A working experimentation model for cyber resilience regulatory sandboxes

Fabio Seferi[1,2]

[1] IMT School for Advanced Studies Lucca, Piazza S. Ponziano 6, 55100, Lucca, Italy
[2] University of Florence, Department of Legal Sciences, Via delle Pandette 32, 50127, Florence, Italy

Abstract

In today's volatile and highly dynamic global environment, regulators and stakeholders encounter significant challenges in addressing cyber risk, particularly considering rapidly evolving digital technologies and of the lack of instruments to anticipate specific scenarios in controlled environments. This paper first examines the potential of cyber risk mitigation through regulatory experimentation, in the context of regulatory sandboxes. Through the analysis of 43 relevant use cases, the research focuses on the evaluation of the role of risk management measures within regulatory sandboxes. Against this backdrop, the article then proposes a working experimentation model for cyber resilience – titled the "3PS model" and comprising Products, Systems, Processes and Services as components, which could be used for Procedural or Security functions. This working experimentation model could serve as a foundation for future real-world applications (e.g., in the field of cyber resilience regulatory sandboxes).

Keywords

regulatory sandboxes, cybersecurity, cyber resilience, Cyber Resilience Act, regulatory experimentation

1. Introduction

Novel digital technologies are transforming the landscape of our society at an unprecedented pace, offering great opportunities for innovation and social advancement. Acceleration is a core feature of diagnoses for contemporary social development [1]. This rapid evolution can outpace the ability of citizens and regulators to understand and mitigate associated risks, leading to societal impacts that are difficult to predict or control. Social control of technology has indeed been a core issue of scientific literature in the past decades, posing the central question of decision makers navigating in the uncharted waters of regulation [2].

Regulatory sandboxes have seen an increasing interest in European Union (EU) and national regulatory efforts as a measure both to govern and regulate new technologies in a timely manner, whilst also supporting innovation. They can be considered as a form of "structured experimentalism" [3], allowing for experimentation in a protected environment through the application of appropriate guardrails to insulate the wider context from possible negative externalities of such experimentation.

In brief, regulatory sandboxes can be described as "schemes that enable firms to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority" [4].[2] They could also include testing in real-world conditions and with real customers. These flexible schemes have also caught the attention of the EU legislator, who in 2024 adopted three different Regulations that foresee the establishment of regulatory sandboxes in the digital domain: the Interoperable Europe Act (Regulation (EU) 2024/903), the Artificial Intelligence Act (Regulation (EU) 2024/1689), and the Cyber Resilience Act (Regulation (EU) 2024/2847).

[1] Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT
fabio.seferi@imtlucca.it
0009-0009-9518-6445

[2] Regulatory sandboxes draw from the concept of sandbox in computer science. This "technical" sandbox can be defined as "a restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized" (as retrieved from the NIST Glossary, source NIST SP 1800-21B from CNSSI 4009-2015, available at: https://csrc.nist.gov/glossary/term/sandbox).

However, there remains a notable gap for a conceptual framework on how experimentation within regulatory sandboxes can effectively support the adoption and testing of cybersecurity requirements. A shared understanding and standardised approach to experimentation is fundamental to ensuring consistent and comparable outcomes across different types of regulatory sandboxes. Such uniformity would strengthen their collective capacity to enhance the cyber resilience of entities and to have in turn better-informed cyber policy formulation. In this view, this paper proposes an experimentation model designed to serve as a starting basis for implementing so-called "cyber resilience regulatory sandboxes". To do so, the paper is structured as follows: Section 2 illustrates the concept of regulatory sandboxes between normative frameworks and relevant literature. Section 3 highlights the role of risk management measures within regulatory sandboxes and identifies some core components to be taken into consideration for their related experimentation. On this basis, Section 4 outlines a working model for experimentation on cyber resilience. Lastly, Section 5 presents the main conclusions derived from the research and some considerations that outline possible future work on the topic.

2. Framing regulatory sandboxes

2.1. Relevant normative frameworks at EU level

Regulatory sandboxes have emerged as important regulatory and policy mechanisms for experimentation and adaptive regulation, especially at EU level. They form one of the tools for better regulation, as envisaged in the 2023 "Better regulation Toolbox" of the European Commission: regulatory sandboxes are listed as one of the approaches under Tool #69 on emerging methods and policy instruments [4]. EU's Better Regulation agenda aims to ensure evidence-based and transparent law-making, also based on the views of the impacted stakeholders. In this context, regulatory sandboxes provide for evidence-based regulation of innovation, while also considering the specific hurdles of participating actors.

To this regard, the Council of the European Union adopted a document of Conclusions on regulatory sandboxes and experimentation clauses in 2020 [5]. These conclusions highlighted the use of regulatory sandboxes in the context of digitalisation, and stressed how this policy instrument can: (a) provide the opportunity for advancing regulation through proactive regulatory learning, thus based on real-world evidence, in contexts of high uncertainty and disruptive challenges; and (b) offer significant possibilities for innovation and growth for businesses (in particular, for SMEs, micro-enterprises as well as start-ups), industry, and public services.

Between legal definitions and real-world examples, regulatory sandboxes generally share several core features [6]. They involve a structured approach to development and testing of innovative technologies before market deployment, in view of the general objective of attaining regulatory learning. Innovations are developed and tested in a controlled environment, which could include (near) real-world conditions. Participation in regulatory sandboxes is governed through a specific plan developed with, and monitored by, a competent authority (the one setting up and running the regulatory sandbox). The operation of regulatory sandboxes with respect to the admitted projects is usually organized on a case-by-case basis: this may involve a temporary loosening of applicable rules (through derogations, waivers or exemptions), while also maintaining specific safeguards to preserve the overall regulatory objectives [6].

For digital solutions, three EU Regulations that entered into force in 2024 envisage the establishment of regulatory sandboxes: the Interoperable Europe Act (IEA), the Artificial Intelligence Act (AIA), and the Cyber Resilience Act (CRA). The Interoperable Europe Act (Regulation (EU) 2024/903) focuses on the promotion of cross-border interoperability of trans-European digital public services, thus applying to entities and public sector bodies that either regulate, provide, manage or implement such services [cf. Article 1(1-2) IEA]. This Regulation foresees the possibility of establishing so-called "interoperability regulatory sandboxes" as a support measure for the overall objectives of an Interoperable Europe [cf. Articles 11 and 12 IEA]. Interoperability regulatory

sandboxes refer to controlled environments for the development, training, testing and validation of innovative interoperability solutions, where appropriate in real world conditions [cf. Article 2(14) IEA]. For a comprehensive analysis of interoperability regulatory sandboxes, refer to [7].

On the other hand, the Artificial Intelligence Act (Regulation (EU) 2024/1689) has the purpose to promote the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety, and fundamental rights against the harmful effects that AI systems may have in the EU. It is the only Regulation from the referred ones at EU level that foresees the mandatory establishment of national "AI regulatory sandboxes", which shall be operational by 2 August 2026 [cf. Article 57(1) AIA]. This type of regulatory sandboxes provides for a controlled framework to develop, train, validate and test – including in real-world conditions – innovative AI systems before market launch, fostering innovation and ensuring regulatory compliance [cf. Article 3(55) AIA]. For more details on AI regulatory sandboxes under the AI Act refer to [8] and [9].

