Schedule 6D

[Draft version]*
Dossier of Agreements and Procedures

KB, National Library of the Netherlands
March, 2026

**This document is provided as a draft/example by the Contracting Authority to give tenderers insight into the expected operational agreements, working methods and governance arrangements. The Programme of Requirements (PoR) takes precedence and is binding; requirements derived from the PoR are not subject to discussion. Yellow-highlighted sections indicate the Contracting Authority's preferred operational approach and require alignment with the successful Tenderer; these sections are subject to discussion and are not final until formally approved.*

Signature Contracting Authority:
Date:

Signature Contractor:
Date:

KB national library of the netherlands

Table of Contents

Version Control

Version	Date	Author	Changes
0.1	..	..	Draft version
0.2	..	..	..

Table 1: Version control for the DAP

1 General

1.1 Purpose

This Dossier of Agreements and Procedures (DAP), forming part of the Framework Agreement [Framework Agreement], defines the operational agreements relating to the delivery of the agreed Services [application(s)/service(s)] by the Contractor to the Contracting Authority.
The DAP provides a detailed operational elaboration of the SLA and contains the full set of processes, procedures and communication guidelines required for the delivery, execution and continuity of the Services.
The DAP does not introduce additional performance obligations but operationalises the SLA.

1.2 Term

- The commencement date of this DAP shall correspond to that of the effective date of the Framework Agreement.
- The duration of the DAP shall correspond to that of the Framework Agreement.

1.3 Related Documents

Hierarchy	Document	Owner	Date	Version
1	Framework Agreement incl. Schedules (incl. SLA and Exit Plan)	..	..	..
2	Data Processing Agreement	..	..	..
3	Verification meeting report	..	..	..
4	Second Memorandum of Clarifications	..	..	..
5	Descriptive Document including Schedules	..	..	..
6	ARBIT 2022	..	..	..
7	Other Schedules	..	..	..
8	The Tender submission	..	..	..

Table 2: Related documents and their hierarchy

1.4 Document Management

- The Contractor is responsible for maintaining the current version of the DAP.
- Changes to the DAP shall be discussed in the tactical consultation, formally agreed in writing, and recorded in the version control.
- Both Parties shall formally approve changes by signing the updated version.

1.5 Documentation & Knowledge Management

- All processes, procedures and work instructions shall be documented in an environment provided by the Contracting Authority (e.g. MS Teams, Confluence, Jira).
- Documentation shall be accessible to the Contracting Authority (e.g. knowledge base).

- Documentation shall be reviewed at least annually and updated where necessary.

1.6 Evaluation of DAP

- The operational functioning of the DAP shall be evaluated at least annually between the Parties.
- Lessons learned, changes in legislation or processes shall proactively lead to updates of this document by the Contractor.

1.7 Signature

- This DAP shall be signed by authorised representatives of both Parties.
- The Contracting Authority shall be represented by a duly authorised signatory.

2 Communication

2.1 Roles & Responsibilities – RACI

- RACI matrices are applied for the processes within this DAP.
- The RACI matrices are indicative and shall be finalised jointly.
- The full RACI matrices are included in Schedule 8.2 and form an integral part of this DAP.
- Changes to RACI matrices shall be agreed in the tactical consultation and formally approved.
- The RACI matrices form the basis for roles in all processes and governance structures.

2.2 Contacts

- Overview of roles and contact details (included in Schedule 8.1).
- Roles correspond to those defined in the RACI matrices.

2.3 Governance Structure

Level	Participants[1]	Frequency	Topics
Operational	Functional administrator (Contracting Authority), support desk (Contractor)	At least fortnightly or monthly	Incidents, changes, ongoing actions
Tactical	Service manager (Contracting Authority), service manager (Contractor), product manager, security, accessibility team	Quarterly	Trends, reporting, security, privacy, accessibility, improvements
Strategic / contract management	Domain owner, contract manager, service coordinator, account manager, CTO	Annually	Contract management, roadmap, vision
Chain	Full ecosystem including suppliers	Semi-annually; at least once per year on-site, if possible.	To be agreed

Table 3: Governance structure

2.4 Escalation & Major Incidents

- Escalation follows the SLA and this DAP.
- Triggered by SLA breaches, recurring incidents, contract issues or security incidents.
- Escalation paths align with the RACI matrices.
- Escalations are registered and tracked.

[1] Participation and responsibilities follow the RACI matrices.

