DORA Statement on Operational Resilience – FundApps Limited

Overview

FundApps Limited ("**FundApps**") takes compliance seriously and we are dedicated to supporting our customers' compliance with regulatory obligations. Compliance is at the heart of everything we do.

For financial entities who are subject to the EU's Digital Operational Resilience Act ("**DORA**"), we offer a DORA Addendum to facilitate their compliance with mandatory contractual requirements and other measures that they need to ensure that they have in place with FundApps. We also have prepared a DORA Statement on Contractual Compliance which sets out how FundApps facilitates financial entities to meet their obligations under DORA with respect to mandatory contractual requirements and the other measures addressed in the FundApps DORA Addendum.

Financial entities who are subject to DORA are also required to meet a range of other obligations regarding operational resilience. Those measures include a range of information security and business continuity measures. DORA requires financial entities – not ICT third-party service providers – to have in place and meet a range of different requirements. These obligations do not apply to FundApps. However, we recognise that, as part of financial entities' requirements to undertake due diligence into the operational resilience of their ICT third-party service providers, financial entities will need to understand if their ICT third-party service providers like FundApps have appropriate technical and organisational arrangements in place to manage ICT risk.

FundApps has prepared this Statement on Operational Resilience to describe how FundApps addresses measures that financial entities themselves need to meet. This Statement is not an operational document – FundApps has in place its own policies and procedures and the means to implement them. However, this Statement does offer a fair description of the measures that FundApps has in place which are aligned to financial entity requirements under DORA. Please refer to the FundApps' DORA Addendum to see how this Statement is referred to in our contractual arrangements with financial entity customers who are subject to DORA. This Statement is therefore provided only for information purposes and FundApps does not provide any guarantee or warranty regarding its completeness, accuracy or otherwise, except to the extent expressly provided in the FundApps DORA Addendum.

This Statement is separated into two parts:

- Part A – which covers the requirements set out in DORA itself; and
- Part B – which covers relevant aspects of Regulatory Technical Standards that are related to operational resilience and ICT risk management.

This Statement does not expressly cover requirements of Regulatory Technical Standards on matters such as threat-led penetration testing and subcontracting, which are governed to the extent relevant to FundApps by the terms and conditions in the FundApps DORA Addendum.

Part A – DORA requirements

1. Governance and organisation

1.1 FundApps has Information Security and Business Continuity policies which ensure a high standard of availability, integrity and confidentiality of data.[1]

[1] DORA, Article 5(2)(b)

1.2 The Roles, Responsibilities and Organisation section of FundApps' Information Security Management System policy sets clear roles and responsibilities in relation to all of FundApps' ICT-related functions and establishes appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions.[2]

1.3 FundApps has business continuity policies and ICT response and recovery plans in place, available here.[3]

1.4 FundApps' customers can request meetings or additional information from FundApps to monitor its information security arrangements.[4]

2. ICT risk management framework

2.1 FundApps has an ICT risk management framework in place to manage ICT-related incidents and continuously improves the framework based on lessons derived from implementation, monitoring, supervisory instructions or conclusions, resilience testing and audit processes. The framework is documented and reviewed at least once a year in compliance with ISO27001, as well as upon the occurrence of a major ICT-related incident.[5]

2.2 FundApps maintains and provides information to customers in the form of a platform overview (available here) which details the ICT reference architecture.[6]

2.3 FundApps has an Incident Response policy which outlines the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from them. Details of FundApps' practices relating to logging, monitoring and alerting are available here.[7]

2.4 FundApps implements digital operational resilience testing as detailed in our Business Continuity Policy.[8]

2.5 FundApps identifies key dependencies on its services, including customer dependencies, third party dependencies and technical dependencies (such as network connections). FundApps maintains a list of identified critical third parties which is reviewed annually for any security changes.[9]

3. ICT systems, protocols and tools

3.1 FundApps uses and maintains updated ICT systems, protocols, and tools that are appropriate to the magnitude of operations supporting the conduct of our activities. FundApps appropriately scopes each customer's requirements to determine the necessary capacity and obtain volume-related information (including customer data types and volumes) in advance of contracting for services.[10]

3.2 FundApps' service levels and repair/replace obligations ensure that customers receive a reliable service.[11]

3.3 FundApps' serverless architecture scales automatically based on traffic or customer growth, which ensures the FundApps services are equipped with sufficient capacity to accurately process the

[2] DORA, Article 5(2)(c)
[3] DORA, Article 5(2)(e)
[4] DORA, Article 5(3)
[5] DORA, Article 6(5)
[6] DORA, Article 6(8)(d)
[7] DORA, Article 6(8)(e)
[8] DORA, Article 6(8)(g)
[9] DORA, Article 6(9)
[10] DORA, Article 7(a)
[11] DORA, Article 7(b)

data necessary for the performance of operations and timely service provision. FundApps ensures readiness to handle peak orders, message or transaction volumes, as needed, including where new technology is introduced.[12]

3.4 The use of serverless architecture (details of which are available here) means that FundApps' ICT systems are resilient and capable of meeting additional information processing needs under stressed market conditions or other adverse situations. Details of the technical resilience measures implemented by FundApps are available here. Sufficient redundancy to handle additional information is offered free of charge to all customers.[13]

4. Identification

4.1 FundApps identifies, classifies, and adequately documents the information assets and ICT assets supporting all of our services in our Information Asset Register and Information Systems Register.[14]

4.2 FundApps continuously identifies all sources of ICT risk and assess cyber threats and ICT vulnerabilities relevant to our services, information assets, and ICT assets. We review risk scenarios impacting customers on a regular basis and at least yearly (as per SEC-3 and DEV-11 controls in SOC 2 security standard). Such risks are identified through formal and informal channels, including in monthly security review meetings, as part of the software development lifecycle and as part of continuous release management. FundApps uses third party services to identify cyber threats and other vulnerabilities, such as CrowdStrike, Synk, Detectify and AWS Inspector. See FundApps' Risk Management Framework and Vulnerability Management Policy for more information.[15]

4.3 In accordance with FundApps' Software Development policy, we perform risk assessments in relation to each major change to our network and information system architecture and to the processes or procedures affecting our services, information assets or ICT assets.[16]