However, the interplay between cybersecurity requirements and regulatory sandboxes finds a practical application in the Cyber Resilience Act (Regulation (EU) 2024/2847). This Regulation provides rules for deploying products with digital elements while ensuring their overall cybersecurity. In this view, it foresees several essential requirements for the design, development and production of such products and for the vulnerability handling processes put in place by manufacturers [cf. Article 1 CRA]. The Regulation lays down the possibility for Member States to establish "cyber resilience regulatory sandboxes", thus providing for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with the provisions envisioned in the Regulation itself [cf. Article 33(2) CRA]. For the many interactions between the Cyber Resilience Act and the Artificial Intelligence Act with respect to regulatory sandboxes, refer to [10] and [11].

There are not many elements yet on how future cyber resilience regulatory sandboxes should and will look like in terms of design, functioning, outcome and effectiveness. Their establishment is driven by the testing of the essential cybersecurity requirements. This paper conceptualizes a possible framework for any type of regulatory sandbox starting from the components of experimentation, leaving the possibility to regulators and participating entities to define the most appropriate cybersecurity requirements and modalities of implementation.

2.2. State of the art

The many facets of regulatory sandboxes have been the focus of a recent collective work [11], to which is referred for further insights and detailed analyses. Regulatory sandboxes have also been at the centre of several specialised studies and reports, including from the European Commission [6], the OECD [12], the European Parliament [14], the Joint Research Centre [15] and the European Supervisory Authorities [16]. The present Subsection, however, briefly highlights some key considerations from scientific literature that are relevant for the continuation of the analysis.

Regulatory sandboxes allow for a crucial environment where to pursue responsible innovation, due to the specific conditions of engagement between stakeholders (regulators and innovators), and to it being an iterative and collaborative process. In principle, in anticipating risks and functioning of innovative solutions that do not currently fit the legal framework, regulators can buttress its development in respect of core societal values, principles and ethical considerations. Their theoretical role of promoting secure and responsible innovations is widely shared across the community of policymakers, regulators, entrepreneurs and researchers [17]. Moreover, the (social) interaction between regulators and regulated entities within sandboxes may increase the latter's risk management capabilities [18]. Indeed, by involving those affected by regulation in the experimentation activity, these spaces enhance legitimacy and trust in both innovative solutions and regulatory practices [19].

One of the main open problems in the research area is that, from a practical perspective, there has not been a common understanding of what a regulatory sandbox should be and what it should entail. Focusing on one feature or the other often leads regulators and policymakers to either frame a

regulatory experiment as a sandbox or disregard it. Indeed, research has shown that the understanding of regulatory sandboxes and experimentation varies significantly also across participating (or interested) entities [20]. This is translated into another key concern: the results of experimentation may not be easily scalable or replicable, as they are often tailored to specific contexts [19]. Moreover, the application of regulations stemming from different sectors to the same product complicates the experimentation process given the need to have a coordinated governance and interplay of multiple different authorities at the same time [21]. Another related problem refers to the practical implementation of this instrument [21]. For example, the effectiveness of regulatory learning within and as an outcome of regulatory sandboxes remains to be seen. In this view, a comprehensive conceptualisation of how this regulatory learning process could work into practice is still lacking, in particular with respect to the testing and implementation of cybersecurity requirements. Coupled to this, regulators and public administration bodies often lack the necessary resources (and even competences) to effectively run these schemes [19].

Ultimately, regulatory experimentation – exemplified in this paper with regulatory sandboxes as one of its main recent applications – implies the testing, piloting or trial of a new product, service, approach or process, in such a way as to generate and gather evidence that can inform the design or administration of a regulatory regime. This is particularly relevant also for cybersecurity law and regulation.

3. The role of risk management

3.1. Regulatory sandboxes as risk management instruments

Regulatory sandboxes, as illustrated, serve as mechanisms for experimenting with innovative solutions under regulatory supervision and before market deployment. A central role is played by the development and testing of products. In this context, cybersecurity requirements guarantee that innovative products are made available in the market without any known vulnerabilities; coupled with this, regulatory sandboxes may enhance the overall risk management posture of the participating entities.

Indeed, many regulatory sandboxes foresee the adoption of specific measures in terms of risk management, which are often envisaged as selection criteria for accessing the sandbox environment: thus, risk management becomes one of the dimensions on which basis the projects are evaluated for admission and for the experimentation to start. This is in line with adopting appropriate safeguards that contribute to having a protected and controlled experimentation. Building on previous work [22], risk management measures have been identified and analysed in 43 relevant use cases of regulatory sandboxes and experimentation initiatives, ranging from financial services to energy, transportation and emerging technologies (see Table 2 in Appendix for the list of uses cases and related risk management measures envisaged).[3]

These measures cover multiple dimensions of risk management. First, a focus on the specific solution is placed in many cases, including the interaction between the product and its end users (i.e., consumers). For example, in the case of "Australia - AEMC's Energy Regulatory Sandboxes" [UC40], adequate consumer protections are required in connection with the trial project. For the "Bahrain - CBB's Financial Services Regulatory Sandbox" case [UC02], it is necessary to adopt cybersecurity and other relevant measures to ensure safety of the innovative solution (or service) – thus, it also places a strong emphasis on cybersecurity measures. In addition, in the cases of "India - RBI's Financial Services Regulatory Sandbox" [UC07] and "Philippines - BSP's Financial Services Regulatory Sandbox" [UC17], two specific aspects emerge: (i) the adoption of adequate built-in safeguards for IT

[3] The financial services sector represents the largest group, with 31 occurrences. This prevalence is not unexpected, as regulatory sandboxes have become a prominent practice within this industry. On the other hand, a total of 8 use cases pertains to cross-sectoral schemes, although they may be focused on specific technologies (such as "Spain - AI Regulatory Sandbox Pilot Scheme" [UC30]). Finally, energy and transportation are represented by 2 use cases each. Please refer to Table 2 in the Appendix for more details.

systems, and (ii) the assessment and mitigation of significant risks. This highlights how (cyber) risk management is not only viewed in relation to the specific solution undergoing experimentation, but also as a general requirement for the IT architecture of the participating entity.

Some of the risk assessments required across regulatory sandboxes are also tailored to the specific type of product considered for experimentation and to its characteristics. In this view, AI systems in the case of "Spain - AI Regulatory Sandbox Pilot Scheme" [UC37] undergo evaluations for their societal impact and for their likelihood of becoming high-risk AI systems (which specific requirements apply to under the Artificial Intelligence Act). This is the case also for "Austria - Framework Conditions for Automated Driving" [UC42], in which it is required the performance of a specific route analysis and risk assessment for the planned test route area: the results of this activity then feed into the risk management process for the test plan, thus incorporating precise feedback loops.

