RIXML.org
Research Information Exchange Markup Language

RIXML Investment Research Linkback Technical Implementation Guide

Background, first steps, and best practices for technical decisions surrounding RIXML Linkback infrastructure

Version 1.0

Published January 11, 2022

Table of Contents

Preface

Copyright information

Contact information

RIXML
website: RIXML.org
email: RIXML_info@rixml.org
phone: 212-655-2945

Revision history

The *RIXML Investment Research Linkback Technical Implementation Guide* has been revised as follows:

Date	Version	Comments
11 Jan 2022	1.0	Finalization of initial *RIXML Investment Research Linkback Technical Implementation Guide*.
05 Nov 2021	---	Final draft version of *RIXML Investment Research Linkback Technical Implementation Guide* released for comment.
03 May 2021	---	Initial agreement on guidance to be provided in initial version of *RIXML Investment Research Linkback Guide*.

Contributors

Thanks to Tim Aitken and Christopher Freeman of S&P Global Market Intelligence for compiling the content for the initial version of this document, as well as the many participants who contributed their time and expertise.

About RIXML

RIXML is a consortium of buy-side financial services firms, sell-side financial services firms, and technology vendors who provide products and services for creating and distributing investment research and/or capturing interactions between research providers and research consumers. The goals of RIXML are to define open protocols that will improve the process of categorizing, aggregating, comparing, sorting, searching for, and distributing global investment research, and to define an open protocol that allows service providers, consumers, and interaction report aggregators to comply with the EU's MiFID II reporting requirements. The individuals who represent their firms include both IT experts and business-side project managers who represent the analysts, portfolio managers, and others who both produce and consume investment research.

Where can I get more information and provide feedback?

Version 1.0 of the *RIXML Investment Research Linkback Technical Implementation Guide* was created by the RIXML Linkback Working Group as an initial guidance document. We welcome your input on additions, clarifications, or changes that would help your firm implement a linkback solution. You can provide any feedback or suggestions to rixml_info@rixml.com.

Overview

What is a linkback?

A *linkback* is a mechanism by which a research provider delivers content that is stored on its portal to end users through URL links provided via research distribution aggregation vendors. When accessed, the link directs the user to a report stored in the provider's database. The aggregation vendor stores a link to the research content, rather than storing a copy of the content itself.

For compliance and other reasons, this document assumes that the delivered content will be in PDF and/or HTML format, recognizing that other formats are possible from a technical perspective, and may be included in the future.

About the RIXML Investment Research Linkback Technical Implementation Guide

The purpose of this document is to summarize the requirements, steps, and best practices for an investment research linkback implementation. It covers:

- a number of best practices surrounding implementing a linkback deployment.
- guidance regarding authentication.
- an overview of the steps involved in implementing a linkback deployment.

Research providers interested in setting up linkback solutions should consult with their research distribution vendors, as each implementation may be slightly different. Additionally, entitlements and readership reporting embargoes are not covered in this document; however, implementing a linkback framework will require the research provider and the aggregation vendor to integrate their existing entitlement strategy and embargo agreements into the linkback solution.

Recommended best practices

The RIXML Linkback Working Group has identified several recommended best practices surrounding implementation of a linkback strategy and have identified details that will need to be discussed and agreed upon by research content providers and aggregation vendors in the process of developing their linkback implementation. This document describes these best practices and discussion points.

Document, link, and interface considerations

The RIXML Linkback Working Group has identified the following considerations:

Requirement for underlying source document

In the current environment, most vendors will require that the RIXML record include references to both the URL that points to the research item stored at the research contributor's site and the file name for the research item itself and will require that the research item (the actual PDF and/or HTML version of the research item) be delivered to the vendor.

The RIXML metadata file will have two resources listed – the link to the research item on the contributor's site and the filename for the research item being delivered to the vendor. Some vendors also require a text file in order to provide additional functionality; in this case, the RIXML metadata file may have three resources listed.