4.4 FundApps has identified information assets and ICT assets, including those on remote sites, network resources and hardware equipment in our Technical & Platform Overview and Information Asset Register. FundApps maps those assets considered critical. Parts of FundApps' service are outsourced to AWS. AWS hosts the FundApps platform and are responsible for managing network resources and hardware equipment used to deliver our services. The assets used by AWS to carry out its hosting services are not tracked in our asset registers. [17]

4.5 FundApps identifies and documents all processes that are dependent on third-party providers in accordance with our Third Party Risk Management policy. FundApps also identifies interconnections with other ICT third-party service providers that provide services which support customers' critical or important functions. These third-party providers are tracked in Whistic and Drata.[18]

4.6 FundApps have change management protocols in place to maintain relevant inventories and update them periodically, and every time a major change occurs.[19]

4.7 On a regular basis and at least annually through FundApps' information security risk register, we conduct a specific ICT risk assessment on all legacy ICT systems and, in any case, before and after connecting technologies, applications or systems.[20]

[12] DORA, Article 7(c)
[13] DORA, Article 7(d)
[14] DORA, Article 8(1)
[15] DORA, Article 8(2)
[16] DORA, Article 8(3)
[17] DORA, Article 8(4)
[18] DORA, Article 8(5)
[19] DORA, Article 8(6)
[20] DORA, Article 8(7)

5. Protection and prevention

5.1 FundApps continuously monitors and controls the security and functioning of ICT systems and tools and minimises the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures. Specifically, FundApps engages independent third party auditors, on an annual basis, to perform security assessments of the FundApps application suite and supporting API. FundApps have a SOC 2 Type 2 Report for Security, Availability and Confidentiality, as well as ISO 27001:2013 certification.[21]

5.2 FundApps implements ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit. See FundApps' Technical Resilience and Cryptographic Policy for more information.[22]

5.3 FundApps uses ICT solutions and processes that are appropriate, that ensure the security of the means of transfer of data and that minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity. FundApps' ICT solutions and processes also prevent data availability, authenticity and integrity issues, breaches of confidentiality and the loss of data, and ensure that data is protected from risks arising from data management (including poor administration, processing-related risks, and human error). See our Information Transfer Policy and our Data Classification and Protection Standard.[23]

5.4 As part of FundApps' ICT risk management framework, FundApps has implements a suite of Information Security Policies that define rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets. Where FundApps' customers require us to comply with additional rules defined by them relating to information security, FundApps will assess the viability of that compliance and, where viable, FundApps will pass any cost associated with complying with additional rules on to the customer accordingly.[24]

5.5 FundApps has in place a network and infrastructure management structure to isolate affected information assets in the event of cyber-attacks (as detailed here). Specifically, FundApps has implemented a tiered network architecture to host its services, which allows information assets to be instantaneously severed or segmented in order to minimise and prevent contagion.[25]

5.6 FundApps' Access Control Policy and Physical Security Policy limit the physical or logical access and ICT assets to what is required for legitimate and approved functions and activities only, and establish procedures and controls that address access rights and ensure a sound administration thereof.[26]

5.7 FundApps' Access Control Policy and Cryptographic Policy set out protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.[27]

5.8 FundApps documents and implements policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of FundApps change management process (as set out in our Risk Management Framework and Information Security in Project Management Policy). This ensures that all changes to ICT systems are

[21] DORA, Article 9(1)
[22] DORA, Article 9(2)
[23] DORA, Article 9(3)(a)-(d)
[24] DORA, Article 9(4)(a)
[25] DORA, Article 9(4)(b)
[26] DORA, Article 9(4)(c)
[27] DORA, Article 9(4)(d)

recorded, tested, assessed, approved, implemented and verified in a controlled manner. In particular, the ICT change management process is approved by appropriate lines of management and includes specific protocols.[28]

5.9 In addition to the above, FundApps has an appropriate and comprehensive Patch Management Policy in place for patches and updates.[29]

6. Detection

6.1 FundApps has mechanisms in place to detect anomalous activities (including ICT network performance issues and ICT-related incidents) and has the ability to identify material single points of failure as set out in our Incident Response policy.[30]

6.2 FundApps' detection measures enable multiple layers of control and define alert thresholds and criteria to trigger and initiate ICT-related incident response processes (including mechanisms to automatically alert relevant staff in charge of ICT-related incident response). Details are available here.[31]

6.3 FundApps monitors for security incidents and cyber-attacks impacting our infrastructure and software. To assist customers to monitor user activity, FundApps makes application audit trails available to all customers via the user interface as an exportable CSV file.[32]

7. Response and recovery

7.1 FundApps has a comprehensive Business Continuity Policy in place.[33]

7.2 FundApps' Business Continuity Policy can be implemented through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms to:

(a) ensure the continuity of customers' critical or important functions (as described here);

(b) quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions (see our Incident Response policy);

(c) activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures;

(d) estimate preliminary impacts, damages and losses; and

(e) set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders.[34]

7.3 FundApps maintains and periodically tests our Business Continuity Plan and conducts disaster recovery tests at least annually.[35]

7.4 FundApps test cyber-attack scenarios as part of our internal security incident tabletop exercises.[36]

[28] DORA, Article 9(4)(e)
[29] DORA, Article 9(4)(f)
[30] DORA, Article 10(1)
[31] DORA, Article 10(2)
[32] DORA, Article 10(3)
[33] DORA, Article 11(1)
[34] DORA, Article 11(2)(a)-(e)
[35] DORA, Article 11(3), (4) and (6)(a)
[36] DORA, Article 11(6)

7.5 Our Business Continuity Policy and ICT response and recovery plans are reviewed annually, taking into account the results of tests carried out and recommendations stemming from audit checks or supervisory reviews as per our SOC 2 report.[37]

8. Backup policies and procedures, restoration and recovery procedures and methods

8.1 FundApps has a documented backup policy and procedure (detailed here) specifying the scope of the data that is subject to continuous backup. FundApps documents and implements restoration and recovery procedures and methods as part of our disaster recovery process.[38]

8.2 FundApps has a backup system in place that can be activated in accordance with our backup policies and procedures and disaster recovery procedures and methods.[39]

8.3 FundApps has a single recovery time objective (4 hours) and recovery point objective (30 minutes) across our services. Such time objectives ensure that, in extreme scenarios, the agreed service levels are met.[40]

