

IEEE Standard for Testing and Performance of a Trusted Data Matrix System

IEEE Computer Society

Developed by the
Standards Activities Board Standards Committee

IEEE Std 3158.1™-2025

STANDARDS

IEEE Standard for Testing and Performance of a Trusted Data Matrix System

Developed by the

Standards Activities Board Standards Committee
of the
IEEE Computer Society

Approved 10 September 2025

IEEE SA Standards Board

Abstract: Performance and test requirements, procedures, and acceptance criteria for a trusted data matrix system are specified in this standard. Based on consensus-made requirements, agreements, and management tools, a trusted data matrix is a data- and resource-sharing digital infrastructure to facilitate trusted, secure, transparent, and accountable data sharing, exchanging, circulation, and trading among different stakeholders.

Keywords: functionality requirements, IEEE 3158, IEEE 3158.1, testing requirements, trusted data matrix

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2026 by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved.
Published 23 January 2026. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-2739-5 STD28352
Print: ISBN 979-8-8557-2740-1 STDPD28352

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all IEEE standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter’s views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the [IEEE SA myProject system](#).¹ An IEEE account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/about/contact/>.

requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this standard was completed, the Trusted Data Matrix Working Group had the following membership:

Sha Wei, *Chair*
Changwei Weng, *Vice Chair*
Chuan Ma, *Secretary*

Wenting Chang	Yan Li	Kaidong Wu
Du Chen	Anan Liu	Tingting Wu
Fei Chen	Tiancheng Liu	Hanning Zhang
Mingyou Chen	Zhaowei Liu	Min Zhang
Yuqian Ding	Ying Ma	Shuo Zhang
Jiabao Dong	Zhenjun Ma	Yingwei Zhang
Liming Fang	Lei Ren	Zhen Zhang
Weiran Guan	Xiang Tao	Lili Zhao
Hongwei Jiang	Yaodong Tao	Aixue Zhong
Chen Jin	Yu Wang	
Jun Li	Yunhe Wang	

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Boon Chong Ang	Chen Jin	Changwei Weng
Pin Chang	Piotr Karocki	Kaidong Wu
Wenting Chang	Daozhuang Lin	Yunlong Xie
Du Chen	Tiancheng Liu	Yida Xu
Fei Chen	Chuan Ma	Zhen Yang
Mingyou Chen	Xiaoqi Ma	Tao Yaodong
Zhiman Chen	Eric Meng	Hanning Zhang
Yuqian Ding	Rajesh Murthy	Min Zhang
Jiabao Dong	Lei Ren	Shuo Zhang
Fan Gao	Walter Struppler	Zhen Zhang
Weiran Guan	Qi Sun	Ma Zhenjun
Stefan Hagen	Xiang Tao	Aixue Zhong
Werner Hoelzl	Yu Wang	
Hongwei Jiang	Sha Wei	

When the IEEE SA Standards Board approved this standard on 10 September 2025, it had the following membership:

Lei Wang, *Chair*
Jon Walter Rosdahl, *Vice Chair*
David J. Law, *Past Chair*
Alpesh Shah, *Secretary*

Edward Au	Tyler L. Jaynes	Daniel Sabin
Ted Burse	Thomas Koshy	F. Keith Waters
Xiaofeng (Alfred) Chen	Howard Li	Sha Wei
Doug Edwards	Xiaohui Liu	Luyang (Eric) Zhang
Nehad El-Sherif	Kevin W. Lu	
J. Travis Griffith	Hiroshi Mano	
Deborah R. Hagar	Daleep C. Mohla	
Guido R. Hiertz	Annette D. Reilly	
Ronald W. Hotchkiss	Robby Robson	

Introduction

This introduction is not part of IEEE Std 3158.1-2025, IEEE Standard for Testing and Performance of a Trusted Data Matrix System.

The rapid evolution of digital infrastructure has necessitated the development of systems that help ensure the secure, transparent, and accountable sharing, exchanging, circulation, and trading of data among diverse stakeholders. In this context, the trusted data matrix (TDM) is a decentralized data infrastructure that builds on existing information networks and facilitates the entire data-sharing life cycle. This document addresses the critical need for standardized performance and testing protocols to validate the functionality, interoperability, and overall effectiveness of TDM systems.

This standard outlines the performance and test requirements, procedures, and acceptance criteria for TDM systems, which are designed to operate within a trusted, secure, and transparent environment for data exchange. A TDM system is built on a set of consensus-driven requirements, agreements, and management tools, and it functions as an infrastructure for seamless data and resource sharing among various stakeholders. The primary objective of this standard is to establish a robust testing framework that helps ensure the reliable operation of TDM systems across multiple modules, including data asset management, supply-demand docking, and compliance functions, among others.

The standard is organized into several key clauses, each focused on a crucial aspect of system testing and performance validation:

Clause 4: Performance and Testing Framework. This clause provides an overarching framework for the performance and testing of the TDM system, ensuring that all components meet the required benchmarks for effective and secure operation.

Clause 5: Functionality Requirements. The functionality of the TDM system is critical to its success. This clause defines the core intramodule functionalities that must be implemented to help ensure effective operation, covering modules such as identification and authentication, data asset management, trusted environment, and data asset control. It specifies mandatory, recommended, and optional requirements to help ensure that each module performs its intended function within the system.

Clause 6: Interoperability Requirements. This clause focuses on the necessary interoperability standards for the modules within the TDM system, ensuring that they can interact efficiently with one another. It addresses interfaces, data exchanges, and communication protocols that guarantee seamless integration and secure data flow throughout the system.

Clause 7: Functionality Testing. To verify the functionality requirements outlined in [Clause 5](#), this clause provides a testing framework that outlines detailed testing methods, criteria, and procedures for each module, ensuring that all functionalities are properly implemented and operational.

Clause 8: Interoperability Testing. Building on [Clause 6](#), this clause defines the testing methods and criteria to assess the interoperability of modules within the TDM system. It helps ensure that all modules can effectively communicate and integrate, validating the system's robustness in real-world, data-sharing scenarios.

Clause 9: Testing Strategies, Metrics, and Test Environments. This clause elaborates on the strategies and metrics to be employed during testing, as well as on the environments in which testing will occur. It serves as a guide for organizations to help ensure that testing is thorough and aligned with industry best practices.

Clause 10: Documentation and Reporting. Comprehensive documentation and clear reporting are essential to help ensure transparency and traceability of testing activities. This clause specifies the documentation requirements and reporting formats necessary for all stages of the testing process.

Through these clauses, this standard provides a comprehensive and structured approach to testing and performance evaluation, enabling organizations to assess the effectiveness of their TDM systems in supporting trusted data management. By ensuring that all components of the system meet rigorous performance and interoperability standards, this standard contributes to the advancement of secure and efficient data exchange frameworks, fostering trust among stakeholders and enabling the secure sharing of data in increasingly complex digital ecosystems.

Contents

1. Overview	13
1.1 Scope	13
1.2 Word usage	13
2. Normative references	13
3. Definitions, acronyms, and abbreviations	14
3.1 Definitions	14
3.2 Acronyms and abbreviations	16
4. Performance and testing framework	17
4.1 Testing categories	17
4.2 Testing levels	18
4.3 Testing strategies	18
4.4 Metrics and benchmarks	18
4.5 Test environments	18
4.6 Documentation and reporting	19
5. Functionality requirements	19
5.1 Identification and authentication module	19
5.2 Data asset management module	21
5.3 Supply-and-demand docking module	27
5.4 Trusted environment module	31
5.5 Data asset control module	34
5.6 Data tool service module	36
5.7 Compliance function module	38
6. Interoperability requirements	42
6.1 Intermodule functional requirements of identification and authentication module	42
6.2 Intermodule functional requirements of data asset management module	44
6.3 Intermodule functional requirements of supply-and-demand docking module	48
6.4 Intermodule functional requirements of trusted environment module	51
6.5 Intermodule functional requirements of data asset control module	55
6.6 Intermodule functional requirements of data tool service module	58
6.7 Intermodule functional requirements of compliance function module	61
7. Functionality testings	64
7.1 Identification and authentication module	64
7.2 Data asset management module	90
7.3 Supply-and-demand docking module	147
7.4 Trusted environment module	188
7.5 Data asset control module	219
7.6 Data tool service module	248
7.7 Compliance function module	269
8. Interoperability testings	297
8.1 Intermodule testing requirements of identification and authentication module	297
8.2 Intermodule testing requirements of data asset management module	307
8.3 Intermodule testing requirements of supply-and-demand docking module	319
8.4 Intermodule testing requirements of trusted environment module	331
8.5 Intermodule testing requirements of data asset control module	343
8.6 Intermodule testing requirements of data tool service module	354
8.7 Intermodule testing requirements of compliance function module	364

9. Testing strategies, metrics, and test environments	376
9.1 Testing strategies	376
9.2 Metrics and benchmarks	379
9.3 Test environments	381
10. Documentation and reporting	383
10.1 Test plans and procedures	384
10.2 Test reports	385
10.3 Issue tracking	386

IEEE Standard for Testing and Performance of a Trusted Data Matrix System

1. Overview

1.1 Scope

Performance and test requirements, procedures, and acceptance criteria for a trusted data matrix system are specified in this standard. Based on consensus-made requirements, agreements, and management tools, a trusted data matrix is a data- and resource-sharing digital infrastructure to facilitate trusted, secure, transparent, and accountable data sharing, exchanging, circulation, and trading among different stakeholders.

1.2 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{6,7}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

⁶ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁷ The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

FIPS-PUB-140-2, Security Requirements for Cryptographic Modules.⁸

IEEE Std 3158™-2024, IEEE Standard for Trusted Data Matrix System Architecture.^{9,10}

ISO/IEC 27001, Information security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements.¹¹

NIST SP 80053, Security and Privacy Controls for Information Systems and Organizations.¹²

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms *and definitions apply*. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.¹³

compliance service provider: A third-party service provider that offers security, compliance, and fairness assurance services for all participants in the trusted data matrix, including identity management service providers, authentication service providers, transaction audit service providers, logging service providers, regulatory entities, and trustworthiness management service providers.

data asset: Any valuable and strategically significant data or data-related resource for an organization or individual.

NOTE—Data assets can include raw data, processed information, databases, data models, data sets, data visualizations, and other data-related artifacts that contribute to the organization’s decision-making, operations, and overall business value.¹⁴

data collection: The systematic process of gathering and capturing information from diverse sources to create a data set or gain knowledge about specific phenomena.

NOTE 1—Data collection involves selecting and defining data variables, designing data collection instruments (e.g., surveys, questionnaires, sensors), and implementing methods to retrieve or record the data.

NOTE 2—Data collection is a fundamental step in data management and analysis, and the quality of the collected data directly influences the validity and reliability of subsequent data-driven activities.

data consumer: A party or entity that accesses, retrieves, or utilizes data from a system or ecosystem for analysis, processing, or decision-making purposes.

data deletion: The activity of permanently and securely erasing data from storage media or systems to render it unrecoverable and reduce unauthorized access.

⁸ FIPS publications are available from the National Technical Information Service, U.S. Department of Commerce (<https://www.ntis.org/>).