Rationale:

Vendors often require the source content itself in addition to the link to the content on the research provider's site for the following reasons:

1. **Batch printing/downloading functionality:** Investment research end users frequently prefer to print and/or download multiple reports at once as a time-saving practice and to allow for offline access. In the current environment, some vendors are only able to provide this functionality for content stored within the vendor's environment.
2. **Indexing/advanced functionality:** Currently, most vendors require the PDF of the research content and/or an HTML version of the content to carry out tasks such as indexing and accessing the research document's full text, creating and displaying relevancy ranking, etc.
3. **Redundancy:** In the event of SAML issues and outages, some vendors are able to serve the version of the research item stored within its database.
4. **Carveouts:** Some clients may not wish to access content via linkbacks, requiring availability of the content in the research aggregation vendor's database. Aggregation vendors will need to be able to provide this functionality.

Requirements and recommendations:

At present, PDF is generally preferred (and often required) over HTML or text files because many vendors' systems are designed to accomplish the above-stated tasks using PDFs rather than HTML or text files.

Discussion points:

Research content providers and aggregators will need to determine whether PDF and/or HTML versions of the research content will need to be provided to the aggregator to accomplish the tasks outlined above and will need to agree upon the rules for deciding whether the local version or the research provider's version will be delivered under various scenarios.

Integrating linkbacks into RIXML-tagged research content

As described below, in a linkback deployment, the link for an individual research item is contained in a metadata file. When the metadata file is delivered in the RIXML Research format (as assumed for the purposes of this guide), the research item will have two *Resources* – one will be the link to the content on the research content provider's site, the other will be the reference to the content file (e.g., the file name for the PDF research report) that is delivered to the research content aggregation vendor along with the RIXML-tagged metadata file.

Requirements and recommendations:

Ideally, the resource tag for the link should be flagged as the primary resource; however, content providers should confirm with service providers during the planning phase, as this may not be possible for all ingestion systems. See *Resource URL in the metadata* section for more information.

Resource URL in the metadata

The RIXML Linkback Working Group recommends that the research provider provides a fully-formed, static URL in the metadata that is linked to the research item within their portal. In some instances, if the research provider is unable to provide a complete URL in the Resource tag set, the vendor may be able to develop a method for creating these links using the tags already in the metadata file, with a hard-coded partial URL provided in the *Resource* tag set. Although possible, this is not ideal as it involves more time, investment, and technology resources. If using partial URLs in the metadata, firms will need to discuss and agree upon the construction method for creating the complete URL.

Requirements and recommendations:

A linkback link should consist of either a fully-formed URL for the research item (preferred) or a partial link that enables a fully-formed URL to be created based on the parameters agreed upon by both parties (see example below).

Discussion points:

If a research provider wishes to create a dynamic URL, the parameters required to create the dynamic portion of the URL should be determined during the planning phase of the linkback project.

Research aggregation vendors have reported that they have seen two different methods for the *Resource* tagging in RIXML records: some contributors tag the HTML link and the PDF as separate resources, others include both in a single resource record. While this can be ingested by most vendors, we are hoping to build consensus around one of these methods to present as either a required or recommended format in the future.

The participants in a linkback implementation should also discuss whether the linkback link *can* be, *must* be, or *must not* be flagged as the primary resource in the RIXML file.

Examples:

In an implementation where a complete URL is provided in the Resource tag set, with the HTML link and the PDF tagged as separate resources, the *Resource* section of the RIXML file would look something like this:

```
<Content>
<Title>Sample Company Report</Title>
<Resource resourceID="318074113573-1275de00-d64a-11db" sizeInBytes="144678"
primaryIndicator="Yes" language="eng"> <MIMEType>application/pdf</MIMEType>
<URL>https://rsch.contributor.com/r?q=g318074113573__</URL> </Resource>
<Resource resourceID="318074113573-1275de00-d64a-11db -2" sizeInBytes="144678"
primaryIndicator="No" language="eng">
<Length lengthUnit="Pages">5</Length>
<MIMEType>application/pdf</MIMEType>
<Name>318074113573.PDF</Name>
</Resource>
</Content>
```

In an implementation where a complete URL is provided in the Resource tag set, with the HTML link and the PDF tagged as a single resource, the Resource section of the RIXML file would look something like this:

```
<Content>
<Title>Sample Company Report</Title>
<Resource primaryIndicator="Yes" resourceID="1" language="eng">
<MIMEType>application/pdf</MIMEType>
<Name>318074113573.pdf</Name>
<Comments>Title of the Research Item</Comments>
<URL>https://live.contributor.com/go/publications/link?contentPubID=FS318074113573</URL>
</Resource>
</Content>
```

