Request for proposals for the development of tools for the COUNTER community

This document and the information it contains are provided solely for allowing potential Bidders to provide a response for the tools being procured.

Please note that COUNTER is not bound to select any Bidder and may reject all proposals and does not bind itself in any way to select the Bidder offering the lowest price. COUNTER may, at its discretion, ask any Bidder for clarification of any part of its proposal.

Contents

1. Introduction

This document describes the process for procurement of tools to support COUNTER's community in the effective implementation of the Code of Practice Release 5 and in the harvesting of the COUNTER usage statistics reports.

The procurement will be overseen by the COUNTER Executive Committee.

Bids must be received by **Friday 6 April 2018.**

2. About COUNTER

Project COUNTER (colloquially referred to as COUNTER) is an international membership organization (operating on a non-profit basis) of libraries, publishers, and vendors, who develop the Code of Practice. The Code of Practice is a standard designed to count the usage of electronic resources, in a library setting. The current release is R4 and compliance with the R5 release is mandated beginning January 2019. Read More.

3. Nature of Request for Proposals

This Request for Proposals is issued for the creation of tools for use by the COUNTER community.
- The tools and their source code will be freely available.
- There are two Lots. The Lots may operate independently of each other, or they may operate from a common platform. (This means Bidders may bid for Lots 1 *and* 2, or Lot 1 only, or Lot 2 only).

LOT 1: COUNTER Release 5 Validation Tool
LOT 2: COUNTER Release 5 Consortium Harvesting Tools

The Validation Tool and the Consortium Harvesting Tools will both support Release 5 of the COUNTER Code of Practice. They serve different purposes but there are several shared features, including self-registration, SUSHI client, (basic) report validation, error handling and reporting. It is not required that Bidders responding to both lots use the same code for shared features -- such reuse of code is at the discretion of the Bidder.

4. Evaluation Process

The scores for the evaluation are as follows:

Criteria	Maximum Score
i. Financial and economic standing	Pass/Fail
ii. Acceptance of open source requirements	Pass/Fail
iii. Information security and data security	Pass/Fail
Each of the following criteria has a maximum score of 5	
iv. **Quality of proposal and robustness of work plan**: The extent to which the proposal addresses the issues and demands outlined in the requirements and shows innovation as appropriate. The quality of the proposal will be assessed on deliverables identified and the evidence provided of how these will be achieved including an assessment of the risks.	5
v. **Impact**: The extent to which the project outcomes will be of overall value to the COUNTER community and included in the assessment under this criterion will be the need for sustainability of the tools. (The Bidder is expected to include an estimate for ongoing maintenance fees). This is to ensure that COUNTER can effectively sustain the tools beyond the development.	5
vi. **Value for money**: The value of the expected project outcomes and the demonstrated understanding of the deliverables.	5
vii. **Previous experience of the project team**: Evidence of the project team's understanding of the technical and management issues involved, and of its ability to manage and deliver a successful COUNTER Report Validation Tool, and/or Consortium Harvesting Tools, for example through work done in similar fields.	5

Notes on criteria i to iii:

i. Bidders should provide a statement and supporting evidence of their economic standing.
ii. Bidders should confirm that all code created as part of the development of the tools will be granted under an Apache License, Version 2.0 (or similar forgiving license) and made available via GitHub.
iii. The Bidder must provide a description of how the outputs would comply with data protection regulations including GDPR and other standards and requirements that may be applicable to users of the tools; and how they would control information security risks.

5. Timescales

- Deadline for clarification requests from bidders: 12:00 noon (UK time) on Wednesday 22 March 2018.
- COUNTER will endeavour to provide responses to Bidder requests for clarification by Wednesday March 29 at 12:00 noon (UK time).
- Deadline for submissions 12:00 noon (UK time) on Friday 6 April 2018.
- Clarifications (if required) sought from Bidders (including negotiation of terms) Friday 20 April 2018.
- COUNTER will endeavour to notify successful bidders by late Friday 27 April 2018.
- Projects should commence in May 2018 and complete no later than November 2018.

COUNTER reserves the right to amend this timeline. Any changes will be posted to the RFP website.

6. Structure of Proposals

The content of the proposal should reflect the evaluation criteria as set out above. To assist in the assessment of proposals, Bidders should structure their proposals as follows:

Cover Sheet – all proposals must include a completed cover sheet with company/organisation name, full address, and contact details.

Statements – all proposals must include a statement regarding criteria i. ii. and iii. See section 4.

Project Description – a description of the intended project plan, timetable and deliverables, risks, and an explanation of how the detailed project outcomes will meet the objectives set out in Section 9 for Lot 1 and Section 10 for Lot 2. Bidders should also include statements regarding intellectual property rights (IPR) and sustainability issues.

Portfolio – provide a list of projects undertaken of similar scale and include links to source code where applicable.

Budget – a summary of the proposed budget, which in broad outline identifies how funds will be spent over the life of the project. Budgets include all costs, including VAT if applicable.

Key Personnel – names and brief career details of staff expected to work on the project, including qualifications and experience in the area of work proposed and evidence of any projects of similar nature successfully completed.

Referees – contact details of two referees for whom work of a similar scale has been undertaken.

