RISK POLICY

June 2017

This report is solely for the use of the
Institute of Certified Public Accountants of Cyprus

Summary of Risk Components / Risk Appetite			
Risk Component		**Risk Appetite**	**External Document**
1. Concentration Risk			
	Investment sector concentration	As per Investment Committee Recommendation	Investment Committee Recommendation
	Country Concentration	As per Investment Committee Recommendation	Investment Committee Recommendation
	Assignment of services concentration	Recognized	Delegation Agreement with CyPAOA
2. Liquidity Risk			
	Liquidity Losses	Zero Tolerance	
3. Operational Risk			
	Operational Losses	As per annual Risk Control Self-Assessment	Risk Control Self-Assessment
4. Internal Fraud			
	Per single incident	Zero Tolerance	
	For aggregate gross losses per annum	Zero Tolerance	
5. External Fraud			
	Per single incident	Zero Tolerance	
	For aggregate gross losses per annum	Zero Tolerance	
6. Conduct Risk			
	Losses incurred from miss-conduct	Zero Tolerance	
7. Members' Complaints			
	Reasonable Time framework for resolving legitimate complaints	Up to 3 months	Complaint procedure
	Low customer satisfaction	Zero Tolerance	Complaint procedure
8. Legal Risk			
	Number of case with potential of losing greater than 50% (as assessed by internal and / or external legal advisors)	Should not exceed 5% of total legal cases filed against ICPAC	
	Single legal case against the Institute with the potential of losing greater than 50%	Estimated loss equal should not exceed €50.000 (exception of loss incurred due to Delegation Agreement with CyPAOA which has been indemnified).	Agreement with CyPAOA & Indemnity.
9. Compliance Risk			
	Regulatory fines	Zero Tolerance	
	Participation in the Decision making or voting on matters by persons that have a conflict of interest	Zero Tolerance	Conflict of interest Policy

	Selection of outsourcing service providers that they are connected with any member of ICPAC's management or Council, external auditors or legal advisors, has not been fully disclosed.	Zero Tolerance	Conflict of interest Policy
	Acts of bribery and corruption by any of its employees or any business partner.	Zero Tolerance	Anti-Bribery Policy
10. Regulatory Risk			
	Total increase in operating cost per annum	10% on Budgeted figure	Annual Budget
11. Damage to Physical Assets			
	Per single incident	€5.000 gross loss	Insurance Cover
	For aggregate gross losses per annum	€50.000	Insurance Cover
12. Business Disruption & System Failure			
	Per single incident	€1.000 gross loss	
	For aggregate gross losses per Quarter	€2.000	
13. Business Continuity		As per Business Continuity Plan	Business Continuity Plan
14. Disaster Recovery			
15. Execution, Delivery and Process Management			
	Per single incident	Zero Tolerance	
	For aggregate gross losses per Quarter	Zero Tolerance	
16. Reputational Risk			
	Internal practices by management and employees that could lead to material reputational impact	Zero Tolerance	
	Negative press coverage assessed as % on total press articles / reports which are assessed as having important reputational impact and have not been managed adequately within a single news cycle	Low Tolerance	
17. Cyber Risks and Security Threats			
	Penetration tests weaknesses identified as "Critical or High"	Zero Tolerance and shall trigger immediate rectification actions within 3 months of reporting. "Medium" or "Low" weaknesses need to be addressed within a 6 month' period.	
	Sserious 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.	
	Systems security not appropriately updated and strengthened to withstand any attacks	Tolerance of a six-month window.	
	Unsupported system (as officially denoted by their vendor)	No tolerance. If this is not feasible special mitigating controls shall be taken to isolate unsupported systems and minimise risks.	
	Non-contained malware	No Tolerance	
18. Information Security Risks			
	Not adopting recommendations as derived from Information Security Risk Assessment, Security Controls Maturity Assessment or any requirements stemmed out from miscellaneous security laws and regulation.	No Tolerance	Risk Committee Approval
	Not adopting security requirements of various systems, IT infrastructure or IT internal processes.	No Tolerance	Risk Committee Approval
	Leakage of information of "Secret" or "Confidential" nature.	No Tolerance	
19. Information Misuse Risks			
	Deliberate misuse of ICPAC's information	No Tolerance	
20. Information Security Governance and Culture			
	Misaligned, non-existent or unclear Security Polices / Governance on its various business processes.	No Tolerance	
	Employment of practises which jeopardise the security of Institute's Information.	No Tolerance	

The Council should approve Appetite limits and review/revise them on an annual basis following recommendations of the Risk Committee.

