Tailored IoT & BigData Sandboxes and Testbeds for Smart, Autonomous and Personalized Services in the European Finance and Insurance Services Ecosystem

D6.14 – Testbeds Support and Certification Services II

Revision Number	3.0
Task Reference	T6.6
Lead Beneficiary	NOVA
Responsible	Pedro Maló
Partners	AGRO AKTIF ATOS BANKIA BOC BOS BPFI CP CXB ENG GFT JRC NBG NOVA UNP UPRC WEA
Deliverable Type	Report (R)
Dissemination Level	Public (PU)
Due Date	2021-03-30
Delivered Date	2022-04-15
Internal Reviewers	GFT, NUIG
Quality Assurance	INNOV
Acceptance	WP Leader Accepted and Coordinator Accepted
EC Project Officer	Beatrice Plazzotta
Programme	HORIZON 2020 - ICT-11-2018
	This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 856632

Contributing Partners

Partner Acronym	**Role**[1]	**Author(s)**[2]
NOVA	Lead Beneficiary	Pedro Maló, Giovanni Di Orio, Guilherme Brito
GFT, NUIG	Internal reviewers	
INNOV	QA reviewer	John Soldatos

Revision History

Version	Date	Partner(s)	Description
0.1	2022-02-01	NOVA	ToC Version
0.2-0.9	2022-04-08	Bogazici University, Innovation Sprint, Bogazici University, INNOV-ACTS LTD, Gradiant, UBITECH Ltd, University of Piraeus Research Center (UPRC) - Bank of Cyprus (BOC), Bogazici University, JSI, IBM, Reportbrain	Declarations of conformance of INFINITECH assets
1.0	2022-04-13	NOVA	First Version for Internal Review
2.0	2022-04-14	NOVA	Version for Quality Assurance
2.1	2022-04-15	NOVA	Final Version
3.0	2022-04-15	GFT	Version ready for the submission

[1] Lead Beneficiary, Contributor, Internal Reviewer, Quality Assurance

[2] Can be left void

Executive Summary

This deliverable is the second delivery of task T6.6. This task implements the defined processes for certifying digital finance/insurance solutions. Special emphasis is paid in regulatory compliance and standards-compliance certification processes. The implemented process follows on the definition and design of the certification model and related methodology/process for the fintech solutions performed in the first deliverable of the task. The certification and compliance services focus on regulatory and security standards compliance. The INFINITECH certification process has been defined to be served on a self-certification mode and using a well-established stepwise process.

Certification and compliance services focuses on regulatory and security standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH which are: ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements; ISO/IEC 27701 Privacy Information Management System (PIMS); Payment Card Industry Data Security Standard (PCI DSS); National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile; GDPR - The General Data Protection Regulation; PSD 2 - Payment Service Directive 2; MiFID II - Markets in Financial Instruments Directive II; 4AMLD – 4th Anti-Money Laundering Directive. Out of these, a set of requirements have been elicited that define the main aspects needed to be considered by duly compliant fintech solutions.

A total of 20 (twenty) assets have been analysed following the defined requirements of regulatory and security standards compliance. These are publicly available assets (i.e., existing in the INFINITECH Marketplace) and that have originated out the project developments. Assets'-owning partners have provided declarations of conformance for their foreground technologies identifying Full Compliance, Partial Compliance or Not Applicable (requirement).

The document provides the assurance of the high levels of compliance of the project's technologies to the most relevant regulatory and security standards for fintech solutions. Out of the 177 requirements considered relevant by the analysed assets, 166 (i.e., 93.8%) have full compliance from the INFINITECH technologies. This gives a clear indication that the project's developments have been performed with the maximum criteria of conformance to regulations and security standards.

Considering the few Partial Compliance to the defined requirements, these are mainly related with different ways to meet the requirement that is not fully aligned the one described by the requirement but that indeed provide general coverage to the requirement. Or also, that for fully fulfilling some requirement it will depend on the deployment setup but indeed these are supported if needed (non-mandatory requirement).

Deliverable D6.14 will be followed by a final deliverable which the following foreseen content: Deliverable D6.15 'Testbeds Support and Certification Services - III' at M36: Report of the conformance analysis for all of the INFINITECH assets and externalisation (in the projects' marketplace) of the conformance method and analyses, for promoting outreaching of fully compliant fintech solutions.

Table of Contents

List of Figures

List of Tables

Abbreviations/Acronyms

Abbreviation	Definition
2FA	Two-factor Authentication
3AMLD	3rd Anti-Money Laundering Directive,
4AMLD	4th Anti-Money Laundering Directive
AML	Anti-money laundering
CTF	Counter-terrorist financing
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
KYC	Know Your Customer
MFA	Multi-Factor authentication
MiFID II	Markets in Financial Instruments Directive II
MiFIR	Markets in Financial Instruments Regulation
NIST	National Institute of Standards and Technology
OTC	Over-the-Counter
PCI DSS	Payment Card Industry Data Security Standard
PIMS	Privacy Information Management System
PSD 2	Payment Service Directive 2
SIEM	Security Information and Event Management

1 Introduction

This deliverable is the second delivery of task T6.6 of the INFINITECH project. This task implements the defined processes for certifying digital finance/insurance solutions. Special emphasis is paid in regulatory compliance and standards-compliance certification processes. The implemented process follows on the definition and design of the certification model and related methodology/process for the fintech solutions performed in the first deliverable of the task. The certification and compliance services focus on regulatory and security standards compliance. The INFINITECH certification process has been defined to be served on a self-certification mode and using a well-established stepwise process.

Certification and compliance services focuses on regulatory and security standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH which are: ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements; ISO/IEC 27701 Privacy Information Management System (PIMS); Payment Card Industry Data Security Standard (PCI DSS); National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile; GDPR - The General Data Protection Regulation; PSD 2 - Payment Service Directive 2; MiFID II - Markets in Financial Instruments Directive II; 4AMLD – 4th Anti-Money Laundering Directive. Out of these, a set of requirements have been elicited that define the main aspects needed to be considered by duly compliant fintech solutions.

A set of 20 (twenty) assets have been analysed following the defined requirements of regulatory and security standards compliance. These are publicly available assets (i.e., existing in the INFINITECH Marketplace) and that have originated out the project developments. Assets'-owning partners have provided declarations of conformance for their foreground technologies identifying Full Compliance, Partial Compliance or Not Applicable (requirement).

1.1 Objective of the Deliverable

Deliverable D6.14 'Testbeds Support and Certification Services - II' provides an analysis of regulatory and security standards conformance for the INFINITECH assets by means of a self-compliance assessment (declaration). The result of this deliverable aims to provide: (1) duly guarantee of the high levels of compliance of the project's technologies to the most relevant regulatory and security standards for fintech solutions; and (2) ease the exploitation pathways of the technological solutions by meeting the highest regulatory and security standards.

Deliverables D6.14 builds on top of the developments described on Deliverable D6.13 'Testbeds Support and Certification Services - I' where it has been provided a specification of the self-certification and support services to be established for fintech solutions and testbeds. In particular, D6.13 defined the certification process, to be used to by developers of fintech solutions, to assure that their solutions comply with relevant and applicable standards and regulations.

Deliverable D6.14 will be followed by Deliverable D6.15 'Testbeds Support and Certification Services - III' at M36, which will report of the conformance analysis for all the INFINITECH assets and on the externalisation (in the projects' marketplace) of the conformance method and analyses, for promoting outreaching of fully compliant fintech solutions.

1.2 Insights from other Tasks and Deliverables

Certification and compliance services focuses on regulatory and security standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH as identified by the work performed already on task T2.4, duly reported in deliverables 'D2.7 – Security and Regulatory Compliance Specifications – Version I' and D2.8 'Security and Regulatory Compliance Specifications – Version II'.

1.3 Updates from the Previous Version

Deliverables D6.14 evolves Deliverable D6.13 'Testbeds Support and Certification Services - I' where it has been provided a specification of the self-certification to be established for fintech solutions and testbeds. D6.13 defined the certification process, to be used to by developers of fintech solutions, to assure that their solutions comply with relevant and applicable standards and regulations. D6.14 reports on the implementation of the self-certification process.

1.4 Structure

Section 2 provides a brief view of the INFINITECH self-certification method. The method includes the description of the declaration of conformance (questionnaire) to assert regulatory and security standards compliance.

Section 3 provides the view of on the conformance analysis of the INFINITECH assets. It includes an overall analysis based on the declarations of conformance of the INFINITECH assets provided by assets' owners.

2 INFINITECH Self-Certification/Compliance

The INFINITECH certification/compliance focuses on regulatory and security standards compliance. The INFINITECH certification is used to by developers of fintech solutions to assure that their solutions comply with relevant and applicable standards and regulations.

The INFINITECH certification process is served on a self-certification mode, meaning that applicants to the certification will perform themselves the certification validation check.

Certification and compliance focus on regulatory and security standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH which are:

- ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements
- ISO/IEC 27701 Privacy Information Management System (PIMS)
- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile
- GDPR - The General Data Protection Regulation
- PSD 2 - Payment Service Directive 2
- MiFID II - Markets in Financial Instruments Directive II
- 4AMLD – 4th Anti-Money Laundering Directive

The full details of these and associated Regulatory and Security Standards compliance requirements have been duly provided/described in deliverable D6.13. Testbeds Support and Certification Services I. For completeness, a summary of these is provided in Appendix A: Conformance Requirements details .