Level	Contact Contracting Authority	Contact Contractor
Operational	Service manager / Functional administrator	Service manager / Support
Tactical	Service Manager / Process Manager	Delivery Manager
Strategic	Contract Manager / CISO	Account Manager / CTO

Table 4: Escalation Matrix

2.5 Complaints Handling

- Complaints are submitted to the Service Manager.
- Scope: behaviour, knowledge, response times, service quality.
- Response within 10 working days.

3 Support

3.1 Incident Management

- Incidents are registered and managed via the ticketing system.
- Priorities and resolution times follow the SLA.
- Security incidents follow SLA timelines (24h / 72h).
- RCA within 5 working days for P1 incidents.

3.2 Problem Management

- The ITIL definition applies.
- Problems originate from P1 or recurring incidents.
- RCA performed and documented.

3.3 Support by Contractor

- Support is provided via the Contractor's portal / support centre; see contact details in Schedule 8.1.
- Service window as defined in the SLA.
- 24/7 support for P1 and security incidents.

3.4 Support & Maintenance

- Maintenance is aligned with the broader service ecosystem.
- Planned maintenance announced ≥10 working days in advance.
    - Includes runbooks, rollback, and validation steps.
- Maintenance activities are aligned with the broader service chain and its dependencies.
- The Contracting Authority's functional management is involved where maintenance has an impact on features or integrations.
- Following execution, the Contractor reports on activities performed, deviations, and validation results.

3.5 Service Request Management

- Distinction between standard and non-standard requests.
- Standard requests handled immediately or within hours.
    - Standard requests include, for example, password reset requests.
- Managed via ticketing system.

3.6 Changes

- Controlled and auditable change and release process.
- Changes tested before production.
- Traceability ensured.

- Separation between environments maintained.

3.7 Releases / CI/CD Pipeline

- Releases planned with the Contracting Authority.
- Includes rollback scenarios.
- Test reports required per release.
- Accessibility testing included (WCAG).

3.8 Notification Procedure

3.8.1 Steps

1. Register
2. Classify
3. Assign
4. Resolve
5. Validate
    - If validation cannot be completed, the notification shall be reopened.

3.8.2 Minimum requirements

- Name
- Description
- Priority

3.8.3 Closure

- Contractor marks resolved
- Contracting Authority validates
- Reopen if necessary

3.9 Root Cause Analysis (RCA)

- RCA within 5 working days
- The probable root cause shall be shared within 24 hours.

4 Security, Compliance and Privacy[2]

4.1 Security Policy

- Security measures are based on the PoR and the SLA.
- The Contractor maintains an up-to-date and regularly tested information security policy that complies with NIS2 / the Baseline Information Security for Government (BIO) (or other applicable standards).
- Audit reports shall be made available to the Contracting Authority upon request, or an accredited audit statement from a recognised audit body shall be provided.
- One designated contact person is responsible for security matters.
- The policy is reviewed semi-annually and communicated to the Contracting Authority.

4.2 Backup and Recovery Policy

- A Disaster Recovery Plan (DRP) is available and up to date.
- The DRP is tested at least annually by means of a full end-to-end recovery test, in which critical systems and data are restored in a test environment.
- Execution is aligned with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as defined in the PoR and SLA.
- Backups are configured according to the 3-2-1 rule (or an agreed equivalent strategy).
- Restore tests are performed at least annually to verify recoverability of data and systems.
- Restore tests include at minimum:
  - restoration of representative datasets and systems;
  - verification of data integrity and usability;
  - measurement of recovery time (in relation to RTO/RPO).
- After each restore test, a report is shared with the Contracting Authority, including at minimum:
  - date and scope of the test;
  - performed recovery actions;
  - achieved results (success/failure);
  - measured recovery times;
  - identified deviations and risks;
  - improvement measures and follow-up actions.
- If a restore test is unsuccessful, a re-test shall be performed within 5 working days after corrective measures have been implemented.
- Findings from DR and restore tests are used to improve the DRP and underlying procedures.
- Backup and recovery processes comply with the RTO and RPO as defined in the SLA.

4.3 Access Management

- Access to systems is granted based on the principle of least privilege.
- Multi-factor authentication (MFA) is mandatory for all administrative access.

[2] Security, Compliance and Privacy requirements defined in the Programme of Requirements (PoR) take precedence over the SLA and DAP. These requirements are binding and non-negotiable. Yellow-highlighted sections do not apply to these requirements and shall not be interpreted as open for discussion or deviation.

