

Our plans include resilience capabilities that leverage our global resources and infrastructure which include but are not limited to relocating impacted business operations using designated and tested business recovery solutions. The Firm has the ability to enable staff to operate from non-GND premises, including their homes, through the use of secure remote access solutions should an incident occur which requires personnel to be dispersed. Our resilience capabilities also include the ability to replicate critical data and applications between geographically dispersed data centers. For example, if a local storm were to render one or more of our facilities inoperable, we could perform critical functions at another GND office with minimal disruption, alternatively staff can also work from home as necessary. If a problem occurred in one of our data centers, effectively shutting down our servers, we could carry on processing from another GND data center with minimal loss of data.

As part of our regular on-going maintenance, we periodically test systems and process failover capabilities, and test staff’s ability to operate from designated sites as well as non-GND premises, including their homes through secure remote access solutions.

No contingency plan can be failsafe or provide absolute assurance that an interruption in business will not occur or that negative consequences will not ensue from a crisis or an event. Because natural and other disruptions — even if anticipated — generally are unpredictable and can change over time, no plan when originally designed or even if later modified can anticipate every contingency or need. That said, GND is committed to ensuring that its program is comprehensive and up-to-date, particularly as new information, techniques, and technologies become available. We may alter, add to, or eliminate specific aspects of the program as we deem appropriate for the protection of all concerned and we will keep both our clients and our own community informed of material changes.

In the event of a crisis or disaster, the Firm will convene to assess the impact of the crisis. Based on this assessment, the GND Representative Donatas DITKUS, or his authority, has the delegated authority to activate the GND Advisory Business Continuity Plan. In the case where the GND Representative is unreachable due to the crisis, the plan should be activated by the next officer-in-charge next according to the order of succession.

[1] State Enterprise Centre of Registers. https://www.registrucentras.lt/jar/index_en.php

This plan follows an all-hazards approach, including all risk reflected in the *Risk Management Plan*[2]. This document outlines the general procedures to be taken by the GND Representative in the event of a serious business disruption affecting the operation of key functions.

This Business Continuity Plan is the property of GND. It is an operational document that is constantly being monitored and updated to reflect our on-going business operation.

3. Business continuity management process

GND Partners has created the following Business Continuity and Disaster Recovery process to ensure the business continuity:

a. Business impact assessment to identify business critical processes
b. Requirements for Business Continuity and Disaster Recovery Plans
c. Testing, assurance and continuous improvement of Business Continuity and Disaster Recovery Plans

3.1. Business impact assessment to identify business critical processes

Business impact assessment is a process to identify business critical processes of GND Partners and allow to identify and priority the order of steps that need to be taken during a disruption that are to be included in the Business continuity and Disaster Recovery plans.

The business impact assessment process consists of the following:

a. The identification of business-critical processes
b. The identification of activities that are critical for each of the business-critical processes
c. The identification of required human resources, facilities, data and information, hardware and software, as well as any third-party dependencies that are critical for continuity of each business-critical process
d. Defining the Maximum, tolerable period of disruption (MTPD), Recovery time objective (RTO) and recovery point objective (RPO) that must be used when determining sequential steps in the Business Continuity and Disaster Recovery plans.

Appendix 2 provides a template for identifying and specifying business critical processes.

3.2. Requirements for Business Continuity

Business Continuity focuses on protecting client assets and assuring that the firm is able to continue business operations in the event of an operational disruption.

Central to the Firm's business recovery efforts is a requirement that GND develop, test, and maintains plans that document its recovery requirements for its core functions. As part of this plan, GND identifies critical risks and puts in place the appropriate level of business controls and functionality necessary to mitigate those risks. The resultant *Risk Management Plan*[2] document the functional requirements — equipment, applications, vital records and regulatory reports, Business Recovery Solutions, and recovery teams and tasks, along with third party dependencies — needed to re-establish essential business operations while accounting for any applicable regulatory restrictions. The plan also assesses the impact of an operational disruption on the firm's business constituents, banks, and counterparties.