2.1 Declaration of conformance (questionnaire)

To assert regulatory and security standards compliance, it was created a comprehensive questionnaire – the declaration of conformance. The declaration includes:

- means of identification of the asset allowing traceability
- a brief description of the asset for comprehension purposes
- identification and address of the organisation owning the asset
- the relevant regulatory and security standards with which the asset complies
- a statement, stating responsibility for the self-conformance
- any supplementary information (if applicable)
- the date the declaration was issued
- your name, position inside the organisation and signature

Asset name	<< Name of the asset >>	**Version/ID**	<< version >>
Asset description	<< Short description of the asset >>>		

Organisation name	<< Name of asset-owning organisation >>	**VAT**	<< VAT >>
Full Address	<< Full address of the asset-owning organisation >>		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)				
GMS-0002 Risk Management/Monitoring				

GMS-0003 Security Awareness & Training				
GMS-0004 Password Policy Enforcement				
GMS-0005 Information Asset Management				
GMS-0006 Anonymization				
GMS-0007 Pseudonymization				
GMS-0008 Authentication and Authorization mechanisms				
GMS-0009 Data Encryption				
GMS-0010 Data Discovery and Classification				
GMS-0011 Pseudonymization				
GMS-0012 Authentication and Authorization mechanisms				
GMS-0013 Secure network				
GMS-0014 Secure cardholder data				
GMS-0015 Vulnerability management				
GMS-0016 Access control				
GMS-0017 Network monitoring and testing				
GMS-0018 Information security				
GMS-0019 Supplier Management				
GMS-0020 Risk Management/Monitoring				
GRS-0001 Strong Multi-Factor authentication (MFA)				
GRS-0003 Patch Management				
GRS-0005 Phone Call Recording				
GRS-0006 Email Logging				
GRS-0007 Examination & Investigation				
GRS-0008 Customer Due Diligence				
GRS-0009 Name/Entity Matching				
GMS-1001 Information Security Policies				
GMS-1002 Business Continuity				
GMS-1003 Risk Assessment				
GMS-1004 Policies and Procedures				
GMS-1005 Management Information & Reporting				
GMS-1006 Reviews & Audits				
GMS-1007 Due Diligence				
GMS-1008 Building Security				
GMS-1009 Disposal				
GMS-1010 Supplier Relationships				

Any other information	<< Any other information deemed relevant >>

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	<< Ful Name of person >>	**Position**	<< Position in Organisation >>
Signature	<< Signature of person >>	**Date**	DD / MM / YYYY

3 Conformance of INFINITECH Assets

3.1 INFINITECH Assets Analysed

The following table identify the assets that were analysed at this stage. These are publicly available assets (i.e., present in INFINITECH Marketplace) and that have originated from the project developments.

Table 1 - 3.1 List of INFINITECH Assets Analysed

ID	Asset Title
01	ERC1155 Token Smart Contract for Hyperledger Fabric
02	Processed Synthetic RWD for binary modelling
03	Processed Synthetic RWD for tristate modelling
04	Binary wellbeing assessment RF model
05	Tristate wellbeing assessment RF model
06	Raw Synthetic RWD
07	Transaction Graph Dataset for the Ethereum Blockchain
08	Portfolio-Value-at-Risk-estimation
09	Sentiment analysis in financial news
10	DeepVaR: Value-at-Risk prediction leveraging Deep Learning
11	Tokenization on Hyperledger Fabric -ERC20 chaincode
12	Automatic data anonymization tool for preserving privacy and utility on datasets
13	Blockchain-enabled Consent Management
14	INFINITECH Open API Gateway
15	INFINITECH Data Collection
16	SMEs Cashflow prediction
17	Scalable Transaction Graph Analysis Component
18	Pseudoanonymizer
19	BC based secure execution environment and data marketplace for federated learning
20	News Sentiment API

3.2 Analysis of the Conformance of INFINITECH Assets

The following table depicts – in a visual tabular representation – the conformance of the analysed INFINITECH assets. Conformance is described as **[.]** = Not Applicable, **[FC]** = Full Compliance, and **[PC]** Partial Compliance.

Table 2 - 3.2 Requirements Vs. Assets Compliance Matrix

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
GMS-0001	.	FC	FC	FC	FC	FC	.	.	.	.	FC	.	FC	PC	PC	.	.	.	FC	FC
GMS-0002	.	FC	FC	FC	FC	FC	.	.	.	.	.	FC	.	.	.	.	.	.	.	FC
GMS-0003	.	FC	FC	FC	FC	FC	.	.	.	.	FC	FC	.	.	.	.	.	.	FC	FC
GMS-0004	.	FC	FC	FC	FC	FC	.	.	.	.	FC	PC	.	.	.	.	.	.	FC	.
GMS-0005	.	FC	FC	FC	FC	FC	.	.	.	.	FC	.	FC	.	.	.	.	.	FC	FC
GMS-0006	.	FC	FC	FC	FC	FC	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-0007	.	FC	FC	FC	FC	FC	.	.	.	.	.	.	.	.	.	FC	.	FC	.	.
GMS-0008	.	FC	FC	FC	FC	FC	.	.	.	.	FC	PC	FC	.	PC	.	.	.	FC	FC
GMS-0009	.	FC	FC	FC	FC	FC	.	.	.	.	.	.	FC	.	.	.	.	PC	.	FC
GMS-0010	.	FC	FC	FC	FC	FC	.	.	.	.	.	.	FC	.	.	.	.	.	.	FC

GMS-0011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC	.	FC	.	FC
GMS-0012	.	.	.	.	.	.	.	.	.	.	FC	.	FC	.	PC	.	.	.	FC	FC
GMS-0013	.	.	.	.	.	.	.	.	.	.	.	.	PC	PC	PC	.	.	.	.	FC
GMS-0014	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-0015	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-0016	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-0017	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-0018	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-0019	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
GMS-0020	.	.	.	.	.	.	.	.	.	.	.	FC	.	.	.	.	.	.	.	FC
GRS-0001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
GRS-0003	.	.	.	.	.	.	.	.	.	.	.	.	FC	FC	FC	.	.	.	.	.
GRS-0005	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
GRS-0006	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
GRS-0007	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
GRS-0008	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
GRS-0009	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-1001	.	FC	FC	FC	FC	FC	.	.	.	.	FC	PC	FC	.	.	.	.	.	.	FC
GMS-1002	.	FC	FC	FC	FC	FC	.	.	.	.	FC	.	.	.	.	.	.	.	.	FC
GMS-1003	.	FC	FC	FC	FC	FC	.	.	.	.	FC	.	.	.	.	.	.	.	.	FC
GMS-1004	.	FC	FC	FC	FC	FC	.	.	.	.	.	PC	.	.	.	.	.	.	.	FC
GMS-1005	.	FC	FC	FC	FC	FC	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-1006	.	FC	FC	FC	FC	FC	.	.	.	.	FC	PC	.	.	.	.	.	.	.	FC
GMS-1007	.	FC	FC	FC	FC	FC	.	.	.	.	.	.	.	.	.	.	.	.	.	FC
GMS-1008	.	FC	FC	FC	FC	FC	.	.	.	.	.	FC	.	.	.	.	.	.	.	FC
GMS-1009	.	FC	FC	FC	FC	FC	.	.	.	.	.	FC	.	.	.	.	.	.	.	FC
GMS-1010	.	FC	FC	FC	FC	FC	.	.	.	.	.	FC	.	.	.	.	.	.	.	FC

It is worth noting that out of the 177 requirements considered relevant from the analysed assets, 166 of these (i.e., 93.8%) have full compliance from the INFINITECH technologies. Most Partial Compliance relates mainly with different options to meet the requirement that is not fully aligned the one described by the requirement but that indeed provide general coverage to the requirement. This is shown in the next figure.

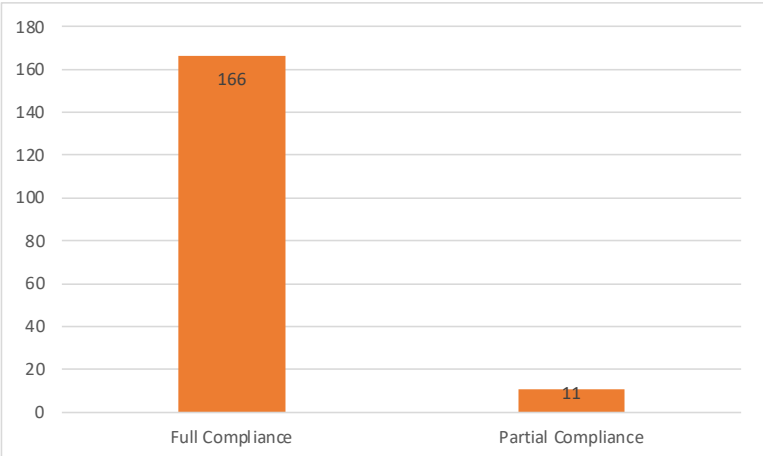


Figure 1 – Number of requirements having Full Compliance and Partial Compliance

3.3 Declarations of conformance of the INFINITECH assets

3.3.1 ERC1155 Token Smart Contract for Hyperledger Fabric

Asset name	ERC1155 Token Smart Contract for Hyperledger Fabric	**Version/ID**	1.0
Asset description	Hyperledger Fabric chain code implementing ERC1155 token contract.		

Organisation name	Bogazici University	**VAT**	Beşiktaş, V.D. 1790015446
Full Address	Bogazici University, Bebek 34342, Istanbul, Turkey		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	N/A			
GMS-0002 Risk Management/Monitoring	N/A			
GMS-0003 Security Awareness & Training	N/A			
GMS-0004 Password Policy Enforcement	N/A			
GMS-0005 Information Asset Management	N/A			
GMS-0006 Anonymization	N/A			
GMS-0007 Pseudonymization	N/A			
GMS-0008 Authentication and Authorization mechanisms	N/A			
GMS-0009 Data Encryption	N/A			
GMS-0010 Data Discovery and Classification	N/A			
GMS-0011 Pseudonymization	N/A			
GMS-0012 Authentication and Authorization mechanisms	N/A			
GMS-0013 Secure network	N/A			
GMS-0014 Secure cardholder data	N/A			
GMS-0015 Vulnerability management	N/A			
GMS-0016 Access control	N/A			
GMS-0017 Network monitoring and testing	N/A			
GMS-0018 Information security	N/A			
GMS-0019 Supplier Management	N/A			
GMS-0020 Risk Management/Monitoring	N/A			
GRS-0001 Strong Multi-Factor authentication (MFA)	N/A			
GRS-0003 Patch Management	N/A			
GRS-0005 Phone Call Recording	N/A			
GRS-0006 Email Logging	N/A			
GRS-0007 Examination & Investigation	N/A			
GRS-0008 Customer Due Diligence	N/A			
GRS-0009 Name/Entity Matching	N/A			
GMS-1001 Information Security Policies	N/A			
GMS-1002 Business Continuity	N/A			
GMS-1003 Risk Assessment	N/A			

GMS-1004 Policies and Procedures	N/A			
GMS-1005 Management Information & Reporting	N/A			
GMS-1006 Reviews & Audits	N/A			
GMS-1007 Due Diligence	N/A			
GMS-1008 Building Security	N/A			
GMS-1009 Disposal	N/A			
GMS-1010 Supplier Relationships	N/A			

Any other information	The asset is an open source ERC1155 token contract Hyperledger Fabric chain code contributed to the Hyperledger Samples at https://github.com/hyperledger/fabric-samples/tree/main/token-erc-1155. Users/Organizations can download and configure/modify it according to their needs and requirements.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Can Özturan	**Position**	Faculty Member
Signature		**Date**	31 / 03 / 2022

3.3.2 Processed Synthetic RWD for binary modelling

Asset name	Processed Synthetic RWD for binary modelling	**Version/ID**	3.1
Asset description	Processed version of the Raw Synthetic RWD into weekly vectors for training, validation, and testing, including 15 input attributes and a binary outcome attribute.		