In an implementation where the dynamic URL is formed by concatenating the base URL with the Resource ID and file name, separated by a dash, the Resource section of the RIXML file would look something like this:

```
<Content>
<Title>Sample Company Report</Title>
<Resource resourceID="20211231180741135 73h" language="eng">
<MIMEType>text/html</MIMEType>
<URL>https://samplefirm.com</URL>
</Resource>
<Resource resourceID="2021123118074113573" language="eng">
<MIMEType>application/pdf</MIMEType>
<Name>sample.pdf</Name>
</Resource>
</Content>
```

Linkback display options

Research distribution vendors may allow for dynamic content, delivered via linkback from a research contributor's site, to be displayed within a static frame in the vendor's platform. Alternatively, clicking the link may redirect the user to the research provider's website.

For content displayed within a frame within the research distribution vendor's site, the vendor may provide a default layout for this content, but in most cases, the research contributors will either provide their own formatting or will work with the vendor to create a custom solution to ensure that their research content renders as expected. Custom solutions may also support additional functionality.

Requirements and recommendations:

If the research content provider utilizes a vendor-supplied viewer for rendering content, both parties will need to ensure that content will be displayed as desired. The vendor may require that certain functionality, such as search / print functionality, not be included to avoid conflicts with the vendor's interface functionality.

For either a vendor-supplied HTML view or a research provider-supplied HTML view, the display of the content within the view must be included in the end-to-end testing to ensure content is rendered as expected.

Discussion points:

When the vendor is providing a static frame within which the research provider's content will be displayed, the two sides will need to determine how the formatting of the content will be defined and who (content provider or vendor) will be responsible for building the solution.

Information security vulnerabilities could require changes to how content is formatted/framed into the vendor application. For example, iFrames have recently been identified as a potential information security threat.

Privacy and accessibility

To comply with various privacy and accessibility regulations and expectations, a linkback implementation will involve discussions surrounding contributor-specific terms of use, ePrivacy, and ADA compliance, as outlined below.

Discussion points:

Terms of Use tracking: if a research contributor has terms of use that need to be agreed to by each individual end user, the planning process will need to determine the manner and timing of receiving end-user acceptance (such as incorporating the contributor's terms of use into the initial terms of use statement for the vendor's site, as an additional step during the entitlement process, or as an additional step upon first clickthrough to contributor's site).

ePrivacy options: the research content provider and vendor will need to agree on how ePrivacy-related management of cookies and end-user privacy settings are implemented within the vendor application for both vendor-stored content and linked-back content.

ADA compliance: the content provider and vendor will need to discuss what ADA-related functionality will be needed (for example, an ADA-compliant screen reader), and will need to ensure that the provider's content will be compliant both when delivered from within the vendor's site and when delivered via linkback.

Minimum duration of link validity

Changes to the organization of content on the research contributor's site can cause the links that have been contributed to research aggregation vendors' sites to become broken.

Discussion points:

The discussion of a linkback implementation should include agreeing on the minimum timeframe that a contributed link should remain valid, what testing (initial and ongoing) will be required to ensure end user access to valid links, what the process would be for discussing and implementing changes if needed due to contributor-side site reorganization, and what sunsetting protocols should be put in place.

Authentication, entitlements, and embargoes

Implementation of a linkback strategy requires the ability to determine and adhere to entitlements, authenticate an end user before the content requested in the link is delivered, and comply with any embargo stipulations in place between the research content contributor and end user.

Usage reporting embargoes

A linkback implementation will need to provide for whatever usage reporting embargo requirements will be needed for the research contributor to fulfill its agreed-upon embargos with individual clients.

Requirements and recommendations:

Because research contributors often have embargo agreements in place with individual clients, any linkback implementation will need to be able to fulfill these requirements.

Discussion points:

Although not covered in this document, the discussion phase of any linkback implementation project will need to include ensuring that these embargo agreements can be fulfilled. This may include:

- creating exceptions and carveouts for delivery of research content via the aggregation vendor's database rather than via linkbacks.
- providing anonymized, non-attributed, and/or rolled-up usage information as described in the *User identification* section, following up with additional details on each transaction once embargo period expires.
- a mutually-agreed-upon system of self-embargoing by the research contributor.