⁹ The IEEE standards or products referred to in [Clause 2](#) are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

¹⁰ IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

¹¹ ISO publications are available from the International Organization for Standardization (<https://www.iso.org/>) and the American National Standards Institute (<https://www.ansi.org/>). IEC publications are available from the International Electrotechnical Commission (<https://www.iec.ch>) and the American National Standards Institute (<https://www.ansi.org/>).

¹² NIST publications are available from the National Institute of Standards and Technology (<https://www.nist.gov/>).

¹³ *IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the *dictionary sign-in page*.

¹⁴ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

NOTE—Data deletion helps ensure that sensitive or confidential information is completely removed from the devices or storage devices of the data consumer before they are discarded, repurposed, or transferred to other parties. The data stored at the data provider and the third-party service provider are preserved.

data exchange: The process of transferring or sharing data between different systems, applications, or entities in a standardized and interoperable manner.

NOTE—Data exchange enables seamless communication and collaboration by allowing data to flow across diverse platforms and environments.

data preparation: The process of cleaning, transforming, and structuring raw data to help ensure quality, consistency, suitability, and security for analysis or use in various applications.

NOTE—Data preparation involves tasks such as data cleaning, data transformation, data integration, and data formatting to prepare the data for further processing, analysis, or modeling.

data preprocess: The systematic and essential step in data analysis and machine learning that involves cleaning, transforming, and preparing raw data to make it suitable for further analysis or modeling.

NOTE—The aim of data preprocessing is to address issues such as missing values, data inconsistencies, and irrelevant features before publishing, ensuring that the data are of high quality and in a format that can be effectively used by algorithms or statistical techniques.

data provider: A party or entity responsible for generating, collecting, or supplying data to a system or ecosystem.

data publishing: The process of making data sets, research findings, or other data-related resources available to a wider audience.

NOTE—Data publishing involves the dissemination of data to promote transparency, collaboration, and reprehensibility in scientific research, business, or any domain that generates and utilizes data.

data transmission: The process of transferring digital information, such as text, images, or multimedia, from one device or system to another through a communication channel or network.

NOTE—Data transmission involves encoding the data, sending it over the medium, and decoding it at the receiving end to help ensure accurate and reliable data exchange.

data usage: The utilization and application of data for various purposes, such as analysis, decision-making, research, or problem solving.

NOTE—Data usage involves extracting insights, patterns, or knowledge from the data to derive meaningful information that can drive actions and support business processes.

digital contract: A machine-readable contract that is agreed upon and formed between a data provider and a data consumer regarding the control requirements, control policies, boundary conditions, and other agreed-upon behaviors during the use of shared data.

IT infrastructure service provider: A third-party service provider that offers IT infrastructure capabilities for all participants, including IT infrastructure service providers and software providers.

postservice process: The activities or operations performed on data or information after a service has been provided or completed.

NOTE—Postservice processing involves data analysis, reporting, archiving, or other postservice tasks that aim to evaluate the service’s performance, gather insights, or maintain records for future reference, which can derive value or knowledge from the data generated during the service and help to help ensure proper documentation and closure of the service-related activities.

supervisor or regulator: An authority or governing party or entity responsible for overseeing and enforcing compliance with data management practices, policies, and regulations within a system or ecosystem. The term may refer to either a supervisory body with internal oversight responsibilities or a regulatory authority with formal legal or policy enforcement powers, depending on the governance structure.

NOTE 1—The role of the supervisor or regulator involves ensuring that data handling and processing activities adhere to relevant legal requirements, industry standards, and ethical guidelines.

NOTE 2—The supervisor or regulator may have the power to monitor data operations, investigate potential violations, and impose penalties or corrective actions when necessary to maintain data integrity, security, and privacy.

third-party service provider: An entity or organization providing services, resources, or tools to other parties within a system or ecosystem.

NOTE 1—Third-party service providers are distinct from the primary data owners and users but collaborate with them to improve data-related operations and functionalities.

NOTE 2—The services provided by third-party service providers may encompass services such as data storage, processing, analysis, authentication, or other specialized tasks associated with data management or utilization.

transaction service provider: A third-party service provider that offers services for data transactions, including metadata query, transaction intermediary, application market, and transaction clearing.

trusted data matrix: A decentralized data infrastructure that builds on existing information networks and facilitates the entire data-sharing life cycle.

value added service provider: A third-party service provider that offers value-added services, including data identification, resolution services, algorithm models, computing services (e.g., secure multiparty computation, federated learning, privacy computing), and data processing apps.

3.2 Acronyms and abbreviations

AES	Advanced Encryption Standard
AI	artificial intelligence
API	application programming interface
app	application
CA	certificate authority
CSV	comma-separated values
GUID	globally unique identifier
HIPAA	Health Insurance Portability and Accountability Act
IdP	identity provider
I/O	input/output
IEC	International Electrotechnical Commission

IP	Internet Protocol
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
KPI	key performance indicator
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OS	operating system
RBAC	role-based access control
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman cryptosystem
SDK	software development kit
SIEM	security information and event management
SMPC	secure multiparty computation
SMS	Short Message Service
SSO	single sign-on
TEE	trusted execution environment
TDM	trusted data matrix
TLS	Transport Layer Security
VM	virtual machine
XML	Extensible Markup Language

4. Performance and testing framework

This clause establishes a comprehensive performance and testing framework for the trusted data matrix (TDM) system. The framework is designed to systematically assess the TDM system's capabilities, ensuring it meets the stringent requirements for trusted, secure, and efficient data management. The framework includes a structured approach to testing that encompasses multiple dimensions of functionality, performance, interoperability, and security. This approach allows for rigorous evaluation of the TDM system's operations in various real-world scenarios, providing stakeholders with the confidence that the system performs reliably and as intended.

4.1 Testing categories

The TDM testing framework is organized into the following specific testing categories, each targeting a critical aspect of the system's functionality:

- **Functionality testing:** Verifies that all core functions of the TDM system are operating correctly, including identification and authentication, data asset management, supply-and-demand docking, trusted environment, data asset control, data tool service, and compliance function.
- **Interoperability testing:** Validates the seamless integration of the TDM system with external systems and internal modules, ensuring compatibility and smooth data exchange.

4.2 Testing levels

Testing is conducted across the following multiple levels to help ensure comprehensive coverage:

- Unit testing: Focuses on individual components or modules, validating their basic functionality in isolation.
- Integration testing: Examines the interactions between integrated components or modules, ensuring they work together as expected.

4.3 Testing strategies

The testing framework employs the following strategic guidelines to help ensure that tests are reproducible, accurate, and reflective of the system's real-world usage:

- Automated testing: Emphasis on automating repetitive and complex test cases to improve efficiency and coverage.
- Simulation and emulation: Use of simulated environments to replicate real-world conditions and scenarios, including stress and load testing.
- Regression testing: Continuous testing of existing functionalities after changes to help ensure new updates do not negatively impact the system.

4.4 Metrics and benchmarks

Clear metrics and benchmarks are defined as follows to objectively measure the TDM system's performance:

- Response time: Measurement of the time taken by the system to respond to various requests, ensuring it meets predefined thresholds.
- Throughput: Evaluation of the volume of data processed by the system within a given time frame.
- Error rate: Monitoring of the frequency and types of errors encountered during operations.
- Scalability metrics: Assessment of the system's ability to handle increased loads without degradation in performance.
- Security metrics: Evaluation of security-related metrics, including incident response times and the effectiveness of access controls.

4.5 Test environments

The framework defines the following guidelines for setting up test environments that closely mirror the operational conditions of the TDM system:

- Test bed configuration: Specifications for hardware, software, network settings, and other environmental factors necessary for testing.
- Data simulation: Use of representative data sets that reflect real-world data characteristics, including size, format, and complexity.
- Environment variability: Consideration of different operating conditions such as peak loads, network latency, and fault conditions to evaluate the robustness of the system.

4.6 Documentation and reporting

To help ensure transparency and traceability, the following framework includes provisions for detailed documentation and reporting:

- Test plans and procedures: Comprehensive documentation of test plans, including objectives, scope, methodologies, and schedules.
- Test reports: Generation of detailed reports capturing test results, including pass/fail status, metrics achieved, and any deviations from expected outcomes.
- Issue tracking: Mechanisms for logging, prioritizing, and addressing issues identified during testing, with a focus on continuous improvement.

5. Functionality requirements

This clause outlines the comprehensive functionality requirements for each module within the TDM system. The functional modules are defined in IEEE Std 3158™-2024 as identification and authentication, data asset management, supply-and-demand docking, trusted environment, data asset control, data tool service, and compliance function, respectively.¹⁵ These requirements define the core intramodule functionalities that must be implemented to help ensure each module operates effectively and meets the system's overall objectives. The clause includes mandatory, recommended, and optional requirements for each module. By clearly defining these functionalities, this clause establishes the foundation for the system's operational capabilities, ensuring that all modules perform their intended functions within the TDM framework.

5.1 Identification and authentication module

The identification and authentication module is a critical component of the TDM system, responsible for ensuring secure and reliable user access. This subclause defines the functionality requirements necessary for this module to perform its key roles in user identification, authentication, and access control. The requirements outlined here cover mandatory, recommended, and optional functionalities that must be implemented to guarantee that only authorized users can access and interact with the system's resources. By adhering to these requirements, the identification and authentication module helps maintain the security, integrity, and trustworthiness of the TDM system, providing a robust foundation for all subsequent operations.

5.1.1 Mandatory requirements

The following mandatory requirements outline the essential functions that the identification and authentication module shall fulfill to help ensure secure and reliable operation. These include core capabilities such as differentiating between personal and enterprise registrations, supporting multimethod authentication, enforcing password security, and managing user roles and access permissions. These requirements are critical to the system's ability to authenticate users accurately and reduce unauthorized access, forming the backbone of the module's functionality:

- a) Personal and enterprise registration: The system shall distinguish between personal and enterprise registration, allowing tailored registration processes for each type, ensuring the appropriate data fields and validation rules are applied.
- b) Verification of registration information: The system shall support the verification of registration information through mobile devices or email, ensuring the authenticity of the user's credentials during the registration process.

¹⁵ Information on references can be found in [Clause 2](#).