- Access rights are reviewed at least annually by the Contractor in alignment with the Contracting Authority.
- Unauthorised or unnecessary access rights are immediately adjusted or revoked.
- Access management is centrally recorded and managed.

4.4 Remote Access

- Remote access to production and acceptance environments is only permitted via authorised accounts.
- Access is managed and monitored by the Contractor unless otherwise agreed.
- Remote access is logged and periodically reviewed.
- Access rights are reviewed at least annually and adjusted where necessary.

4.5 Security Incidents

- Security incidents are registered, classified and handled via the incident management process.
- Security incidents are reported to the Contracting Authority as soon as possible, but no later than within 24 hours.
- Notifications take place via the agreed CSIRT communication channel (email and telephone).
- Incidents are handled in accordance with the priorities and escalation procedures defined in the SLA and RACI matrices.
- All security incidents are documented and evaluated.

4.6 Audits and Vulnerabilities

- An independent audit is conducted annually (e.g. ISO 27001, ISAE 3402 or BIO).
- Penetration tests are performed at least annually.
- Vulnerability scans are conducted at least quarterly.
- Results of audits, penetration tests and vulnerability scans are documented and shared with the Contracting Authority.
- Identified vulnerabilities are addressed via the patch and improvement process.

4.7 Patch Management

- Patch management is performed in accordance with the priorities and timelines defined in the SLA.
- Available patches are assessed for relevance and impact.
- Patches are tested before being implemented in production.
- Patch implementation is recorded and traceable.

4.8 Monitoring

- Continuous monitoring (24/7) is applied to availability, performance, capacity and security of systems.

- Monitoring includes, at minimum:
    - Availability and uptime;
    - Performance indicators such as response times;
    - Usage and load;
    - Security events;
    - Status of certificates and critical components;
    - Detection of failures and downtime;
    - Security incidents (e.g. DDoS, unauthorised access);
    - Events and deviations are automatically detected, recorded and followed up via the incident management process;
    - Deviations are handled in accordance with the incident management process;
    - Monitoring results are recorded and used for reporting and improvement;
    - Monitoring supports proactive identification of disruptions and capacity issues.

4.9 Availability, Capacity and Continuity

- The Contractor manages capacity based on usage, growth and expected load, in order to meet the performance and scalability requirements as defined in the PoR.
- A Disaster Recovery Plan (DRP) is in place and tested, in accordance with the requirements of the Programme of Requirements (PoR).
- Continuity measures are tested and evaluated at least once per year.
- Changes and releases are executed in such a way that continuity and stability of the Services are ensured.
- Capacity and performance are evaluated based on usage, growth and expected load.
- Continuity measures are aligned with the availability and recovery objectives (RTO/RPO) as defined in the Programme of Requirements (PoR).
- Continuity plans are tested, evaluated and adjusted at least once per year.

4.10 Reporting

- Reports are prepared in accordance with the PoR and SLA, and include at minimum KPIs, security information and accessibility information.
- Operational reporting is provided periodically, and security reporting is provided quarterly.
- Reports include test results for each release, in accordance with the PoR and SLA.

4.11 Knowledge Management and Documentation

- Procedures, manuals and work instructions are documented in a central knowledge environment.
- Documentation is current, validated and accessible to the Contracting Authority.
- Documentation is reviewed and updated at least annually.
- Documentation supports the execution of the SLA and is used for transfer, management and continuity of the Services.

4.12 Training and Awareness

- Employees of the Contractor shall complete security awareness training at least annually.
- Participation and results are recorded and shared with the Contracting Authority upon request.

4.13 Supply Chain Transparency

- The Contractor provides insight into the supply chain, including the name, location and role of subcontractors.
- Security and compliance requirements are imposed on subcontractors.
- Supply chain risks are periodically identified, monitored and reported.
- Appropriate mitigating measures are implemented where risks are identified.

4.14 Logging and Monitoring (Security-specific)

- Security logging is implemented across all relevant components.
- Logs are retained for a minimum of 3 months and a maximum of 12 months.
- Logs are protected against unauthorised access and modification.
- Security monitoring is performed on a 24/7 basis.
- Logs and metrics are available for analysis and reporting.
- Where agreed, logs and metrics are exported to systems of the Contracting Authority, preferably via OpenTelemetry or Prometheus.
- Logging and monitoring support forensic investigation and security analysis.