Organisation name	Innovation Sprint Sprl	**VAT**	BE0648786874
Full Address	Clos Chapelle Aux Champs 30,1200, Brussels Belgium		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		X		ISO27001:2013 certification
GMS-0002 Risk Management/Monitoring		X		ISO27001:2013 certification
GMS-0003 Security Awareness & Training		X		ISO27001:2013 certification
GMS-0004 Password Policy Enforcement		X		ISO27001:2013 certification
GMS-0005 Information Asset Management		X		ISO27001:2013 certification
GMS-0006 Anonymization		X		ISO27001:2013 certification. This is a

				synthetic dataset, by definition fully anonymized
GMS-0007 Pseudonymization		X		ISO27001:2013 certification
GMS-0008 Authentication and Authorization mechanisms		X		ISO27001:2013 certification
GMS-0009 Data Encryption		X		ISO27001:2013 certification
GMS-0010 Data Discovery and Classification		X		ISO27001:2013 certification
GMS-0011 Pseudonymization	X			
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies		X		BS 10012 Personal Information Management certification
GMS-1002 Business Continuity		X		BS 10012 Personal Information Management certification
GMS-1003 Risk Assessment		X		BS 10012 Personal Information Management certification
GMS-1004 Policies and Procedures		X		BS 10012 Personal Information Management certification
GMS-1005 Management Information & Reporting		X		BS 10012 Personal Information Management certification

GMS-1006 Reviews & Audits		X		BS 10012 Personal Information Management certification
GMS-1007 Due Diligence		X		BS 10012 Personal Information Management certification
GMS-1008 Building Security		X		BS 10012 Personal Information Management certification
GMS-1009 Disposal		X		BS 10012 Personal Information Management certification
GMS-1010 Supplier Relationships		X		BS 10012 Personal Information Management certification

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Aristodemos Pnevmatikakis	**Position**	R&D Director
Signature		**Date**	06 / 04 / 2022

3.3.3 Processed Synthetic RWD for tristate modelling

Asset name	Processed Synthetic RWD for tristate modelling	**Version/ID**	3.1
Asset description	Random Forest model to predict short term wellbeing variation, learnt from the "Processed Synthetic RWD for binary modelling" dataset, yielding 76.7% balanced accuracy.		

Organisation name	Innovation Sprint Sprl	**VAT**	BE0648786874
Full Address	Clos Chapelle Aux Champs 30,1200, Brussels Belgium		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		X		ISO27001:2013 certification
GMS-0002 Risk Management/Monitoring		X		ISO27001:2013 certification
GMS-0003 Security Awareness & Training		X		ISO27001:2013 certification
GMS-0004 Password Policy Enforcement		X		ISO27001:2013 certification
GMS-0005 Information Asset Management		X		ISO27001:2013 certification

GMS-0006 Anonymization		X		ISO27001:2013 certification. This is a synthetic dataset, by definition fully anonymized
GMS-0007 Pseudonymization		X		ISO27001:2013 certification
GMS-0008 Authentication and Authorization mechanisms		X		ISO27001:2013 certification
GMS-0009 Data Encryption		X		ISO27001:2013 certification
GMS-0010 Data Discovery and Classification		X		ISO27001:2013 certification
GMS-0011 Pseudonymization	X			
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies		X		BS 10012 Personal Information Management certification
GMS-1002 Business Continuity		X		BS 10012 Personal Information Management certification
GMS-1003 Risk Assessment		X		BS 10012 Personal Information Management certification
GMS-1004 Policies and Procedures		X		BS 10012 Personal Information Management certification

GMS-1005 Management Information & Reporting		X		BS 10012 Personal Information Management certification
GMS-1006 Reviews & Audits		X		BS 10012 Personal Information Management certification
GMS-1007 Due Diligence		X		BS 10012 Personal Information Management certification
GMS-1008 Building Security		X		BS 10012 Personal Information Management certification
GMS-1009 Disposal		X		BS 10012 Personal Information Management certification
GMS-1010 Supplier Relationships		X		BS 10012 Personal Information Management certification

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Aristodemos Pnevmatikakis	**Position**	R&D Director
Signature		**Date**	06 / 04 / 2022

3.3.4 Binary wellbeing assessment RF model

Asset name	Binary wellbeing assessment RF model	**Version/ID**	3.1
Asset description	Random Forest model to predict short term wellbeing variation, learnt from the "Processed Synthetic RWD for binary modelling" dataset, yielding 76.7% balanced accuracy.		

Organisation name	Innovation Sprint Sprl	**VAT**	BE0648786874
Full Address	Clos Chapelle Aux Champs 30,1200, Brussels Belgium		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		X		ISO27001:2013 certification
GMS-0002 Risk Management/Monitoring		X		ISO27001:2013 certification
GMS-0003 Security Awareness & Training		X		ISO27001:2013 certification

GMS-0004 Password Policy Enforcement		X		ISO27001:2013 certification
GMS-0005 Information Asset Management		X		ISO27001:2013 certification
GMS-0006 Anonymization		X		ISO27001:2013 certification. This is a model being learnt on a synthetic dataset, by definition fully anonymized
GMS-0007 Pseudonymization		X		ISO27001:2013 certification
GMS-0008 Authentication and Authorization mechanisms		X		ISO27001:2013 certification
GMS-0009 Data Encryption		X		ISO27001:2013 certification
GMS-0010 Data Discovery and Classification		X		ISO27001:2013 certification
GMS-0011 Pseudonymization	X			
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies		X		BS 10012 Personal Information Management certification
GMS-1002 Business Continuity		X		BS 10012 Personal Information Management certification
GMS-1003 Risk Assessment		X		BS 10012 Personal Information Management certification

GMS-1004 Policies and Procedures		X		BS 10012 Personal Information Management certification
GMS-1005 Management Information & Reporting		X		BS 10012 Personal Information Management certification
GMS-1006 Reviews & Audits		X		BS 10012 Personal Information Management certification
GMS-1007 Due Diligence		X		BS 10012 Personal Information Management certification
GMS-1008 Building Security		X		BS 10012 Personal Information Management certification
GMS-1009 Disposal		X		BS 10012 Personal Information Management certification
GMS-1010 Supplier Relationships		X		BS 10012 Personal Information Management certification

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Aristodemos Pnevmatikakis	**Position**	R&D Director
Signature		**Date**	06 / 04 / 2022

3.3.5 Tristate wellbeing assessment RF model

Asset name	Tristate wellbeing assessment RF model	**Version/ID**	3.1
Asset description	Random Forest model to predict short term wellbeing variation, learnt from the "Processed Synthetic RWD for tristate modelling" dataset, yielding 64.2% balanced accuracy.		

Organisation name	Innovation Sprint Sprl	**VAT**	BE0648786874
Full Address	Clos Chapelle Aux Champs 30,1200, Brussels Belgium		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		X		ISO27001:2013 certification
GMS-0002 Risk Management/Monitoring		X		ISO27001:2013 certification

GMS-0003 Security Awareness & Training		X		ISO27001:2013 certification
GMS-0004 Password Policy Enforcement		X		ISO27001:2013 certification
GMS-0005 Information Asset Management		X		ISO27001:2013 certification
GMS-0006 Anonymization		X		ISO27001:2013 certification. This is a model being learnt on a synthetic dataset, by definition fully anonymized
GMS-0007 Pseudonymization		X		ISO27001:2013 certification
GMS-0008 Authentication and Authorization mechanisms		X		ISO27001:2013 certification
GMS-0009 Data Encryption		X		ISO27001:2013 certification
GMS-0010 Data Discovery and Classification		X		ISO27001:2013 certification
GMS-0011 Pseudonymization	X			
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies		X		BS 10012 Personal Information Management certification
GMS-1002 Business Continuity		X		BS 10012 Personal Information Management certification

GMS-1003 Risk Assessment		X		BS 10012 Personal Information Management certification
GMS-1004 Policies and Procedures		X		BS 10012 Personal Information Management certification
GMS-1005 Management Information & Reporting		X		BS 10012 Personal Information Management certification
GMS-1006 Reviews & Audits		X		BS 10012 Personal Information Management certification
GMS-1007 Due Diligence		X		BS 10012 Personal Information Management certification
GMS-1008 Building Security		X		BS 10012 Personal Information Management certification
GMS-1009 Disposal		X		BS 10012 Personal Information Management certification
GMS-1010 Supplier Relationships		X		BS 10012 Personal Information Management certification

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Aristodemos Pnevmatikakis	**Position**	R&D Director
Signature		**Date**	06 / 04 / 2022

3.3.6 Raw Synthetic RWD

Asset name	Raw Synthetic RWD	**Version/ID**	3.1
Asset description	Real World Data from a simulator for 1,000 people belonging to any of four behavioural groups: athletic, normal, unfit and feeble, simulated over 2 years and 3 months.		