User authorization

The implementation team must agree upon a way of sending appropriate authorization credentials from the vendor to the contributor, generally accomplished using a UUID/GUID. The identifier may be unique to the transaction, the session, the individual user, or the firm; it may also be anonymized in order to comply with the client's usage reporting embargo agreements (see *Usage reporting embargoes* section for details).

Discussion points:

As part of the implementation, the parties will need to determine what IDs will be used and how the ID database will be maintained.

Entitlements

A linkback implementation will need to connect to the existing entitlements system to ensure that each user can only access content matching their entitlement profile.

Requirements and recommendations:

Any linkback implementation must include ensuring that the entitlement system already in place can be integrated into the linkback initiative.

Discussion points:

The planning phase of a linkback implementation should include discussion of how entitlements will be maintained both when content is delivered via linkbacks as well as when the content is delivered from the vendor's site.

Authentication vs. entitlements

Authentication refers to the process of the research aggregation vendor confirming that the person is who they say they are, using usernames, passwords, two-factor authentication, etc., so that when they click on a linkback link, the aggregation vendor can assure the research contributor that the person who clicked on the link has been confirmed by the aggregation vendor as someone who should be shown the content.

Entitlements refers to the set of research content that an individual end user is allowed to see based on a pre-defined set of rules applied by the research provider. The research provider conveys this information to the research aggregation vendor, allowing the end user to be allowed access only to the entitled content. Most aggregation vendors apply these entitlement rules such that each end user only sees the content that they are entitled to access to avoid users clicking on links and receiving "*you are not authorized"* error messages.

As described in the *Entitlements* section of this document, a linkback deployment will require that all parties agree upon a method to ensure that the authentication system can sufficiently enforce each individual user's entitlement rules.

Single sign-on (SSO)

In the context of linkbacks, single sign-on means that once an end user has signed into the research aggregation vendor's website, authentication can be passed through to the individual research providers' systems when clicking on linkback links. While the implementation of linkback functionality does not *require* the use of SSO, most (if not all) deployments will involve SSO to allow for a seamless experience.

Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) is strongly recommended for authentication. SAML is an XML-based open standard for exchanging authentication data between parties, providing a link between the authentication of a user's identity and the authorization to use a service.

At the present time, SAML is the only standard that is available across all aggregation vendors involved in the RIXML Linkback Working Group. Alternative authentication protocols such as JWT (JSON Web Token)/OAuth/OpenID Connect (OIDC) may be available with some vendors.

SAML2.0 is the current version of the standard and is recommended for use in a linkback deployment. Some vendors are in the process of migrating to the SAML assertion version Oracle 12.C. (*ETA – July 2020 and onward*).

How SAML works

SAML integration requires two partners – an Identity Provider (IdP) and a Service Provider (SP). SAML works by passing information about users, logins, and attributes between the Identity Provider and the Service Provider. Each user logs in once with the IdP (single sign-on), and then the IdP can pass SAML attributes to the SP when the user attempts to access those services.

