

Service Description Screening Software for Financial Sanction Audits

Procurement of a Standard IT Solution in the Area of Name Screening

Last updated: 07/01/2026

Table of contents

	Page
Table of contents	2
List of abbreviations	5
0 Notes on the tender specifications	6
1 Context and objective	7
1.1 Particularities	7
1.2 System context	8
1.2.1 Description of the Deutsche Bundesbank's IT system landscape	8
1.2.1.1 Description of the container environment (OpenShift)	8
1.2.1.2 Logging and monitoring	9
1.2.1.3 Application communication	9
1.2.1.4 Orchestration/Automation	10
1.2.1.5 Development environment for OpenShift	10
1.2.1.6 Data storage	10
1.2.1.7 Identity Access Management	11
1.2.1.8 Maintenance and system updates	11
1.2.1.9 Staging	12
2 Exclusion criteria	13
2.1 Technical (functional) requirements for the screening engine	13
2.1.1 Detection of sanctioned entities (screening)	13
2.1.2 Name screening	13
2.1.3 Processing of structured and semi-structured data	13
2.1.4 Batch processing	13
2.1.5 Processing of encodings and non-Latin alphabets	13
2.1.6 Scoring/evaluation of results	13
2.1.7 Processing of short names	14
2.1.8 Processing records of at least 200 characters	14
2.1.9 Detection despite a combination of deviations	14
2.1.10 Configurability of name screening/tuning	14
2.1.11 Configurability of the included data sources	14
2.1.12 Parallel (simultaneous) and separate evaluation of datasets	14
2.1.13 Process documentation/reporting/audit trail	14
2.1.14 Interfaces	15
2.1.15 Import relevant data formats	15
2.1.16 Sequence of name elements: Hits despite changes	15
2.2 Technical requirements	15
2.2.1 Integration into the Deutsche Bundesbank's IT system landscape	15
2.2.1.1 Integration into the Deutsche Bundesbank's IT system landscape	15
2.2.2 Implementation of the software	16
2.2.2.1 Installation and basic configuration (establishment of operational readiness)	16
2.2.3 IT security	16
2.2.3.1 Selection of suitable cryptographic procedures (CON.1.A1)	16
2.2.3.2 Use of TLS/SSL proxies (DER.1.A10)	16

2.2.3.3	Continuous monitoring and evaluation of logging data (DER.1.A6).....	16
2.2.3.4	Basic assurance of communication with other networks (NET.1.1.A9).....	17
2.2.3.5	Securing incoming communication from the Internet to the internal network (NET.1.1.A11)	17
2.2.3.6	Information on IT vulnerabilities (OPS.1.1.1.A20).....	17
2.2.3.7	Traceability of administrative activities (OPS.1.1.2.A5)	17
2.2.3.8	Protection of administrative activities (OPS.1.1.2.A6).....	17
2.2.3.9	Use of system-specific protection mechanisms (OPS.1.1.4.A2).....	18
2.2.3.10	Separation of the test environment from the production environment (OPS.1.1.6.A13)	18
2.2.3.11	Conduct penetration tests (OPS.1.1.6.A14).....	18
2.2.3.12	Certification according to security standards	18
2.2.4	Data protection	18
2.2.4.1	Compliance with legal framework conditions (OPS.1.1.5.A5 and CON.2.A1).....	18
2.2.4.2	Requirements from the AI Act.....	19
2.2.5	User accounts / access rights / role concept	19
2.2.5.1	Segregation of duties between incompatible tasks (ORP.1.A4).....	19
2.2.5.2	Setting up, changing and revoking authorisations (ORP.4.A2)	19
2.3	General Requirements	19
2.3.1	Operating language.....	19
2.3.2	Software training	20
2.3.3	Software documentation	20
2.3.4	Maintainability	20
2.3.5	Test data screening.....	20
2.3.6	Test setting/test installation.....	20
3	Desirable criteria.....	21
3.1	Technical (functional) requirements for the screening engine	21
3.1.1	Detection of additional entities	21
3.1.2	Detection of entities, if spelling is different (fuzzy logic)	21
3.1.3	High sensitivity	21
3.1.4	High specificity	21
3.1.5	Processing of payment messages	21
3.1.6	Processing unstructured data	21
3.1.7	Natural language processing (NLP): Inclusion of further information	21
3.1.8	Dates of birth.....	22
3.1.9	Inclusion of further information from sanctions lists.....	22
3.1.10	Parametrisation/configurability of additional context data.....	22
3.1.11	Independent name screening	22
3.1.12	Processing of non-Latin alphabets.....	22
3.1.13	Transparency	22
3.1.14	Explanation of scores.....	22
3.1.15	Processing of unlimited character sets per record.....	23
3.1.16	Selection of data fields to be screened	23
3.1.17	Various configurations for screening individual data fields	23
3.1.18	Discovery even without external mapping to the entity type.....	23
3.1.19	Common names.....	23
3.1.20	Recognition of different languages and differentiated processing	23
3.1.21	Notification of missing, erroneous, inconsistent, unexpected data	23
3.2	Detailed requirements for the screening engine	23
3.2.1	Upper and lower case	23