Note: Proposals for each LOT should be delivered as a single PDF document. All key information MUST be included within the document.

7. Terms and Conditions of Grant

COUNTER will oversee and monitor the progress of projects.

Payment will be in equal staged payments on sign-off of key milestones and deliverables that will be determined during the contract negotiation phase.

Code created will be granted under Apache License, Version 2.0 (or similar forgiving license) and made available via GitHub. Project COUNTER will be given attribution credit. COUNTER will retain Intellectual Property Rights for any other deliverables under this project.

8. Bidding Process

The deadline for submissions is 12:00 noon (UK time) on Friday 6 April 2018.

Late proposals will NOT be accepted.

An electronic copy of the proposal should be sent in PDF format by this deadline to lorraine.estelle@counterusage.org . This is an electronic-only submission process; therefore, all documentation (including letters of support) must be submitted in PDF format. Do not add security settings for PDFs or files.

A selection panel comprising of COUNTER's Executive Committee and Technical Advisory Committee and Consortia Tools working group will evaluate the proposal against the criterion detailed in the Evaluation Process.

COUNTER reserves the right not to commission the work outlined in this Request for Proposals, and to issue a subsequent call to address any remaining work.

9. LOT 1 Requirements: COUNTER Release 5 Validation Tool

9.1. Introduction

COUNTER provides implementers of COUNTER Reports with detailed documentation and guidance on how to create compliant products; however, even with this assistance the rate of interoperability and compliance could be higher. To address this, COUNTER provided the COUNTER Validation Tool for the Release 4 Code of Practice.

The goal of the project described under LOT 1 is to create a web-based Validation Tool that will test compliance of **COUNTER Release 5** Master Reports and Standard Views, delivered in tabular format, or delivered in JSON via the COUNTER_SUSHI API. Reports will be uploaded to the tool or a SUSHI harvest conducted through the tool and a series of test will be conducted on the result. Errors found will be highlighted in a report to the tester. The tool will be made freely available on the web for all to use, though self-registration will be required to allow tracking of the tools use and improve error reporting.

The Validation Tool will enable publishers, vendors and usage consolidation product owners to test their implementation of the COUNTER_SUSHI API and COUNTER Release 5 Reports during the development process, ensuring errors are caught and corrected *before* release. The result will be more efficient deployment and improved interoperability. The tool could also be used by the COUNTER auditors to validate compliance to the required format specified in the COUNTER Code of Practice Release 5, reducing the price of the audit, and increasing the compliance rates by those publishers and vendors that use it as part of their testing.

9.2. Statements of Scope

The following statements are intended to describe the high-level scope of the Validation Tool being built and are presented as a set of user stories (US).

9.2.1. Login and Registration

Before users are permitted to run tests, they must login with a registered account. During registration, users must identify themselves by providing the following information:

- Email Address (must be valid, used as username)
- Name

US1: As an administrator of the Validation Tool, I want to track who is using it by requiring users to register with their email address and name and a self-assigned password, and to login for using the tool. I further need the registration and recovery of lost passwords to be completely self-service.

US1a: As an administrator of the Validation Tool, I want to require users to complete a Captcha or like during registration to reduce the possibility of the tool being the target of spam or robotic use.

9.2.2. Validating COUNTER Reports - tabular form

US2a: As a user of the Validation Tool who has generated any COUNTER Master Report or Standard View in tabular (e.g. Excel) form, I want to verify that the COUNTER report is formatted correctly and the data values it contains meet the formatting requirements.

"Master Report" means: a report including all relevant metrics and attributes; Master Reports are intended to be customizable through the application of filters and other configuration options, allowing librarians to create a report specific to their needs.

"Standard View" means: a pre-filtered view of one of the COUNTER Master Reports covering the most common set of library needs.

The Master Reports and Standard Views are as follows (see section 3.1 of the Code of Practice Release 5 for details):

Platform Master Report (PR)
• Platform Usage (PR_P1)
Database Master Report (DR)
• Database Search and Item Usage (DR_D1) • Database Access Denied (DR_D2)
Title Master Report (TR)
• Book Requests (Excluding OA_Gold) (TR_B1) • Book Access Denied (TR_B2) • Book Usage by Access Type (TR_B3) • Journal Requests (Excluding OA_Gold) (TR_J1) • Journal Access Denied (TR_J2) • Journal Usage by Access Type (TR_J3) • Journal Requests by YOP Requests (Excluding OA_Gold) (TR_J4)
Item Master Report (IR)
• Journal Article Requests (IR_A1) • Multimedia Item Requests (IR_M1)

"Formatted correctly" means: the report layout is exactly as specified in the Code of Practice Release 5 (see sections 3.2, 3.3 and 4 of the Code of Practice Release 5 for details):

A. Report Header Elements exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.

B. Report Body Elements exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
C. Attributes (Metric_Type, Data_Type, Section_Type, Access_Type and YOP), when included in a Master Report or Standard View, exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
D. Attribute Values exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
E. Elements for Usage Data exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
F. All Elements, Attributes and Attribute Values are appropriate for the report and used in valid combinations.
G. Reports do not contain extraneous rows, such as blank rows within the body of the report or extra rows at the end with non-report data or blank rows at the top before the header.
H. Reports do not contain items for which there was zero usage for the entire reporting period.
I. Usage values are zero or positive numbers and do not contain empty cells unless the entire month column in blank signifying usage for that month is not available in the system (e.g. when month is a future month as when in June of 2019 a user asks for usage from January to December of 2019 – June through December must all be blank to be able to discern zero usage from data that is not yet available).
J. Identifiers are formatted correctly or omitted if not available, they do not contain values such as “N/A”, “not specified” or “unknown”.