8.4 When recovering from an ICT-related incident, FundApps can perform checks (including any multiple checks and reconciliations) to ensure that the highest level of data integrity is maintained, as detailed in our Vulnerability Management Policy.[41]

9. Learning and evolving

9.1 FundApps has in place capabilities and staff to gather information on vulnerabilities, cyber threats and ICT-related incidents (in particular cyber-attacks) and to analyse the impact that they are likely to have on FundApps' digital operational resilience. FundApp's approach to gathering information on vulnerabilities is described in the Vulnerability Management Policy.[42]

9.2 FundApps implements a procedure for post ICT-related incident reviews after a major ICT-related incident disrupts core activities (detailed in the Washup and lessons learned section of our Incident Response Policy). These reviews include analysis of the causes of disruption and identification of required improvements to the ICT operations or our Business Continuity Policy and aim to determine whether the established procedures were followed and if the actions taken were effective, including in relation to:

(a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;

(b) the quality and speed of performing a forensic analysis, where deemed appropriate;

(c) the effectiveness of incident escalation within the customer; and

(d) the effectiveness of internal and external communication.[43]

9.3 FundApps implements a process for ensuring that lessons derived from digital operational resilience testing, real life ICT-related incidents (in particular cyber-attacks), challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans and relevant information exchanged with counterparts is incorporated on a continuous basis into our ICT risk assessment process. For more information, see our Risk Management Framework.[44]

[37] DORA, Article 11(8)
[38] DORA, Article 12(1)
[39] DORA, Article 12(2)
[40] DORA, Article 12(6)
[41] DORA, Article 12(7)
[42] DORA, Article 13(1)
[43] DORA, Article 13(2)
[44] DORA, Article 13(3)

9.4 FundApps maps the evolution of ICT risk over time, analyses the frequency, types, magnitude and evolution of ICT-related incidents (in particular cyber-attacks and their patterns) with a view to understanding the level of ICT risk exposure (in particular in relation to services supporting customers' critical or important functions) and enhancing our cyber maturity and preparedness.[45]

9.5 FundApps monitors relevant technological developments on a continuous basis, with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience. FundApps also keeps up-to-date with the latest ICT risk management processes in order to effectively combat current or new forms of cyber-attacks. See our performance evaluation for more information.[46]

10. Communication

10.1 FundApps has crisis communication plans in place enabling a responsible disclosure of major ICT-related incidents or vulnerabilities to our customers. FundApps reserves the right to make disclosures or announcements to regulators and/or the public concerning its services, as appropriate.[47]

11. ICT-related incident management process

11.1 FundApps implements an Incident Response plan to detect, manage and notify ICT-related incidents, which:

(a) puts in place early warning indicators;

(b) establishes procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted;

(c) assigns roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;

(d) sets out plans for communication to staff, external stakeholders and media and for notification to customers, for internal escalation procedures, including ICT-related customer complaints;

(e) ensures that at least major ICT-related incidents are reported to relevant senior management and notified to FundApps' management body (with explanations of the impact, response and additional controls to be established as a result of such ICT-related incidents); and

(f) establishes ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.[48]

11.2 FundApps records all ICT-related incidents and significant cyber threats in an incident log. See our logging, monitoring and alerting policy here.[49]

11.3 FundApps implements appropriate procedures and processes to ensure a consistent and integrated approach monitoring, handling and follow-up of ICT related incidents. These procedures

[45] DORA, Article 13(4)
[46] DORA, Article 13(7)
[47] DORA, Article 14(1)
[48] DORA, Article 17(1) and (6)
[49] DORA, Article 17(2)

and processes ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.[50]

12. Classification of ICT related incidents

12.1 FundApps classifies ICT-related incidents and determines their impact on FundApps (rather than on customers or subcontractors) based on the following criteria:

(a) the number and/or relevance of customers affected and (where applicable) the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;

(b) the duration of the ICT-related incident, including the service downtime;

(c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;

(d) the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;

(e) the criticality of the services affected; and

(f) the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.[51]

13. Reporting of major ICT-related incidents and voluntary notification of significant cyber threats

13.1 FundApps prepares initial notifications and reports for customers following major ICT-related incidents as detailed in the Notification of external parties section of our Incident Response policy. The initial notifications and reports include:

(a) all information necessary for the customer and any relevant competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts; and

(b) the measures that have been taken to mitigate the adverse effects of the incident. [52]

13.2 FundApps will submit intermediate reports after the initial notification as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed (as appropriate) by updated notifications every time a relevant status update is available, as well as upon a specific request from a customer.[53]

13.3 FundApps will prepare a final report at a customer's request when the root cause analysis of a major ICT-related incident has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.[54]

14. Digital operational resilience testing

[50] DORA, Article 17(2)
[51] DORA, Article 18(1)(a)-(f)
[52] DORA, Article 19(1) and (3)
[53] DORA, Article 19(4)(a)-(b)
[54] DORA, Article 19(4)(c)

14.1 FundApps maintains and reviews a sound and comprehensive digital operational resilience testing programme as an integral part of our ICT risk-management framework, as set out in our Vulnerability Management Policy and Business Continuity policies. Our digital operational resilience testing programme includes a range of assessments, tests, methodologies, practices and tools to be applied and duly considers the evolving landscape of ICT risk, any specific risks FundApps is concerned about or might be exposed to, the criticality of information assets and of services provided.[55]

14.2 FundApps ensure that, at least yearly, appropriate tests are conducted on all services that support customers' critical or important functions. The tests cover:

(a) vulnerability assessments and scans;

(b) open source analyses;

(c) network security assessments;

(d) gap analyses;

(e) physical security reviews;

(f) questionnaires and scanning software solutions;

(g) source code reviews where feasible;

(h) scenario-based tests;

(i) compatibility testing;

(j) performance testing;

(k) end-to-end testing; and

(l) penetration testing. [56]

[55] DORA, Article 24(1)-(3)

[56] DORA, Articles 24(6) and 25(1)

Part B – RTS requirements

1. ICT services supporting critical or important functions

1.1 The ICT services that FundApps provide which support customers' critical or important functions are subject to independent audit.[57]

1.2 FundApps can participate in customer risk assessments which consider the impact of the provision by FundApps of ICT services supporting critical or important functions on the customer and all its risks.[58]

1.3 In respect of the ICT services FundApps provides which support our customers' critical or important functions, FundApps:

(a) has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organisational structure, risk management and internal controls and (to the extent required) authorisations and/or registrations to provide the ICT services in a reliable and professional manner;

(b) has the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework;

(c) specifies where FundApps uses or intends to use subcontractors to perform the relevant ICT services;

(d) can specify whether FundApps is located, or processes or stores customer data in a third country and (if this is the case) can specify whether this practice elevates the level of operational risks, reputational risks or the risk of being affected by restrictive measures (including embargos and sanctions) that may impact FundApps' ability to provide the relevant ICT services or the customer's ability to receive those services; and

(e) has a Code of Conduct which demonstrates that FundApps acts in an ethical and socially responsible manner and adheres to human and children's rights, applicable principles on environmental protection, and ensures appropriate working conditions including the prohibition of child labour.[59]

1.4 As part of its customers' due diligence processes, FundApps allows for use by the customer of:

(a) independent audit reports made on behalf of FundApps;

(b) audit reports of FundApps' internal audit function;

(c) relevant appropriate third-party certifications; and

(d) other relevant available information or other information provided by FundApps via its Trust Portal.

1.5 When providing third party certifications, audit reports and/or internal audit reports to a customer, FundApps:

[57] RTS to specify policy on ICT services supporting critical or important functions, Article 3(8)
[58] RTS to specify policy on ICT services supporting critical or important functions, Article 5(2).
[59] RTS to specify policy on ICT services supporting critical or important functions, Article 6(1).

(a) ensures that the scope of its certifications and/or audit reports (as applicable) cover the core function of FundApps' services;

(b) thoroughly assesses the content of its certifications and/or audit reports (as applicable) on an ongoing basis and verifies that the reports and/or certifications (as applicable) are not obsolete; and

(c) ensures that key systems and controls are covered in future versions of the certifications and/or audit reports (as applicable).[60]

2. Classification of major incidents

2.1 For an incident affecting its ICT services, FundApps can establish:

(a) the number of customers (and their clients) affected by the incident;

(b) the amount and number of transactions affected by the incident;

(c) the duration of an incident from the moment the incident occurs (or if not ascertainable, from when the incident was detected) until the moment when the incident is resolved (or is estimated to be resolved);

(d) where FundApps is aware that the incident has occurred prior to its detection, the duration from the moment the incident has been recorded in network or system logs or other data sources;

(e) the service downtime of an incident from the moment the service is fully or partially unavailable to customers and/or other internal or external users to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident;

(f) where the service downtime causes a delay in the provision of service after regular activities or operations have been restored, the downtime measured from the start of the incident (or when it was detected) to the moment when that delayed service is fully provided;

(g) the data losses that the incident entails in relation to the availability of data (taking into account whether the incident has rendered the data on demand by the customer, its clients or its counterparts temporarily or permanently inaccessible or unusable);

(h) the data losses that the incident entails in relation to the authenticity of data (taking into account whether the incident has compromised the trustworthiness of the source of data);

(i) the data losses that the incident entails in relation to the integrity of data (taking into account whether the incident has resulted in non-authorised modification of data that has rendered it inaccurate or incomplete);

(j) the losses that the incident entails in relation to the confidentiality of data from an incident (taking into account whether the incident has resulted in data having been accessed by or disclosed to an unauthorised party or system);

(k) whether the incident represents successful, malicious and unauthorised access to the network and information systems of the customer;

[60] RTS to specify policy on ICT services supporting critical or important functions, Article 8(3).

(l) for the purpose of determining the economic impact of the incident, whether the following types of direct and indirect costs and losses have been incurred as a result of the incident, without accounting for financial recoveries (excluding costs that are necessary to run the business as usual):

(i) replacement or relocation costs of software, hardware or infrastructure;

(ii) staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff;

(iii) fees due to non-compliance with contractual obligations;

(iv) customer redress and compensation costs;

(v) losses due to forgone revenues;

(vi) costs associated with internal and external communication; and

(vii) advisory costs, including costs associated with legal counselling, forensic and remediation services; and

(m) whether the incident is an incident that is recurring (and whether it previously occurred).[61]

2.2 For an incident affecting FundApps ICT services, customers can use FundApps' services to determine whether the incident will mean that the customer will not be able to (or is likely to not be able to) meet regulatory requirements.[62]

3. ICT risk management

3.1 FundApps has a Risk Management Framework policy which:

(a) is intended to: (i) ensure the security of networks, enable adequate safeguards against intrusions and data misuse, (ii) preserve the availability, authenticity, integrity and confidentiality of data (including cryptographic techniques) and (iii) guarantee an accurate and prompt data transmission without major disruptions and undue delay;

(b) specifies the procedure and methodology to conduct ICT risk assessment, identifying vulnerabilities and threats that affect or may affect FundApps' business functions;

(c) includes ICT risk treatment measures for the ICT risk assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within acceptable risk tolerances;

(d) includes provisions on the identification of residual ICT risks;

(e) includes provisions on the assessment of the accepted residual ICT risks at least once a year, including the identification of any changes to the residual risks, the assessment of available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risks are still valid and applicable at the date of the service; and

[61] RTS for classification of major incidents, Articles 1(1), (3) and (4), 2(1)(c), 3, 5, 6, 7(1) and 15(2).
[62] RTS for classification of major incidents, Article 2(1)(c).

(f) includes provisions for the monitoring of changes to the ICT risk and cyber threat landscape, internal and external vulnerabilities and threats and of ICT risk to promptly detect changes that could affect FundApps' ICT risk profile[63]

3.2 FundApps maintains an Information Security Risk Register of residual ICT risks, including an explanation of reasons why they were accepted.[64]

4. ICT asset management

FundApps has policies on ICT asset management as necessary to preserve the availability, authenticity, integrity and confidentiality of data (including an Information Asset Register and Access Control, Technical Resilience and Data Backups policies) which:

(a) provide for the correct identification and classification of ICT assets and information assets;

(b) require the monitoring and management of the life cycle of ICT assets identified and classified;

(c) require FundApps to keep records of the follow in respect of ICT assets in FundApps' possession:

(i) names of ICT assets;

(ii) information on the location, either physical or logical, of all ICT assets;

(iii) the classification of all ICT assets according to the business functions, roles and responsibilities they support;

(iv) business functions or services supported by the ICT asset; and

(v) the links and interdependencies among ICT assets and the business functions using each ICT asset; and

(d) detail the criteria to perform the criticality assessment of information assets and ICT assets supporting FundApps' services and take into account ICT risk related to those business functions and their dependencies on information assets or ICT assets and how the loss of confidentiality, integrity or availability of such information assets and ICT assets would impact FundApps' services.[65]

5. Encryption and cryptographic controls

FundApps has a Cryptographic Policy which:

(a) covers the encryption of internal network connections and traffic with external parties, considering data criticality and classification;

(b) considers leading practices, reliable techniques, and the classification of involved ICT assets (and where FundApps cannot adhere to leading practices or standards, FundApps implements and records mitigation and monitoring measures to maintain resilience against cyber threats);

[63] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 3(1).
[64] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 3(1)(d)(iii).
[65] RTS to further harmonise ICT risk management tools, methods, processes and policies, Articles 4 and 5.