Organisation name	Innovation Sprint Sprl	**VAT**	BE0648786874
Full Address	Clos Chapelle Aux Champs 30,1200, Brussels Belgium		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		X		ISO27001:2013 certification

GMS-0002 Risk Management/Monitoring		X		ISO27001:2013 certification
GMS-0003 Security Awareness & Training		X		ISO27001:2013 certification
GMS-0004 Password Policy Enforcement		X		ISO27001:2013 certification
GMS-0005 Information Asset Management		X		ISO27001:2013 certification
GMS-0006 Anonymization		X		ISO27001:2013 certification. This is a synthetic dataset, by definition fully anonymized
GMS-0007 Pseudonymization		X		ISO27001:2013 certification
GMS-0008 Authentication and Authorization mechanisms		X		ISO27001:2013 certification
GMS-0009 Data Encryption		X		ISO27001:2013 certification
GMS-0010 Data Discovery and Classification		X		ISO27001:2013 certification
GMS-0011 Pseudonymization	X			
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies		X		BS 10012 Personal Information Management certification

GMS-1002 Business Continuity		X		BS 10012 Personal Information Management certification
GMS-1003 Risk Assessment		X		BS 10012 Personal Information Management certification
GMS-1004 Policies and Procedures		X		BS 10012 Personal Information Management certification
GMS-1005 Management Information & Reporting		X		BS 10012 Personal Information Management certification
GMS-1006 Reviews & Audits		X		BS 10012 Personal Information Management certification
GMS-1007 Due Diligence		X		BS 10012 Personal Information Management certification
GMS-1008 Building Security		X		BS 10012 Personal Information Management certification
GMS-1009 Disposal		X		BS 10012 Personal Information Management certification
GMS-1010 Supplier Relationships		X		BS 10012 Personal Information Management certification

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Aristodemos Pnevmatikakis	**Position**	R&D Director
Signature		**Date**	06 / 04 / 2022

3.3.7 Transaction Graph Dataset for Ethereum Blockchain

Asset name	Transaction Graph Dataset for the Ethereum Blockchain	**Version/ID**	1.0
Asset description	Graph dataset constructed from Public Ethereum Mainnet Blockchain transaction data.		

Organisation name	Bogazici University	**VAT**	Beşiktaş, V.D. 1790015446
Full Address	Bogazici University, Bebek 34342, Istanbul, Turkey		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	N/A			
GMS-0002 Risk Management/Monitoring	N/A			
GMS-0003 Security Awareness & Training	N/A			
GMS-0004 Password Policy Enforcement	N/A			
GMS-0005 Information Asset Management	N/A			
GMS-0006 Anonymization	N/A			
GMS-0007 Pseudonymization	N/A			
GMS-0008 Authentication and Authorization mechanisms	N/A			
GMS-0009 Data Encryption	N/A			
GMS-0010 Data Discovery and Classification	N/A			
GMS-0011 Pseudonymization	N/A			
GMS-0012 Authentication and Authorization mechanisms	N/A			
GMS-0013 Secure network	N/A			
GMS-0014 Secure cardholder data	N/A			
GMS-0015 Vulnerability management	N/A			
GMS-0016 Access control	N/A			
GMS-0017 Network monitoring and testing	N/A			
GMS-0018 Information security	N/A			
GMS-0019 Supplier Management	N/A			
GMS-0020 Risk Management/Monitoring	N/A			
GRS-0001 Strong Multi-Factor authentication (MFA)	N/A			
GRS-0003 Patch Management	N/A			
GRS-0005 Phone Call Recording	N/A			
GRS-0006 Email Logging	N/A			
GRS-0007 Examination & Investigation	N/A			
GRS-0008 Customer Due Diligence	N/A			
GRS-0009 Name/Entity Matching	N/A			
GMS-1001 Information Security Policies	N/A			
GMS-1002 Business Continuity	N/A			
GMS-1003 Risk Assessment	N/A			
GMS-1004 Policies and Procedures	N/A			
GMS-1005 Management Information & Reporting	N/A			
GMS-1006 Reviews & Audits	N/A			
GMS-1007 Due Diligence	N/A			
GMS-1008 Building Security	N/A			
GMS-1009 Disposal	N/A			
GMS-1010 Supplier Relationships	N/A			

Any other information	The asset is a graph dataset extracted and constructed from the Ethereum Mainnet Blockchain raw blocks data. The transaction data in raw blocks is publicly available all over the world on the blockchain.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Can Özturan	**Position**	Faculty Member
Signature		**Date**	31 / 03 / 2022

3.3.8 Portfolio-Value-at-Risk-estimation

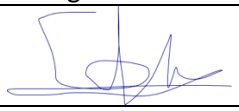
Asset name	Portfolio-Value-at-Risk-estimation	**Version/ID**	6031
Asset description	iPython Jupyter Notebook that demonstrates in an explanatory way how to estimate and evaluate the Value-at-Risk (VaR) of financial portfolios.		

Organisation name	INNOV-ACTS LTD	**VAT**	10364207G
Full Address	6 Kolokotroni Street, 1st Floor, Flat 6, 1101, Nicosia, Cyprus		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	X			N/A since asset demonstrates and explains how to develop risk models for financial portfolios in Python rather than being a service. The used data are open source obtained from Yahoo Finance (1).
GMS-0002 Risk Management/Monitoring	X			N/A (same as (1))
GMS-0003 Security Awareness & Training	X			N/A (same as (1))
GMS-0004 Password Policy Enforcement	X			N/A (same as (1))
GMS-0005 Information Asset Management	X			N/A (same as (1))
GMS-0006 Anonymization	X			N/A (same as (1))
GMS-0007 Pseudonymization	X			N/A (same as (1))
GMS-0008 Authentication and Authorization mechanisms	X			N/A (same as (1))
GMS-0009 Data Encryption	X			N/A (same as (1))
GMS-0010 Data Discovery and Classification	X			N/A (same as (1))
GMS-0011 Pseudonymization	X			N/A (same as (1))
GMS-0012 Authentication and Authorization mechanisms	X			N/A (same as (1))

GMS-0013 Secure network	X			N/A (same as (1))
GMS-0014 Secure cardholder data	X			N/A (same as (1))
GMS-0015 Vulnerability management	X			N/A (same as (1))
GMS-0016 Access control	X			N/A (same as (1))
GMS-0017 Network monitoring and testing	X			N/A (same as (1))
GMS-0018 Information security	X			N/A (same as (1))
GMS-0019 Supplier Management	X			N/A (same as (1))
GMS-0020 Risk Management/Monitoring	X			N/A (same as (1))
GRS-0001 Strong Multi-Factor authentication (MFA)	X			N/A (same as (1))
GRS-0003 Patch Management	X			N/A (same as (1))
GRS-0005 Phone Call Recording	X			N/A (same as (1))
GRS-0006 Email Logging	X			N/A (same as (1))
GRS-0007 Examination & Investigation	X			N/A (same as (1))
GRS-0008 Customer Due Diligence	X			N/A (same as (1))
GRS-0009 Name/Entity Matching	X			N/A (same as (1))
GMS-1001 Information Security Policies	X			N/A (same as (1))
GMS-1002 Business Continuity	X			N/A (same as (1))
GMS-1003 Risk Assessment	X			N/A (same as (1))
GMS-1004 Policies and Procedures	X			N/A (same as (1))
GMS-1005 Management Information & Reporting	X			N/A (same as (1))
GMS-1006 Reviews & Audits	X			N/A (same as (1))
GMS-1007 Due Diligence	X			N/A (same as (1))
GMS-1008 Building Security	X			N/A (same as (1))
GMS-1009 Disposal	X			N/A (same as (1))
GMS-1010 Supplier Relationships	X			N/A (same as (1))

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Georgios Fatouros	**Position**	Data Scientist
Signature		**Date**	22 / 03 / 2022

3.3.9 Sentiment analysis in financial news

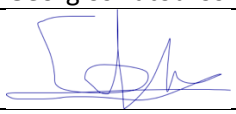
Asset name	Sentiment analysis in financial news	Version/ID	6032
Asset description	This service performs sentiment analysis in financial news using the FinBERT pre-trained model provided by ProsusAI and Hugging Face FinBERT is a pre-trained NLP model to analyse sentiment of financial text. It is built by further training the BERT language model in the finance domain, using a large financial corpus and thereby fine-tuning it for financial sentiment classification.		

Organisation name	INNOV-ACTS LTD	VAT	10364207G
Full Address	6 Kolokotroni Street, 1st Floor, Flat 6, 1101, Nicosia, Cyprus		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	X			N/A since this asset is a standalone REST API that does not store any data nor interacts with other services. It relies on transfer learning with no need for training data and can be used only to infer the sentiment of the input text. (1)
GMS-0002 Risk Management/Monitoring	X			N/A (same as (1))
GMS-0003 Security Awareness & Training	X			N/A (same as (1))
GMS-0004 Password Policy Enforcement	X			N/A (same as (1))
GMS-0005 Information Asset Management	X			N/A (same as (1))
GMS-0006 Anonymization	X			N/A (same as (1))
GMS-0007 Pseudonymization	X			N/A (same as (1))
GMS-0008 Authentication and Authorization mechanisms	X			N/A (same as (1))
GMS-0009 Data Encryption	X			N/A (same as (1))
GMS-0010 Data Discovery and Classification	X			N/A (same as (1))
GMS-0011 Pseudonymization	X			N/A (same as (1))
GMS-0012 Authentication and Authorization mechanisms	X			N/A (same as (1))
GMS-0013 Secure network	X			N/A (same as (1))
GMS-0014 Secure cardholder data	X			N/A (same as (1))
GMS-0015 Vulnerability management	X			N/A (same as (1))
GMS-0016 Access control	X			N/A (same as (1))

GMS-0017 Network monitoring and testing	X			N/A (same as (1))
GMS-0018 Information security	X			N/A (same as (1))
GMS-0019 Supplier Management	X			N/A (same as (1))
GMS-0020 Risk Management/Monitoring	X			N/A (same as (1))
GRS-0001 Strong Multi-Factor authentication (MFA)	X			N/A (same as (1))
GRS-0003 Patch Management	X			N/A (same as (1))
GRS-0005 Phone Call Recording	X			N/A (same as (1))
GRS-0006 Email Logging	X			N/A (same as (1))
GRS-0007 Examination & Investigation	X			N/A (same as (1))
GRS-0008 Customer Due Diligence	X			N/A (same as (1))
GRS-0009 Name/Entity Matching	X			N/A (same as (1))
GMS-1001 Information Security Policies	X			N/A (same as (1))
GMS-1002 Business Continuity	X			N/A (same as (1))
GMS-1003 Risk Assessment	X			N/A (same as (1))
GMS-1004 Policies and Procedures	X			N/A (same as (1))
GMS-1005 Management Information & Reporting	X			N/A (same as (1))
GMS-1006 Reviews & Audits	X			N/A (same as (1))
GMS-1007 Due Diligence	X			N/A (same as (1))
GMS-1008 Building Security	X			N/A (same as (1))
GMS-1009 Disposal	X			N/A (same as (1))
GMS-1010 Supplier Relationships	X			N/A (same as (1))

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Georgios Fatouros	**Position**	Data Scientist
Signature		**Date**	22 / 03 / 2022

3.3.10 DeepVaR: Value-at-Risk prediction leveraging Deep Learning

Asset name	DeepVaR: Value-at—Risk prediction leveraging Deep Learning	**Version/ID**	6033

Asset description	iPython Jupyter Notebook that explains and implements the DeepVaR, which is a Value-at-Risk model based on deep neural networks and Monte Carlo simulations. The DNN is used to estimate the parameters of the portfolio returns' distribution, which are used to produce the MC samples. As far as the DNN is concerned, the DeepAR estimator from GluonTS package is utilized in order to perform probabilistic forecasts, while the VaR is calculated leveraging DeepAR's output.