PURPOSE OF POLICY

The Institute of Certified Public Accountants of Cyprus (ICPAC) aims to embed explicit and robust risk management practices in all areas of its operations and in servicing its members. This is achieved by implementing a sound, coherent and comprehensive risk management framework for the identification, assessment, monitoring and control of risks within the Institute. ICPAC's risk management framework improves the service provided to its members and at the same time protects its reputation. It also allows the Institute to adapt and meet challenges in a structured way, so that it can continuously align its strategy and objectives against a background of changing risk and uncertainty.

ICPAC's risk management framework is based on four key elements:
a) Risk Governance;
b) Organisational model and risk functions (guidelines, monitoring and reporting);
c) Risk Appetite and Risk Policies; and
d) Risk Culture

The risk management framework based on this policy has been developed to:

- Allow the Institute to proactively manage its risks in a systematic and structured way and to continuously refine its processes in order to reduce its risk profile.
- Ensure appropriate strategies are in place to mitigate or transfer risks.
- Ensure that risk management is an integral part of ICPAC's process of strategic decision making and planning.
- Help create a culture of risk awareness amongst all staff and its stakeholders.
- Engage the Institute's Council and management's attention to the management, monitoring, reporting and reviewing of identified risks, as well as consider new and emerging risks on a continuous basis.

The Institute's risk management framework/policy is monitored by the Council's Risk Committee. The policy and its constituent parts are subject to regular reviews and any revisions are subject to the Council's approval.

The Institute's Council are satisfied that these arrangements are appropriate given the risk management framework of ICPAC.

Risk Governance & Policy / Appetite

The Risk components together with the risk appetite of each which form part of this policy and the Institute's risk framework have as follows:

1. Concentration Risk

Concentration risk principally arises from imperfect diversification of certain funds/other investment exposures.

Defined Risk Appetite:
Institutional concentration: it relates to imperfect diversification risk in the Institute's investment portfolio because of large exposures to a single financial institution.

a. Investment sector concentration: It arises from uneven distribution of exposures to particular types of investments or investment products.
b. Country Concentration: It arises from excess concentration of funds/investments in a country/region.
c. Assignment of services concentration: It arises from delegation agreement with CyPAOA. Concentration risk has been recognised and managed through Delegation agreement and indemnities provided / agreed.

2. Liquidity Risk

Defined Risk Appetite:

a. The Institute has a very limited appetite for liquidity risk and maintains strict limits relating to its high quality liquid assets and its cash flow maturity profiles. Further, the Institute has a zero tolerance for any limit breaches.
b. The Institute aims to ensure that it has sufficient liquidity to meet its liabilities as they fall due, under both normal and stressed conditions, without incurring unacceptable losses or risking damage to the Institute's reputation.
c. The Institute needs to monitor and manage its liquidity position on an on-going basis.

3. Operational Risk

Operational risk is defined as the risk of direct or indirect impacts resulting from human factors, inadequate or failed internal processes and systems, not proper and adequate organization structure, lack of segregation of duties and not sufficient number, level, experienced and trained personnel or external events. Operational risks can arise from all business lines and from all activities carried out by the Institute and are thus diverse in nature.

Defined Risk Appetite:

a. Relevant maximum operational loss threshold should be set for aggregate and maximum operational losses following the results of the annual Risk Control Self-Assessment to be carried by the management of ICPAC.
b. Material operational risks must be adequately hedged. The Institute must purchase adequate insurance coverage to this respect.

4. Internal Fraud

The Institute has zero tolerance towards internal fraud. Consequently, any amount relating to internal fraud should trigger management actions to safeguard the Institute's assets and its members' interests, but also to ensure minimal damage to the Institute's reputation/brand. To this end, investigation procedures and disciplinary actions are enacted.

Defined Risk Appetite:

a. Risk tolerance per single incident: No tolerance
b. Risk tolerance for aggregate gross losses per annum: No tolerance

5. External Fraud

The Institute shall endeavour to ensure that its activities and operations are free from External Fraudulent Conduct. Consequently, the Institute will work to prevent and deter Fraudulent Conduct from occurring and, where it does occur, will not tolerate if not addressed it in a timely and expeditious manner.

Defined Risk Appetite:

a. Risk tolerance per single incident: No tolerance
b. Risk tolerance for aggregate gross losses per annum: No tolerance

6. Conduct Risk

Conduct risk is defined as the risk of unexpected or undesirable behaviour by management, staff or other person identified with ICPAC, which results in an adverse impact for the customer and is focused on how the Institute is managed and structured to ensure that it treats its members fairly by having robust systems and controls, adequate skill, care and judgement.

The Institute has very low tolerance in terms of shortfalls in ICPAC's collective competencies, knowledge and skills, as well as to shortfalls in the behaviour of management, staff or other persons identified with the Institute that directly or indirectly impact ICPAC's members.

