



MindBridge for Journal Entry Testing

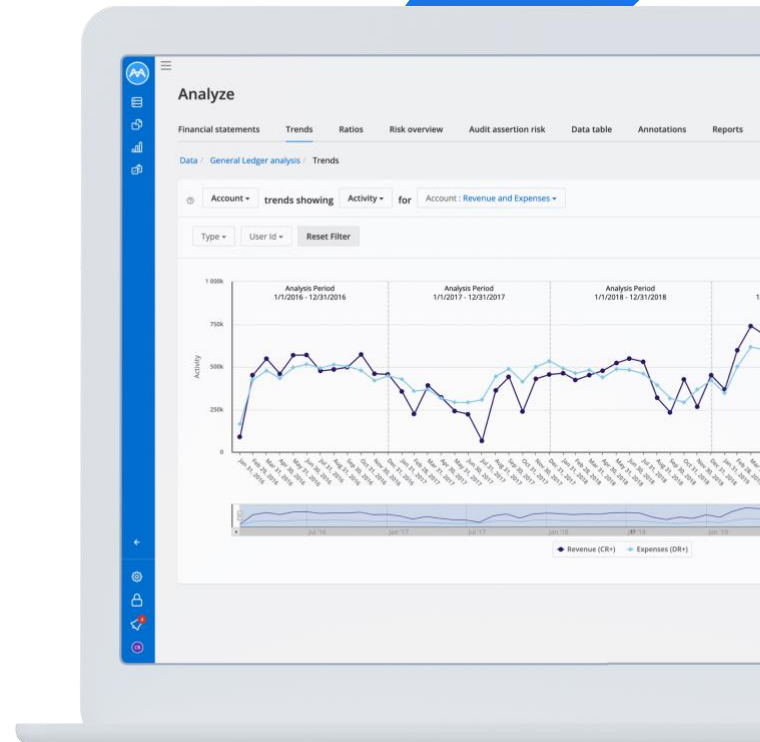


Table of Contents

Disclaimer	4
1.0 Introduction	5
2.0 Overview of Anomaly Detection	6
3.0 Standards Governing Journal Entry Testing	7
4.0 Scoping Approaches Using MindBridge	9
4.1 Full Population Scope	9
4.2 Filtered Scope by Attribute(s)	11
4.2.1 Filter on Certain High Risk Control Point(s)	11
4.2.2 Filter on Certain Criteria of the Data Set	11
5.0 Test Selection Approaches Using MindBridge	12
5.1 Top X Transactions	12
5.2 All High Risk Transactions	12
5.3 Sampling	12
5.3.1 Full Population Sample – Stratified or Random	12
5.3.2 Stratify Based on Specific Criteria	12
5.3.3 Sample of a Sample	13
6.0 Iterative Approaches in Scoping and Selection	14
7.0 Additional Testing Considerations	15
7.1 Interim Testing	16
7.2 Group Audit	16
8.0 Steps to Test Journal Entries in MindBridge	17
Step 1: Ingest Data and Run Analysis	17
Step 2: Assess Reliability of Analysis	17
Step 3: Analyze and Select for Testing	17
Step 4: Export Audit Plan (if Audit Plan Tasks are Used)	18
9.0 Additional Reliance Considerations	18
9.1 Data Cleansing	18
9.2 Data Integrity	18
9.3 Rely on MindBridge	19
10.0 Conclusion	19
Appendix A: Custom Ensembles	20
Appendix B: Using Filter Builder	21

Table of Figures

Figure 1: Process for performing tests of journal entries for management override of controls	8
Figure 2: Example control points from MindBridge that specifically address risks cited in the standards	10
Figure 3: FRC's ADA Refinement Decision Making Model	15
Figure 4: Screenshot of the MindBridge Completeness Report	19
Figure 5: Screenshots of the MindBridge Custom Risk Score Creator	20
Figure 6: Screenshots of the MindBridge Filter Builder	21

Disclaimer

This document and the materials therein are for illustrative and informational purposes only. Supplemental use case documentation herein has not been peer reviewed audit methodology under the various auditing or similar standard setting bodies and are purely illustrative in nature. By using any part of this document, you acknowledge the components are provided as-is, fit for your purposes, and that MindBridge shall not have any liability of any kind relating to this material.

These materials are confidential to MindBridge Analytics Inc., and portions of the approach are patent pending. These materials are intended solely for use by the recipients of the materials and members of their organizations and are not to be distributed to any third party.

Certain links in this document require acceptance of customer terms and conditions, hence require customers to sign into MindBridge. Information that does not require acceptance of customer terms and conditions will link directly to the relevant information. Any MindBridge feature related articles can be found in the [MindBridge knowledge base](#).

1.0 Introduction

Journal entry testing is a required audit procedure that addresses the risk of management override of controls. This guide is designed to help auditors understand the use of anomaly detection in journal entry testing in accordance with:

- PCAOB Auditing Standards AS 2401, pars. 57–62,
- AICPA Auditing Standards AU–C 240, pars. 31–32, and
- International Standard on Auditing ISA 240, pars. 31–32.

Historically, journal entry testing has been cumbersome to perform and yielded minimal value, as substantial professional judgment based on experience and knowledge of the entity, its industry, and accounting norms was required to properly select high risk transactions. Further, due to the increasing volume of transactions in any given ledger, even experienced auditors cannot scan all transactions, limiting their ability to make meaningful judgmental selections.

Therefore, computer-assisted audit techniques (CAAT's) first use cases are primarily centered around journal entry testing (JET).

