

CYBER SECURITY

Cloud Computing Policy

FUNDS  AXIS

Policy title:	Cyber Security Policy: Cloud Computing Policy
----------------------	---

Issue	1.1
Approved by:	Darren Burrows
Approval Date:	March 2024
Next Review Date:	March 2025

Scope:	The policy applies to Funds-Axis Group and all contractors and other people working on behalf of the company.
Responsibility for Implementation & Training:	Day to day responsibility for implementation: ISO Day to day responsibility for training: ISO

Distribution methods:	Methods used to communicate this policy: <ul style="list-style-type: none"> Information Security Training Module
------------------------------	---

CONTENTS

1. Background.....	4
1.1 Public Cloud.....	4
1.2 SAAS.....	4
2. Overview of Document	5
3. Staff, Training and Competence	6
3.1 Appointment of “Cloud Computing Officer”	6
3.2 Training and Competence.....	6
4. Core Responsibilities of the Resource Operator	6
4.1 I.T. policies	6
4.2 Management of the PCCI.....	6
4.3 Cloud Infrastructure Assessment	7
4.4 On-going Oversight of the PCCI and PCCIP	7
4.5 Control Over Access Rights	7
4.6 Control Over Data.....	8
4.7 Risks Assessment and Management	8
4.8 Business Continuity.....	9
4.9 Right of Step-in.....	9
5. Legal Agreement with the PCCIP	9
5.1 Data Access Restrictions.....	10
5.2 Audit Rights	11
6. Notifications by the Resource Operator to the Client.....	11
7. <i>Resource Operator’s</i> Performance of Audit of PCCIP.....	11
8. Customer’s Right to Audit.....	12
9. The Regulator’s Rights of Audit.....	13

1. Background

Funds-Axis deploys its proprietary technology and third-party components on a "Public Cloud" provided by a third-party "physical cloud computing infrastructure provider" (PCCIP), presently Amazon AWS.

The PCCIP makes available a "Client interface", which is the software layer made available by the *Cloud computing service provider* which Funds-Axis uses to manage the *Cloud computing resources* and which include, for example, tools to trace users' access, tools to provide metrics for implemented security settings, lists of users with access to data and systems, and so on.

Funds-Axis is the "Resource Operator" of the PCCI and the *Signatory* to the contract with the PCCIP.

1.1 Public Cloud

Unless otherwise agreed with the Customer, we utilise a "Public Cloud." This is a cloud deployment model where cloud services are potentially available to a number of our customer on the same cloud infrastructure under our control.

1.2 SAAS

We provide Software as a Service (SaaS). The capability provided to the Customer is to use our applications running on a cloud computing infrastructure. These applications are accessible from various client devices through either a thin client interface, such as a web browser, or a programme interface. The Customer does not manage or control the underlying cloud computing infrastructure, including network, servers, operating systems or storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Overview of Document

This Cloud Computing Policy is an integrated part of Funds-Axis's Cyber Security Policy and adheres to international standards and best practices.

It outlines the commitments of Funds-Axis to the Customer in respect of its performance of the role of *Resource Operator* of the PCCI, including those commitments stemming from its role as Signatory to the agreement with the PCCIP.

This document has been designed and is kept under review to meet various international standards and best practice, including those set out below:

Country	Standard/Legislation	URL
UK	FCA Guidance for firms outsourcing to the 'cloud' and other third-party IT services (FG 16/5) - 2019	https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
EU	European Banking Authority (EBA) Recommendations on Outsourcing to Cloud Service Providers - 2017	https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2170121/5fa5cdde-3219-4e95-946d-0c0d05494362/Final%20draft%20Recommendations%20on%20Cloud%20Outsourcing%20%28EBA-Rec-2017-03%29.pdf
EU	ESMA Final Report Guidelines on outsourcing to cloud service providers (ESMA50-157-2403) - 2020	https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf
EU	Digital Operational Resilience Act (DORA) - 2022	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554
Luxembourg	CSSF's publications on IT outsourcing and cloud computing (Circular CSSF 17/654, as amended by Circular CSSF 19/714) - 2017	https://www.cssf.lu/wp-content/uploads/cssf17_654eng.pdf
Ireland	Central Bank of Ireland cross-industry guidance on outsourcing - 2021	https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp138/draft-cross-industry-guidance-on-outsourcing.pdf
International	ISO/IEC 27001:2022	https://www.iso.org/standard/54534.html
US	National Institute of Standards and Technology (NIST) Special Publication 800-144 - 2011	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

3. Staff, Training and Competence

3.1 Appointment of “Cloud Computing Officer”

The *Resource Operator* shall designate among its employees one person, the “*Cloud Computing Officer*”, who shall be responsible for the use of cloud services and shall guarantee the competences of the staff managing *cloud computing resources*.