Defined Risk Appetite:

a. The Institute does not include any unfair term clauses on contracts with its members / associates.
b. Practices or behaviours that lead to potential mis-selling of products/services to its members are not tolerated.
c. No tolerance for personnel who are found to be engaged in illegal activities or have a criminal record.
d. No tolerance for engaging in business with vendors/third parties who are found to be involved in illegal activities.

7. Members' Complaints

Defined Risk Appetite:

a. The Institute takes all reasonable steps to control and deal with members' complaints and will not tolerate having legitimate complaints unresolved for a period exceeding a reasonable time framework e.g. general practice recognizes this to stand at three months.
b. The Institute strives to offer a superior members' experience and will not tolerate low customer satisfaction.

8. Legal Risk

Legal risk is defined as the possibility of the operations and conditions of the Institute to be disrupted or adversely affected given lawsuits, adverse judgements or unenforceable contracts.

Defined Risk Appetite:

a. The number of cases with potential of losing greater than 50% (as assessed by internal and/or external legal advisors) should not exceed 5% of total legal cases filed against ICPAC.
b. No single legal case against the Institute with the potential of losing greater than 50% for an estimated loss equal or greater to a loss limit of €50.000, is tolerated (except of legal loss arise from Delegation Agreement with CyPAOA which has been indemnified).

In the case that ICPAC finds itself in violation of the above risk appetite, the management of the Institute will need to engage to immediate rectification and reporting of actions taken to the Council.

9. Compliance Risk

Compliance risk is defined as the risk of impairment to ICPAC'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:

a. The Institute 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.
b. The Institute maintains a zero tolerance for regulatory fines. Consequently, non-compliance to regulatory requirements shall immediately trigger mitigation/rectification actions including reporting to the Council.
c. The Institute strives to avoid and/or duly disclose obvious or potential conflicts of interest:
    i. The Institute has no tolerance for participation in the decision making or voting on matters by persons that have a conflict of interest.
    ii. The Institute has no tolerance for selection of outsourcing service providers, where the fact that they are connected with any member of ICPAC's management or Council, external auditors or legal advisors, has not been duly disclosed.
    iii. The Institute has no tolerance to acts of bribery and corruption by any of its employees or any business partner. This is clearly disclosed in its relevant policy document.

10. Regulatory Risk

Regulatory Risk is the risk of material impact on Institute's business, sector or market due to change in law or regulations made by the government or a regulatory body. Regulatory Risk may increase cost of operating business, reduce the attractiveness of Institute, lead to changes in the framework of the accounting profession or change the competitive landscape.

Defined Risk Appetite:
To this respect tolerance levels should be set as follows:
a. Risk tolerance for total increase in operating cost per annum: 10% on Budgeted figure.

11. Damage to Physical Assets

The Institute has very low tolerance for losses incurred by damages caused to physical assets due to natural disasters or other events like terrorism and vandalism and it takes all necessary security measures to prevent such events to the maximum possible extent, in addition to securing adequate insurance policies that hedge these risks.

Defined Risk Appetite:
To this respect tolerance levels should be set as follows:
b. Risk tolerance per single incident: €5.000 gross loss
c. Risk tolerance for aggregate gross losses per annum: €50.000

As per Council's decision any damage is fully hedged based on Insurance cover.

12. Business Disruption & System Failures

Defined Risk Appetite:
a. Risk tolerance per single incident: €1.000 gross loss
b. Risk tolerance for aggregate gross losses per Quarter: €2.000

13. Business Continuity

Business Continuity risks refer to risks impacting the capability of the Institute to continue delivery of services to its members/students at acceptable predefined levels following a disruptive incident.

Defined Risk Appetite:
ICPAC 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 Institute to meet its regulatory requirements and contractual obligations to its members/students and have confidence in its ability to recover its business.

14. Disaster Recovery

Defined Risk Appetite:
The Institute 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 ICPAC's servers, which house the Institute's infrastructure and application systems.

15. Execution, Delivery and Process Management

ICPAC has zero risk tolerance for operational risk events that stem from errors in data entry, miscommunication, deadline misses, accounting errors, incomplete documents, inaccurate reports, incorrect members' records, negligent loss of members' assets and vendor disputes.

Defined Risk Appetite:

a. Risk tolerance per single incident: No tolerance
b. Risk tolerance for aggregate gross losses per Quarter: No tolerance

16. Reputational Risk

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

Defined Risk Appetite:

a. The Institute 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.
b. In situations beyond the Institute's control, the impact on earnings could be material and difficult to quantify. The Institute makes sure that it takes all reasonable steps to minimise the likelihood of adverse reputational impact arising from adverse media exposure, regulatory / supervisory investigations or regulatory / supervisory non-compliance.
c. The Institute 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.

