Accounting Solutions

Business Continuity Policy

Code:	SPL17CP0001
Version:	2.20
Date of version:	03/09/2025
Created by:	Vassilis Mataios
Approved by:	Managing Partner
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
31/05/2018	1.00	Vassilis Mataios	
10/12/2018	2.00	Vassilis Mataios	Risk Appetite included
11/03/2020	2.10	Vassilis Mataios	Reviewed and validated
19/04/2021	2.11	Vassilis Mataios	Reviewed and validated
16/09/2024	2.12	Vassilis Mataios	Reviewed and validated
03/09/2025	2.20	Vassilis Mataios	Reviewed and validated

Table of contents

1. Introduction

1.1. Purpose

The purpose of this policy is to ensure that Accounting Solutions has implemented the appropriate procedures in order to manage a serious crisis that causes a cessation of operations in a controlled and structured manner and effectively recover by an unwanted catastrophic event that could have a serious impact at the confidentiality, integrity or availability of business processes.

1.2. Reference documents

- ISO 27001:2022
- ISO 27002:2022
- ISO 22301:2019

1.3. Glossary of terms

Below are some basic definitions and acronyms referred to in this document.

Term	Description
Accountability	The ability to determine responsibility for actions.
Availability	Ensuring that information and vital services are available to requestors when required.
Account	A record about a specific user, token or computer known by the information system; it contains information about the subject important for the information system.
Authentication	The process of verifying the claimed identity of a user; authentication systems are often categorized by the number of factors that they incorporate for the verification; the three factors usually considered in the authentication process are: • What a user knows (a secret), such as a password, a Personal Identification Number (PIN), or an item of personal information. • What a user possesses, such as a token. Examples of tokens include swipe cards, smart cards, mechanical and electronic keys. • What a user is (a biometric), such as a fingerprint, a retina pattern, a voice pattern or a behavior pattern.
Authorization	A phase during access when it is verified that the requested access to the information system resources is allowed for the requester (requesting user).
Business Continuity Plan (BCP)	Documented procedures and instructions regarding the actions / tasks to be performed in order to achieve recovery in accordance with requirements and pre-defined recovery times. The Business Continuity Plan includes, among other things, the resources required, the organizational structure (Teams) and the Recovery Stages.
Back-up	The process of copying data to a separate store in order to protect it from unavailability or corruption of the principal store; also, the data so stored.
Confidentiality	Protecting sensitive information from unauthorized disclosure or intelligible interception.
Credentials	Data that are used as part of the authentication process to establish the claimed identity of a user or entity; they are attributes (permanent or temporary) that are associated to an existing account and used for identification and authentication; typically, a UserID and a Password, in the simplest form of a single factor authentication scheme.

Term	Description
Data	An unprocessed collection or representation of facts, concepts or instructions, which is suitably formed for communication, interpretation or processing by individuals or through automated means.
De-registration	A process through which a user is removed from information system registrant status.
Document	If not otherwise specified, a document in electronic or printed form is implied.
Identification	A process through which the identity of a user is recognized by an information system. The identification process requires the user to enter a unique user identifier (UserID).
Information Asset	Information systems, computer hardware, applications, infrastructures, information and data.
Information	Data as well as the meaning extracted through the collection, analysis, composition, classification and processing of this data
Integrity	Safeguarding the accuracy and completeness of information and computer software.
Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Maximum Tolerable Period of Disruption (MTPD)	The maximum time until the operation of each subsystem with the overrun of which causes irreparable damage to Accounting Solutions. The maximum tolerable period of disruption must be greater than the maximum RTO time of the assets.
Password	A secret that is associated to a user and that this user can use to authenticate his or her identity; passwords are typically character strings.
PIN (Personal Identification Number)	A password consisting only of decimal digits.
Registration	A process through which a user applies to obtain an account.
Recovery Time Objective (RTO)	The maximum time to recover the Software / Hardware asset so as not to affect the operation of the subsystem and by extension the Accounting Solutions Information Systems (the Recovery Time of the subsystem must not be less than the Information System Recovery Time).
Recovery Point Objective (RPO)	Time point for recovering the data needed to perform the operation so that it can be continued in case of interruption. Time point of the Backup Point storage rate so that in case of data loss it is possible to continue the operation (e.g. RPO = 24 hours, indicates that Backup is done every day at the end of work).
Role	A job type defined as a set of responsibilities.
Role-based	When mapped to job function, assumes that a person takes on different roles over time within an organization and various responsibilities in relation to information systems.
Third Parties	Partner companies, suppliers, external consultants, contractors and other service providers.
User	A general term for any person who has authorized access to and uses the Company information systems
UserID	User identifier, a character string used as a unique name for an account; it represents the account to the user and identifies the user or token to the system.