(c) sets rules for the encryption of data at rest and in transit;

(d) contains provisions for cryptographic key management;

(e) includes criteria to select cryptographic techniques and use practices taking into account leading practices and standards;

(f) establishes guidelines for the correct use, protection, and lifecycle management of cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys;

(g) includes controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification and implements methods to replace cryptographic keys where they are lost, compromised or damaged; and

(h) ensures that a register is maintained for all certificates and certificate-storing devices for at least ICT assets supporting customers' critical or important functions, and that this register must be kept up-to-date.[66]

6. ICT operations

FundApps documents and implements policies and procedures to manage the ICT operations of ICT assets in its Information Asset Register, which include the following:

(a) ICT assets descriptions, including: (i) secure installation, maintenance, configuration and deinstallation of ICT systems; and (ii) identification and control of legacy ICT systems;

(b) controls and monitoring of ICT systems, including:

(i) backup and restoration requirements of ICT systems;

(ii) protocols for audit-trail and system log information;

(iii) requirements to ensure that the performance of internal audit and other testing minimises disruptions to business operations;

(iv) requirements on the separation of ICT production environments from development, testing and other non-production environments (which considers all of the components of the environment, such as accounts, data or connections);

(v) requirements to conduct development and testing in environments which are separated from the production environment;

(vi) requirements to conduct development and testing in production environments (including clear identification and justification of instances where testing is performed in the production environment, with such testing to be conducted for limited periods of time approved by customers); and

(vii) ensuring the availability, confidentiality, integrity and authenticity of ICT systems and production data during development and test activities in the production environment; and

[66] RTS to further harmonise ICT risk management tools, methods, processes and policies, Articles 6 and 7

(c) error handling concerning ICT systems, including:

(i) procedures and protocols for handling errors;

(ii) support and escalation contacts, including external support contacts in case of unexpected operational or technical issues; and

(iii) ICT system restart, rollback and recovery procedures for use in the event of ICT system disruption.[67]

7. Capacity and performance management

7.1 FundApps documents and implements capacity and performance management procedures to identify capacity requirements of its ICT systems and applies resource optimisation and monitoring procedures to maintain and improve the availability of data and ICT systems and the efficiency of ICT systems and to prevent ICT capacity shortages. FundApps has built in technical resilience scenarios within its Business Continuity Management System.

7.2 These capacity and performance management procedures ensure that appropriate measures are taken to cater for the specificities of ICT systems with long or complex procurement or approval processes or that are resource-intensive.[68]

8. Vulnerability and patch management

8.1 FundApps documents and implements vulnerability management procedures with a view to ensuring the security of networks against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. These procedures:

(a) identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities;

(b) ensure the performance of automated vulnerability scanning and assessments on ICT assets, with the frequency and scope of these activities commensurate to the classification and the overall risk profile of the ICT asset (including on a weekly basis for ICT assets supporting customers' critical or important functions);

(c) cover handling of vulnerabilities related to the ICT services provided to customers (including investigation of such vulnerabilities, determination of the root causes and implementation of appropriate mitigating actions) and reporting to customers in a timely manner at least the critical vulnerabilities and statistics and trends;

(d) provide for tracking of the usage of third-party libraries, including open source, used by ICT services supporting customers' critical or important functions and ICT services specifically customised or developed for the customer by FundApps (including monitoring the version and possible updates of the third-party libraries) and, in the case of ready to use (off-the-shelf) ICT assets or components of ICT assets acquired and used in the operation of ICT services not supporting customers' critical or important functions, tracking the usage of third-party libraries to the extent possible;

(e) provide for responsible disclosure of vulnerabilities to customers and counterparts as well as to the public, as appropriate;

[67] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 8

[68] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 9

(f) identify criteria to prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified (including, for the purposes of the prioritisation, considering the criticality of the vulnerability and the classification and the risk profile of the ICT assets affected by the vulnerability);

(g) provide for monitoring and verification of the remediation of vulnerabilities; and

(h) require the recording of any detected vulnerabilities affecting ICT systems and the monitoring of their resolution.[69]

8.2 FundApps documents and implements patch management procedures with a view to ensuring the security of networks and enabling safeguards against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. These procedures provide for:

(a) identification and evaluation of available software and hardware patches and updates using automated tools, to the extent possible;

(b) identification of emergency procedures for the patching and updating of ICT assets;

(c) testing and deployment of software and hardware patches and updates; and

(d) setting of deadlines for the installation of software and hardware patches and updates and escalation procedures in case the deadline cannot be met.[70]

9. Data and system security

FundApps documents and implements a data and ICT system security procedure which includes the following elements related to data and ICT system security:

(a) access restrictions supporting the protection requirements for each level of classification;

(b) identification of secure configuration baselines for ICT assets that will minimise their exposure to cyber threats (and take into account leading practices and appropriate techniques referred to in standards) and measures to verify regularly that these baselines are those that are effectively deployed;

(c) identification of security measures to ensure that only authorised software is installed in ICT systems and endpoint devices;

(d) identification of security measures against malicious codes;

(e) identification of security measures to ensure that only authorised data storage media, ICT systems and endpoint devices are used to transfer and store customer data;

(f) requirements to secure the use of portable endpoint devices and private non-portable endpoint devices, including:

(i) the use of a management solution to remotely manage the endpoint devices and remotely wipe customer data;

(ii) the use of security mechanisms that cannot be modified, removed or bypassed by staff members in an unauthorised manner; and

[69] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 10(1)-(3).
[70] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 10(4)