17. 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:

ICPAC 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.

a. 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.
b. 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.
c. Systems shall be appropriately security updated and strengthened to withstand any attacks (with a tolerance of a six-month window).
d. 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 minimise risks.
e. No non-contained malware shall be present on information systems.

<u>To achieve the above ICPAC must</u>:

a. Be in the position to detect and prevent incidents and threats against its information and internal information systems.

b. Protect its internet perimeter by "industry best practice" controls and in accordance with regulatory requirements. The perimeter needs to be monitored on a 24x7 basis for identification of possible intrusions.
c. Have in place strong internal control processes and robust protective technology solutions.
d. Securely configure all its information systems in accordance with international best practices, and up to date (with a tolerance of a six-month window).

18. Information Security Risks

Defined Risk Appetite:
a. ICPAC 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. Risk Committees approval for accepting risks shall be sought in such cases.
b. ICPAC accepts low tolerance on not adopting security requirements during the implementation of various systems, IT Infrastructure or IT internal processes. Risk Committees approval for accepting risks shall be sought in such cases.
c. No leakage of information of "Secret" or "Confidential" nature is tolerated. Appropriate investigation measures shall be instigated and crisis action plan shall be initiated immediately.

19. Information Misuse Risks

Defined Risk Appetite:
ICPAC has no appetite for the deliberate misuse of its information. The Institute is committed to ensuring that its information is appropriately accessed and managed in accordance with legislative and business requirements.

To achieve the above the Institute must:
a. Ensure that information is appropriately classified and accessed.
b. Employ systems which detect and prevent leakage.
c. Embed controls into systems which protect information from being misused.

20. Information Security Governance and Culture

Defined Risk Appetite:
a. ICPAC has zero tolerance on misaligned, non-existent or unclear Security Policies / Governance on its various business processes.
b. ICPAC has zero tolerance for employment practices which jeopardise the security of Institute's Information. To this end all employees shall be frequently trained and become aware through various means on security risks and issues.

21. Business Position

The strength of ICPAC's business operations is a major mitigating factor of the industry risk as well as the economic risk of the environment that the Institute operates. The stability or fragility of ICPAC's franchise, its governance, strategy and quality of its management are all indicators that could combine to increase or reduce the overall risk of the Institute and hence they form an integral part of its Risk policy.

Defined Risk Appetite:
ICPAC must:
a. Develop ways to monitor turnover volumes and is able to assess its stability under severe market conditions.
b. Establish criteria to measure revenue stability.
c. Avoid / Manage overreliance to specific types of income, e.g. subscriptions.
d. Maintains best practice governance standards.

e. Establish processes to effectively manage, prioritize and control the use of resources across disciplines, including staff allocation and program / project planning and execution.

22. Environmental & Social Risk

As part of ICPAC's commitment to environmental and social (E&S) issues, low tolerance is placed on risks arising from these parameters. Environmental and social risk management is considered a key part of the Institute's corporate responsibility and as such an E&S risk framework is applied to the Institute's members/students' servicing activities. This assists the Institute to identify and manage potential negative impacts to the environment and to social issues, as well as the associated risks affecting both the members and ICPAC.
ICPAC will not knowingly engage in any high-risk programmes/sectors, will only engage in such programmes/sectors under stringent criteria and will avoid transactions if there are material environmental and social risks that cannot be properly assessed.

Risk Culture

ICPAC's Council and its Risk Committee have a critical role in strengthening the Institute's risk governance, including setting the 'tone at the top', reviewing strategy, and approving the Group's Risk Policy and its constituent risk characteristics as described above.

It is ICPAC's Council that is ultimately responsible and accountable for the Institute's overall risk governance.

A robust risk culture is a substantial determinant of whether the Institute will be able to successfully execute its chosen strategy within its defined risk appetite. The risk culture that ICPAC wishes to build is reflected in its policies and procedures and these are closely aligned to its risk appetite. Risk culture is manifested in the day-to-day decisions that indicate how risk is identified, understood, discussed and acted upon.

ICPAC should focus primarily on the implementation of a firm-wide effective and pervasive risk culture. This is achieved through the following:

a. Embedding risk culture throughout the Institute with clear ownership and accountability of tasks.
b. Conducting firm-wide risk assessments.
c. Implementing formal risk education presentations to its employees, members and students.
d. Changes in job content and descriptions of key personnel.
e. Changes in policies and procedures, introducing additional risk criteria for the evaluation of credit and investment decisions.
f. Changes in key personnel.

Furthermore, ICPC takes risks in connection with its normal business and as such, the following principles underpin the Institute's inherent risk culture:

a. Risk is taken within a defined risk appetite.
b. Every risk taken needs to be approved within the risk management framework as described above.
c. Risk taken needs to be adequately compensated.
d. Risk should be continuously monitored and managed.