Please see 9.7 for the recommended approach for validating the reports and the validation rules for specific elements.

9.2.3. Validating COUNTER Reports - JSON format

US2b: As a user of the Validation Tool who has generated any COUNTER Master Report or Standard View in JSON format, I want to verify that the COUNTER report is formatted correctly and the data values it contains meet the formatting requirements.

“Formatted correctly” means: the report format is exactly as specified in the Code of Practice Release 5 (see sections 3.2, 3.3, 4 and 8 of the Code of Practice Release 5 for details):

A. The JSON Report Format must comply with the COUNTER_SUSHI API Specification.
B. Report Header Elements exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
C. Report Body Elements exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
D. Attributes (Metric_Type, Data_Type, Section_Type, Access_Type and YOP), when included in a Master Report or Standard View, exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.

E. Attribute Values exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
F. Elements for Usage Data exactly match the Code of Practice Release 5; this includes spelling, spacing and capitalization.
G. All Elements, Attributes and Attribute Values are appropriate for the report and used in valid combinations.
H. Counts are positive numbers; Instance elements with a Count of zero are omitted; Performance elements without Instance element are omitted; Report_Items without Performance elements are omitted.
I. Fields with missing or unknown values are either expressed as empty as appropriate for the data type (if the field is required by the specification) or omitted.
J. Identifiers are formatted correctly, they do not contain values such as “N/A”, “not specified” or “unknown”.
K. The JSON report does not include Reporting_Period_Total (used to provide totals per row in the tabular report).
L. The usage counts are reported as totals by month unless a different granularity is specified in the Report_Attributes header (e.g. totals by year or Reporting_Period total).

Please see 9.7 for the recommended approach for validating the reports and the validation rules for specific elements.

9.2.4. Uploading COUNTER Reports for Validation

US3a: As a user of the Validation Tool, I want to be able to upload a COUNTER Master Report or Standard View in tabular form or JSON format and validate the report.

“Upload” means: the user is offered a form with a file dialog that allows to select a file from user’s system and upload it for the validation. The format of the file (CSV, TSV, Excel, JSON) is automatically detected.

“Validate the report” means: depending on the format of the file the validation described in 9.2.2 (tabular form) or 9.2.3 (JSON format) is performed.

US4a: As a user of the Validation Tool, I want to be able to access the results of the test on screen or download them for evaluating the results (see 9.3).

9.2.5. Testing SUSHI Harvesting of COUNTER Reports

US3b: As a user of the Validation Tool, I want to be able to specify the parameters for any COUNTER Master Report or Standard View, request the report via the COUNTER_SUSHI API and validate the response.

“Specify the parameters” means: the user is offered a form that allows to specify

A. the base URL of the SUSHI server for the COUNTER_SUSHI API,

B. the credentials for the SUSHI server (APIKey, Requestor ID, Customer ID),
C. the Master Report or Standard View to be requested,
D. the data range for the report and
E. if a Master Report is selected, filters and attributes for the report.

Please see section 3.1.1 of the Code of Practice Release 5 for a mock-up of a user interface for selecting date range, filters and attributes for a Master Report.

"Request the report" means: the submitted information is used to build a request that conforms to the COUNTER_SUSHI API Specification (see section 8 of the Code of Practice Release 5) and the request is performed. The result is either an error encountered while performing the request (e.g. connection timeout) or a JSON document.

"Validate the response" means: if the result is a JSON document, depending on the HTTP status code, it either must be a COUNTER report (code 200) or a SUSHI exception. For a report the validation described in 9.2.3 is performed, a SUSHI exception is checked for compliance with Appendix F of the Code of Practice Release 5 (see 9.2.6).

US4b: As a user of the Validation Tool, I want to be able to access the results of the test on screen or download them for evaluating the results (see 9.3).

9.2.6. Testing the COUNTER_SUSHI API

The COUNTER_SUSHI API is a RESTful API for requesting COUNTER reports, the list of supported reports, credentials for members of a consortium and the status of the SUSHI server. The current specification, which defines the methods (paths) and the response formats, is available at https://app.swaggerhub.com/apis/COUNTER/counter-sushi_5_0_api/1.0.0 (see section 8 of the Code of Practice Release 5).

US5: As a user of the Validation Tool, I want to be able to verify that a SUSHI server (for which I have valid credentials) is operating correctly and returning properly formatted SUSHI responses.

"Operating correctly" means:

A. The SUSHI server can be accessed without requiring non-standard authentication.
B. The SUSHI server accepts valid request parameters.
C. The SUSHI server returns a JSON document (unless there is an error, e.g. a connection timeout, while performing the SUSHI request).