Organisation name	INNOV-ACTS LTD	**VAT**	10364207G
Full Address	6 Kolokotroni Street, 1st Floor, Flat 6, 1101, Nicosia, Cyprus		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	X			N/A since this asset demonstrates and explains how to develop a VaR model in Python rather than being a service. The used data are open source obtained from eatradingacademy.com (1)
GMS-0002 Risk Management/Monitoring	X			N/A (same as (1))
GMS-0003 Security Awareness & Training	X			N/A (same as (1))
GMS-0004 Password Policy Enforcement	X			N/A (same as (1))
GMS-0005 Information Asset Management	X			N/A (same as (1))
GMS-0006 Anonymization	X			N/A (same as (1))
GMS-0007 Pseudonymization	X			N/A (same as (1))
GMS-0008 Authentication and Authorization mechanisms	X			N/A (same as (1))
GMS-0009 Data Encryption	X			N/A (same as (1))
GMS-0010 Data Discovery and Classification	X			N/A (same as (1))
GMS-0011 Pseudonymization	X			N/A (same as (1))
GMS-0012 Authentication and Authorization mechanisms	X			N/A (same as (1))
GMS-0013 Secure network	X			N/A (same as (1))
GMS-0014 Secure cardholder data	X			N/A (same as (1))
GMS-0015 Vulnerability management	X			N/A (same as (1))
GMS-0016 Access control	X			N/A (same as (1))
GMS-0017 Network monitoring and testing	X			N/A (same as (1))
GMS-0018 Information security	X			N/A (same as (1))

GMS-0019 Supplier Management	X			N/A (same as (1))
GMS-0020 Risk Management/Monitoring	X			N/A (same as (1))
GRS-0001 Strong Multi-Factor authentication (MFA)	X			N/A (same as (1))
GRS-0003 Patch Management	X			N/A (same as (1))
GRS-0005 Phone Call Recording	X			N/A (same as (1))
GRS-0006 Email Logging	X			N/A (same as (1))
GRS-0007 Examination & Investigation	X			N/A (same as (1))
GRS-0008 Customer Due Diligence	X			N/A (same as (1))
GRS-0009 Name/Entity Matching	X			N/A (same as (1))
GMS-1001 Information Security Policies	X			N/A (same as (1))
GMS-1002 Business Continuity	X			N/A (same as (1))
GMS-1003 Risk Assessment	X			N/A (same as (1))
GMS-1004 Policies and Procedures	X			N/A (same as (1))
GMS-1005 Management Information & Reporting	X			N/A (same as (1))
GMS-1006 Reviews & Audits	X			N/A (same as (1))
GMS-1007 Due Diligence	X			N/A (same as (1))
GMS-1008 Building Security	X			N/A (same as (1))
GMS-1009 Disposal	X			N/A (same as (1))
GMS-1010 Supplier Relationships	X			N/A (same as (1))

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Georgios Fatouros	**Position**	Data Scientist
Signature		**Date**	22 / 03 / 2022

3.3.11 Tokenization on Hyperledger Fabric -ERC20 chaincode

Asset name	Tokenization on Hyperledger Fabric -ERC20 chaincode	**Version/ID**	6037
Asset description	One important aspect of any blockchain (BC), whether public or private, is asset tokenization. This refers to the representation of any asset into its		

	digital form for trading which can later be bought, sold, exchanged or redeemed for any other digital or physical value. This asset implements the ERC20 standard on top of Hyperledger Fabric to enable tokenization.

Organisation name	IBM Research - Haifa	**VAT**	
Full Address	Haifa Mount Carmel. Israel		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		V		Inherent BC capability
GMS-0002 Risk Management/Monitoring	V			Not in the scope of the asset
GMS-0003 Security Awareness & Training		V		Inherent BC capability
GMS-0004 Password Policy Enforcement		V		Inherent BC capability
GMS-0005 Information Asset Management		V		BC inherently provides full provenance of the transactions
GMS-0006 Anonymization	V			No personal information is stored in BC
GMS-0007 Pseudonymization	V			No personal information is stored in BC
GMS-0008 Authentication and Authorization mechanisms		V		Inherent BC capability
GMS-0009 Data Encryption	V			Not relevant for the specific implemented solution
GMS-0010 Data Discovery and Classification	V			All data is stored in BC
GMS-0011 Pseudonymization	V			No personal information is stored in BC
GMS-0012 Authentication and Authorization mechanisms		V		Inherent BC capability
GMS-0013 Secure network	V			
GMS-0014 Secure cardholder data	V			
GMS-0015 Vulnerability management	V			
GMS-0016 Access control	V			
GMS-0017 Network monitoring and testing	V			
GMS-0018 Information security	V			
GMS-0019 Supplier Management	V			
GMS-0020 Risk Management/Monitoring	V			
GRS-0001 Strong Multi-Factor authentication (MFA)	V			
GRS-0003 Patch Management	V			
GRS-0005 Phone Call Recording	V			
GRS-0006 Email Logging	V			

GRS-0007 Examination & Investigation	V			
GRS-0008 Customer Due Diligence	V			
GRS-0009 Name/Entity Matching	V			
GMS-1001 Information Security Policies		V		Inherent BC capability
GMS-1002 Business Continuity		V		No personal information is stored in BC
GMS-1003 Risk Assessment		V		No high-risk data
GMS-1004 Policies and Procedures	V			
GMS-1005 Management Information & Reporting	V			
GMS-1006 Reviews & Audits		V		Inherent BC capability
GMS-1007 Due Diligence	V			
GMS-1008 Building Security	V			
GMS-1009 Disposal	V			
GMS-1010 Supplier Relationships	V			

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Fabiana Fournier	**Position**	Research staff member
Signature	*Fabiana Fournier*	**Date**	23 / 03 / 2022

3.3.12 Automatic data anonymization tool for preserving privacy and utility on datasets

Asset name	Automatic data anonymization tool for preserving privacy and utility on datasets	**Version/ID**	1.0
Asset description	Gradiant's anonymization tool modifies data to preserve privacy. It is especially indicated when a dataset contains personal data and it has to be outsourced/shared with a third party. It provides different anonymization algorithms that aim at avoiding the appearances of data combinations that could lead to a possible re-identification of the data subjects, while monitoring different privacy and utility metrics to assess the impact of the anonymization process.		

Organisation name	Fundación Centro Tecnolóxico de Telecomunicacións de Galicia (GRADIANT)	**VAT**	ESG36997229
Full Address	Carretera do Vilar 56 - 58 36214 Vigo, Pontevedra (Spain)		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	X			
GMS-0002 Risk Management/Monitoring		X		GRADIANT is certified under the ISO/IEC 27001. Among other measures, we follow

				the Secure Software Development Life Cycle (S-SDLC) methodology.
GMS-0003 Security Awareness & Training		X		GRADIANT employees take security training every year, ensuring that the development team is aware of the latest security risks.
GMS-0004 Password Policy Enforcement			X	
GMS-0005 Information Asset Management	X			
GMS-0006 Anonymization	X			Even that the GRADIANT provides anonymization software, the datasets are not stored on GRADIANT's premises
GMS-0007 Pseudonymization	X			
GMS-0008 Authentication and Authorization mechanisms			X	GRADIANT's anonymization tool provides authentication by using passwords or API Keys. In addition, authorisation mechanisms are in place to protect access to user resources to only authorised parties.
GMS-0009 Data Encryption	X			
GMS-0010 Data Discovery and Classification	X			
GMS-0011 Pseudonymization	X			
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring		X		GRADIANT is certified under the ISO/IEC 27001. Among other measures, we follow the Secure Software

				Development Life Cycle (S-SDLC) methodology.
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies			X	GRADIANT has defined different information security policies under ISO/IEC 27001
GMS-1002 Business Continuity	X			
GMS-1003 Risk Assessment	X			
GMS-1004 Policies and Procedures			X	Security Training, Internal phishing campaigns for awareness, S-SDLC methodology enforcement
GMS-1005 Management Information & Reporting	X			
GMS-1006 Reviews & Audits			X	Reviews & Audits of ISO/IEC 27001 and ISO/IEC 9001
GMS-1007 Due Diligence	X			
GMS-1008 Building Security		X		
GMS-1009 Disposal		X		
GMS-1010 Supplier Relationships		X		

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Inés Ortega Fernández	**Position**	Technical Manager for Data Analytics & AI
Signature		**Date**	30/ 03 / 2022

3.3.13 Blockchain-enabled Consent Management

Asset name	Blockchain-enabled Consent Management	Version/ID	1.0
Asset description	A decentralised and robust blockchain-enabled consent management mechanism, that will enable the sharing of the customers' consent to exchange and utilise their customer data across different banking institutions. It enables the financial institutions to effectively manage and share their customers' consents in a transparent and unambiguous manner. It is capable of storing the consents and their complete update history with complete consents' versioning in a secure and trusted manner.		