[2] Risk Management Plan. https://www.gndpartners.com/doc/gnd-risk-management-plan.pdf

3.3. Testing, assurance, and process improvement

Assurance focuses on the regular verification of the effectiveness of our Business Continuity preparedness, including testing of our Technology Resilience and Business Recovery Solutions required to demonstrate the ability to meet business recovery requirements during an actual operational disruption event.

Technology Resilience Assurance is conducted through actual failover tests, and equivalent means, based on their criticality to the businesses that depend on them, to ensure the resilience of applications and infrastructure meets the documented requirements.

Business Recovery Solutions Assurance is conducted through regular testing of each solution depending on the criticality of the business functions. This includes:

- Ensuring critical staff can effectively perform their functions from non-GND premises such as their home through testing their Remote Working Environment;
- Confirming the ability to support business operations through transfer of critical functions to staff at other principal sites of GND.

Compliance with Assurance requirements is tracked and significant issues escalated to management. As of the date of this statement, Assurance requirements for the last fiscal year including testing of Technology Resilience as well as Business Recovery Solutions have been fulfilled with no significant issues outstanding.

For critical third parties that the firm depends on, resilience assessments are conducted on the third parties' business continuity practices.

Process Improvement assesses our state of readiness for foreseeable operational disruptions taking into account internal and external changes that impact Business Resilience. This includes:

- Consideration of any significant issues or gaps identified during testing activities;
- Continual reassessment of risks due to the changing environment and their potential impact to the Firm's resilience posture;
- Identification of changes to GND business operations that may affect Business Resilience requirements;
- Introduction of new strategies and technologies that become available.

This plan should be tested on annual basis and revised accordingly to reflect the changes in the operational environment. The results of these assessments enable us to identify and integrate new risk scenarios into the program as well as drive enhancements to our Technology Resilience and Business Recovery Solutions when needed. Copies of test results and the revised BCP should be shared with the Business Continuity Management Specialist in the HQ <info@gndpartners.com> for corporate records.

4. Business Continuity Planning

Each business area is responsible for preparing a comprehensive Business Continuity Plans that include all Business-Critical processes. Owners of third-party relationships shall ensure there is a Business Continuity Plan covering third party services or products provided to GND Advisory if a such are included in the Business-Critical processes.

Each Business Continuity Plan must be documented using the designed Business Continuity Plan template, which include the following:

a. Roles, responsibilities and contact details of a person holding an authority during a disruptive event
b. Process for activation the Business Continuity Plans
c. Human and technological and other resources needed to recover, main and resume business continuity
d. Dependencies on third party services or products
e. Contact details of suppliers and vendors holding a responsibility during disruptive event, incl. alternative service providers

f. A list of essential data and other information, their storage location and access details relevant for business continuity
g. Devolution process

5. Roles and Responsibilities

Upon receiving notice of BCP activation, all BCP team members, or if they are unavailable, their alternates (see list in Other annexes) should shift to prioritise the implementation of the critical functions assigned to them in this plan.

The GND Representative Donatas DITKUS <donatas@gndpartner.com> or alternate will be responsible for:

- Convening and leading the BCP team;
- Directing GND crisis response;
- Representing GND in the meetings with clients and partners;
- Ensuring the availability of access, and records for maintaining those functions/processes;
- Securing the necessary resources for maintaining those functions/processes;
- Liaising with the devolution as needed;
- Ensuring alternate working arrangements are in place should the office be inaccessible or crisis requires change in current office usage;
- Ensuring that adequate arrangements are in place to provide counselling and other support to staff and dependents affected by an incident;
- Ensuring the smooth transition to normal operations when the BCP is deactivated.

All staff not activated as part of the BCP team should remain on standby and refrain from using the corporate system (office, email, communication) until instructed otherwise to reduce the burden on these systems during the emergency.

6. Plan activation

In the event of a crisis or disaster, the GND Advisory team will convene to assess the impact of the crisis. Based on this assessment, the GND Representative, or his/ delegated authority, has the authority to activate the GND Business Continuity Plan. In the case where the GND Representative is unreachable due to the crisis, the plan should be activated by the next officer-in-charge next according to the order of succession.