4.15 API Security

- APIs are secured in accordance with recognised best practices (e.g. OWASP).
- API access requires authentication and authorisation.
- API traffic is monitored and rate-limited.
- API activities are logged.
- APIs are secured in accordance with agreed authentication and authorisation mechanisms and monitored for misuse.

4.16 AI

- The use of AI components is subject to prior alignment with the Contracting Authority.
- AI components are periodically assessed for security and compliance.
- Risks are monitored and reported.
- AI functionality is governed and applied in accordance with the SLA and applicable laws and regulations.

5 Digital Accessibility

- The Contractor shall provide accessibility reporting in accordance with the PoR and SLA.
- Accessibility reporting shall include at minimum:
    - audit results in accordance with WCAG-EM or an equivalent methodology;
    - mapping of findings to WCAG success criteria;
    - accessibility issues reported by the Contracting Authority and end users;
    - prioritisation of findings (e.g. high / medium / low risk);
    - defined improvement measures and planned resolution timelines;
    - status and progress of previously identified issues.
- The Contractor shall perform accessibility audits upon delivery and subsequently at least once every three (3) years, in accordance with EN 301 549 and WCAG.
- The Contractor shall report at least semi-annually on the progress of accessibility improvements and the implementation status of agreed measures.
- Accessibility shall be tested as part of release and change processes, including regression testing where applicable.
- Where automated accessibility testing is applied, the Contractor shall make test results available to the Contracting Authority.
- Accessibility findings shall be managed as part of the incident, problem and change processes where relevant.

6 Exit

6.1 Communication and Reporting

- During the transition phase, progress shall be reported at least weekly, including status, risks, dependencies and planned actions.
- An escalation path shall be established for risks, blockers and decision-making.
- A central action list shall be maintained, including owner, deadline and status per exit activity.
- A final exit report shall be delivered, confirming completion of the transfer, any remaining issues and confirmation of data deletion.

6.2 Data, Privacy and Security

- The Contractor shall provide a complete description of the data structure, including data models, codifications, reference values and data quality characteristics.
- Data shall be transferred in accordance with applicable privacy and information security requirements, including GDPR.
- Data transfer shall be executed securely and in a controlled manner, ensuring integrity, confidentiality and traceability.

6.3 Activation and Governance

- The exit shall be formally initiated by the Contracting Authority in the event of contract termination, discontinuity of the Contractor, or strategic replacement of the Services.
- Upon activation:
    - the Contractor shall appoint an Exit Manager;
    - the Contracting Authority shall appoint a Project Manager;
    - a governance and consultation structure shall be established;
    - the Exit Plan shall be finalised and agreed.
- During the exit:
    - progress meetings shall take place at least weekly;
    - risks and blockers shall be actively monitored and escalated;
    - decision-making shall be coordinated by the Contracting Authority.

6.3.1 Preparation Phase

- In this phase, the exit shall be prepared and structured.
- Activities include:
    - inventory of systems, data and dependencies;
    - identification of accounts, access rights and certificates;
    - definition of the migration strategy and test approach;
    - definition of fallback scenarios.
    - The result of this phase shall be an approved Exit Plan and a complete and validated inventory.

6.3.2 Transition Phase

- In this phase, the transfer shall be prepared and tested.
- Progress shall be reported at least weekly, including risks, dependencies and actions.
- Activities include:
  - knowledge transfer through documentation and sessions;
  - transfer of configurations, runbooks and architecture;
  - execution of test migrations and test exits;
  - transfer of accounts, keys and domains.
- Validation shall include:
  - data integrity;
  - system functionality;
  - usability of the target environment.

6.3.3 Execution Phase

- In this phase, the actual transition shall take place.
- Activities include:
  - execution of the cut-over according to the agreed plan;
  - transfer of data, systems and management responsibilities;
  - monitoring of availability, performance and incidents.
- During this phase:
  - standby capacity shall be available;
  - changes shall only be implemented after approval.

6.3.4 Aftercare Phase

- In this phase, the exit shall be finalised and stabilised.
- Activities include:
  - resolution of remaining issues;
  - stabilisation of the new environment;
  - revocation of access rights;
  - deletion of data and decommissioning of environments.
- The result of this phase shall be:
  - a completed exit;
  - a data deletion statement;
  - a final report.