Organisation name	GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS	VAT	EL998908360
Full Address	MITHRIDATOU 36-38, ATHINA 11632, Greece		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		X		The solution is based on the blockchain technology that provides this functionality.
GMS-0002 Risk Management/Monitoring	X			Not applicable.
GMS-0003 Security Awareness & Training	X			Not applicable.
GMS-0004 Password Policy Enforcement	X			Not applicable.
GMS-0005 Information Asset Management		X		The solution is based on the blockchain technology that provides this functionality
GMS-0006 Anonymization	X			No personal data are processed or stored
GMS-0007 Pseudonymization	X			No personal data are processed or stored
GMS-0008 Authentication and Authorization mechanisms		X		The solution is based on the blockchain technology that provides this functionality.
GMS-0009 Data Encryption		X		The solution is based on the blockchain technology that provides this functionality.
GMS-0010 Data Discovery and Classification		X		The solution is based on the blockchain technology that provides this functionality.
GMS-0011 Pseudonymization	X			No personal data are processed or stored
GMS-0012 Authentication and Authorization mechanisms		X		The solution is based on the blockchain technology

				that provides this functionality.
GMS-0013 Secure network			X	It depends on the blockchain network setup, but it is supported.
GMS-0014 Secure cardholder data	X			No Cardholder data processed or stored.
GMS-0015 Vulnerability management	X			No Cardholder data processed or stored.
GMS-0016 Access control	X			No Cardholder data processed or stored.
GMS-0017 Network monitoring and testing	X			No Cardholder data processed or stored.
GMS-0018 Information security	X			No Cardholder data processed or stored.
GMS-0019 Supplier Management	X			Not applicable.
GMS-0020 Risk Management/Monitoring	X			Not applicable.
GRS-0001 Strong Multi-Factor authentication (MFA)	X			Not applicable.
GRS-0003 Patch Management		X		A process for patch management is in place.
GRS-0005 Phone Call Recording	X			Not applicable.
GRS-0006 Email Logging	X			Not applicable.
GRS-0007 Examination & Investigation	X			Not applicable.
GRS-0008 Customer Due Diligence	X			Not applicable.
GRS-0009 Name/Entity Matching	X			Not applicable.
GMS-1001 Information Security Policies		X		The solution is based on the blockchain technology that provides this functionality.
GMS-1002 Business Continuity	X			No personal data are processed or stored
GMS-1003 Risk Assessment	X			Not applicable.
GMS-1004 Policies and Procedures	X			Not applicable.
GMS-1005 Management Information & Reporting	X			Not applicable.
GMS-1006 Reviews & Audits	X			Not applicable.
GMS-1007 Due Diligence	X			Not applicable.
GMS-1008 Building Security	X			Not applicable.
GMS-1009 Disposal	X			Not applicable.
GMS-1010 Supplier Relationships	X			Not applicable.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Dimitrios Alexandrou	Position	Business Innovation Director
Signature	Dimitrios Alexandrou	Date	31 /03 / 2022

3.3.14 INFINITECH Open API Gateway

Asset name	INFINITECH Open API Gateway	Version/ID	1.0
Asset description	The INFINITECH Open API Gateway is a sophisticated API Gateway that encompasses the Open API specification in order to provide a single point of entry for the added-value functionalities of INFINITECH which are based on microservices.		

Organisation name	GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS	VAT	EL998908360
Full Address	MITHRIDATOU 36-38, ATHINA 11632, Greece		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)			X	The solution provides logging capabilities on all performed activities that could be analysed if needed.
GMS-0002 Risk Management/Monitoring	X			Not applicable.
GMS-0003 Security Awareness & Training	X			Not applicable.
GMS-0004 Password Policy Enforcement	X			Not applicable.
GMS-0005 Information Asset Management	X			Not applicable.
GMS-0006 Anonymization	X			No personal data are processed or stored
GMS-0007 Pseudonymization	X			No personal data are processed or stored
GMS-0008 Authentication and Authorization mechanisms	X			Not applicable.
GMS-0009 Data Encryption	X			Not applicable.
GMS-0010 Data Discovery and Classification	X			Not applicable.
GMS-0011 Pseudonymization	X			No personal data are processed or stored
GMS-0012 Authentication and Authorization mechanisms	X			Not applicable.
GMS-0013 Secure network			X	It depends on the deployment setup but it is supported if needed (non-mandatory requirement).
GMS-0014 Secure cardholder data	X			No Cardholder data processed or stored.

GMS-0015 Vulnerability management	X			No Cardholder data processed or stored.
GMS-0016 Access control	X			No Cardholder data processed or stored.
GMS-0017 Network monitoring and testing	X			No Cardholder data processed or stored.
GMS-0018 Information security	X			No Cardholder data processed or stored.
GMS-0019 Supplier Management	X			Not applicable.
GMS-0020 Risk Management/Monitoring	X			Not applicable.
GRS-0001 Strong Multi-Factor authentication (MFA)	X			Not applicable.
GRS-0003 Patch Management		X		A process for patch management is in place.
GRS-0005 Phone Call Recording	X			Not applicable.
GRS-0006 Email Logging	X			Not applicable.
GRS-0007 Examination & Investigation	X			Not applicable.
GRS-0008 Customer Due Diligence	X			Not applicable.
GRS-0009 Name/Entity Matching	X			Not applicable.
GMS-1001 Information Security Policies	X			Not applicable.
GMS-1002 Business Continuity	X			Not applicable.
GMS-1003 Risk Assessment	X			Not applicable.
GMS-1004 Policies and Procedures	X			Not applicable.
GMS-1005 Management Information & Reporting	X			Not applicable.
GMS-1006 Reviews & Audits	X			Not applicable.
GMS-1007 Due Diligence	X			Not applicable.
GMS-1008 Building Security	X			Not applicable.
GMS-1009 Disposal	X			Not applicable.
GMS-1010 Supplier Relationships	X			Not applicable.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Dimitrios Alexandrou	**Position**	Business Innovation Director
Signature	*Dimitrios Alexandrou*	**Date**	31 / 03 / 2022

3.3.15 INFINITECH Data Collection

Asset name	INFINITECH Data Collection	**Version/ID**	1.0

Asset description	The INFINITECH Data Collection component is designed and implemented aiming to address the need for a holistic mechanism that will empower the data providers to configure and execute data collection pipelines tailored to their needs.

Organisation name	GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS	**VAT**	EL998908360
Full Address	MITHRIDATOU 36-38, ATHINA 11632, Greece		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)			X	The solution provides logging capabilities on all performed activities that could be analysed if needed.
GMS-0002 Risk Management/Monitoring	X			Not applicable.
GMS-0003 Security Awareness & Training	X			Not applicable.
GMS-0004 Password Policy Enforcement	X			Not applicable.
GMS-0005 Information Asset Management	X			Not applicable.
GMS-0006 Anonymization	X			The component is not handling the anonymisation aspects of the collected information in case it is instructed to collect and store such kind of information by the data consumer. The anonymisation part is a responsibility of the data consumer.
GMS-0007 Pseudonymization	X			The component is not handling the pseudonymisation aspects of the collected information in case it is instructed to collect and store such kind of information by the data consumer. The pseudonymisation part is a responsibility of the data consumer.
GMS-0008 Authentication and Authorization mechanisms			X	The intermediate storage of information is securely guarded. The security of the information that will reside on the final storage solution is not a responsibility of the specific solution.
GMS-0009 Data Encryption	X			Not applicable.
GMS-0010 Data Discovery and Classification	X			Not applicable.

GMS-0011 Pseudonymization	X			The component is not handling the pseudonymisation aspects of the collected information in case it is instructed to collect and store such kind of information by the data consumer. The pseudonymisation part is a responsibility of the data consumer.
GMS-0012 Authentication and Authorization mechanisms			X	The intermediate storage of information is securely guarded. The security of the information that will reside on the final storage solution is not a responsibility of the specific solution.
GMS-0013 Secure network			X	It depends on the deployment setup but it is supported if needed (non-mandatory requirement).
GMS-0014 Secure cardholder data	X			No Cardholder data processed or stored.
GMS-0015 Vulnerability management	X			No Cardholder data processed or stored.
GMS-0016 Access control	X			No Cardholder data processed or stored.
GMS-0017 Network monitoring and testing	X			No Cardholder data processed or stored.
GMS-0018 Information security	X			No Cardholder data processed or stored.
GMS-0019 Supplier Management	X			Not applicable.
GMS-0020 Risk Management/Monitoring	X			Not applicable.
GRS-0001 Strong Multi-Factor authentication (MFA)	X			Not applicable.
GRS-0003 Patch Management		X		A process for patch management is in place.
GRS-0005 Phone Call Recording	X			Not applicable.
GRS-0006 Email Logging	X			Not applicable.
GRS-0007 Examination & Investigation	X			Not applicable.
GRS-0008 Customer Due Diligence	X			Not applicable.
GRS-0009 Name/Entity Matching	X			Not applicable.
GMS-1001 Information Security Policies	X			Not applicable.

GMS-1002 Business Continuity	X			Not applicable.
GMS-1003 Risk Assessment	X			Not applicable.
GMS-1004 Policies and Procedures	X			Not applicable.
GMS-1005 Management Information & Reporting	X			Not applicable.
GMS-1006 Reviews & Audits	X			Not applicable.
GMS-1007 Due Diligence	X			Not applicable.
GMS-1008 Building Security	X			Not applicable.
GMS-1009 Disposal	X			Not applicable.
GMS-1010 Supplier Relationships	X			Not applicable.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Dimitrios Alexandrou	**Position**	Business Innovation Director
Signature	*Dimitrios Alexandrou*	**Date**	31 / 03 / 2022

3.3.16 SMEs Cashflow Prediction

Asset name	SMEs Cashflow Prediction	**Version/ID**	6217
Asset description	This notebook demonstrates in an explanatory way how to predict in a probabilistic way the future outflows and inflows based on historical transactions. It is applied on SME data but it can be fine tuned and applied in general for cashflow prediction.		

