GEORGIAN NATIONAL UNIVERSITY SEU

BUSINESS CONTINUITY AND RISK MANAGEMENT PLAN

2020
TBILISI

Preface

The continuation of the operations of the Georgian National University (SEU) is a paramount priority in all situation. Under normal circumstances, SEU is managed and operated according to its main procedures. It is, however, essential that also risk and mitigation plans and procedures exist for any unforeseen events that pose challenges to the normal operations or might put these at jeopardy.

SEU uses innovative and flexible approaches to respond to different needs and demands of its internal and external environment, anticipating trends and focusing on quality improvement.

SEU continually invests in the development of infrastructure, introduces new processes and improves the effectiveness and quality of traditional processes to increase resilience and capacities for qualified responses in various situations and ensure that business operations continue as usual.

Purpose

SEU has established a plan to ensure business continuity of its major business processes in case of unforeseen events and unfortunate events.

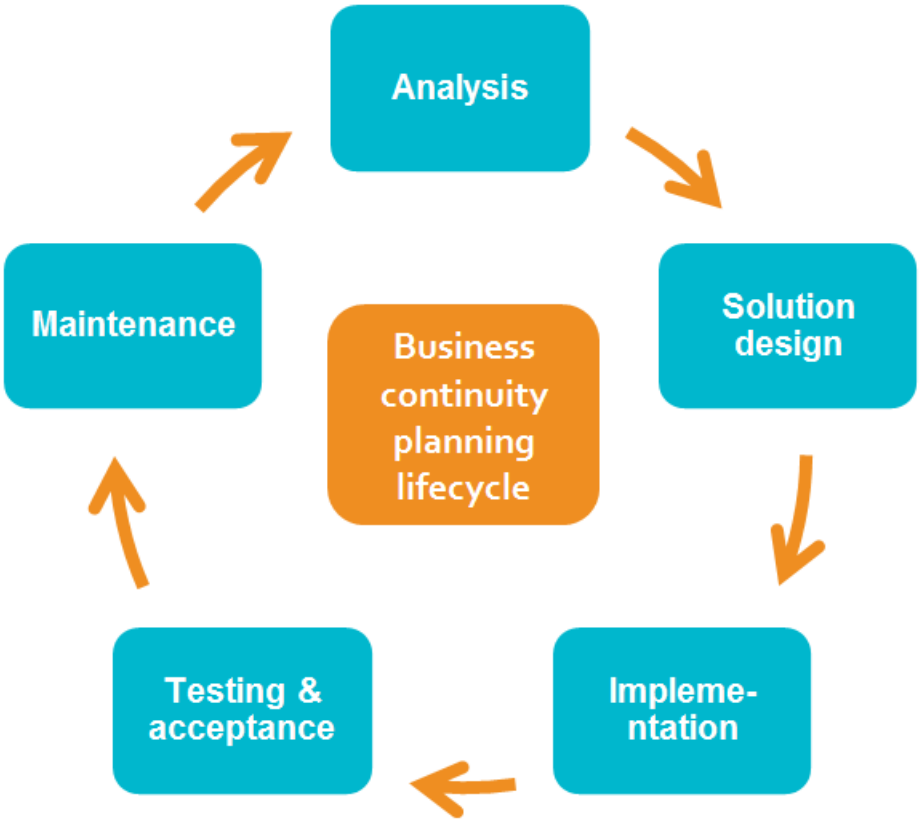
The Business Continuity Plan is a tool to assist in preparing for unforeseen situations that could leave resources such as personnel, records, information, housing and physical facilities unavailable for both short term or extended periods.

The plan prepares SEU to deal with threats and other events that can disrupt its business and impact its operations negatively.

The plan takes into account the SEU internal capacities and external factors, possible risks, mechanisms for their prevention and mitigation, including incident management, IT disaster recovery and crisis management.

Business continuity planning process

SEU Business Continuity planning follows lifecycle developed and applied at the leading institutions, companies and organizations worldwide and consists of five phases:



This 5-step approach in business continuity planning enables SEU to prevent and minimise the effect of disruptions on its staff, students, key stakeholders and general public, and to maintain the SEU's reputation. Finally, it assists SEU to categorize incidents and quickly evaluate their criticality, determine appropriate response procedures, and assign response team members, workflow and resolution of various incidents before they disrupt our business.