2. Roles and Responsibilities

BCP Team Leader

BCP Team Leader has the overall responsibility for managing the BCP Teams and overseeing the handling of a disaster activities as well as for ensuring that the BCP processes and services are followed properly within the Company.

The BCP Team Leader can allocate or request additional resources when needed and may have budgetary control and authority to take actions within the boundaries of certain predefined conditions (e.g., may be empowered to schedule overtime, have systems disconnected from a network, purchase software or hardware, etc.).

Senior Management Team (Gold Team)

The Senior Management Team leads the event strategically. They do not carry out recovery tasks, but are more concerned with strategic decisions, such as longer-term planning for normal business resumption from the incident, liaising with the stakeholders and giving media interviews. They are involved in the BIA phase as well in order to identify the recovery priorities.

Incident Management Team (Silver Team)

Incident Management Team is responsible for central command and control of the incident and assists the critical processes in implementing their recovery plans. Additionally, the members of the Silver Team are responsible for the monitoring of the BCP activities from an information security perspective ensuring that the appropriate countermeasures should be in place after the disaster.

System Recovery Team (Bronze Team)

The BCP Bronze Team members are responsible for the recovery of the affected systems.

Incident Response Team

Incident Response Team is responsible only for the first step in order to receive alerts-warnings and initiate the process as well as to ensure that all personnel evacuate the building and inform Silver Team.

3. Business Continuity Management Policy Statement

The Accounting Solutions Management approves the development and documentation of analytical procedures and the creation of the necessary infrastructure to ensure the continuity of business operations through an organized and integrated Business Continuity Management Framework in the event of a downtime of Accounting Solutions Information Systems and business processes.

Accounting Solutions Management provides the necessary resources for the development, implementation and maintenance of the BCP. The BCP covers all necessary and critical operations of Accounting Solutions.

For the proper design, implementation and maintenance of the BCP, the Accounting Solutions Management is committed to conduct Business Impact Analysis and Risk Analysis with the aim of identifying and analyzing the processes/services, assets/subsystems of Information Systems, their criticality, and the assessment of the consequences (e.g. operational impacts) of any Information Systems downtime.

The BCP must be periodically tested in a simulation environment to ensure that it can be implemented in case of emergency and that management and staff will understand how to implement it.

All personnel will be aware of the BCP and their respective duties on it.

Appropriate procedures and individual security policies are in place to support the policy, including technical and organizational measures of protection.

Compliance with the legislation and requirements of ISO 22301 is ensured and with the ongoing monitoring of the implementation of the BCMS.

The BCP must be renewed to take account of changing circumstances.

4. Business Continuity Management Requirements

4.1. Business Impact Analysis

Accounting Solutions should conduct Business Impact Analysis (BIA) at least once a year in order to identify the critical business processes and services, correlate the services with the information systems and evaluate the consequences in case of a disruption. Specifically, the BIA should be performed by all company departments and should include the following steps:

Step 1: Determine Business Processes and Recovery Criticality: identify the critical business processes and the supported systems and identify the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that Accounting Solutions can tolerate while still maintaining the mission. This should be conducted by the Accounting Solutions Process Owners by taking into account different criteria (such as number of clients affected, number of employees affected, legal requirements etc.) and identify the:

- Maximum Tolerable Downtime (MTD): which represents the total amount of time the Process Owner is willing to accept for a business process outage or disruption and includes all impact considerations. The time after which disruption will become critical to the organization or cause irrevocable damage
- Recovery Time Objective (RTO): RTO defines the maximum amount of time that a business process and a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes and MTD. The period of time within which systems, applications, or functions must be recovered after an outage.
- Recovery Point Objective (RPO): represents the point in time, prior to a disruption or system outage, to which business process data can be recovered (given the most recent backup copy of the data) after an outage.