3.2.2	German Umlauts and special characters	24
3.2.3	Additions and doubling of characters	24
3.2.4	Character omission	24
3.2.5	Phonetic similarities/transcription variants	24
3.2.6	Processing individual characters of other alphabets	24
3.2.7	Direct processing of non-Latin characters	24
3.2.8	Transcription of non-Latin characters	25
3.2.9	Processing of non-Latin defective spelling.....	25
3.2.10	Consideration of language-specific special features of names.....	25
3.2.11	Male vs. female names	25
3.2.12	Consideration of particularly frequent errors	25
3.2.13	Omission of name elements.....	25
3.2.14	Abbreviation of name elements	26
3.2.15	Supplements of name components and additions	26
3.2.16	Names of different persons in a cell.....	26
3.2.17	Delimiters: Additional or missing	26
3.2.18	Very long names	26
3.2.19	Very short names	26
3.2.20	Typical variations	27
3.2.21	Legal forms identification and processing	27
3.2.22	Economic sector and geographical names are included in the screening	27
3.2.23	Recognition of interchangeable designations	28
3.2.24	Recognition of names despite a combination of errors at the character and/or name component level	28
3.3	Technical requirements	28
3.3.1	Implementation of the software	28
3.3.1.1	Integration into a shared cluster.....	28
3.3.1.2	Configuration and fine-tuning	28
3.3.2	Performance and scalability	28
3.3.2.1	Processing large amounts of data	29
3.3.2.2	Scalability.....	29
3.3.2.3	Performance monitoring.....	29
3.3.2.4	Resumption of screening after discontinuation	29
3.3.2.5	Notification of errors and problems	29
3.3.3	IT security.....	29
3.3.3.1	Information on IT vulnerabilities (OPS.1.1.1.A20).....	29
3.3.3.2	System and network level logging configuration (OPS.1.1.5.A3).....	30
3.3.4	Data protection	30
3.3.4.1	Restrictive use of logging data	30
3.4	General Requirements	30
3.4.1	Release and change documentation	30
3.4.2	Ease of use	30
3.4.3	Accessibility	30
3.4.4	Portability.....	30
3.4.5	Equal opportunities compliant	30

List of abbreviations

Abbreviation	Meaning
A criterion	Exclusion criterion
API	Application programming interface
BDSG	Federal Data Protection Act
BGG	Act on Equal Opportunities for Disabled Persons
BGleG	Federal Equal Opportunities Act
BIC	Business Identifier Code
BITV 2.0	Accessible Information Technology Regulation 2.0
B criterion	Assessment criterion
BSI	Federal Office for Information Security
CLI	Command line interface
GDPR	General Data Protection Regulation
EU	European Union
ISIN	International securities identification number
IWA	Integrated Windows Authentication
LAD	Solution architecture document
OCR	Optical Character Recognition
REST	Representational State Transfer
SAML	Security assertion markup language
SEPA	Single euro payments area
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TLS	Transport Layer Security

0 Notes on the tender specifications

All requirements to be met by the application or the contractor are documented within the tender description and the assessment matrix, which consists of several thematic worksheets. In the assessment matrix, all required criteria are shown separately according to exclusion (A criteria) and assessment criteria (B criteria).

- A criteria are MANDATORY requirements: Describe a mandatory/minimum requirement that must be met. Failure to meet any A criterion leads to exclusion.
- B criteria – DESIRABLE requirements: Denote requirements that are to be met as far as possible. Provided that these are not or only partially fulfilled, this must be indicated in the tender. The Contractor shall be free to present alternative solutions to these requirements that can meet the objective pursued in the aforementioned requirement. These criteria are evaluated with points.

The weighting of the individual requirements is denoted in the assessment matrix. The content of the evaluation matrix and the calculations specified in the award criteria are decisive for awarding the contract.

During the assessment process it is to be expected that additional minimum requirements/A criteria are added. It is also possible for existing requirements to be defined more narrowly or upgraded to exclusion criteria. Those criteria which are likely to be subject to this process, are identified in the annex "C4_L1_Annex 2_Valuation matrix 25-2000064042_Lot 1".

1 Context and objective

Pursuant to § 23 para. 1 and 2 of the Foreign Trade and Payments Act (Außenwirtschaftsgesetz), the Deutsche Bundesbank may request information and carry out inspections on the part of obligated parties to monitor compliance with financial sanctions and external reporting requirements. Part of the inspections is a software-based screening of the customer, transaction and trade financing information of the audited enterprise with lists of entities (in particular natural persons and legal entities, organisations and institutions as well as ships, ports, locks and aircraft) that are subject to German and EU law (also taking into account decisions of the UN Security Council pursuant to § 5a AWG). are subject to sanctions (sanctions lists).

To support inspection activities, it is envisaged to procure a new screening software core, which is to be integrated into a Bundesbank-owned audit platform.

We are looking for a screening engine that is available on the market that finds names and name similarities in structured and semi-structured data and also supports full-text searches in unstructured data of the companies under review. Other characteristics such as dates of birth, gender, etc. should be taken into account in this context, if necessary. Additional functionalities to the screening engine, such as a case management system, are not part of this call for tenders. Additional optional services can be tools for list management, data standardisation or data interfaces, for example.

Unlike commercial banks, the software is intended to screen against reporting date/historical sanctions lists; however, the validity of sanctions at certain points in time is taken into account in a separate application. Customer data are not delivered regularly, but the input data, configuration and sanctions lists used change depending on the company being audited. The sanction lists are processed into a standardised format or list management is carried out in a separate application.

No order production, external development or consulting is requested.

1.1 Particularities

By continuously changing audited companies, new and different data are screened with each batch run which entails particular challenges. The screening engine should therefore be configurable and parametrisable as flexibly as possible to be able to use different methods (e.g. degree of consistency or matching algorithms) for each screening. Furthermore, this means that the data volumes to be screened varies from year to year. The specific data volumes shall only be disclosed after the tender contest, once a corresponding confidentiality agreement has been signed by the Contractor. It shall be noted that, unlike the procedure for commercial banks, customer data are only screened once per investigation.

1.2 System context

As mentioned in the introduction, the screening engine to be procured is to become part of an audit platform. A separate application in the audit platform receives data from audited entities, prepares it into a standardised format, and then transmits it to the screening software via an application programming interface (API) along with the sanction lists, so that the data is then screened by batch run. The hits and associated metadata from the screening are then to be sent back to the platform so that they can be processed further. For our use case, the results should be in list form in a machine-readable format. The audit platform described is currently still under development. The screening engine should be able to be operated in the Deutsche Bundesbank's private cloud.

1.2.1 Description of the Deutsche Bundesbank's IT system landscape

The following section describes the Deutsche Bundesbank's IT system landscape. The software must be able to be integrated into the described infrastructure either on a standard server or in the OpenShift environment. It is preferable to integrate with the OpenShift environment. The tender must contain a description of the contractor's system landscape, in particular explaining where there could be problems with implementation (ID 5.2).