Activation of BCP should be informed to the following distribution list:

- Business Continuity Management Specialist in the HQ <info@gndpartners.com>;
- Director of the Firm <Donatas DITKUS, donatas@gndpartners.com>;

Once the crisis is over or considered under control, the GND Representative, or his/ delegated authority can deactivate the Business Continuity Plan. Deactivation should be informed to the same distribution list above.

7. Technology resilience

Technology Resilience focuses on restoration of the Firm's core infrastructure, including networking, applications, market-data feeds, and other shared technologies to ensure the continuation of critical business systems processing. Applications must be classified depending on the criticality of the business operations they support, and their Recovery Time Objective (RTO) must be defined to document their recovery expectations. Applications are then prioritized based on their classification which drives the frequency of application testing.

Wherever practicable, GND separates the people conducting business from the technology infrastructure supporting the business, housing them in separate buildings in order to reduce the likelihood of simultaneous personnel and systems disruptions.

8. Business resilience capabilities

Business Recovery Solutions focus on ensuring that our business operations can quickly resume when the primary workplace hosting those operations becomes inoperable or is inaccessible.

Functional Transfer arrangements are in place as a further safeguard, depending on the kind and extent of the operational disruption, and subject to any local regulatory restrictions, allowing many critical functions to be performed by personnel at other principal sites of GND.

Remote Working Environment capabilities have been developed so that the firm is able to support critical functions by enabling designated staff to work from their homes, or from other non-GND premises through secure remote access connections.

9. Third party suppliers and vendors

This section identifies suppliers and vendors that are included in the Critical Business processes to be contracted during disruptive event as well as alternate suppliers. List is available on the Firm's intranet.

#	Name of the supplier/ vendor and reg. number	Service(s) or product(s) provided for GND Advisory	Contact person	Contact details
1				
2				

10. Data needs, storage location and accesses

These sections identified and described data requirements for Critical Business processes, in which systems and data storages it is placed and what are the needed accesses. List is available on the Firm's intranet.

#	Critical Business Process	Data requirements for Business Continuity	Storage location	Accesses needed
1				
2				

11. Devolution

In the case where it is not possible to maintain some or all critical functions/processes, these functions/processes should be devolved to a pre-agreed alternative office. The critical staff should ensure, prior to the crisis, that the devolution office has the necessary, access, record/data, knowledge and skill to perform the functions/processes requested.

Devolution can be activated in 2 ways:

- Request-based activation

In the event of cataclysmic incident that render the office unable to run the critical functions/processes, the GND Advisory Director or alternate has the authority to request the devolution office to take over the functions/processes;

- Automatic activation

Upon receiving the news of cataclysmic event in a GND location, the head of devolution office should inquire the Firm about the continuity of critical function. If due to the nature of the crisis, the Firm is not reachable, the devolution of functions/and process should be in effect immediately until further notice is received from the GND. In this case, the devolution office should inform the HQ about this activation.

11. Training and Awareness

Employee groups shall receive a training about Business Continuity Plan at GND Advisory according to the relevance and their roles and responsibilities within those plans.

12. Approval

I have read, accept and fully understand the responsibilities detailed under this Business Continuity Plan (BCP) and its annexes. I approve this plan.

Donatas DITKUS
GND Advisory Representative

ANNEXES

Standard Annexes:

1. Risk Management Plan [https://www.gndpartners.com/doc/gnd-risk-management-plan.pdf].
2. Business Critical Processes and their Business Continuity Plans.

Activity x: TBA			
Possibility to work remotely (yes/no)	Number of FTEs needed for this activity	Minimum number of FTEs needed for this activity	Systems needed to run the activity
Yes			
1. Virus prevention plan			
- Working remotely possible and it has been successfully tested. - All FTEs have the required hardware, software and accesses.			
2. Action plan in case of 20% reduction in total FTE capacity			
- Reduced scope -			
3. Action plan in case of 50% reduction in total FTE capacity			
- Reduced scope - Replacement by other employees			
4. Additional actions or decisions needed to execute the plan			
- E.g. additional accesses needed for replacements			

Other Annexes:

1. List of the Firm Key Contacts [available on the Firm’s intranet];
2. Other Critical Contact Lists (Key Vendors, Partners etc) [available on the Firm’s intranet].