The *Resource Operator* shall assign the function of *Cloud Computing Officer* to a qualified person with experience in the challenges of outsourcing to a PCCI.

3.2 Training and Competence

The *Resource Operator* shall retain the necessary expertise to effectively monitor the outsourced services or functions on the PCCI and manage the risks associated with the outsourcing.

The *Resource Operator* shall ensure that staff in charge of cloud computing resources management, including the “*Cloud Computing Officer*”, internal audit and the *Information Security Officer* have sufficient competences (including through certifications and technical training) to take on their functions based on appropriate training in management and security of *cloud computing resources* that are specific to the *cloud computing service provider*. This will include ensuring a satisfactory level of competence in the secured configuration of *Cloud computing resources* on the client interface.

The *Resource Operator* will ensure that the skills of the *Cloud Officer*, the internal audit and the *Information Security Officer* are kept up to date through regular trainings. The *Resource Operator* will keep an attestation proving that the training was followed on a specific date and precisely listing the content of the training. Details of such attestation will be provided to the Customer upon request.

4. Core Responsibilities of the Resource Operator

The core responsibilities of the *Resource Operator* will include the following:

4.1 I.T. policies

The *Resource Operator* will ensure that it maintains up to date I.T. policies that take into account the PCCIP’s security measures in order to ensure overall consistency.

4.2 Management of the PCCI

The *Resource Operator* shall have full awareness of the continuity and security elements remaining under their responsibilities when using a cloud computing solution.

The *Resource Operator* will ensure that the controls operated by the cloud computing service provider are in line with good practice and operate efficiently.

The *Resource Operator* will manage the PCCI through the client interface provided by the PCCIP, and will:

- \\ Select and configure the *Cloud computing resources* in compliance with the documented cloud infrastructure continuity plan.
- \\ Ensure that the data centres used by the PCCI are located in the EU in order to make sure the data resiliency requirements are met.
- \\ Ensure that the network link allows a quick and unlimited access to the information stored in the processing unit (i.e., through an appropriate access path and data rate, as well as through redundancy).
- \\ Ensure regular control of backups and of the facilities to restore backups.
- \\ Manage the isolation of the multi-tenant environments; and
- \\ Implement the technical and organisational security measures to access the client interfaces in order to manage the cloud computing resources.

4.3 Cloud Infrastructure Assessment

The *Resource Operator* will ensure that the PCCI meets the standards for “Cloud Architecture” set out in Appendix 1.

4.4 On-going Oversight of the PCCI and PCCIP

The *Resource Operator* will perform on-going oversight of the PCCI and the PCCIP, including through the collection of indicators to monitor the systems and data on the cloud computing infrastructure, in order to ensure service quality and to note deviations from the contractually expected levels.

4.5 Control Over Access Rights

The *Resource Operator* will ensure that:

- \\ The confidentiality and integrity of data and systems is controlled throughout the IT outsourcing chain.
- \\ Access to data and systems shall follow the “need to know” and “least privilege” principles, i.e., access is only granted to persons whose functions require so, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions; and
- \\ Sufficient protection measures are taken in order to avoid that non-authorized persons access their systems.

The *Resource Operator* shall inform itself about the security measures made available on the PCCI and ensure that the configuration is compliant with its security policy.

The *Resource Operator* shall ensure that, through proper segregation of duties, its staff and staff exercising the *Cloud computing service provider* function, cannot access data.

The *Resource Operator* will ensure that:

- Under no circumstances may staff employed by the PCCIP access the data and systems without prior and explicit agreement of the *Resource Operator* and without monitoring mechanisms available to the *Resource Operator* to control the accesses. These accesses must remain exceptional.
- Under other circumstances, access may be necessary under a legal requirement or in an extreme emergency following a critical incident affecting part of or all the service provided by the PCCIP; and
- All accesses of the PCCIP must be restricted and subject to preventive and detective measures in line with sound security practices and audited at least annually.

The *Resource Operator* will ensure that the cloud service provision does not entail any manual interaction by the PCCIP as regards to the day-to-day management of the *Cloud computing resources* used by the Customer (e.g., provisioning, configuration, or release of cloud computing resources).

The *Resource Operator* alone shall manage its IT environment hosted on the PCCI. However, the PCCIP may intervene manually:

- for global management of IT systems supporting the cloud computing infrastructure (e.g., maintenance of physical equipment, deployment of new non-Customer-specific solutions); or
- within the context of a specific request by the Customer (e.g., provisioning of a *cloud computing resource* that is missing in the catalogue proposed by the *cloud computing service provider* or performing insufficiently).