6.4 Transfer and Validation

- Data and assets shall be transferred according to the following principles:
  - data shall be delivered in open and machine-readable formats;
  - transfer shall include metadata, data models and documentation;
  - data shall be validated for completeness, integrity and usability;
  - transfer shall take place via secure channels and be logged.
- After transfer:

    - access rights shall be transferred or revoked;
    - systems shall be verified for correct authorisation;
    - data deletion shall be executed and demonstrable.
- The Contracting Authority shall validate the transfer based on:
    - completeness of data;
    - usability of systems;
    - completeness of documentation.
- In the event of rejection, the Contractor shall implement corrective measures until acceptance is achieved.

7 Specific Agreements

- Additional agreements between Parties

8 Schedules

8.1 Contact Details

Organisation	Name	Role	Phone	Email	Incident	Change	Distribution
..	..	..	..	..	y	y	x
..	..	..	..	..	y	n	x

Table 5: Contact matrix

8.2 RACI Matrices

8.2.1 Roles and abbreviations

Role	Abbreviation
Contracting Authority	CA
Contractor	CT
Account Manager	AM
Computer Security Incident Response Team	CSIRT
Contract Manager	CM
Domain Owner	DO
Functional Administrator	FA
Product Manager	PM
Security	SEC
Service Coordinator	SC
Service Desk	SD
Service Manager	SM

Table 6: Roles and abbreviations used in RACI matrices

8.2.2 Incident Management

Activity	R	A	C	I
Incident registration	SD CT	SM CT	FA CA	–
Classification & prioritisation	SD CT	SM CT	FA CA	–
Incident resolution	SD CT	SM CT	FA CA	SM CA
Validation of solution	FA CA	SM CA	SD CT	–
Closure	FA CA	SM CA	SD CT	–

Table 7: Incident management RACI matrix

8.2.3 Problem Management

Activity	R	A	C	I
Problem registration	FA CA	SM CA	SD CT	–
Problem investigation	SM CT	SM CT	FA CA, SEC CT	SM CA
Problem resolution	SD CT	SM CT	FA CA	SM CA
Acceptance of solution	FA CA	SM CA	SM CT	–
Status reporting / communication	SM CT	SM CA	CM CA	–

Table 8: Problem management RACI matrix

8.2.4 Change & Release

Activity	R	A	C	I
Submit change request	FA CA	PM CA	SM CT	SM CA
Impact analysis	SM CT	SM CT	FA CA, SEC CT	SM CA
Go / no-go decision	PM CA	PM CA	SM CA, SM CT	CM CA
Release communication	FA CA	PM CA	SM CT	–
Aftercare & evaluation	SM CT	SM CA	FA CA	CM CA

Table 9: Change and release RACI matrix

8.2.5 Monitoring & Event / Security

Activity	R	A	C	I
Monitoring & detection	SD CT	SM CT	–	SM CA
Event follow-up	SD CT	SM CT	FA CA	SM CA
Security monitoring	SEC CT	SEC CT	SM CT	SM CA, CSIRT CA
Patch management	SD CT	SM CT	SEC CT	SM CA
Vulnerability management	SEC CT	SEC CT	SM CT	SM CA

Table 10: Monitoring and Security RACI Matrix

8.2.6 Service Level Management & Reporting

Activity	R	A	C	I
SLA Monitoring	SM CT	SM CA	FA CA	CM CA
Reporting	SM CT	SM CA	FA CA	CM CA
Review & governance	SM CA	CM CA	SM CT	DO CA

Table 11: Service level management and reporting RACI matrix

8.2.7 Exit Management

Activity	R	A	C	I
Exit activation	SM CA	PM CA	SM CT, AM CT	CM CA
Exit Plan	SM CA, SM CT	PM CA	DO CA	CM CA
Inventory	FA CA, SM CT	PM CA	SEC CT	CM CA
Knowledge transfer	SM CT	PM CA	FA CA	SM CA
Data export	SM CT	PM CA	SEC CT	SM CA
Validation	FA CA	PM CA	SM CT	–
Cut-over	SM CT	PM CA	SM CA	CM CA
Data deletion	SEC CT	Security CT	SM CA	CM CA
Reporting	SM CT	PM CA	SM CA	CM CA
Acceptance	PM CA	CM CA	SM CA	–

Table 12: Exit management RACI matrix

8.3 Exit Checklist

- Scope aligned
- Governance confirmed
- Inventory validated
- Migration tested
- Data export validated
- Access revoked
- Data deletion confirmed
- Final acceptance

KB national library of the netherlands