Step 2: Identify resource requirements: identification of the resources (personnel, hardware, software, data files etc.) required to resume business processes and related systems as quickly as possible

Step 3: Identify recovery priorities for system resources: based on the previous steps, Accounting Solutions should identify the recovery priorities for each business process and system

4.2. Risk Appetite

Information Security Risks

Defined Risk Appetite:

1. ACCOUNTING SOLUTIONS has **low tolerance** on not adopting recommendations as derived from Information Security Risk Assessments, Security Controls Maturity Assessments or any requirements stemmed out from miscellaneous security laws and regulations. Any findings from these assessments shall trigger rational rectification of mitigation actions. Information Security Committee approval for accepting risks shall be sought in such cases.
2. ACCOUNTING SOLUTIONS accepts **low tolerance** on not adopting security requirements during the implementation of various systems, IT Infrastructure or IT internal processes. Information Security Committee approval for accepting risks shall be sought in such cases.
3. No leakage of information of "Confidential" nature is tolerated. Appropriate investigation measures shall be instigated and crisis action plan shall be initiated immediately.

Information Security Governance and Culture

Defined Risk Appetite:
a. ACCOUNTING SOLUTIONS has **zero tolerance** on misaligned, non-existent or unclear Security Policies /Governance on its various business processes.
b. ACCOUNTING SOLUTIONS has **zero tolerance** for employment practices which jeopardise the security of Accounting Solutions' Information.

To this end all employees shall be frequently trained and become aware through various means on security risks and issues.

Cyber Risks and Security Threats

Cyber risk refers to risks of cyber-attacks, which are deliberate exploitation of computer systems, technology- dependent processes and networks in the cyber realm. Cyber-attacks use manual and automated means to alter or execute computer code, logic or data, resulting in disruptive consequences that can compromise data in terms of its confidentiality, integrity or availability and lead to cybercrimes, such as data exfiltration and modification or unavailability of systems.

Defined Risk Appetite:
ACCOUNTING SOLUTIONS has a **very low appetite** for threats and losses arising from cyber-attacks or internally malicious actions on its information technology systems, infrastructure and data.

1. Penetration tests weaknesses identified as "Critical or High" are not tolerated and shall trigger immediate rectification actions within 3 months of reporting. "Medium" or "Low" weaknesses need to be addressed within a 6 month' period.
2. Any serious security attacks shall immediately trigger appropriate security incident response mechanisms. Any critical incidents shall be resolved within 24 hours, while High risk incidents shall be resolved within 3 days (72 hours).
3. Systems shall be appropriately security updated and strengthened to withstand any attacks (with a tolerance of a six-month window).
4. No unsupported system (as officially denoted by their vendor) shall be operable. If this is not feasible special mitigating controls shall be taken to isolate unsupported systems and minimize risks.
5. No non-contained malware shall be present on information systems.

To achieve the above ACCOUNTING SOLUTIONS must:

- Be in the position to detect and prevent incidents and threats against its information and internal information systems.
- Protect its internet perimeter by "industry best practice" controls and in accordance with regulatory requirements.
- Have in place strong internal control processes and robust protective technology solutions.
- Securely configure all its information systems in accordance with international best practices, and up to date (with a tolerance of a six-month window).

Reputational Risk

Reputational risk is defined as the risk arising from negative perception, on the part of the stakeholders, that can adversely affect ACCOUNTING SOLUTIONS's ability to maintain existing, or establish new, relationships with members.

Defined Risk Appetite:

1. The Accounting Solutions has **zero tolerance** in respect to internal practices by management and employees that could lead to material reputational impact; i.e., it will not tolerate headline risk associated with unacceptable business practices, privacy and other regulatory breaches and internal fraud.
2. In situations beyond the Accounting Solutions' control, the impact on earnings could be material and difficult to quantify.

   The Accounting Solutions makes sure that it takes all reasonable steps to minimize the likelihood of adverse reputational impact arising from adverse media exposure, regulatory / supervisory investigations or regulatory / supervisory non-compliance.

3. The Accounting Solutions has a **very low appetite** for negative press coverage assessed as % of total press articles/reports which are assessed as having an important reputational impact and have not been managed adequately within a single news cycle.

Business Continuity

Business Continuity risks refer to risks impacting the capability of the Accounting Solutions to continue delivery of services to its clients at acceptable predefined levels following a disruptive incident.

Defined Risk Appetite:

ACCOUNTING SOLUTIONS has **no appetite** for material losses (direct or indirect) caused by failure to implement appropriate Business Continuity Management Programs. A proper and updated Business Continuity Plan (BCP) shall be in place at all times, providing for the recovery of all its critical operations, should a disaster event occur, thereby enabling the Accounting Solutions to meet its regulatory requirements and contractual obligations to its clients and have confidence in its ability to recover its business.