"Properly formatted SUSHI responses" means: the responses must comply with the COUNTER_SUSHI API Specification. For responses that are COUNTER reports see 9.2.3 and 9.2.5, the following user stories cover the other cases.

US5a: As a user of the Validation Tool, I want to be able to verify that a SUSHI server (for which I have valid credentials) responds correctly to error conditions.

"Able to verify" means: it must be possible to enter invalid parameters, e.g. invalid date ranges, when testing the SUSHI Harvesting (see 9.2.5) to trigger error conditions.

“Responds correctly to error conditions” means: a SUSHI exception is returned that is compliant with those listed in Appendix F of the Code of Practice Release 5. The tool should detect the error conditions and check that the SUSHI exception matches the error condition, e.g. that an exception 3020 is returned for an invalid date range.

US5b: As a user of the Validation Tool, I want to be able to request the list of reports supported by the SUSHI server (for which I have valid credentials) and verify that the SUSHI server responds correctly.

“Detect which reports are supported” means: the user is offered a form that allows to specify

A. the base URL of the SUSHI server for the COUNTER_SUSHI API,
B. the credentials for the SUSHI server (APIKey, Requestor ID, Customer ID),
C. a platform name,
D. a search keyword

and trigger a SUSHI request for the /reports method.

“Responds correctly” mean: the response must comply with the COUNTER_SUSHI API Specification, and the report list must only include valid COUNTER reports or custom reports (see section 11.2 of the Code of Practice Release 5).

US5c: As a user of the Validation Tool, I want to be able to request the credentials for members of a consortium from a SUSHI server (for which I have valid credentials) and verify that the SUSHI server responds correctly.

“Request the credentials for members of a consortium” means: the user is offered a form that allows to specify

A. the base URL of the SUSHI server for the COUNTER_SUSHI API,
B. the credentials for the SUSHI server (APIKey, Requestor ID, Customer ID),
C. a platform name

and trigger a SUSHI request for the /members method.

“Responds correctly” mean: the response must comply with the COUNTER_SUSHI API Specification. Note that if the Customer ID used for the request is not a multi-site organisation, the SUSHI server should simply return the details for that customer.

US5d: As a user of the Validation Tool, I want to be able to request the status of a SUSHI server (for which I have valid credentials) and verify that the SUSHI server responds correctly.

“Request the status” means: the user is offered a form that allows to specify

A. the base URL of the SUSHI server for the COUNTER_SUSHI API,
B. the credentials for the SUSHI server (APIKey, Requestor ID, Customer ID),
C. a platform name

and trigger a SUSHI request for the /status method.

“Responds correctly” mean: the response must comply with the COUNTER_SUSHI API Specification.

9.3. Reporting and Logging Errors

The Validation Tool should capture and record the exceptions and errors encountered during testing such that they can be reviewed on screen and downloaded as an error report. Errors should be clearly articulated so that the reader can determine exactly what is wrong and where the error occurred. If possible, errors should be highlighted in the context of the uploaded file or SUSHI response.

US6: As a user of the Validation Tools, if errors are found when validating my report in tabular form or JSON format, I want to know what the errors are and where in the report they were found so that I may efficiently report them to others or correct them.

“What the errors are” means: exact element and problems are enumerated and where possible expectations provided (e.g. Element <123> found X expected Y).

“Where in the report” means: a meaningful position in the report with error is represented (e.g. Line 72, Offset 1: Element <123> found X expected Y).

“Know… and... efficiently report them” means: users should be able to review errors on screen and downloaded an error report that can easily be emailed or otherwise communicated to others.

US7: As an administrator of the Validation Tool, I want the tool to collect statistics about the tests run so that I can conduct a statistical analysis.

“Collect statistics” means: the tool should log for each test run (if applicable)

A. test name
B. session ID
C. base URL of the SUSHI server
D. platform
E. report ID
F. report format
G. success (y/n)
H. number of errors encountered

“Conduct a statistical analysis” means: the administrator should be able to download the log in tabular form so that it can be imported and analysed in a spreadsheet application.

9.4. Architectural Considerations

The COUNTER Report 5 Validation Tool will be made available as Open Source via GitHub, under Apache License, Version 2.0 (or similar forgiving license). Furthermore, there will be a hosted version accessible from the COUNTER website.

US8: As a software developer that may be responsible for maintaining or expanding the Validation Tool, I expect the code to be well organized and modular so that I may quickly diagnose issues, add new test cases, or expand existing ones.

US10: As a software developer that may be responsible for maintaining or expanding the Validation Tool, I expect the code to include methods to automate regression testing so that I can be assured my changes did not negatively affect other areas of the code

The COUNTER Code of Practice Release 5 introduces a continuous maintenance process that will allow the Code of Practice to evolve over time, minimizing the need for major version changes (see section 12 of the Code of Practice Release 5). This might also affect the COUNTER_SUSHI API and the report validation.

US11: As a software developer that may be responsible for maintaining or expanding the Validation Tool, I expect the modules that implement the COUNTER_SUSHI API and the report validation to be organized in a way that supports multiple versions of the Code of Practice Release 5.

9.5. Security

If sensitive data (e.g., access credentials, Customer IDs, Requestor IDs and APIKeys) is stored in or transmitted by the tool, the tool must meet security and privacy requirements, including GDPR and other standards and requirements that may be applicable to users of this tool.