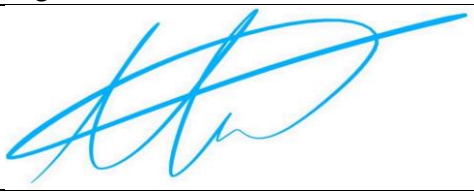
Organisation name	University of Piraeus Research Center (UPRC)	**VAT**	
Full Address	Leof. AL. Papanastasiou 91, Pireaus, 18533		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	X			
GMS-0002 Risk Management/Monitoring	X			
GMS-0003 Security Awareness & Training	X			
GMS-0004 Password Policy Enforcement	X			
GMS-0005 Information Asset Management	X			
GMS-0006 Anonymization	X			
GMS-0007 Pseudonymization		X		The few data displayed in the notebook were already anonymized and tokenized

				begore leave the BOC premises.
GMS-0008 Authentication and Authorization mechanisms	X			
GMS-0009 Data Encryption	X			
GMS-0010 Data Discovery and Classification	X			
GMS-0011 Pseudonymization		X		The few data displayed in the notebook were already anonymized and tokenized begore leave the BOC premises.
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			
GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies	X			
GMS-1002 Business Continuity	X			
GMS-1003 Risk Assessment	X			
GMS-1004 Policies and Procedures	X			
GMS-1005 Management Information & Reporting	X			
GMS-1006 Reviews & Audits	X			
GMS-1007 Due Diligence	X			
GMS-1008 Building Security	X			
GMS-1009 Disposal	X			
GMS-1010 Supplier Relationships	X			

Any other information	The "SMEs Cashflow Prediction" asset provided by the INFINITECH marketplace is a python notebook, where various python libraries were imported. The data incorporated are SMEs transactions data provided by BOC (a subset of them). The data displayed in the notebook are not stored and have already been anonymized and tokenized before leaving the bank premises.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Georgios Makridis	**Position**	Researcher
Signature		**Date**	30 / 03 / 2022

3.3.17 Scalable Transaction Graph Analysis Component

Asset name	Scalable Transaction Graph Analysis Component	**Version/ID**	1.0
Asset description	This application constructs the transaction graph from blockchain transactions and analyses the graph using graph algorithms.		

Organisation name	Bogazici University	**VAT**	Beşiktaş, V.D. 1790015446
Full Address	Bogazici University, Bebek 34342, Istanbul, Turkey		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	N/A			
GMS-0002 Risk Management/Monitoring	N/A			
GMS-0003 Security Awareness & Training	N/A			
GMS-0004 Password Policy Enforcement	N/A			
GMS-0005 Information Asset Management	N/A			
GMS-0006 Anonymization	N/A			
GMS-0007 Pseudonymization	N/A			
GMS-0008 Authentication and Authorization mechanisms	N/A			
GMS-0009 Data Encryption	N/A			
GMS-0010 Data Discovery and Classification	N/A			
GMS-0011 Pseudonymization	N/A			
GMS-0012 Authentication and Authorization mechanisms	N/A			
GMS-0013 Secure network	N/A			
GMS-0014 Secure cardholder data	N/A			
GMS-0015 Vulnerability management	N/A			
GMS-0016 Access control	N/A			

GMS-0017 Network monitoring and testing	N/A			
GMS-0018 Information security	N/A			
GMS-0019 Supplier Management	N/A			
GMS-0020 Risk Management/Monitoring	N/A			
GRS-0001 Strong Multi-Factor authentication (MFA)	N/A			
GRS-0003 Patch Management	N/A			
GRS-0005 Phone Call Recording	N/A			
GRS-0006 Email Logging	N/A			
GRS-0007 Examination & Investigation	N/A			
GRS-0008 Customer Due Diligence	N/A			
GRS-0009 Name/Entity Matching	N/A			
GMS-1001 Information Security Policies	N/A			
GMS-1002 Business Continuity	N/A			
GMS-1003 Risk Assessment	N/A			
GMS-1004 Policies and Procedures	N/A			
GMS-1005 Management Information & Reporting	N/A			
GMS-1006 Reviews & Audits	N/A			
GMS-1007 Due Diligence	N/A			
GMS-1008 Building Security	N/A			
GMS-1009 Disposal	N/A			
GMS-1010 Supplier Relationships	N/A			

Any other information	Scalable Transaction Graph Analysis Component is an MPI program operating on publicly available graph dataset extracted and constructed from the public Ethereum and Bitcoin Blockchains.

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Can Özturan	**Position**	Faculty Member
Signature		**Date**	31 / 03 / 2022

3.3.18 Pseudoanonymizer

Asset name	Pseudoanonymizer	**Version/ID**	89b14474d73e58a9d5e6c6d7188291b3a9db20ef
Asset description	The main goal of the pseudonymization tool is to ensure that sensitive data is hidden both during the development and its production use, while still ensuring that the underlying structure of the data is preserved, supporting analysis and reasoning over the pseudonymized data.		

Organisation name	Jožef Stefan Institute	**VAT**	SI55560822
Full Address	Jamova cesta 39, Ljubljana, 1000 Ljubljana		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)	X			
GMS-0002 Risk Management/Monitoring	X			Risk monitoring is done outside the tool on an organizational level
GMS-0003 Security Awareness & Training	X			Pseudoanonymizer should be an integral part of process with clear lines of separation and training should be provided for operators
GMS-0004 Password Policy Enforcement	X			
GMS-0005 Information Asset Management	X			Logging is being implemented, but is not available in version published on marketplace
GMS-0006 Anonymization	X			Data is fully pseudo anonymized
GMS-0007 Pseudonymization		X		Data is fully pseudo anonymized
GMS-0008 Authentication and Authorization mechanisms	X			Should be provided on organizational and process level
GMS-0009 Data Encryption			X	Available over https
GMS-0010 Data Discovery and Classification	X			Enforced on process level
GMS-0011 Pseudonymization		X		Data is fully pseudo anonymized
GMS-0012 Authentication and Authorization mechanisms	X			
GMS-0013 Secure network	X			
GMS-0014 Secure cardholder data	X			
GMS-0015 Vulnerability management	X			
GMS-0016 Access control	X			
GMS-0017 Network monitoring and testing	X			
GMS-0018 Information security	X			
GMS-0019 Supplier Management	X			
GMS-0020 Risk Management/Monitoring	X			
GRS-0001 Strong Multi-Factor authentication (MFA)	X			
GRS-0003 Patch Management	X			

GRS-0005 Phone Call Recording	X			
GRS-0006 Email Logging	X			
GRS-0007 Examination & Investigation	X			
GRS-0008 Customer Due Diligence	X			
GRS-0009 Name/Entity Matching	X			
GMS-1001 Information Security Policies	X			
GMS-1002 Business Continuity	X			
GMS-1003 Risk Assessment	X			
GMS-1004 Policies and Procedures	X			
GMS-1005 Management Information & Reporting	X			
GMS-1006 Reviews & Audits	X			
GMS-1007 Due Diligence	X			
GMS-1008 Building Security	X			Enforced on process and organizational level
GMS-1009 Disposal	X			
GMS-1010 Supplier Relationships	X			Enforced on process and organizational level

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Maja Škrjanc	**Position**	Researcher, project manager
Signature	*Maja Škrjanc*	**Date**	08 / 04 / 2022

3.3.19 BC based secure execution environment and data marketplace for federated learning

Asset name	BC based secure execution environment and data marketplace for federated learning	**Version/ID**	6459
Asset description	IBM provides a blockchain-based secure execution framework for the distributed fraud algorithm execution, recording all the meta-information regarding the execution, and recording the shared intermediate results on a transparent, immutable, and verifiable ledger. At the end of the execution, a completed model can be shared as a tradeable asset on a blockchain-based data marketplace. The blockchain-based data marketplace provides a tradeable assets catalogue, where consumer organizations can search for available assets and gain access by paying for those assets using tokens		

Organisation name	IBM Haifa Research Lab	**VAT**	
Full Address	Haifa Mount Carmel. Israel		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		V		Inherent BC capabilities
GMS-0002 Risk Management/Monitoring	V			Not in the scope of the asset
GMS-0003 Security Awareness & Training		V		Inherent BC capabilities
GMS-0004 Password Policy Enforcement		V		Inherent BC capabilities
GMS-0005 Information Asset Management		V		BC provides full provenance of assets
GMS-0006 Anonymization	V			No personal information stored on BC
GMS-0007 Pseudonymization	V			No personal information stored on BC
GMS-0008 Authentication and Authorization mechanisms		V		Inherent BC capabilities
GMS-0009 Data Encryption	V			Not relevant for the implemented solution
GMS-0010 Data Discovery and Classification	V			All data stored on BC
GMS-0011 Pseudonymization	V			Not relevant for the implemented solution
GMS-0012 Authentication and Authorization mechanisms		V		Inherent BC capabilities
GMS-0013 Secure network	V			Not applicable
GMS-0014 Secure cardholder data	V			Not applicable
GMS-0015 Vulnerability management	V			Not applicable
GMS-0016 Access control	V			Not applicable
GMS-0017 Network monitoring and testing	V			Not applicable
GMS-0018 Information security	V			Not applicable
GMS-0019 Supplier Management	V			Not applicable
GMS-0020 Risk Management/Monitoring	V			Not applicable
GRS-0001 Strong Multi-Factor authentication (MFA)	V			Not applicable
GRS-0003 Patch Management	V			Not applicable
GRS-0005 Phone Call Recording	V			Not applicable
GRS-0006 Email Logging	V			Not applicable
GRS-0007 Examination & Investigation	V			Not applicable
GRS-0008 Customer Due Diligence	V			Not applicable
GRS-0009 Name/Entity Matching	V			Not applicable
GMS-1001 Information Security Policies		V		Inherent BC capabilities
GMS-1002 Business Continuity	V			No personal data
GMS-1003 Risk Assessment	V			No high-risk data
GMS-1004 Policies and Procedures	V			Not applicable

GMS-1005 Management Information & Reporting	V			Not applicable
GMS-1006 Reviews & Audits		V		Inherent BC capabilities
GMS-1007 Due Diligence	V			Not applicable
GMS-1008 Building Security	V			Not applicable
GMS-1009 Disposal	V			Not applicable
GMS-1010 Supplier Relationships	V			Not applicable

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Inna Skarbovsky	**Position**	Research Staff Member
Signature	*Inna Skarbovsky*	**Date**	23 / 03 / 2022

3.3.20 News Sentiment API

Asset name	News Sentiment API	**Version/ID**	5.0
Asset description	Reportbrain News API - Facilitate News features using our structuring of unstructured data in the News by transforming, normalizing and augmenting it for a specific application. Customers can use Reportbrain's query language to explore that data and retrieve news. articles and their metadata. The Reportbrain News API is accessed through HTTP via a list of available calls and their parameters.		