Risk management is also required throughout the innovation lifecycle, involving continuous risk monitoring and mitigation processes. In the case of "Portugal - Free Zones for Technology" [UC35] it is required to define a monitoring plan for carrying out the testing, and clear risk assessment and mitigation strategies. The latter also applies to the use cases "Saudi Arabia - CST's Emerging Technologies Regulatory Sandbox" [UC36] and "Saudi Arabia - SAMA's Open Banking Regulatory Sandbox" [UC19], or to "Brazil - BCB's Financial Services Regulatory Sandbox" [UC03]. In the "Singapore - MAS's FinTech Regulatory Sandbox" case [UC20], the definition of boundaries to limit the scale of testing and associated risks is also required. In the case of "Oman - CBO's Fintech Regulatory Sandbox Framework" [UC16], an emergency exit strategy is also required for the situations in which live testing either fails or is discontinued. Another aspect is tied to elements such as business continuity and disaster recovery plans, as in the case of "Bahrain - CBB's Financial Services Regulatory Sandbox" [UC02]. Regulatory sandboxes may require the specification of the methods in place to address possible consumer complaints emerging during experimentation (e.g., "United States - Florida's Financial Technology Sandbox Innovator" [UC25]). In the case of "United Arab Emirates - ADGM's FinTech RegLab" [UC24], projects may also be selected to their potential of promoting better risk management solutions for the financial industry. Hence, risk management is not only a requirement but becomes also a clear objective of the overall regulatory sandbox scheme.

As this analysis has shown (see all relevant measures listed in Table 2 in Appendix), regulatory sandboxes play an important role for requiring and pursuing adequate levels of risk management throughout participation and experimentation. This would most likely be reflected also in the regulatory sandboxes to be established under the EU Regulations recalled before. Indeed, for interoperability regulatory sandboxes, a risk management and monitoring mechanism is required as part of the participation plan [cf. Article 12(3) point d) IEA]. For AI regulatory sandboxes, risk management [cf. Article 9 AIA] and cybersecurity [cf. Article 15 AIA] are among the measures that could be tested for high-risk AI systems. For the Cyber Resilience Act, a specific evaluation of the applicable essential cybersecurity requirements is made in Subsection 4.2.

3.2. Main components for risk management in experimentation

There is however a gap in literature when it comes to analysing how cybersecurity requirements are evaluated and adopted in practice within regulatory sandboxes – and how this can be done in future iterations of such schemes. This becomes even more relevant if we consider the possible establishment of cyber resilience regulatory sandboxes as envisaged by the CRA, which should focus on the essential requirements defined therein.

As the analysis above has shown, regulatory sandboxes could be utilized for a broader conceptualisation of risk management. In particular, with respect to cyber risk, the application and testing of requirements may extend beyond products alone, as the very concept of cyber resilience encompasses more than just product safety. Cyber resilience indeed refers to "[t]he ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources; [it] is intended to enable mission

or business objectives that depend on cyber resources to be achieved in a contested cyber environment".[4]

The examination of the measures foreseen as selection criteria in the 43 use cases analysed can be useful in identifying the core components of experimentation. These components should enable a better framing of the scope of experimentation, allowing for cross-regulation testing. By making the experimentation driven by common components, regulatory sandboxes may provide a safe space to apply and test requirements deriving from different regulations simultaneously. This possibility is clearly envisaged in interoperability and AI regulatory sandboxes: both acts foresee guidance, supervision and support in relation to the requirements of the regulations pertaining to the regulatory sandbox's scope, but also, where relevant and appropriate, for other EU and national law [cf. Article 11(2)(g) IEA and Article 57(6) AIA].

The proposed core components for experimentation are products, systems, processes and services. A *product* is a "part of the equipment (hardware, software and materials)"[5]. This component entails experimenting with requirements for the design, development, and testing of products. It implies the application of a modular risk framework that could then allow tailoring assessments based on product type. A focus on products, particularly those with digital elements that fall within the scope of the CRA, ensures they meet cybersecurity requirements and are aligned with evolving compliance and procurement standards. For example, such component can be found in the "Singapore - MAS's FinTech Regulatory Sandbox" case [UC20] (framed as assessment and mitigation of significant risks arising from the proposed solution), in "United States - West Virginia's FinTech Sandbox" [UC30] (as identification of possible risks to consumers in relation to the innovative product), in "United Arab Emirates - RegLab" [UC38] (as identification of risks associated with testing or implementing the proposed solution), or in "Austria - Framework Conditions for Automated Driving" [UC42] (as identification and prevention of further risks through a risk analysis for the entire test project).

A *system* may be defined as a "discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"[6]. This component entails the testing of specific systems, networks and infrastructure. Testing of critical systems, especially those operating in high-risk environments, contributes to developing standardized protocols for broader implementation. This is the case for "India - RBI's Financial Services Regulatory Sandbox" [UC07], which foresees the adoption of adequate built-in safeguards for IT systems to enable their proper protection. In this case, systems are enablers of secure experimentation, thus being ontologically different from single products. The system component may be derived also from the "South Korea - FSC's Financial Services Regulatory Sandbox" case [UC21], in particular for the assessment of the potential systemic risks posed by the proposed solution or service, coupled with the evaluation of the project's impact on the integrity of the financial market. This poses also the question of interconnectedness between different resources – key for market stability – expanding the scope beyond products.

A *process* is a "set of interrelated or interacting activities that use inputs to deliver an intended result"[7]. This component focuses on the experimentation of specific scenarios for the stress-test of defined processes. Testing a process helps regulators identify potential vulnerabilities, enabling the updating of relevant practices and standards. For example, in the case of "Italy - Financial Services Regulatory Sandbox" [UC09], this component is connected to the improvement of risk management systems, procedures and processes for operators, or to the increased effectiveness in identifying and/or measuring and managing risks. The same is true for "Denmark - Regulatory Test Zones for

[4] As retrieved from the NIST Glossary, defined in NIST SP 800-160 Vol. 2 Rev. 1, available at: https://csrc.nist.gov/glossary/term/cyber_resiliency.

[5] As retrieved from the NIST Glossary, defined in NISTIR 8040 under Product (included from ISO 9241-11:1998), available at: https://csrc.nist.gov/glossary/term/product.

[6] As retrieved from the NIST Glossary, defined in NIST SP 800-34 Rev. 1 under Information System from 44 U.S.C., Sec. 3502, available at: https://csrc.nist.gov/glossary/term/system.

[7] As retrieved from the NIST Glossary, defined in NIST SP 800-160v1r1 (included from ISO 9000:2015), available at: https://csrc.nist.gov/glossary/term/process.

energy technologies" [UC41], where the measures foreseen include the identification of adequate protections and risk reduction measures of consumers and companies during the test process – thus, it is the same risk management activity that is considered in its entirety as a process. A similar approach may be seen also in the case of "Taiwan - Regulatory sandbox for self-driving vehicles" [UC43].