9.6. User and System Documentation

US12: As a user of the Validation Tool, I want to have documentation available to assist me in using the tool effectively.

US13: As a software developer, I want access to comprehensive, easy to use documentation about the application, its architectural design, how it is structured, its processing business rules, underlying schemas, underlying web services, error handling, etc. so that I may effectively maintain and extend the application as needed.

9.7. Recommended Approach for Validating COUNTER Reports

The COUNTER Code of Practice Release 5 defines four Master Reports, which are customizable through filters and other configuration options, allowing librarians to create reports specific for their needs. The Code of Practice Release 5 also defines Standard Views as pre-filtered/configured views of the Master Reports to support the most common reporting needs. Additionally, the Code of Practice Release 5 allows Master Reports to be extended by adding custom elements (columns/fields in the tabular/JSON reports) and custom values for enumerated elements.

Since the Master Reports are customizable and extensible, using static rules for validating them (e.g. looking for specific headings in specific columns) does not work. This section outlines an approach that uses the Report Header information to determine the elements and permissible values for the enumerated elements for validating a Master Report (the text below focuses on the tabular format of the report and highlights when there are differences for JSON). Since the

Standard Views are pre-filtered/configured views of the Master Reports, the same approach also works for the Standard Views.

Please note that this section is provided for informational purposes only, implementing the report validation this way isn’t a requirement.

9.7.1. Report Header

All Master Reports and Standard Views in tabular form have a common report header in rows 1 to 12, followed by an empty row 13, as specified in sections 3.2.1 (description of the header elements), 4.1.1, 4.2.1, 4.3.1 and 4.4.1 (Master Reports and Standard Views) of the Code of Practice Release 5.

The header element names are in cells A1 to A12, they must exactly match the specification. Please note that the quotation marks used in the Code of Practice Release 5 to signal that a term is a standard name or value are not part of the actual name or value. The corresponding header element values are in cells B1 to B12, they can be validated using the following rules (tables and sections refer to the Code of Practice Release 5):

Row	Column A	Column B
1	Report_Name	Master Report or Standard View name from tables 3.a-3.e OR Custom Report name in the format <Namespace>:<Name> (see section 11.2)
2	Report_ID	Master Report or Standard View ID from tables 3.a-3.e matching the Report_Name OR Custom Report ID in the format <Namespace>:<ID> matching the Report_Name <Namespace>
3	Release	5
4	Institution_Name	Not empty
5	Institution_ID	Format: <Identifier Type>:<Identifier Value> with multiple Institution IDs separated by semicolon-space (a semicolon followed by a space) OR empty when no institution ID available
6	Metric_Types	Format: semicolon-space delimited list of metric types. Master Report: permissible values as specified by tables 3.q-3s Standard View: exact values as specified by tables 4.a, 4.e, 4.i, 4.j and 4.o
7	Report_Filters	Format: semicolon-space delimited list of report filters in the format <Filter Name>=<Filter Value(s)> with multiple values for the same filter name separated by pipe character “|” OR empty for no report filters Master Report: permissible filter names and values as specified by tables 4.c, 4.g, 4.l and 4.q (excluding Metric_Type, Exclude_Monthly_Details and Include_Component_Details) and

		tables 3.o and 3.p for permissible Data_Type and Section_Type values Standard View: exact values as specified by tables 4.a, 4.e, 4.i, 4.j and 4.o
8	Report_Attributes	Format: semicolon-space delimited list of report attributes in the format <Attribute Name>=<Attribute Value(s)> with multiple values for the same attribute name separated by pipe character "|" OR empty for no report attributes Master Report: permissible attribute names are Attributes_To_Show, Exclude_Monthly Details and, for the Item Master Report, Include_Component_Details. Permissible values for Attributes_to_Show are the column headings marked by "O" in tables 4.b, 4.f, 4.k and 4.p, reserved column names for extending Master Reports (see section 11.5) and custom column names in the format <Namespace>:<Element Name> (see section 11.3). Permissible values for Exclude_Monthly_Details and Include_Component_Details are True and False. Standard View: exact values as specified by tables 4.a, 4.e, 4.i, 4.j and 4.o
9	Exceptions	Format: semicolon-space delimited list of exceptions in the format <Code>: <Message>[(<Data>)] Permissible values for exception codes and messages as specified by table F.1 (in Appendix F). Please note that <Data> might contain semicolon-space, therefore <Code>: should be used to split the list.
10	Reporting_Period	Format: Begin_Date=<yyyy-mm-dd>; End_Date=<yyyy-mm-dd>
11	Created	Format: <yyyy-mm-dd>
12	Created_By	Not empty

For COUNTER reports in JSON format the header is in the Report_Header field (see the COUNTER_SUSHI API Specification for details). The differences compared to the header in the tabular reports are:

- The header includes an additional element Customer_ID, the value is the Customer ID used for the SUSHI request (not empty).
- The header does not include the elements Metric_Types and Reporting_Period. These elements are actually report filters which are separate header elements in the tabular reports for easier reading. In the JSON report these elements are included in Report_Filters.
- Exceptions include additional information (Severity, Help_URL).
- Arrays are used for multiple values instead of encoding them into a string.