Phase I – **Analysis**

Analysis is the pillar of effective institutional resilience and transformation within the scope of Business Continuity Plan. Its aim is to identify critical business processes and analyse their business impact. At SEU, the analysis is performed once a year, and includes inputs from self-evaluation of academic-related processes and contents, and about progress regarding implementation of strategic priorities and action lines, including advancement of already operational processes, as well as development and implementation of new ones.

Phase II - **Solution design**

Solution design has to be embedded within the conclusions of the Phase I - *Analysis*. It is a plan how to mitigate the perceived impact of disruption of critical business processes. Planning is an essential pre-requisite for introduction of new processes and enhancement of the existing ones. It defines the

recovery time objective (RTO) for each process, which is the time period in which the critical business process must be restored before the impact of the interruption becomes intolerable.

Solutions at SEU are tailor-made according to the institutional specificities. These solutions are mainly developed by institutional management, academic staff and in-house IT developers that are fully involved in the Analysis phase and preparatory consultations and decision-making process.

Phase III - **Implementation**

Implementation of the plan is the third business continuity planning lifecycle phase. Implementation activities include all preparatory tasks which are necessary for testing and acceptance of new solutions, starting from the identification and description of specific resources needed for each process, both internally and externally. Throughout the implementation phase it is possible to do fine tuning of designed solutions (and potentially adapt list of IT infrastructure procurement in case next generation equipment is available and required to support the designed solutions).

Phase IV - **Testing and acceptance**

Testing and acceptance enable exercising of the designed solutions and assessment whether their impact improves the resilience of the operations, as well as continuity, quality and stability of services and processes. In this phase the strategies and mitigation measures to restore critical processes within the RTO are tested. In addition, testing and acceptance phase is used for adjustments to the new solutions in case the end user and/or customer proposes upgrades.

Phase V – **Maintenance**

Maintenance is the final phase of the business continuity planning lifecycle. Regular refinement and maintenance of collected plans and data how to proceed in case of disruption enable sustainable operation of the critical processes.

The final outcome of this process is the Business Continuity Plan, which is annually reviewed and updated accordingly, following the same 5-step process.

Role of IT services in SEU Business Continuity Plan

SEU takes all reasonable steps to ensure that in the event of a major incident, critical activities will be maintained, and normal services resumed as soon as possible. The top priority is to ensure the safety of the people and the security of the work environment. IT services are recognised as one of the main pillars to prevent operations disruptions and to shorten the time to recover during and after emergencies and disasters. IT services provide consistent, coordinated and automated approach to risk assessment, documenting and testing recovery plans, while they also automate the process of

activating business continuity, disaster recovery and crisis plans to facilitate a coordinated and aligned response to crisis events. Therefore, SEU invests in IT infrastructure and processes to ensure:

1. Neutralising all types of errors;
2. Increasing quality of services;
3. Improvement of customer satisfaction;
4. Decreasing of deadweight losses;
5. Automatization of all standardised and routine tasks.

New IT solutions have been applied in following departments:

1. Student Service – all services are digitalized;
2. Career Development – all services are digitalized;
3. Library – all services are digitalized;
4. Research – collection and classification of research results;
5. Academic affairs:
   a) Organization of the education process;
   b) Exams;
   c) ECTS verification; and
   d) Online and distance learning.
6. Quality Enhancement – evaluation of the education quality and quality of all support services;
7. Finance – financial management and accounting.

Business Continuity Plan Implementation

The Business Continuity Plan is primarily addressed to the Business Continuity Management Group (BCMG). They have the responsibility of preparing for, responding to, and recovering from any event that affects SEU's ability to perform its mission. However, the Plan extends to all SEU activities and operations.

The BCMG consists of seven members – The Rector and the Vice-Rector for Finance and Resources are ex-officio members of the BCMG and the Rector elects additional three members of the BCMG:

- Two representatives of administration;
- One SEU IT developer;

The BCMG annually reviews the Business Continuity Plan and proposes updates and relevant adjustments in light of new findings. The BCMG prepares an annual report by February 15th of the following year, including implemented activities and, as required, policy options and, investment alternatives based on comprehensive analyses.

Rector approves the Report and updated Business Continuity Plan.