A *service* may be defined as the "performance of activities, work, or duties"[8]. This component includes the testing of specific services before widespread adoption. Testing innovative services can inform regulatory requirements by highlighting practical challenges and solutions for real-world applications. This is exemplified by the case of interoperability regulatory sandboxes illustrated in Subsection 2.1, considering that they focus on the development, training, testing and validation of innovative interoperability solutions (meant for providing trans-European digital public services). Moreover, this component is also considered in use cases such as "Jordan - CBJ's FinTech Regulatory Sandbox" [UC10] (for the identification of the risks associated with the service in scope of experimentation, together with the definition of a comprehensive risk mitigation plan), or "Australia - AEMC's Energy Regulatory Sandboxes" [UC40] (which implies the adoption of measures to mitigate adverse effects on safety, reliability or security of electricity supply).

In this conceptualisation, the type of technology – such as artificial intelligence or distributed ledger – is an independent variable, since it is related to the specific projects interested in participating to the regulatory sandbox. On the other hand, data[9] elaboration and protection represents a cross-component dimension to be duly evaluated and considered within every regulatory sandbox, depending also on the type of participating project. In this view, it is worth noticing that data provisioning is an element that is gaining increasing value in the standard operation of regulatory sandboxes.[10]

Incorporating multiple components within this framework could significantly enhance its capacity to address the complexities of risk management in diverse sectors. By expanding the scope beyond products to include systems, processes, and services – with data as a cross-component dimension, and technology as an independent variable – this approach fosters a more comprehensive and precise assessment of cybersecurity requirements and, in turn, of cyber resilience. Indeed, cybersecurity requirements should be tested at different levels of abstraction, from single software to large-scale infrastructure and supporting essential services. The four proposed components thus allow experimentation at varying levels of complexity, which is essential for the feasibility and efficacy of cyber resilience regulatory sandboxes.

4. The 3PS experimentation model

4.1. Outlining the working model with respect to contextual cyber risk

Against this backdrop, a clarification is necessary: the proposed components should be contextualised with respect to the function that they serve. Experimentation should be tailored differently with respect to the role that the component will have for the participating entity. Of course, cyber risk is different for core security components, requiring specific mitigation measures – and higher assurance levels. In this view, the working model should distinguish at least two perspectives in which products, systems, processes, and services may be utilized.

[8] As retrieved from the NIST Glossary, defined in NIST SP 800-160v1r1 (included from ISO/IEC/IEEE 15288:2015), available at: https://csrc.nist.gov/glossary/term/service.

[9] Data means the "representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means", as defined in the NIST Glossary from NIST SP 800-160v1r1, available at: https://csrc.nist.gov/glossary/term/data.

[10] See, for example, the case of Zurich's AI Innovation Sandbox which couples regulatory guidance with data provisioning (visit https://www.innovationsandbox.ai/), the activities of the Datasphere Initiative related to regulatory sandboxes (visit https://www.thedatasphere.org/), or the African Union's 2024 Continental AI Strategy (available at https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf).

The first one is the business perspective. Components could be used specifically to achieve business objectives, thereby fulfilling *procedural or operational functions*. This involves ensuring support to day-to-day operations within an organisation or sector. In this case, cybersecurity requirements are aimed at increasing the safety and correct implementation of these components, while protecting data and information they may process. This perspective may be appreciated in the "Bahrain - CBB's Financial Services Regulatory Sandbox" case [UC02], where cybersecurity measures are undertaken to ensure the safety of the innovative solution or service. It also envisages the adoption of measures to mitigate major risks, such as business continuity and disaster recovery. The nature of the solutions in this case is not specified. However, an examination of the register of previous participants suggests that it predominantly includes business-related components such as digital trading platforms, cashless tipping solutions, and e-money and crowdfunding platforms.

The second perspective involves ensuring reliability[11]. Indeed, components could also be used to ensure the robustness of digital ecosystems. From a *security function*, this perspective focuses on ensuring that products, systems, processes, and services are consistently functioning, even when confronted with disruptions, incidents, or attacks since they serve basic cybersecurity needs with respect to the overall architecture. In this second case, cybersecurity serves as a core feature for ensuring stability of critical infrastructure. Additionally, due to the importance of security components, the required level of assurance for cybersecurity requirements should be higher: unlike procedural components, security ones need to provide a reliable degree of resilience in adverse conditions. This may be the case envisaged by "United Arab Emirates - ADGM's FinTech RegLab" [UC24], for which the potential of promoting better risk management solutions for the financial industry may be evaluated when selecting a project for the regulatory sandbox.

Therefore, the experimentation model should consider both functions in relation to each component proposed in Subsection 3.2. The 3PS model is thus named after the initials of (P)roducts, (S)ystems, (P)rocesses and (S)ervices on the one hand, which are foreseen as components of experimentation; and, on the other hand, of the (P)rocedural and (S)ecurity functions for each one of them. The functions are "project dependant", since it is only with a specific component (and its objective) that such evaluation can be made. This also enriches the carrying out of experimentation, since it makes it sensitive to the defined context in which the component is deployed. Figure 1 below illustrates the proposed 3PS experimentation model.

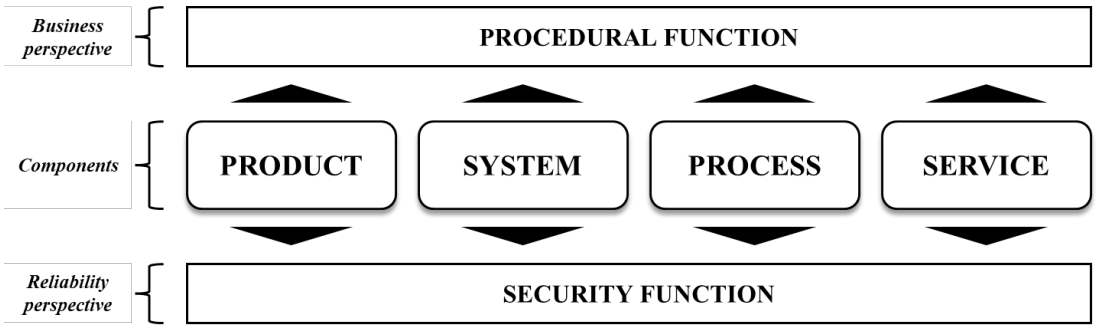

Figure 1: Visual representation of the 3PS experimentation model.

The 3PS model would allow for the testing and evaluation of multiple components of cyber resilience, expanding the scope beyond the narrower focus of traditional product safety regulations. Moreover, while testing one type of component (e.g., product), the competent authority and the participating entity may agree to experiment with the applicability of cybersecurity requirements in other connected components (e.g., process). In addition, having a concrete framework of

[11] Reliability can be understood as "[t]he ability of a system or component to function under stated conditions for a specified period of time", as retrieved from the NIST Glossary, defined in NIST SP 800-160 Vol. 2 Rev. 1 (included from IEEE Standard Computer Dictionary), available at: https://csrc.nist.gov/glossary/term/reliability.

experimentation allows for more structured regulatory learning: evidence from the regulatory sandbox could be grouped with respect to the components and functions represented, allowing also for a more direct comparison of outputs between different schemes.