- c) **Multimethod login:** The system shall support login for registered users using at least the following methods: a mobile number or email address combined with a password or a mobile number or email address combined with a one-time verification code.
- d) **Login failure limitations:** The system shall enforce a limit on the number of failed login attempts, temporarily locking the account or requiring additional verification to reduce unauthorized access.
- e) **Password reset capability:** The system shall allow users to reset their passwords through secure methods, such as email or mobile verification, ensuring continued access while maintaining security.
- f) **Encryption of sensitive information:** The system shall encrypt passwords and other sensitive user information during storage using encryption algorithms and key management practices that comply with FIPS 140-2 Level 1 or higher [for example, Advanced Encryption Standard (AES) with a minimum key length of 256 bits or Ron Rivest, Adi Shamir, and Leonard Adleman cryptosystem (RSA) with a minimum key length of 2048 bits], or equivalent standards approved by the implementing organization's security governance policy, thereby protecting against unauthorized access and data breaches.
- g) **User management:** The system shall support comprehensive user management capabilities, including the addition, modification, and deletion of user information, and role assignment, ensuring that user data are kept current and access rights are appropriately managed.
- h) **Registration information review:** The system shall support an administrative review of registration information, allowing for the approval or rejection of user registration based on predefined criteria.
- i) **Password complexity requirements:** The system shall enforce password complexity rules, such as requiring a combination of uppercase letters, lowercase letters, numbers, and special characters, to enhance password security.
- j) **Sensitive information masking:** The system shall mask sensitive information, such as user credentials, in displays, ensuring that sensitive data are not exposed unnecessarily during user interactions.
- k) **Credential authentication:** The system shall authenticate user credentials accurately, validating the legitimacy of users before granting access to the system.
- l) **Role-based access control (RBAC):** The system shall support role-based access control, enabling administrators to assign permissions based on user roles, ensuring that users have access only to the resources necessary for their role.
- m) **Menu and feature authorization:** The system shall support authorization for specific menu items and features, allowing granular control over what users can see and interact with based on their role and permissions.
- n) **Data catalog authorization:** The system shall support authorization for access to data catalog, ensuring that users can only access data for which they have explicit permissions.
- o) **Session timeout management:** The system shall manage user sessions by automatically ending sessions after a period of inactivity, helping to reduce unauthorized access from unattended sessions.

5.1.2 Recommended requirements

The following recommended requirements highlight additional functionalities that the identification and authentication module should implement to enhance security and user experience. These requirements include advanced authentication options like multifactor authentication and anomaly detection for abnormal login behaviors. While they are not mandatory, these features significantly strengthen the security posture of the TDM system and provide additional layers of protection against emerging threats:

- a) The system should support multifactor authentication (MFA) methods, including hardware tokens, biometric verification, or app-based authentication, providing additional layers of security.

- b) The system should support anomaly detection for login behaviors, such as triggering alerts or account locks for logins from unfamiliar locations or devices.

5.1.3 Optional requirements

The following optional requirements provide a set of functionalities that the identification and authentication module may include to offer extra flexibility and capabilities. These optional features, such as continuous authentication and integration with external identity providers for single sign-on, cater to specific use cases or environments where enhanced convenience or security is desired. These functions are not essential but can provide added value to the system based on stakeholder needs:

- a) The system may support continuous authentication methods, such as monitoring user behavior patterns or regularly refreshing session tokens, to maintain security throughout the session.
- b) The system may include integration with external identity providers () for single sign-on (SSO) capabilities, enhancing user convenience and security through federated authentication.

5.2 Data asset management module

The data asset management module is fundamental to the TDM system, overseeing the generation, identification, and maintenance of data assets. This subclause details the functionality requirements for managing data assets effectively throughout their life cycle. These requirements include mandatory, recommended, and optional functionalities that help ensure data assets are accurately generated, properly classified, securely stored, and efficiently maintained. The data asset management module plays a vital role in transforming raw data into valuable assets, maintaining data integrity, and supporting compliance with organizational and regulatory standards. By meeting these requirements, the module contributes to the overall reliability and efficiency of the TDM system's data management processes.

5.2.1 Mandatory requirements

The mandatory requirements outline the essential functions that the data asset management module shall perform to help ensure the generation, identification, and maintenance of data assets. These functions are critical to the module's operation, ensuring that data assets are accurately generated, classified, and protected throughout their life cycle.

5.2.1.1 Data asset generation

- a) The module shall collect data from various data sources, including files, databases, and application programming interfaces (APIs), for generating data assets.
- b) The system shall support the collection of data from diverse types of sources to help ensure comprehensive data acquisition.
- c) The module shall enforce that data collection processes comply with formats and protocols defined and documented by the implementing organization in its data governance policy or system configuration, enabling consistent and reliable data acquisition.
- d) Data assets shall be generated in standardized formats to help ensure consistency and interoperability across the system.
- e) The module shall perform data preprocessing tasks, including data cleaning, normalization, and transformation, to prepare raw data for asset generation.
- f) The module shall collate and process collected data, applying transformation operations to convert raw data into valuable and usable data assets.

- g) The module shall help ensure that each data asset is processed according to the system's predefined data asset generation workflows.
- h) All data sources and operations involved in the data asset generation process shall be recorded to help ensure traceability and audit-ability.
- i) The module shall generate a detailed description (metadata) for each data asset, including identifiers, categories, grades, versions, and other relevant descriptive information.
- j) The module shall help ensure that metadata are retrievable and can be used by the data catalog management system for organizing data assets.

5.2.1.2 Data asset identification

- a) The module shall assign a globally unique identifier (GUID) to each data asset during its generation.
- b) The identifier shall be immutable, ensuring it remains consistent throughout the asset's life cycle.
- c) The module shall classify data assets according to their type, category, and grade, based on technical characteristics, business needs, security sensitivity, and privacy considerations.
- d) The module shall support multiple classification systems, enabling flexible categorization of data assets according to organizational standards or domain-specific requirements.
- e) The data asset category management system shall support the creation, updating, retrieval, and deletion of categories.
- f) Each data asset shall have at least one category, with support for category updates. If classified by the system, the classification rules should be configurable.
- g) The module shall manage the identifiers across the system, ensuring that different parties can resolve identifiers and trace data asset exchanges and usage.
- h) If multiple identifier systems coexist, an identifier mapping mechanism shall be implemented in the data exchange process to help ensure that different parties can resolve identifiers and trace the data asset exchange and usage.

5.2.1.3 Data asset maintenance

- a) The module shall help ensure persistent storage of data assets, supporting creation, update, query, and deletion operations.
- b) The storage system shall guarantee the integrity of stored data assets and provide mechanisms to validate their integrity over time.
- c) The storage system shall support asset creation, update, query, and deletion operations.
- d) The module shall monitor updates to data assets, maintaining version control and logging all changes.
- e) The system shall record detailed logs for each update, ensuring traceability of modifications over the asset's life cycle.
- f) The module shall support backup operations, ensuring that data assets can be restored in the event of data loss or corruption.
- g) The module shall implement access control policies to manage who can access or modify data assets, enforcing these policies consistently.
- h) The module shall monitor access to data assets, tracking access frequency, response times, and data volumes, and generating reports for operational analysis.

- i) The module shall help ensure that data assets can be traced through their entire life cycle, from creation to deletion, maintaining records of all transactions and usage.

5.2.2 Recommended requirements

The recommended requirements suggest additional functionalities that enhance the effectiveness and efficiency of the data asset management module. While they are not mandatory, these functions contribute to better data management practices, improving the module's overall performance and adaptability to various data management scenarios.

5.2.2.1 Advanced data classification

- a) The module should support automated classification of data assets based on predefined rules and algorithms, reducing the need for manual intervention.
- b) The module should support automated classification of data assets based on predefined rules and algorithms, reducing the need for manual intervention.
- c) The system should allow administrators to configure and update classification rules, enabling dynamic categorization of data assets as new data types and business needs arise.
- d) The module should support multidimensional classification, allowing data assets to be categorized under multiple categories simultaneously. This flexibility enables more granular and versatile data management.
- e) The system should support the classification of data assets by grade, considering factors such as data security, sensitivity, and privacy.
- f) Data asset grade management should support the creation, updating, retrieval, and deletion of grades, with the ability to update the grade of a data asset as needed.
- g) If classified by the system, the classification rules should be configurable.

5.2.2.2 Enhanced data asset description

- a) The module should support extended metadata fields, allowing additional descriptive information such as data quality indicators, usage restrictions, and lineage information to be included in the data asset description.
- b) Metadata should be structured to support integration with external data management systems and facilitate data discovery and governance.

5.2.2.3 Data quality management

- a) The module should include tools for assessing the quality of data assets, such as completeness, accuracy, consistency, and timeliness.
- b) Quality metrics should be automatically calculated and stored as part of the data asset's metadata, enabling users to evaluate the suitability of data for their specific needs.
- c) The system should continuously monitor data quality, alerting administrators to any degradation in quality over time, and suggesting remediation actions where possible.

5.2.2.4 Data asset life-cycle management

- a) The module should support the management of data asset life-cycle states, such as active, archived, deprecated, or retired.
- b) The system should provide mechanisms to transition data assets between states based on predefined policies or manual intervention by administrators.
- c) The module should support configurable retention policies for data assets, ensuring that data are retained or deleted in accordance with organizational and regulatory requirements.

5.2.2.5 Scalable data storage solutions

- a) The module should support dynamic storage allocation, allowing the system to automatically allocate and reallocate storage resources based on the current demands and priorities.
- b) This feature should include scalability options to handle increasing volumes of data without compromising performance.

5.2.2.6 Interoperability with external systems

- a) The module should support integration with external data repositories, enabling seamless data transfer and synchronization between the TDM system and external systems.
- b) The module should support industry-standard data interchange formats [e.g., JavaScript Object Notation (JSON), Extensible Markup Language (XML), comma-separated values (CSV)] to facilitate interoperability with other data management systems and platforms.

5.2.2.7 User-friendly data asset management interface

- a) The module should offer customization dashboards that allow users to monitor key metrics and manage data assets efficiently.
- b) Dashboards should be configurable to display relevant data based on user roles and preferences, enhancing the user experience.

5.2.2.8 Data asset reporting and analytic

- a) The module should provide advanced reporting tools, allowing users to generate detailed reports on data asset status, usage patterns, and compliance with policies.
- b) The system should offer customization reporting tools, enabling users to generate detailed reports on data asset status and performance, with support for various output formats.
- c) The module should include basic analytic capabilities to provide insights into data asset usage, performance trends, and areas for improvement.
- d) The data asset storage system should support advanced backup operations beyond the basic module-level requirement, including but not limited to configurable scheduling for full, incremental, and differential backups; off-site or cross-region replication of backup sets; automated integrity verification of backup media; and configurable retention and versioning policies.

- e) The system should monitor asset access, tracking access count, response time, throughput, data volume, and other relevant metrics.

5.2.3 Optional requirements

The optional requirements provide a set of functionalities that the data asset management module may include to offer enhanced capabilities for specific use cases or operational environments. These functions, while not essential, can provide added value to the system depending on the organization's needs and priorities.

5.2.3.1 Dynamic storage allocation

- a) The system may support dynamic storage allocation, enabling automatic scaling of storage resources based on real-time demands. This feature would allow the system to optimize storage utilization and manage increasing data volumes without compromising performance.
- b) The system may include mechanisms for reallocation of storage resources, allowing for flexible management of storage based on changing priorities or data asset requirements.

5.2.3.2 Interoperability with external systems

- a) The system may support integration with external data repositories, enabling seamless data transfer, synchronization, and interoperability between the TDM system and other platforms or data management systems.
- b) The system may provide support for standard data interchange formats (e.g., JSON, XML, CSV) to facilitate easy integration with external systems and help ensure compatibility across different environments.

5.2.3.3 Data retention and archiving

- a) The system may allow the configuration of advanced data retention and archiving policies, including options for automatic archival of data assets based on predefined criteria such as age, access frequency, or regulatory requirements.
- b) The system may provide options for automated deletion or anonymization of data assets after their retention period expires, ensuring compliance with data governance and privacy regulations.