(iii) the authorisation to use removable data storage devices only where the residual ICT risk remains within the customer's risk tolerance level;

(g) the process to securely delete data, present on premises or stored externally, that customers no longer need to collect or store;

(h) the process to securely dispose of or decommission data storage devices present on premises or stored externally containing confidential information;

(i) the identification and implementation of security measures to prevent data loss and leakage for ICT systems and endpoint devices;

(j) the implementation of security measures to ensure that teleworking and the use of private endpoint devices do not adversely impact customers' ICT security; and

(k) in respect of FundApps' ICT assets and services, the identification and implementation of requirements to maintain digital operational resilience (in accordance with the results of the data classification and ICT risk assessment), with identification of these requirements to involve consideration of:

(i) implementation of vendor recommended settings on the elements operated by FundApps;

(ii) clear allocation of information security roles and responsibilities;

(iii) ensuring and maintaining adequate competences within FundApps in the management and security of the service used; and

(iv) technical and organisational measures to minimise the risks related to the infrastructure considering leading practices and standards.[71]

10. Logging

FundApps has a Logging, Monitoring and Alerting policy which includes:

(a) the identification of the events to be logged, the retention period of the logs and the measures to secure and handle the log data, considering the purpose for which the logs are created (with the retention period taking into account the business and information security objectives, the reason for recording the event in the logs and the results of the ICT risk assessment);

(b) alignment of the level of detail of the logs with their purpose and usage to enable the effective detection of anomalous activities;

(c) the requirement to log events related to:

(i) identity management and logical and physical access control;

(ii) capacity management;

(iii) change management;

(iv) ICT operations, including ICT system activities; and

[71] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 11

(v) network traffic activities, including ICT network performance;

(d) measures to protect logging systems and log information against tampering, deletion and unauthorised access at rest, in transit and, where relevant, in use;

(e) measures to detect failure of logging systems; and

(f) synchronisation of the clocks with customers' ICT systems upon a documented reliable reference time source.[72]

11. Network security management

FundApps documents and implements policies and procedures on network security management which include the following elements:

(a) the segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support and the classification and overall risk profile of ICT assets using them;

(b) the documentation of all of FundApps' network connections and data flows;

(c) the identification and implementation of network access controls to prevent and detect connections to our customers' network by any unauthorised device or system, or any endpoint not meeting our customers' security requirements;

(d) the encryption of network connections passing over corporate networks, public networks, domestic networks, third-party networks and wireless networks, for communication protocols used taking into account the results of the approved data classification and the results of the ICT risk assessment and in accordance with the policy on encryption and cryptographic controls;

(e) the design of networks in accordance with ICT security requirements and taking into account leading practices to ensure the confidentiality, integrity and availability of the network;

(f) the securing of network traffic between the internal networks and the internet and other external connections;

(g) the identification of the roles and responsibilities and steps for the definition, implementation, approval, change and review of firewall rules and connections filters (and for the ICT systems supporting customers' critical or important functions, FundApps verifies the adequacy of the existing firewall rules and connection filters at least every six months);

(h) the measures to temporarily isolate (where necessary) subnetworks and network components and devices;

(i) the implementation of a secure configuration baseline of all network components and hardening the network and network devices according to vendor instructions and (where applicable) standards and leading practices;

(j) the procedures to limit, lock and terminate system and remote sessions after a predefined period of inactivity; and

[72] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 12

(k) with reference to network services agreements, the identification and definition of ICT and information security measures, service levels and management requirements of all network services.[73]

12. Securing information in transit

FundApps documents and implements policies, procedures, protocols and tools to protect information in transit taking into account the results of the approved data classification and the ICT risk assessment processes to ensure:

(a) the availability, authenticity, integrity and confidentiality of data during network transmission, as well as the establishment of procedures to assess compliance with these requirements;

(b) the prevention and detection of data leakage and the secure transfer of information between customers and external parties; and

(c) that requirements on confidentiality or non-disclosure arrangements reflecting customers' needs for the protection of information for staff and third parties are implemented, documented and regularly reviewed.[74]

13. ICT project management

FundApps documents and implements an Information Security in Project Management policy that:

(a) defines the elements to ensure the effective management of the ICT projects related to the acquisition, maintenance and, where applicable, development of the ICT systems; and

(b) includes the following elements:

(i) project governance, including roles and responsibilities;

(ii) project risk assessment;

(iii) change management requirements; and

(iv) testing of all requirements, including security requirements, and the respective approval process when deploying an ICT system in the production environment.[75]

14. ICT systems acquisition, development and maintenance

14.1 FundApps documents and implements a policy governing the acquisition, development and maintenance of ICT systems which:

(a) identifies security practices and methodologies relating to the acquisition, development and maintenance of ICT systems;

(b) requires the identification of technical specification and ICT technical specification of requirements relating to acquisition, development and maintenance of ICT systems, with a particular focus on ICT security requirements and on their approval by the relevant

[73] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 13

[74] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 14(1).

[75] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 15

business function and ICT asset owner according to FundApps' internal governance arrangements; and

(c) defines measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development, maintenance and deployment in the production environment.[76]

14.2 FundApps documents and implements an ICT systems' acquisition, development and maintenance procedure which includes:

(a) the requirements to test and approve all ICT systems prior to their use and after maintenance, to a level that is commensurate to the criticality of the concerned business functions and ICT assets and is designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally;

(b) the requirements to perform source code reviews covering both static and dynamic testing, including security testing for internet-exposed systems and applications, to identify and analyse vulnerabilities and anomalies in the source code, adopt an action plan to address them and monitor their implementation;

(c) the requirement to perform security testing of software packages at no later than the integration phase;

(d) the requirement that non-production environments only store anonymized, pseudonymized or randomized production data and that the integrity and confidentiality of data is protected in non-production environments;

(e) the requirement to implement controls to protect the integrity of the source code of ICT systems that are developed by FundApps and delivered to customers; and

(f) the requirement that proprietary software and (where feasible) the source code provided by third parties or coming from open-source projects, shall be analysed and tested prior to their deployment in the production environment.[77]

15. ICT change management

FundApps documents and implements ICT change management procedures which include the following elements:

(a) verification that ICT security requirements have been met;

(b) mechanisms to ensure independence between the functions that approve changes and those responsible for requesting and implementing them;