To enable a more practical understanding of the model, Table 1 below highlights examples from the financial services sector, showcasing combinations of components for each envisaged function.

Table 1
3PS experimentation model matrix with examples from financial services

	PRODUCT	**SYSTEM**	**PROCESS**	**SERVICE**
PROCEDURAL	*Mobile banking apps*	*Financial market trading platforms*	*Account opening procedures*	*Wealth management services*
SECURITY	*Fraud detection software*	*Identity verification systems (e.g., KYC platforms)*	*Transaction monitoring workflows*	*Anti-money laundering (AML) monitoring*

The 3PS model may be utilised in different ways with respect to the different stakeholders involved in the cyber resilience regulatory sandbox. A clarification is needed when it comes to the main types of actors that are usually involved in the experimentation. In order to have a regulatory sandbox, two main actors are needed: (i) the regulator (i.e., the competent authority setting up the scheme), which is in charge of overall supervision and of regulatory guidance; (ii) the innovator (i.e., the participating entity), which proposes the project for testing and experimentation, and may be either public or private. The latter, however, may include both the manufacturer of a specific component and its deployer, thus the entity actually using it. They may be the same entity in case of in-house development or be separate in case of an entity acquiring off-the-shelf items for their networks and infrastructure. Apart from regulators and innovators, regulatory sandboxes may also include other actors, such as standardisation organisations, testing and experimentation facilities, research labs, centres of excellence, or individual researchers [cf. Article 58(2) point (f) AIA]. However, the analysis of their possible role in utilising the 3PS model falls beyond the scope of this paper.

Considering the core stakeholders briefly outlined above, the utilisation of the 3PS model may be evaluated taking into account two dimensions. First of all, it is important to highlight what stakeholders could do *with* the model. In this sense, the latter could support in the structured definition of sandbox plans, where the scope of experimentation and related requirements, testing activities, and methodologies are outlined and agreed upon. By using a standardised approach, the model could simplify and streamline this procedure. On the other hand, it is also key to define what stakeholders could do *within* the model. By defining the core structural components of experimentation, the model could also guide stakeholders when producing evidence and performing their reporting duties, clearly grouping the collected evidence for better processing. This would enable a more coherent regulatory learning process, while also supporting structured change management for participants with respect to the components under experimentation. In this view, also exit reports – i.e., a document summarising the activities carried out by a project in the regulatory sandbox [cf. Article 57(7) AIA] – and cumulative evaluation reports of the overall scheme could present possible input for policy or regulatory change in an optimised manner.

4.2. Evaluating CRA's essential cybersecurity requirements

A main starting point for any cyber resilience regulatory sandbox lies in the essential cybersecurity requirements described in Annex I of the CRA. These requirements not only set the baseline for compliance but also shape the framework for testing and experimentation. Understanding how they integrate with the components defined above is therefore essential for designing effective and adaptive experimentation environments.

While the CRA focuses on products with digital elements, cybersecurity practices extend far beyond this scope, embodying a holistic approach that transcends product safety alone. This is the case also for the essential cybersecurity requirements foreseen in the CRA. Therefore, it is important to understand how these requirements apply to products, systems, processes and services.

With respect to products, key requirements pertain to:

- *Secure design and development*. Products with digital elements should be designed, developed and produced to ensure an appropriate level of cybersecurity with respect to the specific risks they face [Part I(1) of Annex I CRA].
- *Default configurations*. Products should be made available with secure-by-default settings and allow a reset to original state [Part I(2) point (b)].
- *Data confidentiality and integrity*. Data confidentiality should be protected by applying at rest or in transit encryption [Part I(2) point (e)]. Data integrity should be protected against any manipulation or modification [Part I(2) point (f)].

With respect to systems, key requirements pertain to:

- *Access control*. Authentication, identity or access management systems should be adopted [Part I(2) point (d)].
- *Interconnected systems' integrity*. Products should minimize possible negative impacts on connected networks and devices [Part I(2) point (i)].
- *Dependencies' mapping*. A software bill of materials should be maintained, also by tracking top-level dependencies [Part II(1)].

With respect to processes, key requirements pertain to:

- *Risk assessment*. A cybersecurity risk assessment should be performed to address identified risks [Part I(2)].
- *Vulnerability handling*. Vulnerabilities should be identified and remediated without delay [Part II(1) and (2)]. Regular security tests and reviews should be conducted [Part II(3)]. A policy for coordinated vulnerability disclosure should be defined and enforced [Part II(5)].
- *Incident handling*. Measures should be implemented to reduce incident impacts [Part I(2) point (k)] and maintain availability of services [Part I(2) point (h)].

With respect to services, key requirements pertain to:

- *Security updates*. Automatic and timely updates should be addressed and, where applicable, enabled by default [Part I(2) point (c]. Mechanisms for securely distributing updates and mitigating vulnerabilities should be provided [Part II(7)].
- *User guidance*. Product users should be notified of relevant updates, advisory messages, and possible mitigation actions [Part II(8)].
- *Vulnerability information sharing*. Details on fixed vulnerabilities should be shared, together with clear remediation steps [Part II(4)]. Channels for receiving and disseminating information about vulnerabilities should be established [Part II(4)].

In conclusion, starting from requirements on the specific product, this Regulation also entails controls that are applicable to the other components considered: to have safe and secure products with digital elements in the European market involves also testing requirements on connected systems, processes and services. However, these requirements are designed to functionally support and enhance the security of the product under experimentation. Hence, in this case, the basis is always product driven. Moreover, to understand the applicability of the model in evaluating the

CRA's essential cybersecurity requirements across the procedural and security functions, it is fundamental to follow real cases of experimentation within regulatory sandboxes.

5. Conclusion and future work

This paper aims to bridge a research gap on how sandboxes could become regulatory sandboxes to enhance cyber resilience. While they are referred to in several EU directives and regulations, such as the Interoperable Europe Act, the Artificial Intelligence Act, and the Cyber Resilience Act, there is limited research that embodies the utilization of shared models or frameworks that can result in experimentation within the safe environment in a bid to apply and test appropriate cybersecurity requirements.

Here, the article introduces an experimentation framework called the 3PS model. The initial analysis used 43 use cases from various industries and demonstrated that regulatory sandboxes can be employed as effective tools for testing and implementing risk management strategies. The research revealed that risk management in regulatory sandboxes encompasses a broad range of activities beyond traditional product-oriented applications. Thus, the paper sets out the basic constituents of risk management based on a use case analysis and suggests four basic components which are essential to the model: products, systems, processes, and services. They have a twofold nature: they might be expressly designed for business-related functions or with the objective to facilitate or aid organizational functioning's dependability. Thus, the four elements which were identified might have two possible roles—a procedural role and a security role. Thus, the 3PS model is framed by considering the elements (P)roduct, (S)ystem, (P)rocess, and (S)ervice into their two respective roles (P)rocedural and (S)ecurity. Some of the possible real-life solutions for every situation have also been explained. The model envisioned not only bridges a concept gap in describing how cybersecurity requirements might be tested within regulatory sandboxes but also encompasses the broader exigences of policymakers under the likes of the Cyber Resilience Act, an additional analysis on which has been performed in terms of the cybersecurity requirements that are considered necessary pursuant to it.