SAML terminology as used for research linkbacks

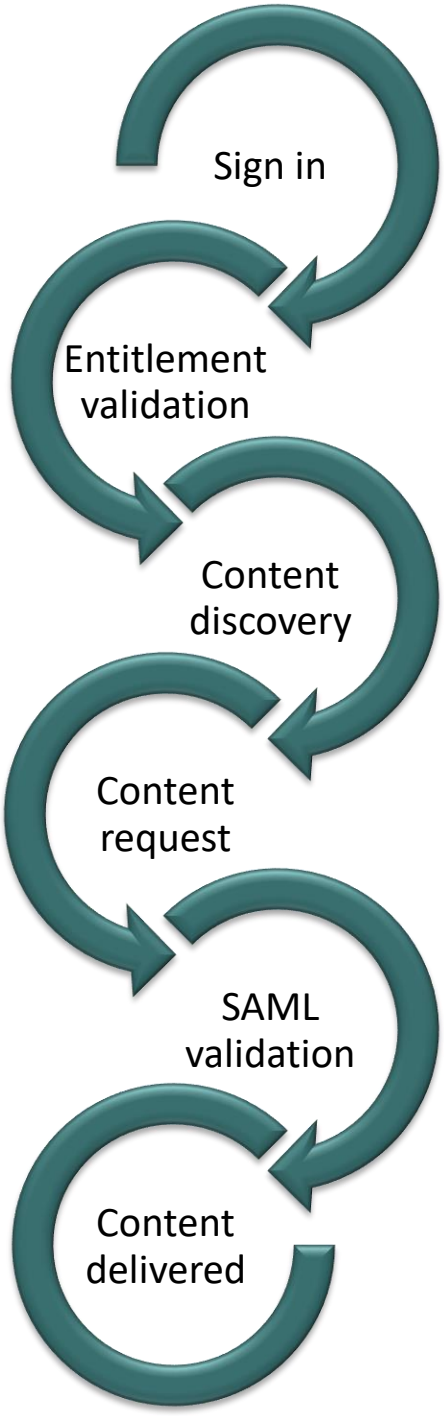
Below is some of the SAML-related terminology used in this document, along with some linkback-related context surrounding how SAML terminology relates to the participants and processes in a linkback strategy:

Authentication:	the process of checking usernames and passwords, verifying account status, etc. in order to provide a single sign-on experience for clients.
Client:	the individual end user, for example, a research consumer at a buyside firm.
Identity Provider (IdP):	the software/service that performs the authentication of each individual client. The IdP server is part of the research aggregation vendor's environment and enables the client to access multiple external sources, including one or more research content provider websites, without needing to sign in to each separately.
Service Provider (SP):	the web application that has the external content the client wants to access without needing to sign in again. In this document, this refers to the research content provider's website; an example of the external content is an individual research item delivered in HTML5 format and displayed in a content area within the research aggregator's site.
SAML assertion:	an XML file asserting a user's identity (see below) and transmitting any other needed attributes. The IdP *asserts* the identity of the user, and the Service Provider consumes the *assertion*. The IdP provides an authentication token that the SP uses to ensure that the content requester is authorized to receive the requested research content.
IdP-initiated vs SP-initiated:	A linkback implementation can be structured such that the SAML assertion is obtained by the research aggregation vendor and is passed to the research content provider along with the content request (IdP-initiated), or such that the SAML assertion is obtained by the research content provider upon receiving the research content request (SP-initiated).
User identity:	In a linkback deployment, the user's identity could either be the user's actual username, a cloaked but unique identifier for each user, or a separate identifier for each request to enable compliance with embargo rules. Additional other attributes, such as the types of research content the client is entitled to, may also be part of the assertion, particularly if the end user is able to access additional content once in the research contributor's website.

SAML steps

The steps involved in the authentication process vary somewhat from implementation to implementation and can utilize either IdP-initiated or SP-initiated SAML validation.

Below is a high-level overview of the steps involved. Slightly more detailed workflows for both IdP-initiated and SP-initiated workflows can be found at rixml.org/standards/linkbacks.



- End user signs into research aggregation vendor's portal using single sign on (SSO)
- Research aggregation vendor applies entitlement rules, etc.
- Aggregation vendor displays available content (recent research, search results, etc.)
- End user clicks on link to request access to individual research content
- Request for content sent to contributor
- SAML request made
- SAML request validated
- SAML response given
- Research content provider serves requested content to end user
- End user accesses content

NOTE: method for requesting and receiving SAML response varies depending on whether IdP-initiated or SP-initiated workflow is used. This may affect the order of the steps in this diagram.

Note that the above shows the steps involved when the request is successful. The implementation plan will also need to define what occurs if a user clicks on a link for content they are not entitled to, and what occurs if/when the IdP system is unavailable.

SAML guidelines

The RIXML Linkback Working Group has identified the following required, recommended, and optional guidelines:

Requirements and recommendations:

REQUIRED:	Procure and exchange IdP SAML Metadata
REQUIRED:	Procure and exchange SP SAML Metadata
REQUIRED:	Identify unique identity to be exchanged between the two partners (UUID vs.email)
REQUIRED:	Identify method of SAML initiation (IdP-initiated vs.SP-initiated) to determine workflow
REQUIRED:	Vendor and research provider need to agree on an approach and support model to manage the expiration of certificates. The two sides need to be in sync to avoid disruptions in clients being able to access linkback research content.
RECOMMENDED:	Use of the latest version of SAML (SAMLv2.0) is recommended. Details are available on the OASIS web site: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
RECOMMENDED:	An implementation that supports SHA2 certificates is preferred.
OPTIONAL:	Identify additional attributes to pass in SAML Response by IDP to SP. Additional attributes may be helpful to further identify the user (ex. location), although the use of a unique user ID (UUID) that links to a CRM system is recommended.
OPTIONAL:	Identify whether user information needs to be passed in encrypted fashion.