4.6 Control Over Data

The *Resource Operator* shall know at any time where the data and systems are located globally, be it production environments, replications, or backups.

At any time, the *Resource Operator* shall be able to demonstrate the proper isolation of the multi-tenant environments of its Customers.

The *Resource Operator* shall make sure that telecommunications are encrypted or protected through other available technical measures to ensure the security of the communication.

4.7 Risks Assessment and Management

The *Resource Operator* shall control the risks linked to a cloud computing infrastructure.

The *Resource Operator* shall pay special attention to the outsourcing to a PCCI of critical activities in respect of which the occurrence of a problem may have a significant impact on the Customer's and *Resource Operator's* ability to meet the requirements, including any regulatory requirements, or even to continue their activities.

The *Resource Operator* shall pay special attention to the concentration and dependence risks which may arise when large parts of their activities or important functions are outsourced to a single cloud computing service provider during a sustained period.

The *Resource Operator* shall consider the risks associated with chain outsourcing (“sub-outsourcing”, where a PCCIP outsources part of the activities to other service providers). In this respect, they shall pay special attention to the safeguarding of the integrity of the internal and external control.

4.8 Business Continuity

The *Resource Operator* will ensure that it is in a position to adequately transfer the outsourced activities on a PCCI to a different PCCIP or to perform those activities itself whenever the continuity or quality of the service provision are likely to be affected.

The *Resource Operator* will be able, financially, and operationally, to recover the data and systems of the Customer, so that the Customer can use the data and continue its activities.

4.9 Right of Step-in

In the event of Funds-Axis insolvency and its inability to ensure continuity of software availability, Funds-Axis agrees to take all necessary steps to enable customers or agreed designated 3rd party appointees to step-in and take over the function of Resource Operator. This would enable a third party to step in and manage the PCCI to ensure the on-going availability of the technology, without interruption in the event of our failure.

This is instead of providing Escrow, which is an outdated concept. Escrow / source code access is largely ineffective as (i) the conditions for release are stringent and challenged and (ii) clients would still need to be able to install and maintain the code once released. Clients would need to be able to properly implement the software, train employees, maintain and support the software, purchase the necessary hardware and third-party software under the escrow method.

5. Legal Agreement with the PCCIP

The *Resource Operator* will ensure that the legal agreement, including through the specifications of the solutions subscribed to, with the PCCIP will provide, inter alia, that:

- ✓ Defined levels of service (defined qualitatively and quantitatively) are provided for.
- ✓ There is resiliency of the cloud computing services provided in the EU. In this way, in case of spread of processing, data and systems over different data centres worldwide, at least one of the data centres shall be located in the EU and data centres located in the EU shall, if necessary, allow taking over the shared processing, data and systems in order to operate autonomously the cloud computing services provided under the contracts. If all data centres backing the cloud computing services are located within the EU, the resiliency requirement is by default fulfilled.
- ✓ The PCCIP shall provide regular indicators of service quality to the Report Operator that will enable the *Resource Operator* to efficiently assess service quality and to note deviations from the contractually expected levels.

- \\ The *Resource Operator* can recover the data and systems of the Customer, at any time, including on termination or on the occurrence of a business continuity event.
- \\ The PCCI will report to the *Resource Operator*:
 - \\ any significant problem having an impact on the activities outsourced to a cloud computing infrastructure as well as any emergency situation; and
 - \\ Any change in the application functionality by the *Cloud computing service provider* - other than the changes relating to corrective maintenance, prior to its implementation, so that the latter may take the necessary measures in case of material change or discontinuity.
 - \\ The isolation of the Customer's systems and data shall be regularly controlled by the *Cloud computing service provider*, notably by means of penetration tests performed by professionals with adequate skills;
 - If the contract with the PCCIP is terminated, the PCCIP shall contractually commit to definitively erase the data and systems of the signatory within reasonable time frame without prejudice to legal provisions.
 - The contact details for communication and for escalation are clearly documented.
 - In the event of an incident, regulatory needs or other specific requirement, the *Resource Operator* shall have an appropriate means of contact at the *Cloud computing service provider*; and
 - The contract is subject to laws of an EU Member State.

5.1 Data Access Restrictions

The agreement will provide that:

- \\ Under no circumstances may staff employed by the PCCIP access the data and systems without prior and explicit agreement of the *Resource Operator* and without monitoring mechanism available to the *Resource Operator* to control the accesses. These accesses must remain exceptional.
- \\ Under other circumstances, access may be necessary under a legal requirement or in an extreme emergency following a critical incident affecting part of or all the service provided by the PCCIP; and
- \\ All accesses of the PCCIP must be restricted and subject to preventive and detective measures in line with sound security practices and audited at least annually.