The model should serve as a template for future regulatory sandboxes, particularly cyber resilience ones. Future research must advance in three areas to build on this work. First, one must conduct a comprehensive examination of relevant EU-level regulations (such as the NIS2 Directive) in order to gather additional cybersecurity mandates and insert them into the 3PS model, ensuring adaptability to evolving regulatory environments and potential enhancement of the model. This would facilitate cross-regulation testing and implementation, an emerging issue in regulatory sandboxes. A contextualised examination would also evaluate national norms of cybersecurity, sectoral regulation and nuanced cybersecurity controls for a better understanding of all the layers applicable to the chosen component. Second, attention should be paid to observing cases of cybersecurity testing in operational regulatory sandboxes, employing as well the 3PS model. Examining these real-world cases could help in identifying challenges, best practices, and loopholes in the proposed 3PS model, and verify its efficacy. Finally, there should be an attempt at mapping admitted projects within regulatory sandboxes to the 3PS model matrix. This would increase the conceptual basis of the model by providing concrete examples for all categories of components and functions. In general, these directions aim to develop knowledge in cybersecurity experimentation, enhance the useability of the 3PS model, and inform the development of cyber resilience regulatory sandboxes for future initiatives.

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] H. Rosa, W. E. Scheuerman, High-Speed Society: Social Acceleration, Power, and Modernity, Pennsylvania State University Press, Pennsylvania, United States, 2009.

[2] D. Collingridge, The Social Control of Technology, Frances Pinter (Eublishers) Ltd, London, United Kingdom, 1980.

[3] D. A. Zetzsche, R. P. Buckley, J. N. Barberis, D. W. Arner, Regulating a revolution: From regulatory sandboxes to smart regulation, Fordham J. Corp. & Fin. L., 23.31 (2017): 31-103, retrieved from https://ir.lawnet.fordham.edu/jcfl/vol23/iss1/2/.

[4] European Commission, Better Regulation Toolbox, European Union, 2023, retrieved from https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en.

[5] Council of the European Union, Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, European Union, 2020, retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XG1223%2801%29.

[6] European Commission, Staff Working Document. Regulatory learning in the EU: Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy, European Union, 2023, retrieved from https://research-and-innovation.ec.europa.eu/document/download/fc6f35cd-a8d6-4770-aefe-c09ca85cff8c_en?filename=swd_2023_277_f1.pdf.

[7] E. Bonel, Regulatory sandboxes under the Interoperable Europe Act: Tools for regulatory experimentation, in: F. Bagni, F. Seferi (Eds.), Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders, CINI's Cybersecurity National Lab, Italy, 2025, ISBN: 9788894137378, retrieved from https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.

[8] F. Bagni, Commento all'Articolo 57, in: A. Mantelero, G. Resta, & G. M. Riccio, Commentario al Regolamento sull'Intelligence Artificiale, Wolters-Kluwer, Italy, 2025.

[9] F. Bagni, F. Seferi, Commento all'Articolo 58, in: A. Mantelero, G. Resta, & G. M. Riccio, Commentario al Regolamento sull'Intelligence Artificiale, Wolters-Kluwer, Italy, 2025.

[10] F. Bagni, The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act, Rivista Italiana di Informatica e Diritto, N. 2, 2023, retrieved from https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/166/139.

[11] F. Bagni, Regulatory sandboxes as a bridge between AI and cybersecurity: Exploring the interplay between the AI Act and the Cyber Resilience Act, in: F. Bagni, F. Seferi (Eds.), Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders, CINI's Cybersecurity National Lab, Italy, 2025, ISBN: 9788894137378, retrieved from https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.

[12] F. Bagni, F. Seferi (Eds.), Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders, CINI's Cybersecurity National Lab, Italy, 2025, ISBN: 9788894137378, retrieved from https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.

[13] A. Attrey, M. Lesher, C. Lomax, The role of sandboxes in promoting flexibility and innovation in the digital age, OECD Going Digital Toolkit Note, No. 2, 2020, retrieved from https://goingdigital.oecd.org/data/notes/No2_ToolkitNote_Sandboxes.pdf.

[14] R. Parenti, Regulatory Sandboxes and Innovation Hubs for FinTech: Impact on innovation, financial stability and supervisory convergence, Study for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, European Union, 2020, retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf.

[15] F. Gangale, A. M. Mengolini, L. Covrig, S. Chondrogiannis, R. Shortall, Making energy regulation fit for purpose. State of play of regulatory experimentation in the EU, Joint Research Center, European Union, 2023. doi:10.2760/3225.

[16] European Supervisory Authorities, Update on the functioning of innovation facilitators – innovation hubs and regulatory sandboxes. European Union, 2023, retrieved from https://www.eiopa.europa.eu/document/download/c72d7a3d-64c8-4370-9b94-466e8ec2e315_en?filename=Joint%20ESAs%20Report%20on%20Innovation%20Facilitators%202023%20-%20innovation%20hubs%20and%20regulatory%20sandboxes.pdf.
[17] S. Ranchordás, V. Vinci, Regulatory Sandboxes and Innovation-friendly Regulation: Between Collaboration and Capture, Italian Journal of Public Law, Vol. 1(2024), retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4696442.
[18] A. Alaassar, A. L. Mention, T. H. Aas, (2020). Exploring how social interactions influence regulators and innovators: The case of regulatory sandboxes, Technological Forecasting and Social Change, Vol. 169 (2020). doi:https://doi.org/10.1016/j.techfore.2020.120257.
[19] K. Kert, M. Vebrova, S. Schade, Regulatory learning in experimentation spaces, Joint Research Center, European Union, 2022, retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC130458.
[20] J. Gorenstein Dedecca, M. Ansarin, K. Afrodit Adsal, K. Blind, Study on Regulatory Sandboxes in the Energy Sector, Energy Transition Expertise Centre (EnTEC), European Union, 2023, retrieved from https://op.europa.eu/en/publication-detail/-/publication/86c18e4c-1ecb-11ee-806b-01aa75ed71a1/language-en.
[21] M. Giusti, Tecniche alternative di regolazione: Stato dell'arte e prospettive, Rivista trimestrale di diritto pubblico, 3 (2024).
[22] F. Seferi, A comparative analysis of regulatory sandboxes from selected use cases: Insights from recurring operational practices, in: F. Bagni, F. Seferi (Eds.), Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders, CINI's Cybersecurity National Lab, Italy, 2025, ISBN: 9788894137378, retrieved from https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.