Discussion points:

Encryption rules, if needed, will need to be determined and agreed upon.

Some aggregators may be able to implement either IdP-initiated vs. SP-initiated profile.

Contributor-side requirements

Each vendor may have certain contributor-side requirements involved in a linkback implementation, which will need to be discussed during the planning phase.

Requirements and recommendations:

Any linkback implementation must include ensuring that the entitlement rules and protocols already in place are integrated into the linkback initiative, as described in the *Entitlements* section.

Discussion points:

The planning phase of a linkback implementation should include discussion of the following contributor-side requirements (not all will apply to every implementation):

- minimum downtime / performance requirements on contributor site.
- how entitlements will be maintained both when content is delivered via linkbacks as well as when the content is delivered from the vendor's site (as described above).
- required adjustments for the interface to be delivered (such as requiring that the vendor-contributed content hide the search / print functionality).
- requiring that any additional links to other reports within publications be wrapped to require re-authentication if clicked.
- If the link is a redirect to the contributor's site, how entitlements will be maintained once the user has entered the contributor's site (e.g., by passing an entitlement code that indicates the set of content the user is entitled to access).

Test environment and steps to deployment

Deploying a linkback implementation requires that the research content provider and the research distribution vendor work together to design, test, and implement the system. Each implementation may have some differences, but the RIXML Linkback Working Group has identified the following steps involved in most deployments. Note that this is simply high-level guidance and should not be considered a complete set of steps involved in a linkback deployment initiative.

Availability of non-production (test) environment

The RIXML Linkback Working Group highly recommends that both parties establish a testing environment to carry out all linkback-related testing before going live on production environments. Most, if not all, vendors and contributors will require this; some contributors may not be able to proceed without this.

The testing environment should be separate from the production environment. Ideally, the test document set will consist of a complete match of documents in production. It is critical that end-to-end testing be completed for all document types that will be accessed via linkback.

This testing should include confirming that:

- single sign on (SSO) works as intended
- the entitlements engine connects properly into the linkback mechanism
- the URLs, either complete or constructed, are properly formed
- the procedure for creating constructed links works as intended (if applicable)
- the backup and carveout delivery methods work as expected
- the client embargo requirements can be fulfilled
- the usage reporting requirements can be fulfilled

Planning

In advance of a linkback deployment, the research content provider and the research content distribution vendor will need to discuss and agree upon various issues related to a successful linkback deployment, including:

- user identification (UUID/GUID – one per transaction, per session, per user, per firm, etc.)
- integration with entitlement systems (vendor side and contributor side)
- construction of URLs
- delivery of source content in addition to link
- rules outlining circumstances in which source content rather than link will be used
- customization options
- amount of history that will be available
- expected end-user experience
- timing
- redundancy
- usage reporting for source content and for content provided via linkback
- ongoing availability of non-production environment

See the relevant section(s) in this document for important information about many of these items.

Establishing test environment

An end-to-end test of the implementation is critical to the successful outcome of the initiative. Facets involved in the end-to-end test include:

Complete test environment required

To accomplish an end-to-end test, all parts of the process must be in the test environment. That is, a test metadata file should point to a test document stored in a test environment on the contributor's site. Assuming SAML is being used, the research provider will send vendors their non-production SAML metadata for ingestion in vendor non-production system.

Likewise, the SSO link used in testing should be in the test environment and should be validated by the provider as well as the vendor. The provider needs to confirm that the connection is made, and that they are getting calls from vendor's UAT system.

Entitlements

The research provider should ensure that all test users are entitled in their non-production CRM system, and the vendor needs to confirm that test users are also entitled on their non-production system.