If the report is a Custom Report the validation should be aborted, and the user should be informed that the report cannot be validated. If the report is a Master Report that has been extended with additional columns, i.e. if Attributes_To_Show includes reserved column names for extending Master Reports or custom column names, the report body should not be validated, and the user should be informed that the report body cannot be validated because of the additional columns.

9.7.2. Report Body

The report body for all Master Reports and Standard Views in tabular form starts in row 14, after the empty row 13 that separates report header and report body. The column headings, i.e. the names of the data elements included in the report, are in row 14, the actual data starts in row 15. Neither blank rows nor blank columns are permitted in the report body.

The columns included in a Master Report and the column headings are determined by tables 4.b, 4.f, 4.k and 4.p of the Code of Practice Release 5, the Report_Attributes header and the Reporting_Period header:

- Columns mandatory for the report, marked with “M”, are included.
- Columns optional for the report, marked with “O”, are only included if they are listed in Attributes_To_Show in the Report_Attributes header or, for the Item Master Report, if Include_Compoment_Details=True is included in the Report_Attributes header (all component columns included).
- The Report_Period_Totals column is always included in the tabular reports.
- Unless Exclude_Monthly_Details=True is included in the Report_Attributes header, one column per month in the Reporting_Period is included in the report with column heading in the format <Mmm-yyyy>.

The order of the columns is: mandatory and optional columns in the order specified by tables 4.b, 4.f, 4.k and 4.p, followed by Report_Period_Totals and the columns per month in chronological order (ascending, if included).

The ordered list of column headings allows to validate row 14 and to determine which rule should be applied to which column for validating the usage data from row 15 on. The following table lists the validation rules, excluding elements without specific validation rule (tables and sections refer to the Code of Practice Release 5):

Element Name	Validation Rule
Database	Not empty
Title	Not empty
Item	Not empty
Publisher_ID	Format: <Identifier Type>:<Identifier Value> OR empty when no publisher ID available
Platform	Not empty

DOI Parent_DOI Component_DOI	Format: <DOI Prefix>/<DOI Suffix> with DOI prefix starting with 10. OR empty when no DOI available
Proprietary_ID Parent_Proprietary_ID Component_Proprietary_ID	Format: <Namespace>:<ID> OR empty when no proprietary ID available
ISBN Parent_ISBN Component_ISBN	Format: ISBN-13 without hyphens, i.e. 13-digit number starting with 978 or 979, OR empty when no ISBN available
Print_ISSN Online_ISSN Parent_Print_ISSN Parent_Online_ISSN Component_Print_ISSN Component_Online_ISSN	Format: ISSN with hyphen, i.e. in the format <dddd-dddc> where d is a digit from 0-9 and c is a digit from 0-9 or the capital letter X, OR empty when no ISSN available
URI Parent_URI Component_URI	Valid URL or URN (according to RFC 3986) OR empty when no URI available
Publication_Date Parent_Publication_Date Component_Publication_Date	Format: <yyyy-mm-dd> OR empty when no publication date available
Article_Version Parent_Article_Version Component_Article_Version	Valid ALPSP/NISO code (usually AM, VoR, CVoR or EVoR) OR empty when no article version available
Data_Type	Permissible value as specified by tables 3.o, 4.c, 4.g, 4.l and 4.q (i.e. must not be empty). If a Data_Type filter is included in the Report_Filters header only permissible values specified in the filter are permitted.
Parent_Data_Type Component_Data_Type	Permissible value as specified by tables 3.i, 3.j and 3.o OR empty when no data type available
Section_Type	Permissible value as specified by tables 3.p, 4.c, 4.g, 4.l and 4.q (i.e. must not be empty). If a Section_Type filter is included in the Report_Filters header only permissible values specified in the filter are permitted.
YOP	Format: <yyyy> (0001 for publication year unknown and 9999 for articles in press permitted, 0000 not permitted) OR empty Value must be present for all request, investigation and access denied metric types. If a YOP filter is included in the Report_Filters header only values specified in the filter are permitted.

Access_Type	Permissible value as specified by tables 3.t, 4.c, 4.g, 4.l and 4.q (i.e. must not be empty). If an Access_Type filter is included in the Report_Filters header only permissible values specified in the filter are permitted.
Access_Method	Permissible value as specified by tables 3.u, 4.c, 4.g, 4.l and 4.q (i.e. must not be empty). If an Access_Method filter is included in the Report_Filters header only permissible values specified in the filter are permitted.
Metric_Type	Permissible values as specified by tables 3.q-3s, 4.c, 4.g, 4.l and 4.q (i.e. must not be empty). If the Metric_Types header is not empty only permissible values specified in the header are permitted.
Reporting_Period_Total	Format: positive number (i.e. must not be zero or empty, such rows must be omitted according to section 3.3.8) Value must be the sum of the monthly values (if included).
<Mmm-yyyy>	Format: non-negative number OR empty If the column represents the current month or a future month (based on the Created date in the header), the cell must be empty to indicate that the usage data is not yet available. If the column represents a past month (based on the Created date in the header), the cell must not be empty unless the Exception header includes a 3031 exception (usage not ready) or 3040 exception (partial data returned) for the month in question.