Appendix

Table 2
Relevant use cases of regulatory sandboxes and related key risk management measures and criteria

USE CASES (UC)	RISK MANAGEMENT MEASURES AND CRITERIA
Financial services (31 occurrences)	
[UC01] Austria - FMA's Financial Services Sandbox *(more information available at: https://www.fma.gv.at/en/fintech-point-of-contact-sandbox/fma-sandbox/)*[12]	Identification of possible threats to financial market stability or consumer protection.
[UC02] Bahrain - CBB's Financial Services Regulatory Sandbox *(more information available at: https://www.cbb.gov.bh/fintech/)*	Cybersecurity and other relevant measures to be undertaken to ensure safety of the innovative solution or service. Identification of major risks associated with the innovative solution or service, including measures to mitigate these risks, such as business continuity and disaster recovery.

[12] All links have been last accessed on 19 February 2025. Unavailable direct links have been retrieved through Internet Archive's Wayback Machine service.

USE CASES (UC)	RISK MANAGEMENT MEASURES AND CRITERIA
[UC03] Brazil - BCB's Financial Services Regulatory Sandbox *(more information available at: https://www.bcb.gov.br/en/financialstability/regulatorysandbox)*	Assessment of the nature and magnitude of the risks inherent to the innovative project. Implementation of a structure for risk management, that allows for identification, measurement, evaluation, monitoring, reporting, control and mitigation operational, credit and other relevant risks.
[UC04] Hong Kong - HKIA's Insurtech Sandbox *(more information available at: https://www.ia.org.hk/en/aboutus/insurtech_corner.html#1)*	Adoption of adequate safeguards for protecting the interests of customers during the trial. Adoption of risk management controls and control procedures to achieve the objectives of the relevant supervisory requirements.
[UC05] Hong Kong - HKMA's Fintech Supervisory Sandbox *(more information available at: https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/)*	Adoption of measures for protecting the interests of customers during the trial. Adoption of risk management controls for lack of full compliance possible negative effects posed to the financial system and customers.
[UC06] Hong Kong - SFC's Financial Services Regulatory Sandbox *(more information available at: https://www.sfc.hk/en/Welcome-to-the-Fintech-Contact-Point/SFC-Regulatory-Sandbox)*	Implementation of adequate investor protection measures to address actual or potential risks or concerns identified when they operate in the regulatory sandbox.
[UC07] India - RBI's Financial Services Regulatory Sandbox *(more information available at: https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1262)*	Implementation of measures in compliance with existing norms on consumer data protection and privacy. Adoption of adequate built-in safeguards for IT systems to protect against unauthorized access, alteration, destruction, disclosure or dissemination of records and data. Assessment and mitigation of significant risks arising from the proposed solution or service.
[UC08] Indonesia - FSA's Digital Finance Innovation Initiative *(more information available at: https://web.archive.org/web/20230614121758/https://www.ojk.go.id/iru/BE/uploads/regulation/files/file_35a2beef-e4c8-4ca8-8f42-4cfc0f180246-07092022161630.pdf)*	Compliance with consumer protection and data protection rules.
[UC09] Italy - Financial Services Regulatory Sandbox *(more information available at: https://www.bancaditalia.it/focus/sandbox/index.html?com.dotmarketing.htmlpage.language=1)*	Improvement of the risk management systems, procedures and processes for banking, financial or insurance operators: optimization in terms of cost and/or internal resources, increased effectiveness in identifying and/or measuring and managing risks.

USE CASES (UC)	RISK MANAGEMENT MEASURES AND CRITERIA
[UC10] Jordan - CBJ's FinTech Regulatory Sandbox *(more information available at: https://www.cbj.gov.jo/EN/Pages/Regulatory_laboratory)*	Application of terms and conditions to ensure consumer protection, rights of consumers, and to maintain the integrity and financial stability. Identification of the risks associated with the solution or service and definition of a comprehensive risk mitigation plan.
[UC11] Malaysia - BNM's Financial Services Regulatory Sandbox *(more information available at: https://www.bnm.gov.my/sandbox)*	Demonstration of ability to identify and mitigate risks associated with the proposed solution (considering scale of the project and nature of risks). Identification of potential risks to financial institutions and consumers stemming from the testing; proposal of appropriate safeguards to address the identified risks.
[UC12] Malta - MFSA's FinTech Regulatory Sandbox *(more information available at: https://www.mfsa.mt/fintech/regulatory-sandbox/)*	Definition of a dedicated plan accounting for possible risks, demonstrating the existence of a suitable mitigation plan which ensures consumer protection, market integrity and financial soundness.
[UC13] Mauritius - FSC's Financial Services Regulatory Sandbox License *(more information available at: https://www.fscmauritius.org/media/167529/regulatory-sandbox-guidelines.pdf)*	Existence of a proper risk management strategy that incorporates appropriate safeguards to mitigate potential risks, control their impact, and address possible failures effectively.
[UC14] Mauritius - MEDB's Regulatory Sandbox License *(more information available at: https://edbmauritius.org/wp-content/uploads/2022/06/Consult-the-Guidelines-to-apply-for-a-Regulatory-Sandbox-Licence-for-Fintech-Projects.pdf)*	Proposal of adequate safeguards, and specific terms and conditions to mitigate foreseeable risks associated with the project.
[UC15] Nigeria - CBN's Regulatory Sandbox *(more information available at: https://web.archive.org/web/20240725232213/https://sandbox.cbn.gov.ng/)*	Limitation of transactions' value and volume for better risk management and mitigation.
[UC16] Oman - CBO's Fintech Regulatory Sandbox Framework *(more information available at: https://cbo.gov.om/sites/assets/Documents/English/Fintech/FRSProposalFramework.pdf)*	Evaluation of potential risks and planned mitigation measures, including an emergency exit strategy for cases where live testing fails or is terminated due to non-compliance. Outline of safeguards to protect customers, offering necessary guarantees and compensation.
[UC17] Philippines - BSP's Financial Services Regulatory Sandbox *(more information available at: https://www.bsp.gov.ph/Regulations/Issuances/2022/1153.pdf)*	Adoption of measures to protect the rights and interests of consumers during the experimentation. Identification of significant risks (including IT and cybersecurity, data integrity and data privacy, and consumer protection) and of safeguards and risk mitigation strategies.