Type of risks that could disrupt normal operations

The Business Continuity planning processes are an integrated approach to risk management. Risk management enables organization to understand the full range of its risk exposure, including the likelihood that a risk event may occur, the reasons it may occur, and the potential severity of its impact. It also helps organizations prioritize risks, map them to the applicable risk owners, and effectively allocate resources to their mitigation and prevention, if possible.

Below are listed mapped risks that may occur in academic environment, which are classified in regard to areas of university operations they might affect:

- Academic risks:
    - teaching (insufficient number of teaching staff; low competence level of teaching staff; lack of teaching resources; improper testing methods; decline in entry grades of students, etc.);
    - research (lack of relevant equipment; low innovation capacity; inadequate IT support and services; lack of research competences; insufficient number of research staff; low relevance of research findings; unpublished results, etc);
    - quality (low level of student satisfaction; pressure for higher grades which dictates easier exams; low employability rate of graduates; significant fall of the institution's ranking in a major ranking system; loss of accreditation and licence for work, etc.);
- Financial risks – insufficient funds for teaching, research, maintenance and development; incomes suspensions; insufficient enrolment and tuition payments; accounting errors; downturn in revenue; bankruptcy;
- Operational risks – legal issues, lack of leadership; vague management procedures; lack of effective management structure; lack of monitoring and feedback; unclear allocation of tasks and responsibilities; insufficient resources (classrooms, laboratories, equipment, knowledge); human errors, technical errors and glitches (slowdown, connectivity issues, system crashes, incorrect calculation, etc);
- Compliance risks – legal penalties; threats to workplace, employees' and students' health and safety; security threats; negligence of social responsibility; corruption;
- Reputational risks – decline in overall reputation; decline in reputable rankings; bad PR; lack of trust from stakeholders;
- Strategic risks – declining admission standards/progression rates; insufficient enrolment of students; lack of transparency in academic promotion policies; governance issues; lack of academic autonomy; emerging competitors.

Critical functions and major disruptions

Not all risks have the same probability rate, nor they affect all business functions equally. Majority of the risks listed above may affect quality of operations, timely delivery of outputs, success rate on the market, customer satisfaction level, etc. but generally they will not, if occur, jeopardise the entire business operation or organization, causing significant financial loss, serious injury or even loss of life. On the other hand, there are some risks, which might cause major or disastrous disruption of business by affecting its critical functions. Therefore, in order to be able to plan, prevent and manage continuity of its business, SEU has identified its critical functions:

- Conducting classes
- Conducting research and scientific publishing
- Keeping academic records and student evidence
- Payroll processing
- B2B payments
- Incomes and revenues management

Following these, SEU identified major risks that, if they occur, may fundamentally impact its critical functions. They are listed below and classified in three main groups:

- Communications:
    - IT failure – digital transformation increases the risk to experience a significant business disruption due to a cyber-attack, cloud outage or other technological glitches;
    - Data loss and data corruption (destroyed information by failures or neglect in storage, transmission, or processing);
    - Data theft (unauthorised access to obtain private and sensitive information, e.g. staff evaluation files)
    - Data hacking (unauthorised access to alter private and sensitive information, e.g. student records)
- Physical infrastructure (estate and IT hardware):
    - Natural and man-made disasters (e.g. flood, fire, earthquake, epidemic, war/civil disorder etc.) – damage of premises, loss of systems;
    - Utility failure (e.g. power outage, light failure, pluming and water leak, natural gas leak) – denial of access to premises;
- Human resources:
    - Loss of personnel (departure, voluntary or otherwise, of key-personnel) – loss of knowledge, reputation, capacities);
    - Security threat (terrorism, theft of vital information and material, lack of proper security controls, outdated policies).

The following table presents the above listed major risks with the assessment of their expected impact level, the areas of SEU operations which might be affected and the critical functions which are expected to be disturbed if these risks occur.