5.2.3.4 Advanced data asset search and retrieval

- a) The system may include advanced search functionalities that allow users to perform complex queries on data assets based on multiple criteria, including metadata fields, content keywords, and access history.
- b) The system may support full text search and indexing of data assets to enable faster and more accurate retrieval of relevant data.

5.2.3.5 Customization data asset dashboards

- a) The system may offer customization dashboards that allow users to monitor key metrics, such as data asset health, usage patterns, and compliance status. Users may be able to configure these dashboards based on their specific roles or preferences.
- b) Dashboards may include visualization tools, such as graphs and charts, to help users quickly interpret and act on data asset information.

5.2.3.6 Data asset annotation and collaboration

- a) The system may support annotation of data assets, allowing users to add notes, comments, or tags to data assets to facilitate collaboration and shared understanding among stakeholders.
- b) The system may provide version-controlled annotations, ensuring that all changes and comments are tracked and can be reviewed as part of the data asset's history.

5.2.3.7 Data asset version rollback

- a) The system may include a feature that allows users to revert data assets to previous versions in case of errors or the need to restore older data states. This capability would support better management of data integrity and recovery processes.

5.2.3.8 Custom metadata fields

- a) The system may allow the creation of custom metadata fields, enabling organizations to capture and manage additional information specific to their data governance needs or industry standards.
- b) These custom fields may be integrated into the overall data asset management process, allowing for tailored data categorization, search, and reporting.

5.2.3.9 Data asset access insights

- a) The system may include features to analyze and report on data asset access patterns, providing insights into which data assets are most frequently accessed, by whom, and under what conditions.
- b) This feature could support strategic decisions related to data asset management, security, and resource allocation.

5.2.3.10 User-driven data asset organization

- a) The system may provide tools that allow individual users to organize data assets according to their personal workflows or preferences, such as creating custom folders, labels, or virtual groupings that do not affect the overall system's structure.
- b) This feature could enhance user productivity by enabling more intuitive navigation and management of data assets.

5.3 Supply-and-demand docking module

The supply-and-demand docking module is essential for managing the interactions between data providers and consumers within the TDM system. This subclause defines the functionality requirements for the module, focusing on its ability to catalog data resources, manage contracts, evaluate data and services, and handle financial transactions. The requirements are divided into mandatory, recommended, and optional categories, reflecting the different levels of importance and flexibility in implementing these functionalities. By meeting these requirements, the supply-and-demand docking module helps ensure that data resources are efficiently organized, contractual obligations are fulfilled, and financial processes are executed with accuracy and transparency.

5.3.1 Mandatory requirements

The mandatory requirements for the supply-and-demand docking module define the essential functionalities that must be implemented to help ensure the effective management of data resources, contracts, and financial transactions within the TDM system. These requirements are critical to the operation of the module, providing a foundation for the secure and efficient handling of data catalog management, contract management, metering, and clearing processes. The mandatory functionalities help ensure that data assets are organized, contracts are managed centrally, data usage is accurately tracked, and financial obligations are settled with precision.

5.3.1.1 Data catalog management

- a) The system shall classify, organize, and manage data resources systematically, ensuring that all data assets are categorized according to predefined classification schemes, such as data type, source, and relevance.
- b) The system shall create and maintain an index of all data resources, facilitating efficient search and retrieval processes.
- c) Indexes shall be updated automatically whenever new data resources are added or existing ones are modified.
- d) The system shall support comprehensive metadata management, allowing for the storage, retrieval, and updating of metadata associated with each data resource.
- e) Metadata shall include key attributes such as data owner, creation date, last modification date, and access permissions.
- f) The system shall support integration with other modules and external data sources, ensuring the catalog is comprehensive and reflects all available data assets.
- g) The system shall track changes and updates to the data catalog, maintaining version history and providing audit trails for all modifications.
- h) The system shall help ensure that previous versions of data assets are accessible for audit and review purposes.

5.3.1.2 Contract management

- a) The system shall provide a centralized repository for storing and managing all contracts related to data and services, ensuring that contracts are easily accessible and organized in a structured manner.
- b) The system shall manage the entire life cycle of contracts, including creation, negotiation, approval, execution, renewal, and termination, with built in workflow support to guide users through each stage.

- c) The system shall monitor contract compliance, tracking key performance indicators (KPIs) and milestones to help ensure that all contractual obligations are met and flagging any deviations or breaches.
- d) The system shall automatically send notifications and alerts for important contract events, such as upcoming renewals, expiration, or potential breaches, to relevant stakeholders.
- e) The system shall maintain a detailed audit trail for each contract, recording all actions taken, including changes, approvals, and communications, to help ensure traceability and accountability.
- f) [For data developer only] The system shall provide a mechanism for the data developer to review and accept contractual terms relevant to their role, including agreements on intellectual property rights, confidentiality, and liability in the data-sharing process.
- g) [For data developer only] The system shall allow data developers to specify and document their contributions (e.g., algorithms, models, or tools) in the contract repository, ensuring traceability and alignment with agreed deliverable.
- h) [For data developer only] The system shall enable collaborative workflows where data developers can interact with both data providers and data consumers during contract creation and negotiation to clarify roles, responsibilities, and deliverable.
- i) [For data developer only] The system shall track and manage contractual obligations specific to the data developer, such as performance criteria for algorithms, timelines for tool delivery, or updates to models, ensuring compliance and flagging any deviations.
- j) [For data developer only] The system shall provide notification and alert mechanisms for data developers regarding key contract events, such as deadlines for deliverable, review milestones, or updates to the contract.
- k) [For data developer only] The system shall include a detailed audit trail for data developer actions within the contract life cycle, documenting interactions, approvals, modifications, and communications to help ensure accountability and transparency.

5.3.1.3 Metering

- a) The system shall accurately track and calculate data usage or consumption, capturing details such as the volume of data accessed, frequency of access, and specific user interactions.
- b) The system shall support multiple metering methods, such as volume-based, time-based, or transaction-based, depending on the type of data and service being consumed.
- c) The system shall provide real-time monitoring of data usage, allowing for immediate visibility into consumption patterns and identifying any unusual or unexpected spikes in usage.
- d) The system shall securely store all metering data and generate detailed reports on data usage, including trends, peak usage times, and potential cost implications.
- e) Reports shall be customized to meet the specific needs of different stakeholders and should be available in various formats.
- f) [For data developer only] The system shall allow the data developer to integrate metering mechanisms into their algorithms, models, or tools, ensuring accurate tracking of data usage during algorithmic or model-based operations.
- g) [For data developer only] The system shall enable data developers to define and implement customized metering methods tailored to the data-sharing process, considering the type of data and computational resources consumed.

- h) [For data developer only] The system shall provide data developers with access to real-time monitoring tools to observe data consumption metrics during the development and execution of algorithms or models, ensuring efficient and transparent resource usage.
- i) [For data developer only] The system shall require data developers to securely log and document metering activities related to their algorithms or tools, ensuring traceability and alignment with organizational metering policies.
- j) [For data developer only] The system shall support data developers in generating detailed usage reports for their algorithms or models, including metrics such as data volume processed, computational cycles utilized, and time intervals of operations, presented in customization formats for stakeholder review.

5.3.1.4 Clearing

- a) The system shall verify the accuracy of all financial transactions related to data usage, ensuring that the recorded data reflects actual usage and that all financial obligations are fulfilled.
- b) The system shall automatically process and settle accounts between parties, ensuring that payments are accurately distributed according to the terms of the contract.
- c) The system shall function as a clearinghouse, managing the exchange of financial information between parties and ensuring that all transactions are processed smoothly and efficiently.
- d) The system shall generate comprehensive reports on all cleared transactions, providing transparency into the financial flows within the system.
- e) Detailed audit trails shall be maintained for all clearing operations, documenting every step of the process and ensuring compliance with financial regulations.
- f) [For data developer only] The system shall provide data developers with tools to integrate mechanisms into their algorithms or models to track and verify the accuracy of financial calculations related to data usage during shared processes.
- g) [For data developer only] The system shall enable data developers to define and implement logic within their tools to automate the calculation and reconciliation of costs, ensuring that financial obligations align with the agreed terms in the contract.
- h) [For data developer only] The system shall facilitate data developers in incorporating clearing protocols into their tools or models, ensuring smooth financial information exchange and alignment with the clearinghouse functions.
- i) [For data developer only] The system shall support data developers in generating detailed financial reports linked to their algorithms or tools, offering insights into transaction flows and compliance with contractual obligations.
- j) [For data developer only] The system shall require data developers to help ensure that their tools maintain audit trails for financial calculations and clearing processes, documenting all steps to meet regulatory and organizational compliance standards.

5.3.2 Recommended requirements

The recommended requirements for the supply-and-demand docking module provide additional functionalities that enhance the module's effectiveness and flexibility. While they are not strictly necessary, these features offer significant benefits, such as improved evaluation of data and services, better billing management, and enhanced reporting capabilities. Implementing these recommended functionalities can help organizations optimize their data and service management processes, help ensure more accurate billing, and gain deeper insights into the performance and usage of their data assets.

5.3.2.1 Data and service evaluation

- a) The system should evaluate and analyze key indicators of data and services, such as quality, security, reliability, and performance, providing comprehensive metrics that inform decision-making processes.
- b) The system should automate the evaluation process, applying standardized criteria consistently across all data assets and services to help ensure uniformity and accuracy in assessments.
- c) The system should allow users to define and customize evaluation criteria based on specific business needs, industry standards, or regulatory requirements, ensuring that the evaluation process is aligned with organizational goals.
- d) The system should generate detailed reports on the evaluation results, highlighting areas of excellence or concern, and providing actionable insights for improvement.

5.3.2.2 Billing

- a) The system should calculate charges based on data usage or consumption, applying the pricing models defined in contracts or organizational policies to help ensure accurate and fair billing.
- b) The system should generate invoices that provide a detailed breakdown of usage, costs, applicable taxes, and fees, ensuring transparency in the billing process.
- c) The system should support integration with external payment processing systems, facilitating seamless payment collection from users or customers and ensuring timely settlement of bills.
- d) The system should generate billing reports that provide insights into billing patterns, outstanding payments, and revenue streams, helping organizations manage their financial operations effectively.

5.3.3 Optional requirements

The optional requirements for the supply-and-demand docking module provide additional functionalities that enhance the module's capabilities, offering advanced features that cater to specific operational needs or optimize system performance. While these functionalities are not essential for the basic operation of the module, their implementation can provide added value by improving user experience, increasing efficiency, and offering greater flexibility in managing data, contracts, and financial transactions. Organizations may choose to implement these optional features based on their specific business requirements, operational context, and long-term strategic goals.

5.3.3.1 Enhanced data catalog integration

- a) The system may support integration with external data repositories, enabling seamless data transfer, synchronization, and interoperability between the TDM system and other data management platforms. This feature would allow for the incorporation of external data sources into the internal data catalog, expanding the range of available data assets and improving data resource management.
- b) The system may support industry-standard data interchange formats (e.g., JSON, XML, CSV) to facilitate interoperability with other data management systems and platforms. This helps ensure that data can be easily exchanged, shared, and integrated across different systems, enhancing the versatility and reach of the TDM system.