For COUNTER reports in JSON format the body is in the Report_Items field (see the COUNTER_SUSHI API Specification for details). The differences compared to the body in the tabular reports are:

- The usage data is reported in a Performance, Period and Instance structure which also includes the Metric_Type (i.e. all rows in a tabular report which only differ by Metric_Type and the usage data are included in one Performance element in the JSON report).
- Instance elements with a Count of zero are omitted; Performance elements without Instance element are omitted; Report_Items without Performance elements are omitted.
- Fields with missing or unknown values are either expressed as empty as appropriate for the data type (if the field is required by the specification) or omitted.
- Reporting_Period_Total must not be included.
- If a granularity is specified in the Report_Attributes header, the usage counts might not be totals by month but for example totals by year or Reporting_Period totals.

10. LOT 2 Requirements: COUNTER Release 5 Consortium Harvesting Tool

10.1 Introduction

COUNTER Release 5 Code of Practice eliminated explicit Consortia Reports because of challenges with the COUNTER Release 4 Consortium Reports and because fixing scalability problems in Release 5 was not practical. To address the needs of consortia, Release 5 took a different approach. Rather than having a requirement for consolidated consortia usage, Release 5 COUNTER_SUSHI introduced a new "/members" that allowed for the harvesting, from a content provider, a list of consortia members and their COUNTER_SUSHI credentials. By taking this approach, consortia managers should be able to harvest *any* COUNTER Release 5 Report for members. From a technical operation, the process would work something like this:

Consortia Tool	Content Provider
Requests list of members from provider using "/members" service. Includes the customer ID and other credentials for the consortial account.	**Responds** with the list of members for the requested consortia and includes all the necessary credentials to request an R5 report for each.
For each COUNTER R5 report to harvest	
- **For each** member	
○ **Request** COUNTER R5 report for that member.	**Responds** with the requested usage for that member.
○ **Outputs** member usage to disk file (or database table) in desired format.	
○ **… Next member** until all harvested.	

● … **Next report** until all harvested.	

By taking this approach, a consortial system has a reasonably straightforward way of retrieving all member usage with the providers only needing to deliver one customer's usage at a time and thus addressing the previous scalability problem.

10.2 Expectations for the Tool

10.2.1. General

A. Open Source adhering to Apache License, Version 2.0 (or similar forgiving license) (free to use and free to adapt with all enhancements made open) and made available via GitHub.
B. Uses technology that does not require special installation.
C. Available in multiple implementations
  - a. Web-based (local or SaaS)
  - b. Excel option (Visual Basic)
    - i. Excel limited for large consortia

D. Does not require licensing special software to implement.
E. Expect developer of tool to also support for a fee (Include in bid request for quote for maintenance, i.e. an annual fee for the first year, with option to extend for three years).

10.2.2. Security and Data Protection

A. Requirements:
  - a. Consortium administrator has credentials, such as APIKey, Requestor ID and/or Customer ID for the consortium account (as supplied by content providers)
  - b. Individual institutions can "opt-out" with publishers/vendors (this is not a requirement of the tool, but clarification of the landscape).

B. Option:
  - a. Web-based version of the tool may also allow librarians/consortium administrators to create personal account with self-registration to track tool usage and prevent misuse.
    - i. Registered users must be provided with tools to reset/recover their account credentials/passwords.
    - ii. Option to disable self-registration (for local installations)
  - b. Web-based tool may also allow consortium administrators (the tools' 'personal users') to store configuration (of reports) accessible only through personal login.

C. For SaaS option: If sensitive data (e.g., access credentials, usage logs, temporary files such as configuration files and any transmission including Requestor IDs and APIKeys) is stored in the tool it must meet security and privacy requirements, including GDPR and other standards and requirements that may be applicable to users of this tool.

D. The tool should include a license agreement and/or terms of use and users of the tool agree to terms and that COUNTER can easily update these terms as needed.

10.2.3. **Tool Capabilities**

10.2.3.1. General Operation

A. Fail gracefully if limits are reached.
B. Tool must include any disclaimers about the suitability of the tool for any given consortium laying out limitations that may exist for number of members, time to harvest, file sizes, etc.
C. Allow interrupted processes to be restarted (e.g. if harvesting reports for 100-member consortium is interrupted, there should be an option to continue the run with the member's usage where the process was interrupted).

10.2.3.2 Set-up and Configuration

A. Configuration: Allow consortium administrator to manage their credentials for each content provider and which reports to harvest:
    a. Configuration data is considered sensitive information that may be covered by GDPR or other standards; therefore, the tool must protect such data.
    b. A consortium must be able to store configuration details in an external configuration file which is ingested at run time and not persisted in tool storage.
    c. The tool may also allow storage of credentials within the tool in a manner that ensures that security, privacy, and data protection standards are met.
    d. Configuration details will include:
        i. What providers:
            1. The list of content providers and, for each include:
                a. A unique provider "code" that matches the identifier assigned by COUNTER and used in the COUNTER Registry (platform identifier).
                b. The consortium's COUNTER SUSHI_R5 credentials
                c. A list of COUNTER R5 reports and views to harvest for this provider.
                d. URL for provider's COUNTER_SUSHI R5 endpoint (where possible, this should be retrieved automatically from the COUNTER Registry).
        ii. Consortial Members for each provider, with options for librarian to
            1. Retrieve and store consortial member details for a given content provider (use "/members" service).
            2. Option to "refresh" member list and details.
            3. View and edit member details (in case things need to be tweaked).
        iii. General settings, such as:
            1. Location for exported files: e.g., "C:\consortialUsage\".