Organisation name	Reportbrain	**VAT**	GB102495244
Full Address	Office 6 42 Westbourne Grove, London, England, W2 5SH		

Regulatory and security Standards compliance	Not Applicable	Full Compliance	Partial Compliance	Explanation / Comments
GMS-0001 Security Information and Event Management (SIEM)		x		
GMS-0002 Risk Management/Monitoring		x		
GMS-0003 Security Awareness & Training		x		
GMS-0004 Password Policy Enforcement	x			
GMS-0005 Information Asset Management		x		
GMS-0006 Anonymization		x		
GMS-0007 Pseudonymization	x			
GMS-0008 Authentication and Authorization mechanisms		x		
GMS-0009 Data Encryption		x		
GMS-0010 Data Discovery and Classification		x		
GMS-0011 Pseudonymization		x		
GMS-0012 Authentication and Authorization mechanisms		x		

GMS-0013 Secure network		x		
GMS-0014 Secure cardholder data		x		
GMS-0015 Vulnerability management		x		
GMS-0016 Access control		x		
GMS-0017 Network monitoring and testing		x		
GMS-0018 Information security		x		
GMS-0019 Supplier Management	x			
GMS-0020 Risk Management/Monitoring		x		
GRS-0001 Strong Multi-Factor authentication (MFA)	x			
GRS-0003 Patch Management	x			
GRS-0005 Phone Call Recording	x			
GRS-0006 Email Logging	x			
GRS-0007 Examination & Investigation	x			
GRS-0008 Customer Due Diligence	x			
GRS-0009 Name/Entity Matching		x		
GMS-1001 Information Security Policies		x		
GMS-1002 Business Continuity		x		
GMS-1003 Risk Assessment		X		
GMS-1004 Policies and Procedures		X		
GMS-1005 Management Information & Reporting		x		
GMS-1006 Reviews & Audits		x		
GMS-1007 Due Diligence		x		
GMS-1008 Building Security		x		
GMS-1009 Disposal		x		
GMS-1010 Supplier Relationships		x		

I, hereby declare that the information provided here is accurate, correct, and complete. This form describes the status of regulatory and security standards compliance (relevant from INFINITECH's perspective) for the abovementioned asset by the date when this declaration has been issued.

Full Name	Victoria Michailidou	**Position**	Business Operations Manager
Signature		**Date**	22 / 03 / 2022

4 Conclusions

This document provides an analysis of regulatory and security standards conformance for the INFINITECH assets by using a self-compliance assessment (declaration of conformance). Document reports on the implementation of the defined processes for certifying digital finance/insurance solutions focusing o regulatory compliance and standards-compliance certification processes. The implemented process follows on the definition and design of the certification model and related methodology/process for the fintech solutions performed in the first deliverable of the task. The INFINITECH certification process has been defined to be served on a self-certification mode.

The document provides insights that give the guarantee of the high levels of compliance of the project's technologies to the most relevant regulatory and security standards for fintech solutions. Out of the 177 requirements considered relevant by the analysed assets, 166 (i.e., 93.8%) have full compliance from the INFINITECH technologies. This gives a clear indication that the project's developments have been performed with the maximum criteria of conformance to regulations and security standards.

Also, considering the few Partial Compliances to the defined requirements, these are mainly related with different ways to meet the requirement that is not fully aligned the one described by the requirement but that indeed provide general coverage to the requirement. Or also, that for fully fulfilling some requirement it will depend on the deployment setup but indeed these are supported if needed (non-mandatory requirement).

The next steps will be to perform the conformance analysis for all the INFINITECH assets and to perform the externalisation (in the projects' marketplace) of the conformance method (questionnaire) and analyses, for promoting outreaching of fully compliant fintech solutions. This will ease the exploitation pathways of the technological solutions by upholding the highest levels of regulatory and security standards.

Appendix A: Conformance Requirements details

Requirements from ISO/IEC 27001

GMS-0001 Security Information and Event Management (SIEM)	Logging capabilities on security events for enterprises used to analyse and/or report on the log entries received.
GMS-0002 Risk Management/Monitoring	Track risk and mitigations, rank hazards by their critical value, produce reports and manage compliance.
GMS-0003 Security Awareness & Training	Provide awareness training and set out key security requirements and practices within the context of the applications and/or services being provided.
GMS-0004 Password Policy Enforcement	Gives administrators the power to impose certain password policies on users when they choose a password such as: complexity, contained in a dictionary, keyboard pattern, repeating patterns or similarity.
GMS-0005 Information Asset Management	To identify and record the data subjects, volumes held, retention periods and who has access to the assets and their contents.
GMS-0006 Anonymization	The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
GMS-0007 Pseudonymization	A technique that is used to reduce the chance that personal data records and identifiers lead to the identification of the natural person (data subject) whom they belong too.
GMS-0008 Authentication and Authorization mechanisms	Strong and secure Access Management to prevent unauthorised access.
GMS-0009 Data Encryption	Method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.
GMS-0010 Data Discovery and Classification	Visibility of sensitive data held by the organisation with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in the enterprise.

Requirements from ISO/IEC 27701 PIMS

GMS-0006 Anonymization (see above)	The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
GMS-0011 Pseudonymization	A technique that is used to reduce the chance that personal data records and identifiers lead to the identification of the natural person (data subject) whom they belong too.
GMS-0012 Authentication and Authorization mechanisms	Method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.
GMS-0009 Data Encryption (see above)	Strong and secure Access Management to prevent unauthorised access.
GMS-0010 Data Discovery and Classification (see above)	Visibility of sensitive data held by the organisation with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in the enterprise.

Requirements from PCI DSS

GMS-0013 Secure network	A firewall configuration must be installed and maintained. System passwords must be original (not vendor-supplied).
GMS-0014 Secure cardholder data	Stored cardholder data must be protected. Transmissions of cardholder data across public networks must be encrypted.

GMS-0015 Vulnerability management	Anti-virus software must be used and regularly updated. Secure systems and applications must be developed and maintained.
GMS-0016 Access control	Cardholder data access must be restricted to a business need-to-know basis. Every person with computer access must be assigned a unique ID. Physical access to cardholder data must be restricted.
GMS-0017 Network monitoring and testing	Access to cardholder data and network resources must be tracked and monitored Security systems and processes must be regularly tested
GMS-0018 Information security	A policy dealing with information security must be maintained

Requirements from NIST Cyber Security Framework

GMS-0019 Supplier Management	Maintain quality, safety, and risk management processes throughout the supply chain. Monitor Supplier Compliance and Capability.
GMS-0001 Security Information and Event Management (SIEM) (see above)	Logging capabilities on security events for enterprises used to analyse and/or report on the log entries received.
GMS-0020 Risk Management/Monitoring	Track risk and mitigations, rank hazards by their critical value, produce reports and manage compliance.
GMS-0003 Security Awareness & Training (see above)	Provide awareness training and set out key security requirements and practices within the context of the applications and/or services being provided.
GMS-0004 Password Policy Enforcement (see above)	Gives administrators the power to impose certain password policies on users when they choose a password such as: complexity, contained in a dictionary, keyboard pattern, repeating patterns or similarity.
GMS-0005 Information Asset Management (see above)	To identify and record the data subjects, volumes held, retention periods and who has access to the assets and their contents.
GMS-0008 Authentication and Authorization mechanisms (see above)	Strong and secure Access Management to prevent unauthorised access.
GMS-0009 Data Encryption (see above)	Method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.

Requirements from GDPR

GMS-1001 Information Security Policies	Maintain an information security policy and develop appropriate procedures to support and implement that policy.
GMS-1002 Business Continuity	Protocols and measures should be in place to back-up personal data and ensure that it can be recovered and maintained in the event of an incident.
GMS-1003 Risk Assessment	Comprehensive assessments should be carried out for high-risk data and processing activities and mitigating solutions/procedures should be in place to prevent or reduce risks.
GMS-1004 Policies and Procedures	Implement robust policies and procedures so that the whole organisation and its employees know what their obligations are and what to do if certain situations occur.
GMS-1005 Management Information & Reporting	Regular reports and information are passed to upper management is essential for ensuring that the adequate resources and funding are made available and for accountability at all levels.
GMS-0005 Security Awareness & Training	A culture of security and data protection awareness will ensure that employees, contractors, and any third-party working for or with the organisation, know what is expected of them and how to maintain compliance.

GMS-1006 Reviews & Audits	This ensures that policies, controls and/or measures that are put in place can be monitored for effectiveness, accurate and fit for purpose.
GMS-1007 Due Diligence	Carrying out due diligence checks on suppliers and service providers (and in some sectors, customers); is an essential and often legal requirement (i.e., fraud checks, anti-money laundering measures).
GMS-1008 Building Security	You should have robust measures and protocols for securing access to any office or building and ensure that all employees are aware of such controls.
GMS-1009 Disposal	Specify the appropriate procedures compliant with GDPR for the disposal of paperwork and devices and appropriate controls for anything that is registered as lost.
GMS-0004 Password Policy Enforcement	Specify a password policy that enforces strong passwords that are changed on a regular basis.
GMS-1010 Supplier Relationships	Implement procedures to manage third-party risks coming into your organization and systems resulting from a failure to follow good security practice by suppliers, e.g. AWS.

Requirements from PSD 2

GRS-0001 Strong Multi-Factor authentication (MFA)	A requirement for the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
GRS-0002 SIEM (Security Information Event Management) systems (equals GMS-0001 above)	Used to collect and aggregate log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters.
GRS-0003 Patch Management	Distributing and applying updates to software. It will support the following objectives: Security, System uptime, Compliance and Feature improvements.

Requirements from MiFID II

GRS-0002 SIEM (Security Information Event Management) systems (equals GMS-0001 above)	Auditing logs for maintaining and monitoring the security and integrity of data.
GRS-0005 Phone Call Recording	Phone call recording to maintain a record of all interactions with customers providing an evidence trail of all advice and information provided.
GRS-0006 Email Logging	Email logs to maintain a record of all interactions with customers providing an evidence trail of all advice and information provided.
GRS-0001 Strong Multi-Factor authentication (MFA)	Strong authentication, preferably multi-factor, and authorization mechanisms.

Requirements from 4AMLD

GRS-0007 Examination & Investigation	AML compliance, AML/Suspicious transaction monitoring, trade surveillance, operational risk, and anti- fraud case management.
GRS-0008 Customer Due Diligence	Single data entry point and risk rating for all existing and new customer and account data in support of Know Your Customer (KYC) requirements incorporating third party data sources and registers.
GRS-0009 Name/Entity Matching	Matching and scoring tools and techniques that improve the searching of account and transaction information across systems, regions, and business lines to create one view of the customer or to improve the name/entity screening,