5.3.3.2 Advanced contract management features

- a) The system may provide customization contract templates that allow organizations to create contracts more efficiently by standardizing commonly used terms and conditions. This feature can reduce the time and effort required to draft new contracts, ensuring consistency across different agreements.
- b) The system may include collaboration tools that allow multiple stakeholders to work on contract documents simultaneously, facilitating real-time editing, commenting, and approval workflows. This enhances the efficiency and transparency of the contract management process, ensuring that all relevant parties are involved and informed.

5.3.3.3 Enhanced reporting and analytic

- a) The system may offer advanced reporting tools that allow users to generate detailed, customized reports on various aspects of the supply-and-demand docking module, including contract performance, data usage, and financial transactions.
- b) Reports may be tailored to meet the specific needs of different stakeholders and can be output in various formats.
- c) The system may include predictive analytic capabilities that provide insights into future trends based on historical data, helping organizations anticipate changes in data usage, contract renewals, or financial obligations. This feature would support strategic decision-making and long-term planning.

5.3.3.4 User-friendly dashboards and interfaces

- a) The system may offer user-friendly, customization dashboards that provide a visual overview of key metrics related to data catalog management, contract status, and financial performance.
- b) Dashboards may be configured to display the most relevant information for different user roles, improving the efficiency of data management and decision-making processes.
- c) The system may feature an intuitive user interface that simplifies navigation and task execution, reducing the learning curve for new users and enhancing overall user satisfaction.

5.4 Trusted environment module

The trusted environment module is a critical component of the TDM system, ensuring that all aspects of the system's operations—ranging from configuration and execution to monitoring—are conducted within a secure and trustworthy environment. This module is designed to protect the integrity, confidentiality, and reliability of the system's configuration files, software, hardware, and execution processes. Additionally, it monitors the system's activities in real time to reduce and respond to potential threats. The mandatory requirements outlined in this subclause focus on the essential functionalities that the trusted environment module must support to achieve these objectives. These requirements are vital for maintaining the security and trustworthiness of the TDM system.

5.4.1 Mandatory requirements

The mandatory requirements for the trusted environment module define the core functionalities necessary to help ensure the security and integrity of the TDM system. These requirements are essential for the verification and protection of configuration files, the secure execution of programs, and the continuous monitoring of system activities. By implementing these requirements, the system can maintain a trusted environment that

safeguards against unauthorized access, helps ensure data integrity, and supports the overall reliability of the system.

5.4.1.1 Trusted configuration

- a) The system shall verify and protect configuration files, software, and hardware in a computer system to help ensure their integrity and trustworthiness.
- b) The system shall have the capability to document and track all configuration changes, including modifications to configuration files and software updates.
- c) The system shall record the history of all configuration changes, including the user making the change, the content of the change, and the time of the change.
- d) The system shall verify the validity of configuration files and settings based on preset security policies.
- e) The configuration function shall be able to detect whether the connected client has been authenticated before allowing any data-sharing activities.
- f) The system shall support the ability to implement version control for configuration files, allowing for quick rollback to previous configurations and aiding in troubleshooting in case of issues.
- g) Communication between systems related to data-sharing activities shall be encrypted and secure, ensuring the integrity and confidentiality of the data being exchanged.

5.4.1.2 Trusted execution

- a) The system shall verify running code to help ensure that it is unaltered and originates from a trusted source, thereby guaranteeing the trustworthiness and reliability of the execution process.
- b) The system shall protect the execution environment, ensuring that only authorized users can execute programs and use data, and that their permissions are properly managed.
- c) The system shall verify the security of the execution environment, including the operating system and hardware, before data sharing begins.
- d) The system shall include secure storage solutions, such as trusted databases and encrypted storage, to protect sensitive data from unauthorized access or modification.
- e) The system shall support encryption and decryption operations to help ensure the security of data during transmission and storage.

5.4.1.3 Trusted monitoring

- a) The system shall monitor and audit the operating status and activities of the computer system in real time to help ensure the credibility and security of the system.
- b) The system shall continuously monitor network and application activities to detect anomalies or potential threats.

5.4.2 Recommended requirements

The recommended requirements for the trusted environment module provide additional security measures that enhance the overall trustworthiness of the system. These requirements, while not mandatory, offer significant benefits by strengthening the verification processes, improving the security of execution environments, and

enhancing monitoring capabilities. Implementing these recommended features can help organizations better protect their data, reduce unauthorized access, and respond more effectively to potential security threats.

5.4.2.1 Trusted configuration

- a) The trusted environment function should include the ability to implement version control for configuration files, allowing for quick rollback to previous configurations and facilitating troubleshooting in case of issues.
- b) The system should verify the legality of configurations during the configuration process and provide alerts in case of any abnormal situations.
- c) The configuration function should verify whether the connected client has been authenticated before allowing data-sharing activities to proceed.

5.4.2.2 Trusted execution

- a) The system should help ensure that data are processed in an isolated environment to reduce data leakage or tampering when interacting with other programs or operating systems.
- b) The system should verify the security of the execution environment, including the operating system and hardware, before data sharing or execution begins.
- c) The system should support encryption and decryption operations to help ensure the security of data during execution and storage, reducing the risk of unauthorized access or data breaches.

5.4.2.3 Trusted monitoring

- a) The system should continuously monitor network and application activities to detect anomalies or potential threats, enabling proactive responses to security issues.
- b) The system should utilize analytical techniques to identify abnormal behavior patterns of users and devices, enhancing the system's ability to detect and respond to potential threats.
- c) The system should audit and monitor the implementation of access control policies to help ensure that only authorized users and devices can access sensitive data and resources.

5.4.3 Optional requirements

The following optional requirements for the trusted environment module offer advanced functionalities that can further enhance the security and efficiency of the system. These features, while not necessary for the basic operation of the module, provide additional layers of protection and flexibility. Organizations may choose to implement these optional features based on their specific security needs, operational requirements, and long-term strategic goals:

- a) The system may implement advanced analytic tools, such as behavioral biometric, to analyze user interactions within the trusted environment. This could enhance the detection of subtle anomalies or potential insider threats that might not be detected by standard monitoring tools.
- b) The system may allow administrators to create and customize security policy templates that can be applied across different components of the trusted environment. This would enable more flexible and adaptable security management tailored to specific organizational needs.

- c) The system may support integration with external SIEM systems to enhance the analysis of security events and provide a more comprehensive security overview. This could facilitate more sophisticated incident response and threat detection across multiple systems.
- d) The system may implement blockchain technology for logging and auditing purposes, ensuring that logs are immutable and can be securely verified. This could add an additional layer of trust and transparency to the monitoring processes.
- e) The system may include advanced security features for virtualized and containerized environments, such as runtime protection and isolation techniques. These enhancements could provide additional protection in environments where virtual machines or containers are heavily used.

5.5 Data asset control module

The data asset control module is responsible for managing the life cycle of data assets from preprocessing to destruction. This module helps ensure that data assets are handled securely and efficiently, with robust control mechanisms in place to manage data access, monitor data status, and execute control strategies. The requirements for this module are designed to maintain the integrity, availability, and security of data assets throughout their life cycle, supporting the system's overall goals of trusted data management.

In addition to the data consumer, if a data developer participates in the specific data-sharing process, the following requirements shall also apply to them. Data developers, as integral stakeholders in the data life cycle, must adhere to the same standards of integrity, availability, and security in managing data assets. This helps ensure that their contributions—such as algorithms, models, or tools—are developed, tested, and deployed within the framework of robust data control mechanisms. By extending these requirements to data developers, the system helps ensure cohesive and secure data management across all roles involved in the sharing process.

5.5.1 Mandatory requirements

The mandatory requirements for the data asset control module define the essential functionalities necessary for the secure and efficient management of data assets. These requirements help ensure that data assets are preprocessed, monitored, controlled, and when necessary, securely destroyed in accordance with organizational policies and regulatory standards. Implementing these functionalities is critical for maintaining the integrity, availability, and security of data assets throughout their life cycle, ensuring that they are handled in a way that meets the high standards of the TDM system.

5.5.1.1 Data preprocessing

- a) The system shall have the capability to clean shared data, including identifying and processing missing data (e.g., filling, deleting, or interpolating missing values), identifying and processing outliers (e.g., deleting, correcting, or transforming them), and dealing with duplicate data (e.g., deleting or merging duplicate records).
- b) The system shall have the capability to integrate shared data, merging data from different sources into a unified view and resolving data consistency issues when conflicts exist between data sources.
- c) The system shall have the capability to transform data, including normalizing data to a consistent scale, converting data formats (e.g., converting continuous data into categorical data), and extracting new features from raw data to enhance predictive capabilities. Additionally, the system shall help ensure that data processing is encrypted, protecting privacy during these operations.
- d) The system shall have the capability to reduce data, such as selecting the most important features from the original data set to reduce dimension and using sampling techniques to manage data volume.
- e) The system shall help ensure data privacy and security during the preprocessing phase, including desensitizing sensitive data and complying with relevant data protection regulations.

5.5.1.2 Control policy configuration

- a) The system shall read and configure control policies and requirements based on contractual agreements, including defining policies for subjects, tools, objects, actions, time, and location.
- b) The system shall dynamically monitor and manage control policies during data usage, issuing alerts when potential data leakage or noncompliant behavior is detected.
- c) The system shall execute control policies in response to boundary conditions, such as denying operations or prohibiting data use, as stipulated in the contract.

5.5.1.3 Data status monitoring

- a) The system shall monitor and inspect data status in real time or at regular intervals to help ensure its accuracy, completeness, and availability.
- b) The system shall continuously monitor data usage according to the policies stipulated in the contract and issue alerts when anomalies or noncompliant activities are detected.

5.5.1.4 Control policy execution

- a) The system shall execute control policies as defined in the contract, including actions triggered by boundary conditions such as data deletion, issuing warnings, or prohibiting data use.
- b) The system shall respond quickly and appropriately to abnormal situations or when contract boundary conditions are triggered, as stipulated in the contract.

5.5.1.5 Data deletion

- a) The system shall delete data as required by the data provider, using methods such as file destruction, data content deletion, key invalidation, or physical erasure.
- b) The destroyed data shall be irrecoverable.
- c) After data usage is complete, the system shall securely process all copies, process data, cache data, and so on, according to the contract's stipulations.

5.5.2 Recommended requirements

The following recommended requirements for the data asset control module offer additional functionalities that enhance the module's capabilities in managing data assets. These features provide improved control, monitoring, and security mechanisms that go beyond the basic requirements. Implementing these recommended functionalities can help organizations optimize their data asset management processes, improve compliance with regulatory requirements, and enhance the overall security of data assets within the TDM system:

- a) The system should log the details of data destruction, including information about the data, the environment in which destruction occurred, the methods used, and the outcomes achieved. This helps ensure traceability and accountability in data destruction processes.

- b) The system should handle derivative data according to the stipulations outlined in the contract, ensuring that any data generated during processing is managed securely and in compliance with agreed-upon policies.
- c) The system should help ensure that all data processing activities comply with relevant data protection regulations, incorporating mechanisms to enforce compliance during preprocessing and control policy execution.