USE CASES (UC)	RISK MANAGEMENT MEASURES AND CRITERIA
[UC18] Qatar - CBQ's FinTech Sandbox & Licensing Registration Platform *(more information available at: https://sandbox.qcb.gov.qa/login)*	Preparation of risk analysis and a corresponding risk mitigation plan.
[UC19] Saudi Arabia - SAMA's Open Banking Regulatory Sandbox *(more information available at: https://www.sama.gov.sa/en-US/Regulatory%20Sandbox/Documents/Regulatory_Sandbox_Framework_English-NOV2020.pdf)*	Identification and addressing of any risks for consumers and markets resulting from the proposed innovation (comprehensive risk assessment and mitigation plan).
[UC20] Singapore - MAS's FinTech Regulatory Sandbox *(more information available at: https://www.mas.gov.sg/development/fintech/regulatory-sandbox)*	Definition of appropriate boundary conditions for experimenting while maintaining consumer protection, and market safety and soundness. Assessment and mitigation of significant risks arising from the proposed solution or service.
[UC21] South Korea - FSC's Financial Services Regulatory Sandbox *(more information available at: https://sandbox.fintech.or.kr/?lang=en)*	Assessment of measures to ensure the security and privacy of consumer information, and consumer protection at large. Determination of the robustness of the risk management framework, including measures to mitigate financial and operational risks. Assessment of the potential systemic risks posed by the proposed solution or service; evaluation of the project's impact on the integrity of the financial market.
[UC22] Spain - Financial Services Regulatory Sandbox *(more information available at: https://www.tesoro.es/en/sandbox/solicitudes-para-el-espacio-controlado-de-pruebas)*	Evaluation of the impact of the project on the financial system.
[UC23] Taiwan - FSC's Financial Technology Innovative Experimentation *(more information available at: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380254)*	Identification of protection measures for participants. Assessment of potential risks and preparation of relevant response measures.
[UC24] United Arab Emirates - ADGM's FinTech RegLab *(more information available at: https://www.adgm.com/setting-up/fintech)*	Identification of potential to promote better risk management solutions for the financial industry. Existence of a regulatory plan, setting out activities, internal controls and resources to address identified risks. Adoption of safeguards with respect to associated risks and the type of clients potentially impacted by the proposed solution or service.

USE CASES (UC)	RISK MANAGEMENT MEASURES AND CRITERIA
[UC25] United States - Florida's Financial Technology Sandbox Innovator *(more information available at: https://flofr.gov/sitePages/FinancialTechnologySandbox.htm)*	Evaluation of the potential risk to consumers, including the methods that will be used to protect consumers and resolve complaints during the experimentation.
[UC26] United States - Kentucky's Insurance Regulatory Sandbox *(more information available at: https://casetext.com/statute/kentucky-revised-statutes/title-25-business-and-financial-institutions/chapter-304-insurance-code/subtitle-3043-authorization-of-insurers-and-general-requirements/regulatory-sandbox)*	Evaluation of how the innovation provides suitable consumer protection and not pose an unreasonable risk of consumer harm.
[UC27] United States - Nevada's Financial Services Sandbox Program *(more information available at: https://business.nv.gov/Programs/Nevada_Sandbox_Program/)*	Evaluation of the ability to conduct experimentation that does not place undue risk on consumers.
[UC28] United States - North Carolina's Financial and Insurance Regulatory Sandbox *(more information available at: https://www.innovation.nc.gov/)*	Identification of the methods used to protect consumers during the experimentation.
[UC29] United States - Vermont's Insurance Regulatory Sandbox *(more information available at: https://dfr.vermont.gov/industry/insurance/regulatory-sandbox)*	Assessment of risks such as the experimentation does not substantially or unreasonably increase any risk to consumers.
[UC30] United States - West Virginia's FinTech Sandbox *(more information available at: https://dfi.wv.gov/fintech/Pages/default.aspx)*	Identification of possible risks to consumers in relation to the innovative product or service. Definition of risk mitigation measures to limit potential harm to consumers.
[UC31] United States - Wyoming's Financial Technology Sandbox *(more information available at: https://wyomingbankingdivision.wyo.gov/banks-and-trust-companies/financial-technology-sandbox)*	Identification of potential risk to consumers and of risk mitigation methods to protect consumers during experimentation.

Cross-sectoral (8 occurrences)	
[UC32] France - France Experimentation *(more information available at: https://www.modernisation.gouv.fr/transformer-laction-publique/france-experimentation)*	Development of a detailed framework to evaluate the exemption's impact, including defining data collection and transmission protocols for assessing associated risks and the methods used. Identification of mitigation measures for potential additional risks; establishment of a plan for post-implementation evaluation of socio-economic effects, such as economic, environmental, health, and safety outcomes (ensuring a comprehensive risk assessment).
[UC33] Italy - Italy Experimentation *(more information available at: https://innovazione.gov.it/progetti/sperimentazione-italia/)*	Adoption of requirements deemed necessary to mitigate the risks connected to the experimentation.
[UC34] Malta - MDIA's Technology Assurance Sandbox *(more information available at: https://web.archive.org/web/20240522201002/https://mdia.gov.mt/technology-assurance-sandbox/)*	Identification and assessment of risks in terms of impact, severity, and probability of occurrence, including mitigation plans against the identified risks.
[UC35] Portugal - Free Zones for Technology *(more information available at: https://portugaldigital.gov.pt/en/accelerating-digital-transition-in-portugal/testing-and-incorporating-new-technologies/technological-free-zones-zlt/)*	Definition of a monitoring plan for the tests to be carried out. Drawing up an adequate risk assessment and a clear risk mitigation strategy.
[UC36] Saudi Arabia - CST's Emerging Technologies Regulatory Sandbox *(more information available at: https://www.cst.gov.sa/en/services/Pages/Emerging_Technologies_sandbox.aspx)*	Identification and addressing of any risks for consumers and markets resulting from the proposed innovation (comprehensive risk assessment and mitigation plan).
[UC37] Spain - AI Regulatory Sandbox Pilot Scheme *(more information available at: https://www.boe.es/buscar/doc.php?id=BOE-A-2023-22767)*	Evaluation of the relative and absolute impact on economy and society of general-purpose AI models; evaluation of their potential to be transformed into high-risk AI systems. Evaluation of compliance with rules on personal data protection.
[UC38] United Arab Emirates - RegLab *(more information available at: https://reglab.gov.ae/)*	Identification of risks associated with testing or implementing the proposed solution or service. Definition of a risk management plan.

[UC39] United Arab Emirates - TDRA's ICT Regulatory Sandbox *(more information available at: https://tdra.gov.ae/en/Pages/ict-regulatory-sandbox)*	Definition of detailed risk management strategies.
Energy (2 occurrences)	
[UC40] Australia - AEMC's Energy Regulatory Sandboxes *(more information available at: https://www.aemc.gov.au/market-reviews-advice/regulatory-sandboxes)*	Adequate consumer protection in connection with the trial project. Measures to mitigate adverse effects on AEMC's operation of the power system and market. Measures to mitigate adverse effects on safety, reliability or security of electricity supply.
[UC41] Denmark - Regulatory Test Zones for energy technologies *(more information available at: https://ens.dk/ansvarsomraader/forskning-udvikling/regulatoriske-testzoner)*	Identification of adequate protections and risk reduction measures of consumers and companies during the test process (e.g., financial and supply-related risks).
Transportation (2 occurrences)	
[UC42] Austria - Framework Conditions for Automated Driving *(more information available at: https://www.bmk.gv.at/en/topics/mobility/alternative_transport/automated/framework/roads.html)*	Performance of a route analysis and risk assessment for the planned test route or the planned test area; results to be incorporated into risk management for the test plan. Identification and prevention of further risk requirements through a risk analysis for the entire test project.
[UC43] Taiwan - Regulatory sandbox for self-driving vehicles *(more information available at: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0030147)*	Establishment of protective measures for experimentation participants and stakeholders. Assessment of potential risks, and adoption of relevant response measures and other safety or risk control measures.