As part of the tender procedure, a technical test must be carried out before the contract is signed, in which integration into the Deutsche Bundesbank's IT system landscape is checked (see Section 2.3.6). In particular, it is checked whether the system context described in this chapter and the application are compatible.

1.2.1.1 Description of the container environment (OpenShift)

The container platform operated by the Bundesbank is based on the established cloud standard Kubernetes. Specifically, the Kubernetes distribution Red Hat OpenShift is used, which extends Kubernetes to include additional business functions and simplifies common integrations with other tools in the IT landscape.

The container platform enables OpenShift to develop, manage and operate applications in isolated and portable units in the form of containers. The containers can be operated within the Red Hat OpenShift cluster in a multi-tenant shared cluster with appropriately configured namespaces and operators.

- **Service Mesh:** The Service Mesh (integrated proxy, load balancer, firewall) for the uniform and fully integrated management of communication between applications is implemented on the basis of the implementation provided by OpenShift (Istio). If Service Mesh is not supported, the encryption of intra-cluster communication must be ensured differently. Currently, Service Mesh version 3 is used.

- **Storage:** Dynamic provisioning and management of NFS and block that can be used by the containers for persistent data storage.
- **Container Runtime Security:** The Red Hat Advanced Cluster Security (RHACS) RASP tool is used as a security solution for Kubernetes for risk detection and compliance monitoring.
- **Worker nodes:** A worker node has 40 CPU cores and 512 GiB of RAM by default, which is why a single pod must not require more than 36 CPU cores and/or 500 GiB of RAM.
- **Namespaces:** In OpenShift cluster namespaces, the maximum available resources (CPU and RAM) are controlled by performance constraints. There are standard sizes (from 2 CPU and 8 GiB RAM to 16 CPU and 64 GiB RAM), but individual sizes can also be defined.
- **Backup and restore:** The application data is stored in persistent volumes in the Red Hat OpenShift cluster using the VCF vSAN; for long-term backups, see Section 1.2.1.6 on data storage.

1.2.1.2 Logging and monitoring

The container platform is connected to the Deutsche Bundesbank's central logging platform and automatically transfers the application logs there. The product Elastic Cloud Enterprise (ECE) is used. In the OpenShift clusters of the container platform, the application logs and other system information are collected using Elastic Agents and forwarded to Elasticsearch. To do this, the application logs must be written to the standard data streams *StdOut* and *StdErr*. If the application is running on a standard server, log files must be written.

For central enterprise monitoring, the product Dyntrace is used. The OpenShift clusters of the container platform are integrated into the Dynatrace platform using Kubernetes API and Prometheus.

The standard servers are connected via the Dynatrace Agent.

1.2.1.3 Application communication

It is possible to communicate with third-party applications via an interface (e.g. REST API or CLI) and initiate batch runs from there.

1.2.1.4 **Orchestration/Automation**

The OpenText Operations Orchestration product is used to deploy and manage systems (OpenShift Clusters and Namespaces), storage (S3 Buckets, NFS), databases (Oracle, Microsoft SQL Server), and other components.

1.2.1.5 **Development environment for OpenShift**

In the OpenShift environment, the following basic services are available:

- **CodeArtefakt:** Provides a Binary Repository Manager using the JFrog Artifactory product
- **CodeDeploy:** Provides a continuous deployment service that can be used to deliver applications to the container platform. The OpenShift GitOps or ArgoCD product is used for deployment.

1.2.1.6 **Data storage**

Database Management Systems (DBMS):

The DBMS are operated on virtual Windows servers (Microsoft SQL Server) and thus provided outside the container platform.

Storage:

For temporary data ephemeral local storage in the Red Hat OpenShift Pod is used. For persistent data persistent volumes in the Red Hat OpenShift Cluster using VCF vSAN (File RWO/RWX, Block RWO) is used.

Storage File Services:

The Storage File Service includes file services for applications and server systems, and the provision of persistent volumes for container environments:

- For standard Windows-based servers, storage areas are provided via the CIFS protocol.
- For standard RHEL-based servers, storage areas that are used for data storage are released via NFS. Since the storage system manages the storage area, the data areas can be used by several servers if necessary.