5.5.3 Optional requirements

The following optional requirements for the data asset control module provide advanced features that offer additional flexibility and enhanced capabilities for managing data assets. While they are not essential for the basic operation of the module, these optional functionalities can add significant value by allowing for more customized control strategies, advanced monitoring, and improved data security. Organizations may choose to implement these optional features based on their specific operational needs, security concerns, and long-term data management strategies:

- a) The system may use advanced analytic to assess user behavior and detect patterns that could indicate potential policy violations, enhancing the proactive enforcement of control policies.
- b) The system may implement blockchain technology to create immutable logs of data processing and control policy execution, ensuring that all actions are securely recorded and can be independently verified.
- c) The system may support integration with external Security information and event management (SIEM) systems, allowing for comprehensive monitoring and analysis of security events across multiple platforms.

5.6 Data tool service module

The data tool service module is responsible for managing the life cycle of data tools used within the system. This module encompasses the installation, execution, and removal of data tools, as well as their listing, operation, and removal. By ensuring that data tools are effectively managed and maintained, the data tool service module plays a crucial role in supporting the efficient processing and analysis of data assets. The following subclauses outline the mandatory, recommended, and optional requirements for this module, detailing the functionalities necessary to maintain the reliability, security, and efficiency of data tool operations.

IEEE Std 3158-2024 analyzes the relevant functions of data tools from the perspective of using the role of stakeholders, and the definition of functions are relatively abstract. But this standard refines the operation and practice of functions from the perspective of product implementation. The subclause will give specific requirements to provide effective guidance for data tools developers and standardize the data tools management and utilization in data tools store, trusted environment and specific computing services.

5.6.1 Mandatory requirements

The mandatory requirements for the data tool service module define the essential functionalities required to help ensure that data tools are properly installed, executed, uninstalled, and managed within the TDM system. These requirements focus on the core processes that enable the effective deployment and operation of data tools, ensuring that they are secure, reliable, and aligned with the system's overall objectives. Implementing these functionalities is critical for maintaining the integrity and availability of data tools throughout their life cycle.

5.6.1.1 Data-tools onboarding

- a) The data tools store shall have the capability to onboard data tools, ensuring that they are properly uploaded and made available for use within the system.
- b) The system, via the data tools store interface, shall facilitate the issuance of a certification from a recognized certificate authority (CA). The certification shall include key details such as the data tool's version and summary information.
- c) The types of data tools, such as applications (apps), software development kits (SDKs), and third-party application plugins or packages, shall be listed on the data tools store.

5.6.1.2 Data-tools maintenance

- a) The data tools store shall have the capability to maintain data tools, including listing, searching, ordering, recommending, upgrading, and repairing data tools as necessary.
- b) The data tools store shall support the removal of data tools. Recertification and onboarding again of data tools shall also be supported when required.
- c) The data tools shall be installation, operation, and removal in the trusted environment and specific computing service of TDM systems normally and stability.

5.6.1.3 Data-tools compliance and verification

- a) If data tools provide external interfaces, they shall be verified by the data tools store or a compliance assessment service. The verification process shall confirm that the functionality and performance of the data tools align with their technical specifications document (data sheets) and meet the requirements of applicable use cases.
- b) Data tools shall have robust data security capabilities, employing effective techniques to protect sensitive and private data. Additionally, they shall exhibit stability, ease of use, and secure operation without vulnerabilities or leaks.
- c) Data tools shall be utilized following the digital contract in the trusted environment and specific computing service of TDM systems, to make sure the data process is in accordance with configured control policies.

5.6.2 Recommended requirements

The following recommended requirements for the data tool service module provide additional functionalities that enhance the module's capabilities in managing data tools. These features support improved security, efficiency, and user experience in handling data tools, offering advanced options for their deployment, monitoring, and management. Implementing these recommended functionalities can help organizations optimize their use of data tools, ensuring that they are effectively integrated into the TDM system and aligned with best practices for data management:

- a) The data tools store should support interfaces for uploading data tools, including the ability to upload technical documents and sample of trial data set, and provide support-related services.
- b) The data tools store should support the evaluation and scoring of data tools, allowing users to provide feedback on the functionality, performance, and overall user experience.

- c) The data tools should support secure input/output (I/O) to docking with interfaces of other modules to help ensure the easy and reliable processing of data asset.
- d) The trusted environment should record the usage and operation information of data tools, providing detailed logs that can be used for monitoring and auditing purposes.
- e) Data tools providing external interfaces should be compatible with major operating systems, containers, or compilation environments. This helps ensure broader usability and integration across various platforms.
- f) The data tools in SDK form should support common compilation environments and provide comprehensive technical documentation, tools, and function libraries to assist developers and users.

5.6.3 Optional requirements

The following optional requirements for the data tool service module offer advanced features that provide additional flexibility and customization in managing different types of data tools, such as apps, SDKs, and application plugins. While they are not essential for the basic operation of the module, these functionalities can add significant value by enabling more tailored management strategies, enhanced monitoring, and greater adaptability in the use of data tools. Organizations may choose to implement these optional features based on their specific needs, operational contexts, and long-term goals for data tool management:

- a) The data tools in app form may provide different versions for common operating systems, enhancing their usability across diverse environments.
- b) Third-party application plugins or extension packages may be designed to be compatible with common versions of third-party applications, or they may support the instantiation and containerization of customized applications.
- c) The data tools store may support advanced removal options, such as securely removing all traces of data tools from the system and managing recertification processes for tools that are onboard again.
- d) Data tools in SDK or plugin form may be optimized for use in containerized environments, providing greater flexibility in how these tools are deployed and managed.

5.7 Compliance function module

The compliance function module is responsible for ensuring operational security, regulatory compliance, and traceability. This module provides functionalities that focus on log recording, auditing, tool certification, regulatory interface, and interfaces to support dispute resolution processes as defined by contractual agreements or applicable governance policies. The requirements outlined in this subclause include mandatory functionalities that must be implemented, along with recommended and optional features to comprehensively monitor system activities, help ensure compliance with regulations, resolve disputes, and enhance system integrity. By implementing these functionalities, the compliance function module helps ensure full visibility, traceability, and control over the TDM system, improving its reliability, security, and alignment with relevant compliance standards.

5.7.1 Mandatory requirements

The mandatory requirements for the compliance function module define essential functionalities that must be implemented to help ensure the system's security, traceability, and regulatory compliance. These requirements focus on core aspects such as comprehensive, event auditing, and basic certification processes, which are necessary to meet legal and operational standards. By implementing these features, the compliance function module enables the system to maintain detailed records of user activities, contract management, and data operations, ensuring that all actions are verifiable and compliant with internal policies and external regulations.

5.7.1.1 Log recording and management

The following mandatory requirements for log recording and management define the essential functionalities that help ensure a comprehensive and secure audit trail throughout the TDM system. This functionality encompasses the recording of critical operational events, which are vital for security analysis, system audits, and regulatory compliance. The module shall record detailed logs for key events such as user login history, event management, asset control, configuration changes, and service operations. These records provide transparency and accountability, helping maintain system integrity and traceability across its life cycle:

- a) The system shall record all user login events, including login, logout, and any configuration changes made during the session.
- b) The system shall record user roles, permissions, authorizations, permission changes, and any anomalous behaviors (e.g., attacks, intrusions).
- c) The system shall record all user and role authentication events, including authentication attempts, successes, failures, and any subsequent changes.
- d) The system shall record key asset control events, including timestamps, associated data, participant details, and the outcomes of control actions.
- e) The system shall record all trusted environment scoring activities, including score records, timestamps, and the users responsible for the scoring.
- f) The system shall record all configuration changes, including the user initiating the change, the content of the changes, and the timestamp of the event.
- g) The system shall record all events related to detecting whether connected clients have been authenticated, ensuring all connections are secure.
- h) The system shall record all operations related to changes in the data catalog, ensuring an audit trail of data resource management.
- i) The system shall record contract classification history, documenting any reclassifications or adjustments made to contracts within the system.
- j) The system shall record key information about data usage contracts, including the approval process, signatories, contract type, signing date, expiration date, and negotiation outcomes.
- k) The system shall record all data quality assessments and service evaluations, including relevant metadata and results.
- l) The system shall record the entire metering process, including user details, data involved, and the final metering results.
- m) The system shall record all third-party service provider settlement events related to data sharing, exchange, or usage services.
- n) The system shall record all changes related to data tool installations, including version updates, content, and any adjustments made during installation.
- o) The system shall record the operational history of data tools, documenting actions taken and outcomes during tool usage.
- p) The system shall record removal events, including timestamps, the user performing the action, and any related configuration changes.
- q) The system shall record all login events for data tools, including the timestamp, user, and the duration of the data tool usage.
- r) The system shall record all maintenance activities related to data tools, including deployment, removal, and debugging events.

- s) The system shall record computation service executions based on digital contracts, ensuring traceability of all actions performed within the platform.
- t) The system shall record data destruction events, including the data involved, the environment in which destruction occurred, the methods used, and the outcomes of the destruction process.
- u) The system shall help ensure that the record retention period exceeds the contract validity period which is agreed by all parties, guaranteeing that audit trails are maintained for future reference and compliance.

5.7.1.2 Auditing

The following auditing functionality of the compliance function module helps ensure the ongoing monitoring, recording, and analysis of system operations, events, and activities. Regular audits and analysis of records and data usage patterns are required to detect anomalies, help ensure compliance with policies, and maintain system integrity. The auditing process is essential for verifying that access controls, data security, and transactional processes meet the required standards. The following auditing requirements outline the necessary steps to maintain comprehensive oversight of system activities:

- a) The system shall help ensure that only authorized personnel have access to specific data, enforcing access control policies. The system shall review data access records to verify that appropriate monitoring and tracking mechanisms are in place. Regular reports shall be generated to document access events and any identified issues. For the extraction of audit materials, the system shall help ensure that an application is submitted to the relevant dispute resolution body as defined by the contract or governing policies.
- b) The system shall help ensure that all data are securely stored in trusted environments, reducing unauthorized access or modification. The audit shall regularly verify the integrity and confidentiality of stored data.
- c) The system shall regularly analyze data usage patterns to detect anomalies, ensuring that data are used, retained, and destroyed within the authorized scope. Audits shall help ensure compliance with data usage policies and regulatory requirements.
- d) The system shall audit the security verification, download status, and authentication of clients, ensuring that clients originate from secure and trusted third-party service providers. Any inconsistencies or risks identified shall be documented and addressed.
- e) The system shall audit records related to metering, billing, and settlement processes to help ensure that all transactions and settlement information are accurately recorded. Audits shall validate that all parties involved in transactions are properly documented and that financial information is correctly tracked and reported.

5.7.2 Recommended requirements

The recommended requirements for the compliance function module provide additional features that enhance system security, operational oversight, and certification processes. These functionalities, while not mandatory, offer significant value by improving the integrity and transparency of system operations, particularly through enhanced logging record, advanced tool certification mechanisms, regulatory interface improvements, and dispute resolution capabilities. Implementing these recommended features can help organizations strengthen their compliance posture, proactively detect and resolve issues, and help ensure seamless adherence to evolving industry standards and regulatory frameworks.