Carveouts

The test environment will need to accommodate testing for non-linkback clients to ensure that this delivery method continues to work as expected.

Front-end interface

Whether a default or custom front-end interface will be used, the vendor needs to create a non-production front-end interface.

Test file repository

The research provider will establish a non-production test file repository that replicates as closely as possible the production environment.

Transmission of test files should be done in a way that is similar to the production method, not via email, to enable both parties to test the distribution system.

Generally, a minimum of fifty test records (RIXML files + affiliated content) are required and should contain a selection of all research report types.

The linkback URL in the test files must direct into the non-production environment of the provider.

Execution of testing

Preparing for testing

In preparation for the end-to-end testing of the system, both parties should ensure that:

- test files in the non-production repository are available and accessible in non-production environment.
- test records include RIXML file and source document file (the PDF or HTML file).

Successful testing

A full test of the non-production environment should be completed by both the vendor and the research provider.

Signoff

Signoff confirming successful testing by research content provider and vendor is required.

Preparing for production go-live

Once sufficient successful testing has been accomplished, the following tasks will be needed to prepare for the production release of the linkback initiative:

- Content contributor will need to identify external escalation contact, should any buyside clients wish to discuss the transition to content delivery via linkback.
- Content contributor will need to Identify which of their client firms will be provisioned for a carveout, thus will be continuing to receive content stored at vendor site rather than via linkbacks.
- Vendor and contributor will need to complete any needed changes in entitlement and/or product groups.
- Vendor and contributor will need to complete any needed changes to entitlement APIs.

Production go-live

Once sufficient successful testing has been accomplished, the following tasks will be needed to prepare for the production release of the linkback initiative:

Determine go-live date

Discuss & agree on production go-live date. A weekend deployment is highly recommended to limit potential impact to clients and enable enough time for rollback if needed.

Upload SAML metadata

The research provider will need to send vendors their production SAML metadata for ingestion in vendor system.

Begin including linkback URLs in production workflow

Content providers will need to begin including production URLs in the live RIXML production feed; it is recommended that this begin to occur at least one week before go-live. This will enable time for both provider and the vendor to test linkback links in the production environment before end users begin accessing content via linkbacks.

Update entitlements and exceptions

The content provider needs to ensure entitled users are set up and entitled in their production CRM system. Vendors should ensure users are also entitled on their system. Entitlements between provider and vendor should remain in sync.

The vendor will exclude any carve out clients from the linkback transition.

Update settings

The vendor will update settings within its systems to enable linkbacks for the clients who will be transitioning to linkback content delivery.

Production testing

The vendor and research provider should complete full testing in production environment before the start of the next business day.

Signoff

Signoff by provider and vendor is required.

Subsequent modifications

The research provider should consult with the vendor if they intend to make modifications to the linkback implementation, such as adding content types, changing link structure, etc. These modifications should be fully tested in the UAT environment before adjustments to the production system are made.

Discussion points for the future

Although we were able to incorporate many of the observations, requests, and comments we received during the initial review period, we received some that will require additional research and discussion among members of the Linkback Working Group. Thus, we are identifying the following as areas for future discussion:

- Request for standardization regarding what the required file type is (PDF, text, or HTML) for research content stored at the vendor site and allowing the research contributor to determine the file type.
- Request for standardization regarding proper RIXML tagging for linkback links.
- Adding *vendor-side requirements* section based on input from research contributor firms.
- Adding *client-side requirements* section based on input from research content end users of linkback-enabled solutions.

Conclusion

The above represents an overview of the steps involved in a typical linkback deployment.

If you are not sure who to contact at a particular vendor, contact the RIXML Program Office, who will assist you in identifying a contact at the research distribution vendor.

Appendix: Resources for additional information

SAML additional information

Additional information about SAML can be found here: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

An executive summary can be found here: https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf

OAuth additional information

Open **Auth**orization, an open authentication protocol, developed within the IETF OAuth Working Group. OAuth is supported by some, but not all, vendors involved in the RIXML Linkback Working Group. Additional information about the protocol can be found on the OAuth website: https://oauth.net/.

OIDC additional information

OpenID is an open standard authentication protocol that works in conjunction with an OAuth deployment. It is supported by the OpenID Foundation. Additional information can be found on the OpenID website: https://openid.net.