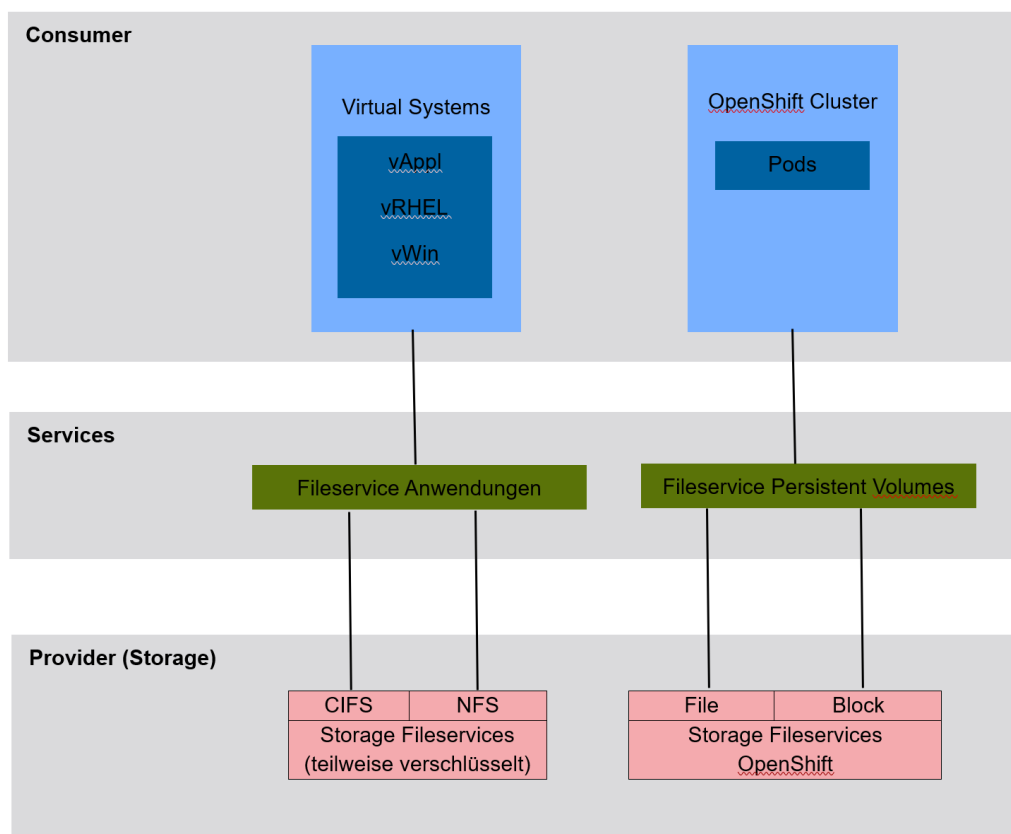


Figure 1: Overview of file services

1.2.1.7 Identity Access Management

User and authorisation management at the Deutsche Bundesbank is currently carried out in the Active Directory (AD). The software must be able to access the users and their groups defined in the AD so that they can be used for authorisation (assignment of rights and roles). The technical connection to the AD is via LDAP.

There are currently two options for authenticating users:

- (1) Authentication via AD using Integrated Windows Authentication (IWA) using Kerberos
- (2) Active Directory Federation Services (AD FS) authentication using SAML

1.2.1.8 Maintenance and system updates

The Deutsche Bundesbank's Private Cloud systems are updated regularly.

Red Hat OpenShift uses at least the penultimate Red Hat-supported EUS/LTS version. This is currently version 4.18.

1.2.1.9 Staging

The software must be deployable in three different stages (For more details, see Separation of the test environment from the production environment in Section 2.2.3).

For information purposes only - legally not binding

2 Exclusion criteria

2.1 Technical (functional) requirements for the screening engine

2.1.1 Detection of sanctioned entities (screening)

The software must match entities (in particular natural persons and legal entities, organisations and institutions) in provided sanctions lists against names in the data of the entities under investigation using various characteristics (see 2.1.2), identify matches and similarities, assign them into pairs and provide them as output (screening). The probability of identity or degree of similarity must be¹ specified as a score. Both the customer/transaction ID and the sanction IDs from the sanction lists must also be provided as output. The audit shall include both natural persons as well as legal and other entities. The aim is to achieve the best possible sensitivity, while at the same time achieving a high degree of specificity (see 3.1.3 and 3.1.4).

2.1.2 Name screening

The software must be able to screen entities by name. (Additional name screening requirements are described in Section 3.2 (B criteria).)

2.1.3 Processing of structured and semi-structured data

The software must use one or more screening algorithms that support the matching of names or terms in structured and semi-structured data.

2.1.4 Batch processing

The software must be able to perform batch screening (further batch processing requirements are described in Section 3.3.2 (B-Criteria).)

2.1.5 Processing of encodings and non-Latin alphabets

The software must be able to process at least UTF-8 and ANSI encodings.

2.1.6 Scoring/evaluation of results

The software must determine the results and partial results of the screening and display them as a meaningful and sufficiently differentiated score. The score must indicate the hit quality of the name with the sanction list entry. The scores for checking the other components (e.g. date of birth, country details) must be issued separately. The hits of a name against multiple sanctions list entries must be output separately.

¹ See also 2.1.6

2.1.7 Processing of short names

The software must also be able to take short names (ideally starting from one character) from the EU sanctions lists into account when screening.

2.1.8 Processing records of at least 200 characters

The software must be able to process names of at least 200 characters.

2.1.9 Detection despite a combination of deviations

The software must be able to match sanctioned entities even if their names are changed by deviations, also including different types.

2.1.10 Configurability of name screening/tuning

The software must allow users to flexibly configure, remove, and add rules, parameters, and other name screening settings.

The software must allow users to configure screening runs in such a way that the user can define and change the trade-off between sensitivity and specificity.

2.1.11 Configurability of the included data sources

The software must enable different screenings to be carried out with different sanctions lists.

2.1.12 Parallel (simultaneous) and separate evaluation of datasets

The software must enable the screening of different datasets in parallel (simultaneously) and separately from each other, even with different configurations and sanctions lists. The data of different audited entities must be processed and issued in a strictly separate manner. The status (overview/progress) of various parallel screenings must be visible.

2.1.13 Process documentation/reporting/audit trail

The screening process as well as possible errors and problems must be documented in a comprehensible and informative manner to provide actionable information on the causes of problems and to be able to assess their consequences. These include:

- All changes to system settings
- The batch history (times, data volumes, actions such as importing input data, etc.);
- Documentation of problems, e.g. program cancellations, errors when loading input data, inconsistencies in data from different audited companies (e.g. inconsistent data formats), etc., i.e. type, occurrence, frequency of errors;

- Transparent documentation of conflict resolution, e.g. how the software has processed problematic or missing input data (e.g. by ignoring errors, ignoring data, modifying data, etc.);
- Documentation of the consequences of errors or problems (e.g. when cancelling or skipping (sub-)tasks)

2.1.14 Interfaces

The software must provide standardised interfaces (e.g. REST) and connectors for common systems. This also includes API-based communication. The integration of the screening engine is described in 1.2 System context. The basic set of typical input attributes includes the first and last names of natural persons, alias, company names and former names. Labels, dates, country and identification numbers.

2.1.15 Import relevant data formats

The software must be able to load and process structured data in a common format (at least csv, xml, or txt).

2.1.16 Sequence of name elements: Hits despite changes

The Software must also meet sanctioned entities if the order of one or more elements of the name is changed (e.g. first names, surnames, patronyms, titles, academic degrees or corresponding elements of company names or organisations).

2.2 Technical requirements

This section describes the technical exclusion criteria for the software solution.

2.2.1 Integration into the Deutsche Bundesbank's IT system landscape

2.2.1.1 Integration into the Deutsche Bundesbank's IT system landscape

The software must be able to be operated in the Deutsche Bundesbank's private cloud. This can be done either on Red Hat Enterprise Linux servers or Windows servers (abbreviated as "Standard Server") or in a container environment based on a current version of the Kubernetes distribution Red Hat OpenShift (abbreviated as "OpenShift").