(c) definition of clear roles and responsibilities to ensure that changes are defined, planned, that an adequate transition is designed, that the changes are tested and finalised in a controlled manner and that there is effective quality assurance;

(d) documentation and communication of change details, including purpose and scope of the change, the timeline for implementation and the expected outcomes;

[76] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 16(1)

[77] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 16(2)-(3) and (5)

(e) identification of fall-back procedures and responsibilities, including procedures and responsibilities for aborting changes or recovering from changes not successfully implemented;

(f) procedures, protocols and tools to manage emergency changes that provide adequate safeguards; and

(g) procedures to document, re-evaluate, assess and approve emergency changes after their implementation, including workarounds and patches.[78]

16. Physical and environmental security

16.1 FundApps documents and implements a physical and environmental security policy (available here) designed according to the cyber threat landscape, the classification and the overall risk profile of ICT assets and information assets that can be accessed. The policy includes:

(a) measures to protect the premises, data centres and sensitive designated areas where ICT assets and information assets reside from attacks, accidents and from environmental threats and hazards (and the measures to protect from environmental threats and hazards are commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there);

(b) measures to secure ICT assets, both within and outside the premises of FundApps, taking into account the results of the ICT risk assessment related to the relevant ICT assets (including measures to provide appropriate protection to unattended ICT assets);

(c) measures to ensure the availability, authenticity, integrity and confidentiality of data information assets and physical access control devices through the appropriate maintenance; and

(d) measures to preserve the availability, authenticity, integrity and confidentiality of data, including a clear desk policy for papers and a clear screen policy for information processing facilities (a clear desk is required as part of FundApps Employee Guide).[79]

16.2 FundApps has a separate policy on control of access management rights (available here).[80]

17. Human Resources policy

FundApps' human resource or other relevant policies include the following ICT security elements:

(a) identification and assignment of any specific ICT security responsibilities;

(b) requirements for staff using or accessing ICT assets of FundApps to:

(i) be informed about, and adhere to, FundApps' ICT security policies, procedures and protocols;

(ii) be aware of the reporting channels put in place by customers for the purpose of detection of anomalous behaviour; and

[78] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 17(1)
[79] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 18
[80] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 18(2)(a)

(iii) upon termination of employment, requirements for the staff to return all ICT assets and tangible information assets in their possession that belong to FundApps or its customers.[81]

18. Identity management

FundApps documents and implements identity management policies and procedures to ensure the unique identification and authentication of natural persons and systems accessing customer information to enable assignment of user access rights. These policies include:

(a) the assignment of a unique identity corresponding to a unique user account to each staff member of the customer or FundApps accessing FundApps' information assets and ICT assets;

(b) the maintenance of records of all identity assignments to be kept after the end of the contractual relationship with the customer without prejudice to the retention requirements set out in EU and national law; and

(c) a lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation and termination of all accounts, including where applicable, deploying automated solutions for the lifecycle identity management process.[82]

19. Access control

FundApps' policy on control of access management rights include all of the following elements:

(a) assignment of access rights to ICT assets based on need-to-know, need-to-use and least privilege principles, including for remote and emergency access;

(b) segregation of duties designed to prevent unjustified access to critical data or to prevent the allocation of combinations of access rights that may be used to circumvent controls;

(c) provision on user accountability, by limiting to the extent possible the use of generic and shared user accounts and ensuring that users are identifiable for the actions performed in the ICT systems at all times;

(d) provision on restrictions of access to ICT assets, setting out controls and tools to prevent unauthorised access;

(e) account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. The procedures include provision on the following:

(i) assignment of roles and responsibilities for granting, reviewing and revoking access rights and definition of the retention period for logs;

(ii) assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems and:

(A) where possible, us of dedicated accounts for the performance of administrative tasks on ICT systems; and

[81] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 19

[82] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 20

(B) where applicable, deployment of automated solutions for the privileged access management;

(iii) revoking of access rights without undue delay upon termination of employment or when the access is no longer necessary;

(iv) update of access rights where changes are necessary and at least once a year for all ICT systems (other than ICT systems customers' supporting critical or important functions) and at least every six months for ICT systems supporting customers' critical or important functions;

(f) authentication methods including:

(i) the use of authentication methods commensurate to the classification and to the overall risk profile of ICT assets and considering leading practices; and

(ii) the use of strong authentication methods in accordance with leading practices and techniques for remote access to FundApps' and its customers' networks, for privileged access and for access to ICT assets supporting customers' critical or important functions or that are publicly accessible; and

(g) physical access control measures including:

(i) identification and logging of natural persons who are authorised to access premises, data centres and sensitive designated areas identified by FundApps where ICT and information assets reside which is commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there;

(ii) granting of physical access rights to critical ICT assets to authorised persons only according to the need-to-know, least privilege principles and on an ad-hoc basis;

(iii) monitoring of physical access to premises, data centres and sensitive designated areas where ICT and information assets reside which is commensurate to the classification and the criticality of the area accessed; and

(iv) review of physical access rights to ensure that unnecessary access rights are promptly revoked.[83]

20. ICT-related incident management policy

FundApps documents and implements an ICT-related incident management policy through which it:

(a) documents the ICT-related incident management process;

(b) establishes a list of relevant contacts with internal functions and external stakeholders that are directly involved in ICT operations security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management;

[83] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 21

(c) establishes, implements and operates technical, organisational and operational mechanisms to support the ICT-related incident management process, including mechanisms to enable a prompt detection of anomalous activities and behaviours;

(d) retains all evidence (in a secure manner) relating to ICT-related incidents for a period no longer than necessary for the purposes for which the data is collected, commensurate with the criticality of the affected business functions, supporting processes and ICT and information assets, and with any applicable retention requirement under EU law; and

(e) establishes and implements mechanisms to analyse significant or recurring ICT-related incidents and patterns in the number and the occurrence of ICT-related incidents.[84]

For information about how long FundApps retains incident logs, see FundApps' Data Retention Policy.