2. If exported files should be a single file by provider or separate files for each member and provider.
3. Format for exported file (TSV, XLSX, JSON).

10.2.3.3 Reports Supported

A. Must support all the following COUNTER Master Reports and Standard Views:

Platform Master Report (PR)
• Platform Usage (PR_P1)
Database Master Report (DR)
• Database Search and Item Usage (DR_D1) • Database Access Denied (DR_D2)
Title Master Report (TR)
• Book Requests (Excluding OA_Gold) (TR_B1) • Book Access Denied (TR_B2) • Book Usage by Access Type (TR_B3) • Journal Requests (Excluding OA_Gold) (TR_J1) • Journal Access Denied (TR_J2) • Journal Usage by Access Type (TR_J3) • Journal Requests by YOP Requests (Excluding OA_Gold) (TR_J4)
Item Master Report (IR)
• Multimedia Item Requests (IR_M1)

Master Reports may be supported without additional filters (no custom reports required).

- Note: Master Reports include data not included in standard views and options for extensions.
- Note: Some content providers will extend the Master Reports to include proprietary columns and values (e.g. proprietary Access_Methods or Metric_Types). Proprietary columns and values must be output (use the JSON element name as the column heading).

10.2.3.4 Harvesting

A. Requesting a harvest: The administrator would have a form/screen to:
   a. Specify date range for usage
   b. Pick a report (or All)

            i. Optionally, specify additional filters and attributes for any Master Report selected
        c. Pick a content provider (or All)
        d. If picking a content provider…
            i. Pick a member (or All)
        e. Submit!
    B. Harvesting Logic: What the tool does once the harvest request is submitted.
        a. For each report selected…
            i. For each provider selected…
                1. For each member selected…
                    a. Make COUNTER SUSHI request for report
                    b. Handle exceptions returned during harvest (i.e., server busy, requestor not authorized) by producing an error/exception log; notice in header that there were errors
                        i. Perform sensible retries (e.g., retry every hour for a 24-hour period, then daily for 30 days) -- local installations only not SaaS
                    c. Ingest report usage and perform basic validation (see section on validation and exception handling)
                    d. Transform valid input for output following the general rules for COUNTER Release 5 tabular reports.
                    e. Output to chosen file/format
                        i. Need consistent file naming that includes provider, member, report, COUNTER Release, usage range and date run.
                        E.g.
                        {PROVIDER}_{REPORT}_{RELEASE}_{DATESTART}-{DATEEND}_{LIBRARY}_{DATERUN}
                    f. Pause for a few seconds, if the next request is from the same provider to ensure their system isn't overloaded
        b. Show progress on the screen
        c. Allow for restarts
        d. Log harvest activity (see section on viewing activity logs)
            i. If logging to a database, institution credentials must not be logged.
        e. Show summary of run showing success/failure with metrics for:
            i. Number of reports loaded successfully, with drill-down to view log details
            ii. Number of reports with exceptions encountered by exception type with drill-down to view log details.

10.2.3.5 Output Report Data

A. Option to usage data in native JSON -- note that in this format, the output, by definition, is one file per member-report retrieved.

B. Output usage as tab-separated text files (TSV) -- required output format. Provide all the following

        a. Administrator can request member level usage details with option to choose to output reports as:
            i. One report per member; OR
            ii. One report with breakouts for each member with add Customer_ID and Customer_Name column.
        b. Administrator can request a summary report (see COUNTER R5 CoP section 10.3.4 - required but totals may not match sum of individual member usage; there may be overcounting) - this option bypasses the need to load separate reports for each member.
            i. Add note saying that the summary report might not be accurate due to overcounting
    C. Output (XLSX) -- optional output format
        a. Same options apply as described in Output usage as TSV.
        b. Additional limitations on file size will apply (Excel's maximum file size is 1,048,576 rows). See requirement to fail gracefully.

10.2.3.6 Validation, Exception Handling and reporting issues

A. Validation expectations:
    a. Meet COUNTER_SUSHI JSON Schema
        i. Element names correct
        ii. Structure correct
    b. Usage dates consistent with request
B. When issues found, include in the report insert in the "Exceptions" row in the header. "Exceptions found, see activity log."
C. Log issues encountered:
    a. Exceptions returned from SUSHI calls
    b. Errors encountered making SUSHI calls (e.g. connection timeout; 500 error, etc.)
    c. Exceptions encountered through validation and processing.

10.2.3.7 View activity logs

It should be possible for a consortium administrator (user of the tool) to:

A. Obtain a list of runs by provider
B. View log details for a given run
C. Obtain statistics for a given run

Note: This may be achieved by logging within the tool with required data security or allowing the user of the tool to save session logs to files for later viewing and analysis.

10.2.3.8 Overall Administration for the Web-based tool (not consortium-level administrators)

A. Administration role
B. Add/edit/delete users