The Bundesbank's IT system landscape is described in Section 1.2.1.

2.2.2 Implementation of the software

2.2.2.1 Installation and basic configuration (establishment of operational readiness)

The Contractor must provide support with the installation and basic configuration of the screening software, including adaptation to the specific requirements of the Deutsche Bundesbank and the creation of the solution architecture document (LAD) for documenting the system architecture.

2.2.3 IT security

The abbreviations used denote the sections from the IT-Grundschutz-Kompodium of the Federal Office for Information Security (BSI) of Edition 2023.²

2.2.3.1 Selection of suitable cryptographic procedures (CON.1.A1)

All data must be protected by appropriate encryption methods both during transmission ("in transit") and in idle mode ("at rest"). This applies to all communication connections, including internal connections (e.g. to the database), as well as to all storage solutions.

Appropriate cryptographic procedures with established algorithms must be used for encryption. No relevant security gaps must be known for these algorithms. Currently recommended key lengths must also be used. The currently established algorithms and key lengths to be applied are defined in the BSI's Technical Directive TR-02102-1.

2.2.3.2 Use of TLS/SSL proxies (DER.1.A10)

In the case of transitions from external networks to the internal network of the Deutsche Bundesbank, the application should be able to deal with the interruption of data traffic (due to content scanning, schema validation and content validation) without any further problems (e.g. without timeouts).

2.2.3.3 Continuous monitoring and evaluation of logging data (DER.1.A6)

The software must create log data that includes activities (such as Log on attempts, file access, deletion logs, configuration settings, or error messages). These records are used to identify problems or suspicious activity at an early stage.

² See Federal Office for Information Security (BSI): https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html; direct link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

2.2.3.4 Basic assurance of communication with other networks (NET.1.1.A9)

The IT solution must authenticate users' access, in which case multi-factor authentication (MFA) must be used.

The IT solution must support mutual authentication between the IT solution and other IT solutions.

2.2.3.5 Securing incoming communication from the Internet to the internal network (NET.1.1.A11)

The IT solution must ensure that all access from the Internet to the internal network is via secure communication channels.

The IT solution must also function without free internet access.

2.2.3.6 Information on IT vulnerabilities (OPS.1.1.1.A20)

The contractor must check the IT solution for malware and backdoors before delivery. The Customer shall be provided with a corresponding test result.

2.2.3.7 Traceability of administrative activities (OPS.1.1.2.A5)

Administrative activities must be verifiable and logged in the software. For this purpose, at least

- Which change was made during an activity;
- Who carried out the activity;
- When the activity was carried out.

To do this, all administrators must have their own access ID. Representatives of administrators must also receive their own access IDs. Every login process via an administration ID must be logged.

2.2.3.8 Protection of administrative activities (OPS.1.1.2.A6)

Administrative interfaces and functions may only be available to authorised persons. Appropriate authentication procedures must be defined for these interfaces and functions. It must be ensured that administrative activities can only be carried out if the corresponding authentication has been carried out beforehand. Administration must be done via secure protocols.

2.2.3.9 Use of system-specific protection mechanisms (OPS.1.1.4.A2)

The software must be compatible with the customer's IT systems and use their protection mechanisms, for example with regard to logging and monitoring, the role concept, authentication methods and firewall rules.

These mechanisms must be used, provided that there is no replacement of at least equivalent value.

2.2.3.10 Separation of the test environment from the production environment (OPS.1.1.6.A13)

The software must be built as a 3-stage model (development, test, production). The test environment must be able to be operated separately from the production environment. The Contractor shall ensure that the technical configuration of the IT solution can be delivered transparently across the stages. The architectures and mechanisms used in the test environment must be documented. It must be possible to operate the stages with different release levels.

2.2.3.11 Conduct penetration tests (OPS.1.1.6.A14)

The Contractor must agree that the Customer may, if necessary, carry out a penetration test at its own expense to be able to verify for itself the security of the services provided. The Contractor shall ensure that pentest findings are rectified in accordance with their criticality for use at the Deutsche Bundesbank.

2.2.3.12 Certification according to security standards

The Contractor shall have an appropriate, implemented and documented security concept and information security management system (ISMS) based on ISO Standard 27001 for the provision of the service or IT solution. For operation in the private cloud environment, the security concept shall also be aligned with ISO 27017. The IT solution must be installable and operable in accordance with the standards 200-2 "IT-Grundschutz-Methodik" and 200-3 "Risikomanagement" of the Federal Office for Information Security (BSI) and the listed ISO 27001 and ISO 27017 standards or alternative security standards with a comparable level of security. The current edition of the listed modules of the IT-Grundschutz-Kompendium applicable to the IT solution must be applicable for the entire term of the agreement. Alternatively, proof of compliance with comparable international standards is to be provided to meet the requirement.

2.2.4 Data protection

2.2.4.1 Compliance with legal framework conditions (OPS.1.1.5.A5 and CON.2.A1)

The software must make it possible to comply with the statutory provisions and legal requirements on data protection (in particular GDPR, BDSG (Federal Data Protection Act)).

Furthermore, the Contractor shall provide a description of its implemented technical and organisational protection measures.

2.2.4.2 Requirements from the AI Act

Provided that AI components are also to be used in the screening software, the provisions of the AI Regulation must also be observed in addition to the provisions of the GDPR.

2.2.5 User accounts / access rights / role concept

The software must enable the implementation of an individual authorisation concept. To do this, it must be possible to create different users, control access and log user actions. (For logging and reading out user activities, see Section 2.2.3.3 Continuous monitoring and evaluation of logging data (DER.1.A6).)

The software must enable the implementation of a role concept that meets the following requirements:

2.2.5.1 Segregation of duties between incompatible tasks (ORP.1.A4)

The software must enable operational and control functions to be distributed among different individuals. For incompatible functions, a segregation of duties must be defined and documented. Representatives must also be subject to the segregation of duties.