21. Anomalous activities detection and criteria for ICT-related incidents' detection and response

FundApps implements detection mechanisms allowing it to:

(a) collect, monitor and analyse:

(i) internal and external factors, information from business and ICT functions and any problem reported by users;

(ii) potential internal and external cyber threats, considering scenarios commonly used by threat actors and scenarios based on threat intelligence activity; and

(iii) ICT-related incident notifications detected in its ICT systems and networks and which may affect customers;

(b) identify anomalous activities and behaviour and implement tools generating alerts for anomalous activities and behaviour, at least for ICT assets and information assets supporting customers' critical or important functions (including tools that provide automated alerts based on pre-defined rules to identify anomalies affecting the completeness and the integrity of the data sources or log collection);

(c) prioritise the alerts to allow the detected ICT-related incidents to be managed within the expected resolution time, as defined by customers, both during and outside working hours;

(d) record, analyse and evaluate any relevant information on all anomalous activities and behaviours automatically or manually.

(e) protect any recording of anomalous activities against tampering and unauthorised access at rest, in transit and, where relevant, in use;

(f) log all relevant information for each detected anomalous activity to enable identification of the data and time of occurrence and detection, and the type of anomalous activity; and

(g) consider the following criteria to trigger ICT-related incident detection and response processes:

[84] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 22

(i) indications that malicious activity may have been carried out in an ICT system or network or that such ICT system or network may have been compromised;

(ii) data losses detected, in relation to the availability, authenticity, integrity and confidentiality of data;

(iii) adverse impact detected on customers' transactions and operations; and

(iv) ICT systems' and network unavailability.[85]

22. Components of the ICT business continuity policy

FundApps' ICT business continuity policy (available here) includes the following:

(a) definition of the objectives, including the interrelation of ICT and overall business continuity, and considering the results of the business impact analysis (BIA);

(b) definition of the scope (including limitations and exclusions) to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms;

(c) definition of the timeframe to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms;

(d) description of the criteria to activate and deactivate ICT business continuity plans, ICT response and recovery plans and crisis communications plans;

(e) provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the ICT business continuity policy and to ensure that sufficient resources are available;

(f) provisions on the alignment between the ICT business continuity plans and the overall business continuity plans, including concerning:

(i) potential failure scenarios; and

(ii) recovery objectives, specifying that FundApps shall be able to recover the operations of its critical or important functions after disruptions within our recovery time objective (< 4 hours) and a recovery point objective (< 30 minutes).

(g) provisions on the development of ICT business continuity plans for severe business disruptions as part of these plans, and the prioritisation of ICT business continuity actions using a risk-based approach;

(h) provisions on the development, testing and review of ICT response and recovery plans; and

(i) provisions on the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms.[86]

23. Testing of the ICT business continuity plans

[85] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 23(2)-(5)
[86] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 24(1)

FundApps has a Business Continuity Plan which it tests on a regular basis in accordance with its Business Continuity Policy. Redacted copies of any business continuity tests performed including remediations taken can be accessed via our Trust Portal at any time.

24. ICT response and recovery plans

FundApps' ICT response and recovery plans:

(a) specify the conditions prompting their activation, deactivation and any exceptions;

(b) describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least ICT systems and services supporting customers' critical or important functions;

(c) are designed to meet the recovery objectives of the operations of our customers;

(d) are documented and made available to the staff involved in their execution and are readily accessible in case of emergency, with clearly defined roles and responsibilities to that extent;

(e) provide for both short-term and long-term recovery options including partial systems recovery;

(f) lay down the objectives and the conditions to declare a successful execution of the plans;

(g) identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of the occurrence of disruption;

(h) develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions;

(i) take into account:

(i) cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities;

(ii) scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly consider the potential impact of the insolvency or other failures of any relevant third party providers;

(iii) partial or total failure of premises, including office and business premises, and data centres;

(iv) substantial failure of ICT assets or of the communication infrastructure;

(v) the non-availability of a critical number of staff or staff members in charge of guaranteeing the continuity of operations;

(vi) the impact of climate change and environment degradation related events, natural disasters, pandemic, and physical attacks, including intrusions and terrorist attacks;

(vii) insider attacks;

(viii) political and social instability, including, where relevant, in the jurisdiction from where third party providers provide their services and the location where the data is stored and processed; and

(ix) widespread power outages.[87]

25. Reports on ICT risk management framework review

FundApps keeps reports on its reviews of its ICT risk management framework covering the following:

(a) summary of major changes in the ICT risk management framework;

(b) summary of the current and near-term ICT risk profile, threat landscape, assessed effectiveness of controls and security posture;

(c) date of approval of the report;

(d) the reason for review;

(e) where the review was initiated following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes, the report contains explicit references for initiating the review;

(f) where the review was initiated following ICT-related incidents, the report contains the list of all ICT-related incidents with incident root-cause analysis;

(g) start and end dates of the review period;

(h) indication of the function responsible for the review;

(i) description of the major changes and improvements to the ICT risk management framework since the previous review (including an analysis of the impact of the changes on FundApps' digital operational resilience strategy, on the ICT internal control framework and on FundApps' ICT risk management governance); and

(j) summary of the findings of the review and detailed analysis and assessment of the severity of the weaknesses, deficiencies and gaps in the ICT risk management framework during the review period;

(k) description of the measures to address identified weaknesses, deficiencies and gaps, including all of the following:

(i) summary of measures taken to remediate identified weaknesses, deficiencies and gaps;

(ii) expected date for implementing the measures and dates related to the internal control of the implementation, including information on the state of progress of their implementation as at the date of drafting of the report, explaining, where applicable, if there is a risk that deadlines may not be respected;

(iii) tools to be used and identification of the function responsible for carrying out the measures, detailing whether they are internal or external;

[87] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 26

(iv) description of the impact of the changes envisaged in the measures on FundApps' budgetary, human and material resources, including resources dedicated to the implementation of corrective measures; and

(v) if the weaknesses, deficiencies or gaps identified are not subject to remedial measures, a detailed explanation of the criteria used to analyse their impact, to evaluate the related residual risk and for the acceptance of such a risk;

(l) information on planned further developments;

(m) conclusions resulting from the review of the ICT risk management framework;

(n) information on past reviews, including:

(i) list of past reviews to date;

(ii) if applicable, state of implementation of the mitigation measures identified by the last report; and

(iii) where applicable, description of whether the proposed remedying measures in past reviews have proven ineffective or created unexpected challenges, and how they could be improved; and

(o) sources of information used in the preparation of the report, including the following:

(i) results from internal audit;

(ii) results from compliance assessments; and

(iii) external sources.[88]

[88] RTS to further harmonise ICT risk management tools, methods, processes and policies, Article 27