Major risks	Impact	Areas of university operations affected	Critical functions affected
Communications			
IT failure	Major	Academic (teaching and research); Operational (management, allocation of task and resources); Financial (accounting errors)	Conducting classes; Conducting research and scientific publishing; Academic records and student contact lists; Payroll processing; B2B payments
Data loss and data corruption	Major	Academic (research); Operational (administration, data management); Financial (accounting and financial management)	Conducting research and scientific publishing; Academic records and student contact lists; Payroll processing; B2B payments; Incomes and revenues management
Data theft	Major	Operational (data management); Financial (problems with payments); Compliance (security threats); Reputational (bad PR, lack of trust)	Academic records and student contact lists; Payroll processing; B2B payments; Incomes and revenues management
Data hacking	Major	Operational (data management); Financial (problems with payments); Compliance (security threats); Reputational (bad PR, lack of trust)	Academic records and student contact lists; Payroll processing; B2B payments; Incomes and revenues management

Physical infrastructure (estate and IT hardware)			
Natural and man-made disasters	Catastrophic	Operational (denied access to resources, data loss); Academic (teaching, research); Reputational (threat to overall reputation), Strategic (decline in critical strategic operations)	Conducting classes; Conducting research and scientific publishing; Academic records and student contact lists; Payroll processing; B2B payments; Incomes and revenues management
Utility failure	Major	Operational (functionality of premises and resources); Compliance (workplace, employees' and students' safety); Academic (teaching and research premises and methods)	Conducting classes; Conducting research and scientific publishing; Payroll processing; B2B payments;
Human resources			
Loss of personnel (key academic and administrative staff)	Major	Strategic (loss of key personnel and competences); Academic (insufficient number of teaching/research staff and expertise); Operational (loss of key administrative staff, delays, lack of knowledge and skills); Reputational (threat to overall reputation, bad PR)	Conducting classes; Conducting research and scientific publishing; Incomes and revenues
Security threats	Major	Operational (access to premises and materials); Compliance (security threat, workplace, employees' and students' safety); Reputational (bas PR, lack of trust)	Conducting classes; Conducting research and publishing; Academic records and student contact lists; Payroll; processing B2B payments; Incomes and revenues management

Business Continuity Plan and mitigation measures

While risk management identifies risks and develops plans for their prevention and mitigation, the business continuity planning addresses the operational responses to critical functions disruption and related major risks.

The plans below are based on the actual needs of SEU and when its critical operations are required to be resumed. At this time in the recovery process the normal functionality, response and capabilities are not available or expected. The table below summarises the SEU Business Continuity Plan. It provides the overview of the functions recognised as "critical", with a brief description of impact their major disruptions will cause (what processes will be jeopardised) and what resources and conditions are directly dependent on and most likely will be affected. Finally, it outlines the mitigation measures, which are the principal outcome of the business continuity planning process, with the expected recovery time.

Critical function	Impact description	Dependencies	Mitigation measures	Recovery Time Objective
Conducting classes	Could jeopardise students' ability to graduate on time and institutional reputation	Available classrooms, power, ability of faculty/staff to work, IT services, working computers, lab, and other equipment	Ensure availability of key personnel; maintain capacities; hold classes online; arrange IT support and schedule; hold classes off campus; arrange transportation for students and faculty to alternate location	< 1 Week
Conducting research and scientific publishing	Could jeopardise implementation of research projects, grant funding, publishing agenda; threat to institutional reputation	Access to critical data, key personnel, working computers, lab	Ensure availability of key personnel; use IT support; access to data; conduct research at off campus facilities; reallocation of tasks and resources	< 1 Week

Academic records and student contact lists	Could jeopardise students' progress; potential loss of contact information of students; threat to institutional reputation	Access to critical data, key administrative personnel, IT services, hard copy records	IT support and services; access to data; regular (weekly) update and backup (both electronic and hard copy)	< 1 Week
Payroll processing	Could jeopardise workforce (loss of personnel, knowledge and capacities)	Available funds and access to data to support payroll, key administrative personnel	Use IT support (secure software, data access); access to data; regular (weekly) update and backup (both electronic and hard copy)	< 1 Week
B2B payments	Could jeopardise functioning of the institution, relationship with stakeholders and service providers, and institutional reputation	Available funds and access to data to support payments; key personnel; stakeholders' relations	Use IT support for accounting services (secure software, data access); access to data; regular (weekly) update and backup (both electronic and hard copy)	< 1 Week
Incomes and revenues management	Could jeopardise functioning and liquidity of the institution, institutional reputation and capacities	Available funds and access to data about tuition and other payments	Financial resilience plan; use IT support (secure software, data access); access to data, regular (weekly) update and backup (both electronic and hard copy)	< 2 weeks