2.2.5.2 Setting up, changing and revoking authorisations (ORP.4.A2)

The software must enable user IDs and authorisations to be assigned only on the basis of actual requirements and the need to perform tasks, i.e. according to the principles of *Least Privileges* and necessity (*Need-to-know*). In the event of personnel changes, it must be possible to remove the permissions that are no longer required.

The software must enable: If staff apply for permissions that go beyond the standard, these may only be granted after additional justification and review.

All permissions must be set up via separate administrative roles.

2.3 General Requirements

2.3.1 Operating language

The software must be able to be operated in German or English, although the Bundesbank would prefer a German-language solution. Background system settings, log files, and other functions must also be available in either German or English.

2.3.2 Software training

The Contractor must provide training for the relevant Deutsche Bundesbank staff. First, administrators and technical integrators are to be trained, and second, workshops are to be held on the configuration and use of the software. In addition, training materials are to be provided. The training courses (including the associated materials) must be provided in German or English, with the Bundesbank preferring to receive a German-language training course.

2.3.3 Software documentation

The Contractor must provide comprehensive and understandable documentation of the software. These include a user manual for regular users, an operating manual for technical administrators, an interface description for integration into the Deutsche Bundesbank's IT landscape, and a description of the configuration options (e.g. test rules, parameters). In the event of software modifications, the Contractor must provide appropriate release notes with a transparent description of the changes. The documentation must be provided in German or English, although the Bundesbank would prefer German-language documentation.

2.3.4 Maintainability

The Contractor shall also ensure necessary functional adjustments in addition to maintenance work resulting from IT security incidents (see point 2.2.3). The software should be designed to enable updates, patches and configuration changes to be made with minimal effort.

2.3.5 Test data screening

The bidder agrees to screen the synthetic test dataset provided by the contracting authority in its systems in a timely manner upon request and to make the test results available. In subsequent negotiations, the selected bidders have the option of setting up and configuring their systems to suit the client's requirements. The test data should be provided by email, on a CD or similar media, or by downloading from a website.

2.3.6 Test setting/test installation

The Contractor agrees to carry out a test in the form of a test installation in the Customer's systems to verify the technical feasibility. The extent to which this test installation is carried out and which aspects are considered in this context can be determined from the description of the technical design (ID 5.2). The test installation is not carried out until the negotiation phase.

3 Desirable criteria

3.1 Technical (functional) requirements for the screening engine

3.1.1 Detection of additional entities

In addition to natural persons and legal entities, organisations and institutions, the software should also be able to identify other entities (in particular ships, ports, locks and aircraft).

3.1.2 Detection of entities, if spelling is different (fuzzy logic)

The software should be able to detect various variations of a name, including misspelling, typing errors, typical OCR errors, transcriptions, abbreviations, omissions, and phonetic similarities. The requirement is evaluated using the test data and the detailed requirements under 3.2.

3.1.3 High sensitivity

The software should be highly sensitive during screening. The requirement is evaluated using the test data under section 4. of the assessment matrix.

3.1.4 High specificity

The software should have a high degree of specificity during screening. The requirement is evaluated using the test data under 4. of the assessment matrix.

3.1.5 Processing of payment messages

The software should be able to screen names directly in SWIFT, SEPA and, if applicable, other payment messages (without additional data standardisation). The software should therefore be able to process all standard SWIFT and SEPA formats and, if necessary, other formats (current and historical). It shall be possible to configure which fields are screened within payment messages; the Contractor shall ensure that the software can be adapted flexibly in the event of changes to payment standards; The Contractor warrants that the software can in principle be configured or extended in such a way that possible new message types or messages from other payment systems can be screened. It should be noted here that no data standardisation should be explicitly carried out for payment messages.

3.1.6 Processing unstructured data

In addition to 2.1.3, the entity search should be possible as a (fuzzy) full-text search in unstructured input data (e.g. PDF documents). This means that different spelling methods should also be found.

3.1.7 Natural language processing (NLP): Inclusion of further information

The software should also be able to include additional information related to the name in the screening. These include, for example:

- Country data;
- Gender,
- Type of person;
- Meta data (e.g. addresses),

3.1.8 Dates of birth

The software should also be able to include birth data in the screening in connection with the name. The degree of match of the birth data should be configurable. If birth data are taken into account, the software should be able to correctly record, convert and reconcile various other calendar systems from sanctions lists (in particular EU regulations) in addition to the Gregorian calendar. In particular, the Islamic lunar calendar and the Islamic solar calendar should be able to be processed.

3.1.9 Inclusion of further information from sanctions lists

The software should also be able to include additional information in the screening, regardless of name. This includes, for example, commodity lists, HS codes, ISINs, BICs or other information from commercial banks' data, sanctions lists or other sources.

3.1.10 Parametrisation/configurability of additional context data

The inclusion of further information (see 3.1.7) should be configurable.

3.1.11 Independent name screening

The matching results from the name screening should also be able to be output independently of any other information included.

3.1.12 Processing of non-Latin alphabets

In particular, the software should be able to process Latin, Cyrillic, Arabic, Persian, Korean and Chinese characters. Processing additional alphabets is an advantage. Names should be able to be matched both if they are in the original alphabet and if they have been transcribed. The software should be flexibly expandable at no additional cost, so that additional alphabets can be included if necessary, due to changes in sanctions law (e.g. Burmese).

3.1.13 Transparency

The method of screening should be disclosed, comprehensible and plausible. The algorithms used must be explained. When using AI models, it should be clear which model is used. The results should generally be reproducible.

3.1.14 Explanation of scores

The software is intended to provide a clear representation of how the respective score was determined in detail for each individual result. For example, if different algorithms are used, all scores should be visible.

3.1.15 Processing of unlimited character sets per record

The software should be able to screen the entire content of data attributes, regardless of the number of characters contained and the data type transmitted. It should also be possible to process very long field contents.

3.1.16 Selection of data fields to be screened

The software should allow to configure which and how many data fields are to be screened per data record.