5.7.2.1 Tools certification

Tools certification is essential for ensuring that tools comply with specific standards and policies within the TDM system. The certification process involves a multilayered policy approach that verifies the compliance

and security of tools before they are granted access to data and services. The following policies are enforced to safeguard the integrity of the data space and help ensure that only authorized and verified participants and tools are able to operate within the system:

- a) The first line of policy defense is the membership policies, which are required to join a data space. These policies help ensure that only organizations with specific, verifiable attributes are granted membership. Applicants must demonstrate compliance with predefined criteria to be accepted as participants.
- b) Once an organization becomes a participant, access policies come into effect. These policies define the attributes required for participants to access data contracts within the system. Access to data is tightly controlled to help ensure compliance with the terms and conditions of the data space.
- c) When a participant gains access to a data contract, contract policies govern the attributes required for the participant to engage with the data contract. Contract policies help ensure that participants meet the specific criteria outlined in the contract, further safeguarding data and service integrity.
- d) The system may employ blockchain technology, certificate authority certification, or other related technologies to facilitate tool certification. These technologies help ensure that records of tool certifications are maintained securely and transparently, providing an immutable audit trail for compliance verification.

5.7.2.2 Regulatory interface

The regulatory interface is responsible for overseeing software, products, and systems to help ensure compliance with relevant standards and regulations. This interface supervises critical processes, such as metering, billing, and settlement, while maintaining detailed records to support audits and provide evidence for regulatory oversight. Additionally, the interface includes the following mechanisms to investigate noncompliant behavior and apply corrective measures when necessary:

- a) The system shall maintain detailed records of settlement, billing, and metering activities. These records must be available for supervisory services and can be used as evidence in audits or regulatory investigations.
- b) The system shall provide interfaces to identify, investigate, and address potential noncompliant behavior. It shall have mechanisms to take corrective or punitive measures when necessary, ensuring that all regulatory standards are met and enforced.

5.7.2.3 Dispute resolution interface

The dispute resolution interface facilitates the resolution of disputes related to software, platforms, and systems within the TDM system. This interface provides functionality for submitting evidence and resolution applications when conflicts arise. It allows supervisory entities to retrieve contracts, records, and usage reports upon official requests from judicial institutions, supporting the resolution process with the necessary documentation, as follows:

- a) The system shall provide a mechanism for submitting evidence and applying for resolution when disputes occur. This functionality shall be accessible to participants and relevant authorities.
- b) Upon the submission of a resolution request to a judicial institution, the system shall allow supervisory parties to retrieve relevant contracts, records, and data usage reports. These records shall support the resolution process by providing comprehensive documentation of system activities and contract compliance.

5.7.3 Optional requirements

Blockchain technology and other relevant technologies are recommended for secure record keeping and enhancing the integrity of system processes. These technologies can be applied to auditing, tool certification, regulatory oversight, and dispute resolution processes to help ensure that all records are securely preserved, tamper resistant, and fully traceable. While they are not mandatory, the implementation of the following technologies provides an additional layer of security and transparency:

- a) The system may utilize blockchain technology or similar secure technologies to preserve records related to auditing processes. This helps ensure that audit logs are immutable and can be reliably verified for integrity and authenticity.
- b) Blockchain technology or CA certification may be used for tool certification processes. These technologies help ensure that certification records are securely stored and can be easily audited, maintaining the integrity of the certification process.
- c) The regulatory interface may implement blockchain technology to securely store and track records related to metering, billing, settlement, and compliance activities. This provides a verifiable audit trail that supports regulatory oversight and investigation processes.
- d) The interface for dispute resolution may employ blockchain technology or other secure technologies to preserve records related to disputes, ensuring that evidence, contracts, and related records are securely stored and readily retrievable in accordance with the applicable resolution procedures.

6. Interoperability requirements

This clause details the interoperability requirements for the modules within the TDM system, focusing on how each module interacts with others to help ensure cohesive and efficient operations across the system. These requirements specify the necessary interfaces, data exchanges, and communication protocols that must be supported to enable seamless integration between modules. The clause is structured to cover mandatory, recommended, and optional interoperability requirements, ensuring that data flows smoothly and securely throughout the system. This approach guarantees that all modules can work together harmoniously, supporting the TDM system's goals of trusted, secure, and transparent data management.

6.1 Intermodule functional requirements of identification and authentication module

The intermodule functionality requirements outline how the identification and authentication module interacts with other modules within the TDM system. These interactions are critical to ensuring that identity and access management processes are seamlessly integrated across the entire system. The effective operation of the identification and authentication module depends not only on its internal functions but also on its ability to communicate and collaborate with other modules, such as data asset management, trusted environment, and compliance functions. This subclause details the required, recommended, and optional interfaces and functionalities that facilitate secure and efficient intermodule operations, ensuring that authentication and identity verification processes are consistent and reliable throughout the system.

6.1.1 Mandatory requirements

The following requirements specify the essential intermodule functionalities that the identification and authentication module must support to help ensure the secure and reliable operation of the TDM system. Each mandatory requirement is accompanied by a description of the corresponding interface and its role in system-wide operations:

- a) Interface between identification and authentication module and data asset control module

- 1) The identification and authentication module shall establish a secure interface with the data asset control module to authenticate user identities before granting access to data assets. This interface helps ensure that only authenticated users with the appropriate permissions can access sensitive data, maintaining the integrity and security of the data management process.
- 2) Scenario 1: When a user requests access to a data asset (Requester A), the identification and authentication module authenticates the user and transmits the user's credentials to the data asset control module, which then processes the access request and provides feedback on whether access is granted or denied.
- b) Interface between identification and authentication module and trusted environment module
 - 1) The identification and authentication module shall support secure communication with the trusted environment management module to verify the identity of users and processes within a trusted execution environment (TEE). This interface helps ensure that only authorized users can initiate and manage operations within a TEE, safeguarding sensitive computations and data.
 - 2) Scenario 2: When a secure data processing task is initiated, the trusted environment module requests user identity verification from the identification and authentication module. After verification, the trusted environment module proceeds with the secure operation.
- c) Interface between identification and authentication module and supply-and-demand docking module
 - 1) The identification and authentication module shall authenticate users involved in activities within the supply-and-demand docking module, particularly for contract management and accessing the data catalog. This helps ensure that only authorized users can engage in these activities, securing sensitive transactions and data exchanges.
 - 2) Scenario 3: During the creation or execution of a contract within the supply-and-demand docking module, the module interfaces with the identification and authentication module to verify the legitimacy of the user initiating or approving the contract.
- d) Interface between identification and authentication module and data tool service module:
 - 1) The identification and authentication module shall verify the identity of users accessing the data tool service module, ensuring that only authorized users can download, install, or interact with data tools provided within the system.
 - 2) Scenario 4: When a user attempts to access or use tools from the data tool service module, the module interfaces with the identification and authentication module to authenticate the user before granting access.
- e) Interface between identification and authentication module and compliance function module
 - 1) The identification and authentication module shall provide an interface for logging authentication events and access decisions to the compliance function module. This helps ensure that all actions related to user authentication and access control are recorded for audit purposes, supporting the system's overall compliance with data governance and regulatory requirements.

6.1.2 Recommended requirements

The following recommended requirements suggest additional intermodule functionalities that enhance the overall security and efficiency of the system. While they are not mandatory, these features are strongly encouraged to provide a more robust and resilient system:

- a) Enhanced interface for real-time monitoring
 - 1) The identification and authentication module should include an interface for real-time monitoring by the compliance function. This interface would allow continuous oversight of authentication processes, immediately flagging any anomalies or security breaches.

- 2) Scenario 5: The real-time monitoring interface enables the compliance function to receive immediate updates on failed login attempts, suspicious access patterns, or unusual authentication behaviors, facilitating prompt investigation and response.
- b) Integration with external identity providers
 - 1) The system should support integration with external identity providers (IdPs) for federated authentication, enabling SSO capabilities across different systems and applications. This enhances user convenience while maintaining a high level of security.
 - 2) Scenario 6: When a user attempts to access the system, the identification and authentication module interfaces with an external IdP to validate the user's credentials, after which access is granted based on the received authentication tokens.

6.1.3 Optional requirements

The following optional requirements provide additional functionality that may be included to enhance specific use cases or operational environments. These features are not essential but can offer added benefits depending on the system's needs:

- a) Continuous authentication across modules
 - 1) The identification and authentication module may support continuous authentication mechanisms that work across multiple modules to help ensure that user identities are verified throughout their session. This could involve reauthenticating users at key points during their interaction with different modules.
 - 2) Scenario 7: For high-security operations, such as initiating a financial transaction within the data tool service module, the system may require the user to reauthenticate through the identification and authentication module, adding an extra layer of security.
- b) Dynamic role adjustment interface
 - 1) The module may support a dynamic role adjustment interface that allows other modules, such as the data asset management or compliance function modules, to request and apply real-time changes to a user's role or permissions based on evolving operational contexts.
 - 2) Scenario 8: If a user's role is dynamically adjusted due to a compliance requirement, the compliance function module can interface with the identification and authentication module to immediately update the user's access rights across all relevant modules.

6.2 Intermodule functional requirements of data asset management module

The intermodule functional requirements for data asset management outline the necessary interactions and dependencies between the data asset management module and other modules within the TDM system. These requirements help ensure that data assets are properly generated, identified, maintained, and shared across different modules. The intermodule functionality facilitates seamless communication, integration, and data exchange, supporting the efficient and secure management of data throughout the system. This subclause defines the mandatory, recommended, and optional intermodule functionalities that help ensure the proper handling of data assets, enabling secure collaboration between the data asset management module and other relevant system components.

6.2.1 Mandatory requirements

The following mandatory intermodule requirements for data asset management define the essential interactions between the data asset management module and other modules. These interactions facilitate data asset generation, access, validation, and control, while maintaining security and auditability across the system.

These requirements are critical to ensuring the integrity, availability, and security of data assets as they are exchanged or managed across modules. They provide the foundation for secure data generation, classification, and maintenance within the broader TDM system. The following scenarios outline the essential steps involved in these intermodule interactions:

- a) Interface between data asset management module and identification and authentication module
 - 1) The data asset management module shall establish a secure interface with the identification and authentication module to validate user identities before allowing access to or modification of data assets. This interface helps ensure that only authenticated users with proper permissions can interact with sensitive data, maintaining the security and integrity of data assets.
 - 2) Scenario 1: When a user requests to generate a data asset, the data asset management module sends a request to the identification and authentication module for identity validation. Upon successful validation, the identification and authentication module sends an access token back to the data asset management module, allowing the data generation process to proceed.
- b) Interface between data asset management module and access control module
 - 1) The data asset management module shall establish an interface with the access control module to enforce data access policies and control mechanisms. This interface helps ensure that access to data assets is governed by predefined control policies and that unauthorized access is reduced.
 - 2) Scenario 2: When a request to access a data asset is received, the data asset management module queries the access control module to retrieve the applicable control policy. The access control module sends the policy to the data asset management module, which applies the policy before allowing the data asset to be accessed.
- c) Interface between data asset management module and supply-and-demand docking module
 - 1) The data asset management module shall support an interface with the supply-and-demand docking module (specifically the data catalog management) to provide relevant data asset metadata and descriptions. This interface allows the supply-and-demand docking module to list and manage available data assets in the system.
 - 2) Scenario 3: The supply-and-demand docking module sends a request to the data asset management module for information about a specific data asset. The data asset management module retrieves the asset's metadata and transmits it to the supply-and-demand docking module for cataloging and further actions.
- d) Interface between data asset management module and log recording service module
 - 1) The data asset management module shall maintain an interface with the log recording service module to record all key operations, such as data asset generation, access, modification, and deletion. This helps ensure a full audit trail of interactions with data assets, supporting compliance with governance and security policies.
 - 2) Scenario 4: When a user generates or accesses a data asset, the data asset management module logs the event by sending relevant details (e.g., user ID, data asset ID, timestamp) to the log recording service module. The log recording service module records the operation and confirms successful records to the data asset management module.
- e) Interface between data asset management module and compliance function module
 - 1) The data asset management module shall provide an interface for logging and reporting activities to the compliance function module, ensuring that data asset interactions are fully compliant with regulatory and internal governance standards. This interface enables continuous oversight of data usage, access control, and policy enforcement.