Disaster Recovery

Defined Risk Appetite:

Accounting Solutions has **low tolerance** for critical business outages as a result of system failures. To this end, a Disaster Recovery Plan shall be in place with recovery sites to become operational and within a maximum tolerable period of disruption, in the event of a disaster occurring to the ACCOUNTING SOLUTIONS's servers, which house the Accounting Solutions' infrastructure and application systems.

Business Disruption & System Failures

Defined Risk Appetite:

1. Risk tolerance per single incident: €1.000 gross loss
2. Risk tolerance for aggregate gross losses per Quarter: €2.000

Compliance Risk

Compliance risk is defined as the risk of impairment to ACCOUNTING SOLUTIONS's business model, reputation and financial condition from failure to meet laws and regulations, internal standards and policies and expectations of key stakeholders such as members, students, employees and society as a whole.
Defined Risk Appetite:

1. The Accounting Solutions ensures that it adopts all regulatory, legal and compliance requirements in a proportionate way that satisfies the requirements of the regimes in a pragmatic, cost-effective manner.
2. The Accounting Solutions maintains **a zero tolerance** for regulatory fines. Consequently, non-compliance to regulatory requirements shall immediately trigger mitigation/rectification actions including reporting to the Council.
3. The Accounting Solutions strives to avoid and/or duly disclose obvious or potential conflicts of interest:
    i. The Accounting Solutions has no tolerance for participation in the decision making or voting on matters by persons that have a conflict of interest.
    ii. The Accounting Solutions has no tolerance for selection of outsourcing service providers, where the fact that they are connected with any member of ACCOUNTING SOLUTIONS's management or Council, external auditors or legal advisors, has not been duly disclosed.
    iii. Accounting Solutions has no tolerance for acts of bribery and corruption by any of its employees or any business partner.

4.3. Business Continuity Strategy

All Accounting Solutions Department Managers along with the members of the Information Security Committee should develop the Business Continuity Strategy and the Top Management should approve it. The Business Continuity Strategy should take into account the results of the BIA as well as the Risk Appetite and should define the Business Continuity Objectives and the Recovery Priorities of each Business Process of the Accounting Solutions. The Business Continuity Strategy should be reviewed at time intervals (at least once a year) in order to ensure its effectiveness.

4.4. Business Continuity Plan

Business Continuity Plan is a process that identifies all critical functions, services and activities that must be accomplished to enable Accounting Solutions to continue business during a time of disaster or serious disruption (e.g. power outages, natural disasters, acts of sabotage, or other incidents).

All Accounting Solutions Department Managers along with the members of the Information Security Committee are responsible for developing and maintaining the Business Continuity Plan for their department. This should include at least the following (in digital and hardcopy format):

- Roles and Responsibilities in case of a Catastrophic Event.
- Contact Persons in case of a Catastrophic Event.
- Preventive Controls.
- Backup Policy and Restore Procedures.
- Business Continuity Recovery Steps.
- Disaster Recovery Plan including IT Systems recovery steps.
- Business Continuity Asset Inventory with all required information by the BCP.

Business Continuity Plan should be reviewed at time intervals (at least once a year) in order to ensure its effectiveness.

5. Business Continuity Management Training and Awareness

Training should be provided at least annually; new staff who will have plan responsibilities should receive training shortly after they are hired.

Accounting Solutions personnel should be trained to the point in order to be able to execute their respective business continuity responsibilities without the aid of the documents. Training encompasses:

- Purpose of the Disaster Recovery Plan.
- Disaster Recovery Team co-ordination and communication.
- Reporting procedures.
- Security arrangements.
- Team specific processes.
- Individuals responsibilities.

6. BCP Testing and Review

6.1. Testing

Testing of the ability to recover critical business functions as intended is an essential component of effective business continuity management. As a result, effective BCP tests should be conducted periodically based on indicative scenarios. Tests should contain Tabletop and Functional tests. All BCP tests results should be evaluated in order to ensure that the test goals were achieved and the corrective actions were identified and implemented.

Additionally, internal audits should ensure that the BCP activities are properly followed.

6.2. Review

Review of the Business Continuity Policy and BCP components should be conducted annually or additional reviews should be conducted when any of the following occur:

- Regulatory changes.
- Resources or organizational structures change.
- Funding or budget level changes.
- When changes to the threat environment occur.
- When significant changes to the organization's IT infrastructure take place.
- After every BCP Test in order to incorporate findings/comments.

Managing Partner
Vangelis Fakos

_____