3.1.17 Various configurations for screening individual data fields

The software should also be able to selectively screen different data fields with different settings, e.g. different weights, parameters or algorithms. The software should be able to screen the same data fields in a targeted manner using various methods.

3.1.18 Discovery even without external mapping to the entity type

The software is intended to match sanctioned entities, regardless of whether an entity is labeled at all or incorrectly as a natural person or legal entity (or lock, aircraft, etc.) in the data under review.

3.1.19 Common names

The software shall have appropriate methods to limit false positives that take into account common names or name elements.

3.1.20 Recognition of different languages and differentiated processing

The software should be able to recognise names from different languages and apply testing rules in different ways. Recognition could be based on both the character set and, for example, the sanction regime.

3.1.21 Notification of missing, erroneous, inconsistent, unexpected data

The software should report/output during the screening process if irregularities in the input data (e.g. empty columns, incorrect encoding) have been detected.

3.2 Detailed requirements for the screening engine

3.2.1 Upper and lower case

The software is designed to hit sanctioned entities regardless of letter-case.

3.2.2 German Umlauts and special characters

The software should also hit sanctioned entities if their names contain German umlauts, special characters, accents, diacritical characters, etc. This also applies to typical errors related to

- Excel (e.g. ü → Ã¤);
- Umlauts in other systems, e.g. complete elimination of umlauts or diacritical characters, accents, etc., replacement with spaces, question marks, dots or quotation marks.

3.2.3 Additions and doubling of characters

The software should hit sanctioned entities even if one or more characters are added. Additions should not be weighted in the same way; particularly frequent additions (e.g. quotation marks, hyphens, brackets) and additions from payment messages etc. (e.g. 1/, // etc.) should be considered only to a small extent or not at all.

3.2.4 Character omission

The software is intended to hit sanctioned entities even if one or more characters are omitted. Omissions should not be weighted in the same way, but, for example, according to their frequency (e.g. missing doubling).

3.2.5 Phonetic similarities/transcription variants

The software is intended to hit sanctioned entities even if the string is changed in one or more places. If there is a phonetic similarity or transcription variant, the deviation should be less significant than for other deviations. This also applies to phonetic similarities in other languages (e.g. double or single letters, i-ie, d-dt, etc.).

3.2.6 Processing individual characters of other alphabets

For names that are written predominantly in the Latin alphabet, characters from other alphabets should be recognised and replaced by the corresponding Latin characters (e.g. "B" and "B" in Latin and Cyrillic). This applies accordingly to names written in other alphabets that contain identical-looking characters from the Latin alphabet.

3.2.7 Direct processing of non-Latin characters

The software should be able to match non-Latin characters without first transcribing them into the Latin alphabet. In addition to Latin letters, the EU's sanctions-relevant regulations (and possibly other source documents) contain, in particular, characters of the Cyrillic, Korean, Chinese, Arabic and extended Arabic alphabets as well as numerous special and diacritical characters. These should be able to be processed directly.

3.2.8 Transcription of non-Latin characters

The software must also match sanctioned entities if their names have been transcribed from non-Latin alphabets or need to be transcribed by the software. Where:

- Never only a single transcription standard should be used;
- transparency is provided about which standards are used;
- The official transcription standards of the country whose identification documents would be used by a sanctioned person are also used;
- The most common transcription standards in Germany are used;
- The world's most common standards are used.

3.2.9 Processing of non-Latin defective spelling

The software is intended to match sanctioned entities even if their names exhibit the then usual transcription characteristics due to the transcription from consonant letters, e.g. names from Arabic, Farsi, Urdu and Pashtu. These are mainly the omission of short vowels and duplications, the transcription of paragraphs, the assimilation and attachment of articles.

3.2.10 Consideration of language-specific special features of names

The software is intended to incorporate linguistic peculiarities of names from different language areas into the screening in a meaningful way to increase the selectivity, e.g. via the frequency of names or name elements.

3.2.11 Male vs. female names

The software should be able to recognise male and female names of natural persons to reduce the number of false-positive hits (e.g. Amin Mohammed vs. Amina Mohammed).

3.2.12 Consideration of particularly frequent errors

The software is intended to hit sanctioned entities even if the string is changed in one or more places. In certain cases, the deviations should be less significant, especially in the case of:

- Typical OCR errors;
- Transposition of letters;
- Characters that are on adjacent keys (e.g. O-0);
- Phonetic similarities

3.2.13 Omission of name elements

The Software shall also match sanctioned entities if one or more elements of the name are omitted (in particular, first names, surnames or parts of surnames, patronyms, titles, academic degrees or corresponding elements of company names or organisations).

3.2.14 Abbreviation of name elements

The software is intended to affect sanctioned entities even if one or more name elements are abbreviated. This is particularly true for legal entities and legal forms in which all elements of the name may be abbreviated.

3.2.15 Supplements of name components and additions

The software should also hit sanctioned entities if one or more name elements have been added, e.g.:

- Other first or last names and patronyms;
- Titles and honours, academic degrees,
- Job titles, official titles, etc.,
- Business names, geographical terms, etc.

The software should also apply to sanctioned entities if one or more other additions are provided to a name, e.g. address data, explanatory notes, codes (especially for legal entities).

3.2.16 Names of different persons in a cell

The software should also match sanctioned entities if the names of two or more natural persons or legal entities are in a single cell, e.g. in joint accounts or in payment data. If the names of two sanctioned individuals, organisations, and entities are in one cell, both should be displayed. This also applies to attached birth names or previous names of legal entities (see also unstructured data).

3.2.17 Delimiters: Additional or missing

The software should also hit sanctioned entities if their name components are incorrectly separated (e.g. by spaces, line breaks, hyphens, periods, etc.), e.g. if delimiters:

- are not present at all,
- are partially missing,
- are additionally inserted;
- are missing or added in large numbers and
- exhibit any combination of these errors.

3.2.18 Very long names

The software should also use all long names from the sanctions lists (in particular EU sanctions lists) (at least 200 characters).