- 2) Scenario 5: When data access or generation events are recorded, the compliance function module can retrieve records and audit reports from the data asset management module, ensuring that all activities align with established data governance policies.

6.2.2 Recommended requirements

The following recommended intermodule requirements for data asset management provide additional capabilities that enhance the functionality and efficiency of data exchanges between modules. While they are not strictly required, these features offer significant value by improving data classification, tracking, and operational efficiency. The implementation of these recommended functionalities can strengthen collaboration between modules and support more complex data asset management scenarios, ensuring compliance with best practices and enhancing system performance:

- a) Enhanced interface for real-time data monitoring
 - 1) The data asset management module should include an enhanced interface for real-time data monitoring by the compliance function module. This interface allows continuous oversight of data asset activities, including real-time tracking of data creation, access, and modification. It helps detect anomalies, potential security breaches, and helps ensure compliance with data governance policies.
 - 2) Scenario 1: The compliance function module monitors real-time data access events occurring within the data asset management module. The enhanced interface continuously streams data usage records and alerts to the compliance function module, enabling immediate investigation of suspicious activities.
- b) Interface for integration with external data management systems
 - 1) The data asset management module should support an interface for integration with external data management systems or third-party data platforms. This interface enables the secure sharing and exchange of data assets across different systems while maintaining control over data access and compliance.
 - 2) Scenario 2: A request to access data from an external platform is made to the data asset management module. The module interfaces with the external system, ensuring that data are securely transferred and access policies are enforced. Data exchanges between the systems are recorded and monitored to help ensure compliance with relevant regulations.
- c) Interface for advanced data classification and tagging
 - 1) The data asset management module should implement an interface that supports advanced data classification and tagging capabilities. This interface enables the module to dynamically classify data assets based on their content, usage, or security level, improving the organization and retrieval of data across the system.
 - 2) Scenario 3: When a data asset is generated or updated, the advanced classification interface automatically tags the asset with metadata based on predefined criteria (e.g., sensitivity level, usage category). This allows other modules, such as the supply-and-demand docking module, to easily search and filter data assets based on these classifications.
- d) Automated policy enforcement interface
 - 1) The data asset management module should support an automated policy enforcement interface with the access control module. This interface allows for real-time enforcement of data usage and access policies without manual intervention, ensuring that all data access requests are automatically checked and handled according to established control policies.
 - 2) Scenario 4: When a request is made to access a data asset, the automated policy enforcement interface helps ensure that the access control module dynamically enforces applicable policies

(e.g., access restrictions based on user roles or location). This process is automated, minimizing delays and potential human error.

6.2.3 Optional requirements

The following optional intermodule requirements for data asset management provide advanced functionalities that offer additional flexibility and adaptability to the system. These features, though not necessary for basic operation, may be implemented to improve data handling, streamline complex data management processes, or introduce cutting-edge technologies. Organizations may choose to implement these optional requirements based on their specific operational needs or long-term goals, tailoring the data asset management module to their unique requirements:

- a) Interface for blockchain-enabled data asset tracking
 - 1) The data asset management module may implement an interface for blockchain-based tracking of data assets. This interface enhances the integrity and security of data assets by providing an immutable audit trail, ensuring that all data asset transactions are securely recorded and verifiable.
 - 2) Scenario 1: When a data asset is created or modified, the blockchain-enabled interface records the transaction on a blockchain, creating a tamper proof record of the event. Any subsequent access or modification to the data asset is similarly recorded, allowing for complete traceability and auditability of the data asset's life cycle.
- b) Interface for AI-assisted data asset optimization
 - 1) The data asset management module may support an interface for AI-assisted data asset optimization, which helps improve data asset quality, reduce redundancy, and optimize storage. This interface allows for automated analysis of data assets and provides recommendations for data cleaning, consolidation, or reorganization based on artificial intelligence (AI)-driven insights.
 - 2) Scenario 2: The AI-assisted interface analyzes existing data assets within the module and identifies redundant or outdated assets. It then provides suggestions for optimizing storage by consolidating similar assets or removing unnecessary duplicates. The system can implement these recommendations automatically or with administrative approval.
- c) Interface for multicloud data integration
 - 1) The data asset management module may integrate with multicloud environments through a dedicated interface, allowing data assets to be shared, accessed, and managed across different cloud platforms. This interface helps ensure secure, seamless interactions with cloud service providers while maintaining data integrity and compliance with cloud governance policies.
 - 2) Scenario 3: The data asset management module interfaces with multiple cloud environments, enabling users to store, retrieve, and manage data assets across various cloud service providers. The interface helps ensure secure transmission and enforces access controls based on preconfigured policies for each cloud provider.
- d) Interface for advanced data life-cycle management
 - 1) The data asset management module may include an interface for advanced data life-cycle management, allowing for automated control over the complete life cycle of data assets, from creation to archival and deletion. This interface enables administrators to set rules for the retention, archiving, and destruction of data assets based on business requirements or regulatory guidelines.
 - 2) Scenario 4: Upon the creation of a data asset, the advanced life-cycle management interface assigns life-cycle rules, specifying retention periods, archival timelines, and destruction

protocols. The interface monitors the asset's life cycle and triggers archival or deletion actions when conditions are met.

- e) Interface for automated reporting
 - 1) The data asset management module may support an interface for generating operational reports by aggregating data from multiple sources, including records, access records, and other operational data. This interface allows users to request reports summarizing system activity and performance, with reports generated in real time or on demand.
 - 2) Scenario 5: The Requester triggers the generation of a report by the data asset management module. The data asset management module sends a request to the log recording service module to retrieve operational records. The log recording service module provides the requested records, and the data asset management module compiles the operational report and delivers it to the Requester.

6.3 Intermodule functional requirements of supply-and-demand docking module

The intermodule functional requirements for the supply-and-demand docking module define the necessary interactions between this module and other components of the TDM system. These interactions facilitate the management of data catalogs, contracts, metering, billing, and settlement processes across different system modules. The effective communication and integration between the supply-and-demand docking module and other modules are essential for ensuring that the system operates efficiently, securely, and in compliance with contractual and regulatory obligations. This subclause details the mandatory, recommended, and optional functionalities required to establish and maintain intermodule interactions for the supply-and-demand docking module.

6.3.1 Mandatory requirements

The following requirements specify the essential intermodule functionalities that the supply-and-demand docking module must support to help ensure secure, efficient, and reliable operations within the TDM system. The supply-and-demand docking module plays a central role in managing the data catalog, contracts, metering, billing, and clearing processes. Each mandatory requirement details the necessary interactions between the supply-and-demand docking module and other key modules, ensuring seamless integration for the core functions of data resource management and financial transactions:

- a) Interface between supply-and-demand docking module and data asset management module
 - 1) The supply-and-demand docking module shall establish an interface with the data asset management module to retrieve and display relevant data asset metadata in the data catalog. This helps ensure that data resources are properly classified, organized, and available for users within the TDM system.
 - 2) Scenario 1: The supply-and-demand docking module sends a request to the data asset management module for metadata related to a specific data asset. The data asset management module responds with the requested metadata (e.g., identifier, description, and classification), which is used to update the data catalog.
- b) Interface between supply-and-demand docking module and identification and authentication module
 - 1) The supply-and-demand docking module shall interface with the identification and authentication module to verify user identities before they access the data catalog, create or modify contracts, or perform other sensitive operations. This helps ensure that only authorized users can engage in these activities.

- 2) Scenario 2: When a user attempts to create or modify a contract, the supply-and-demand docking module requests user authentication from the identification and authentication module. Upon successful verification, the user is granted access to perform contract-related actions.
- c) Interface between supply-and-demand docking module and compliance function module
 - 1) The supply-and-demand docking module shall interface with the compliance function module to help ensure that all key contract-related events (e.g., contract creation, modification, data access) are recorded in the system's records for auditing and governance purposes. This helps ensure compliance with regulatory standards and provides traceability for all contract-related actions.
 - 2) Scenario 3: When a contract is created, modified, or executed, the supply-and-demand docking module logs the event by sending the relevant details (e.g., user ID, contract metadata, timestamps) to the compliance function module for record keeping.
- d) Interface between supply-and-demand docking module and trusted environment module
 - 1) The supply-and-demand docking module shall establish an interface with the trusted environment module to verify and secure the execution of contracts and data access processes. This interface helps ensure that all operations related to contract execution and data access take place within a secure, trusted environment.
 - 2) Scenario 4: When a contract is executed, the supply-and-demand docking module requests the trusted environment module to verify the environment's integrity before processing data. The trusted environment module helps ensure that the system is operating in a secure state before allowing the contract to proceed.
- e) Interface between supply-and-demand docking module and metering and clearing functions
 - 1) The supply-and-demand docking module shall interface with the metering and clearing functions to handle the measurement of data usage and the subsequent settlement of financial transactions. This interface helps ensure that metering and clearing are carried out in accordance with the terms of the contract.
 - 2) Scenario 5: After data are accessed or a service is delivered under a contract, the supply-and-demand docking module sends usage data to the metering function to calculate data consumption. The clearing process then helps ensure that financial settlements are executed based on the metered data.

6.3.2 Recommended requirements

The following recommended intermodule functionalities enhance the efficiency, security, and flexibility of the supply-and-demand docking module. Although not mandatory, these features provide significant value by improving operational processes, strengthening system integration, and ensuring better oversight and optimization of data and service exchanges. Implementing these features will enable the TDM system to handle more complex scenarios while maintaining a high level of security and reliability:

- a) Interface for enhanced data and service evaluation
 - 1) The supply-and-demand docking module should implement an enhanced interface with the data asset management and trusted environment modules to perform detailed evaluations of data quality, service performance, and security before any contractual agreement. This helps ensure that the system has a thorough assessment of the assets and services being exchanged.
 - 2) Scenario 1: Before a contract is finalized, the supply-and-demand docking module requests data evaluation from the data asset management module and service performance evaluation from the trusted environment module. These evaluations, including data quality, reliability, and security assessments, are then provided to the supply-and-demand docking module for final decision-making.