It will ensure that the PCCI provision does not entail any manual interaction by the PCCIP as regards to the day-to-day management of the *Cloud computing resources* used by the Customer (e.g., provisioning, configuration, or release of *Cloud computing resources*).

The *Resource Operator* alone shall manage its IT environment hosted on the PCCI. However, the PCCIP may intervene manually:

- \\ for global management of IT systems supporting the cloud computing infrastructure (e.g., maintenance of physical equipment, deployment of new non-Customer-specific solutions); or

- within the context of a specific request by the Customer (e.g., provisioning of a *Cloud computing resource* that is missing in the catalogue proposed by the *Cloud computing service provider* or performing insufficiently).

5.2 Audit Rights

The contract between the *Resource Operator* and the PPCIP will also provide the *Resource Operator* has a right to audit the PPCIP, within the scope of the services used.

The right to audit shall comprise, among other things:

- Access to the relevant documentation of the cloud computing service provider (this documentation shall notably include audit reports, certification reports, policies, and procedures).
- Access to the staff of the cloud computing service provider, subject to prior notification within a reasonable time frame; and
- The possibility to carry out on-site inspections.

The contract shall also provide that the *Resource Operator* can mandate a third party (which could be the Customer) to perform its right of audit.

6. Notifications by the Resource Operator to the Client

The *Resource Operator* will notify any of the following to the Customer:

- Any proposed change to the PCCIP.
- Any material change to the PCCI operating levels subscribed to.
- Any significant problem having an impact on the activities outsourced to a PCCI or PCCIP as well as any emergency situation.
- Any change in the application functionality by the PCCI or the PCCIP - other than the changes relating to corrective maintenance; and
- Any change to where their data and systems are located globally, be it production environments, replications, or backups.

7. Resource Operator's Performance of Audit of PCCIP

The *Resource Operator* will perform its right of audit proportionately to the risks, in order to get sufficient assurance about the PCCIP's fulfilment of its contractual obligations and management of risks associated to the services provided, especially regarding the quality, the continuity and the security of the outsourced services.

This will include through the on-going assessment and through periodic audit and assessment.

Periodic audit will include deeply reviewing the PCCIP's detailed audit reports or detailed third-party certification reports. In particular, the *Resource Operator* will ensure that:

- ✓ It has open access to all the reports made available by the *Cloud service provider* (as opposed to only receiving the information that the cloud service provider has been audited or certified).
- ✓ The scope of the certification or audit report covers its needs:
 - the systems (i.e., processes, applications, infrastructure, data centre, etc.) which are relevant to the institution are in scope of the report; and
 - the key controls as identified by the signatory in its risk assessment are in scope of the report.
- ✓ It assesses the available information and documentation continuously (i.e., ensure key controls are still covered in future versions of an audit report) and check that the certification or audit report is not obsolete.
- ✓ It is satisfied with the aptitude of the certifying or auditing party (e.g., rotation of the certifying or auditing company, qualification, expertise).
- ✓ The certifications and audits are done against widely recognized standards and contain a test of operational effectiveness of the key controls in place, noting that generic assessments that only confirm the existence of controls (without verifying their operational effectiveness) are not sufficient.
- ✓ It is satisfied that penetration tests confirming the isolation of the Customer's systems and data have been performed by professionals with adequate skills.

8. Customer's Right to Audit

The Customer will have a right to audit the *Resource Operator* at any time, within the scope of the services used.

It will perform its right of audit proportionately to the risks, to get sufficient assurance about the *Resource Operator's* fulfilment of its contractual obligations.

The right to audit will include the right to access data related to the outsourced activities, including access to relevant indicators of service quality, as well as the right to perform, on its own initiative and any time, an assessment of the *Cloud computing service provider's* processes, systems, networks, premises, data and infrastructure used for providing the services outsourced, including the parts of the services that may be sub-outsourced, including to the PCCIP.

The right to audit will not be subject to such conditions that its performance is significantly impeded (e.g., excessive costs invoiced by the cloud service provider).

The Customer shall have the power to mandate an agreed third party to perform its right of audit.

9. The Regulator's Rights of Audit

In respect of clause 6 above, the Customer will also be able to mandate the institution which supervises it (the "Regulator") to perform the right of audit of the *Resource Operator* and the PCCIP. This will include the right to communicate observations to the Customer.

This right exists solely to the extent required under relevant Regulations and within the scope of the services used by the Customer and is further limited to where the outsourced activity is material.

END



FUNDS AXIS




CONTACT US





 +44 (0) 28 9032 9736



 info@funds-axis.com



 www.funds-axis.com

 12 Gough Square, London,
United Kingdom, EC4A 3DW