3.2.19 Very short names

The software is intended to ensure the following:

- Screening shall be possible for at least 2 characters or more;
- The minimum number of characters included should be configurable;
- It should also be possible to screen for individual characters (especially UTF-8 characters), e.g. in Chinese datasets.

3.2.20 Typical variations

The software should be able to find names even if they have been modified in a typical way, e.g. nicknames such as: Sascha instead of Alexander, Aleksandr or Aleksaschka; Dima instead of Dimitri or Dmitrij; Kolja instead of Nikolai or Nikolaj, etc.

The function should be adjustable depending on the language area or sanctions regime.

The function should not be used for languages from the Islamic culture, as variations of common names are used as independent names (e.g. Ahmed, Achmad, etc. of Muhammad).

3.2.21 Legal forms identification and processing

The software is intended to identify legal forms and integrate them into the evaluation in a meaningful way to increase the quality of screening:

- Foreign language names should also be recognised.
- The settings should be configurable.
- It should be possible to apply screening solely to the name core (without legal form) or, alternatively, to filter the results in such a way that the legal forms are not taken into account.
- The processing of legal forms should be subject to the same requirements as the matching of names. They should also be recognised, for example, if there are spaces, typing errors, abbreviations, etc. (E.g. Ltd., Ltd, Limited, Limited, etc.)
- Very similar designations should be identified (e.g. Ltd., GmbH, OOO (i.e. a "Russian GmbH"), etc.)

3.2.22 Economic sector and geographical names are included in the screening

The software is intended to recognise economic sector and geographical names (e.g. city names, country data) and integrate them into the scoring in a meaningful way to increase the quality of the screening:

- Foreign language names should also be recognised.
- The settings should be configurable.
- It should be possible to apply screening to the name core alone or, alternatively, to filter the results in such a way that economic sector and geographical names are not taken into account.

3.2.23 Recognition of interchangeable designations

The software should be able to identify if differences in name elements are due to the same or very similar terms and take this into account when assessing similarity. Some terms that fall under this heading are, for example, Handelsbank, Commercial Bank, Banque commerciale and Коммерческий банк. The software should be configurable.

3.2.24 Recognition of names despite a combination of errors at the character and/or name component level

The software should also hit sanctioned entities if they are modified at several points at the level of the characters and/or the name elements or by adding additional information.

3.3 Technical requirements

3.3.1 Implementation of the software

3.3.1.1 Integration into a shared cluster

If the software is operated in the container environment, the authorisation concept should be compatible with a shared cluster with multi-client capability and do not require authorisation at the cluster level.

3.3.1.2 Configuration and fine-tuning

The Contractor shall provide support in the configuration of test rules and parameters, the execution of tests for the validation of configuration, interfaces and data consistency, and the optimisation of the software for the processing of large amounts of data. The quantity framework will be disclosed after the competitive tender if a corresponding confidentiality statement (see Document "T13_L1_Verschwiegenheitserklärung_25-2000064042_Los 1.docx ") was signed and submitted with the tender.

3.3.1.3 Simulation environment

An additional simulation environment should exist in the software to be able to test configurations.

3.3.2 Performance and scalability

In this use case, the data volumes are very variable; large datasets in particular are rare, but should be able to be processed due to the future viability of the software.

3.3.2.1 Processing large amounts of data

The quantity framework will be disclosed after the competitive tender if a corresponding confidentiality statement (see Document "T13_L1_Verschwiegenheitserklärung_25-2000064042_Los 1.docx ") was signed and submitted with the tender.

3.3.2.2 Scalability

The application should be temporarily scalable for processing large volumes of data (e.g. by scaling horizontally). The software should be able to process 1.5 times the quantity structure to meet future requirements.

3.3.2.3 Performance monitoring

The software is designed to be reliable and stable, and to provide integrated performance monitoring to continuously monitor system performance (e.g. processing speed, system utilisation, memory consumption). If necessary, optimisation measures should be taken to improve efficiency.

In the Deutsche Bundesbank's container environment, IT monitoring is carried out using the Dynatrace application.

3.3.2.4 Resumption of screening after discontinuation

The software should be able to continue screening at the right place after discontinuation without having to re-run the entire screening.

3.3.2.5 Notification of errors and problems

The software is intended to actively notify the users of the software in the event of aborts, errors and other problems, as well as missing, erroneous, inconsistent and unexpected data.

3.3.3 IT security

The abbreviations used denote the sections from the IT-Grundschutz-Kompendium of the Federal Office for Information Security (BSI) of Edition 2023.³

3.3.3.1 Information on IT vulnerabilities (OPS.1.1.1.A20)

When IT security vulnerabilities and security-related events relating to the integrated or used technologies become known, the Contractor shall inform the Customer of this information, including customary security classification (e.g. CVSS scoring).

³ See Federal Office for Information Security (BSI): https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html; direct link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

3.3.3.2 System and network level logging configuration (OPS.1.1.5.A3)

The Contractor shall provide detailed documentation for the analysis of log reports. Access to the log files may only be secured and can only be granted by specially authorised persons.

3.3.4 Data protection

3.3.4.1 Restrictive use of logging data

It should not be possible to create user-related reports (due to co-determination and personal rights). Access to users and personal data in the log files must be restricted – in accordance with the need-to-know principles.

3.4 General Requirements

3.4.1 Release and change documentation

In addition to the software documentation described in section 2.3.3, new software versions shall be delivered with a detailed release documentation describing the changes, new features, and corrected errors. This also includes information on installing and configuring updates.

3.4.2 Ease of use

The software shall be sufficiently user-friendly in terms of learning, operability and intelligibility to make errors in software use and evaluation of results unlikely.

3.4.3 Accessibility

The software is intended to meet the requirements of the Disabled Persons and Equal Opportunities Act (BGG) and the Barrier-free Information Technology Regulation (BITV 2.0).

3.4.4 Portability

The software should be able to be adapted to a new technical infrastructure (possibly also by the contractor).

3.4.5 Equal opportunities compliant

The software and all documents provided or sent during the term of the contract are intended, within the meaning of the Federal Equal Opportunities Act (BGleig), to express the equal opportunities of women and men, where possible.