The use of anomaly detection via [Ensemble AI](#) is the next innovative method in understanding and testing the general ledger. It re-envision the audit approach to allow auditors to focus on what matters.

2.0 Overview of Anomaly Detection

MindBridge (MB) uses a suite of machine learning, statistical, and rule-based [control points](#) or tests to find anomalies in financial data. MindBridge's unique Ensemble AI™ risk scoring system leverages control points to analyze the financial data and provides a general risk score for each entry and transaction based on a weighted average of all control point results.

Like an auditor, accurate analysis requires multiple techniques to create robust and dependable results, especially when dealing with real-world data, where no two companies' operations are exactly the same. Relying on a single algorithm may result in missing essential context in the dataset that a different algorithm could detect. To mitigate the intrinsic risks of using a "single point of failure" methodology, MindBridge uses the Ensemble AI suite of techniques to analyze financial data and provide risk-based scoring on 100% of transactions. The results are presented in an intuitive, visual interface that augments the capabilities of audit and investigative professionals by allowing them to focus their analysis on the most relevant activities.

Currently, the general ledger analysis in MindBridge performs 32 tests simultaneously on up to 500 million records of data, which is equivalent to analyzing 16 billion general ledger data points¹. MindBridge has also taken steps to provide transparency in both data security and the data science behind the control points, so auditors can rely upon the outputs of the system. See [Additional Reliance Considerations](#) in this document.

The MindBridge approach aligns with SAS 142 Audit Evidence, par. 60,

The "use of audit data analytics may enable auditors to identify areas that might represent specific risks relevant to the audit, including the existence of unusual transactions and events, and amounts, ratios, and trends that warrant investigation. An analytical procedure performed using audit data analytics may be used to produce a visualization of transactional detail to assist the auditor in performing risk assessment procedures."

The standard goes on to describe how these procedures can be done through automated techniques, such as MindBridge, in par. A61 by stating, "analytical procedures involve the auditor's exercise of professional judgment and may be performed manually or by using automated tools and techniques. The auditor also might use automated tools and techniques to scan an entire population of transactions and identify those transactions meeting the auditor's criteria for a transaction being unusual."²

¹ Each test (i.e., control point) is applied to each row of data (i.e., a single entry) within the general ledger. Hence, 32 control points applied across 500 million rows of data would result in 16 billion individual scores that are available for analysis.

² Similar concepts are included in the IAASB Audit Evidence project. In the proposed revisions draft presented for the June 2022 IAASB Board Meeting, A3 in current form states:

The auditor may use manual techniques or automated tools and techniques, individually or in combination with each other, to perform audit procedures to obtain audit evidence. In some circumstances, due to the form of the underlying information, an automated tool and technique may be more effective or provide more persuasive audit evidence than a manual technique, or the auditor may need to use an automated tool and technique because a manual technique may not be possible. For example, an automated tool and technique may be more effective in analyzing, processing, organizing, structuring, or presenting large volumes of data or information.

<https://www.ifac.org/system/files/meetings/files/20220613-IAASB-Agenda-Item-3-A-Audit-Evidence-Draft-Proposed-ISA-500-Revised-Mark-up-final.pdf>

3.0 Standards Governing Journal Entry Testing


Journal entry testing is an audit procedure that should be designed to address the risk of management override of controls. The requirements to perform journal entry testing are set out in AS 2401, pars. 57–62, AU–C 240, pars. 31–32, and ISA 240, pars. 31–32.

The goal of journal entry testing was to look for evidence of management override of controls. Approaches to journal entry testing have since evolved, and now incorporate refined scoping and selection criteria based on professional judgement using traditional rules or statistical based analytical techniques.

However, the use of anomaly detection can transform the approach to scoping and selection criteria. MindBridge provides a transactional score that captures risk through anomaly detection by analyzing whole population characteristics such as monetary flows, frequencies, amounts, and testing of business rules. The identification of an anomaly may represent an absent or bypassed control. A higher score may indicate a more anomalous transaction or entry, and therefore can be indicative of unusual behavior or a lack of controls due to a variety of operational reasons.³

The Ensemble AI approach layers a multitude of tests to determine the extent to which a transaction is anomalous, which directly aligns with the intent of standards to determine what behavior may be outside the norm (i.e., subjected to normal controls) and, therefore, present a different risk profile.

Since MindBridge scores the entire population of transactions, it can also support the auditor's understanding and planning requirements of journal entry testing. Auditors are required to understand the entity's financial reporting process as it may assist in identifying the type, number, and monetary value of journal entries and other adjustments as cited in AS 2401, par. 59.

Most firms have similar processes and procedures to the ones listed below to understand and test journal entries. The areas that MindBridge typically assists with in this typical approach are identified on the next page with the MindBridge logo, .


³ Examples include weak control environments, rare, infrequent, or new occurrences in operations, etc.

Figure 1: Process for performing tests of journal entries for management override of controls





Perform Risk Assessment Procedures

- Document understanding of the Financial Reporting Process (FRP)
- Identify common types of journal entries 
- Evaluate controls relating to initiating, recording, and processing journal entries
- Make inquiries of entity personnel involved in the FRP

Plan Scope

- Determine the types of journal entries that will be tested 
- Determine and document the period throughout which journal entries and other adjustments will be tested
- Determine characteristics of fraudulent entries that are specific to the entity
- Consider interim testing

Test Journal Entries and Other Adjustments

- Obtain a report of all journal entries and any other adjustments made during the period being tested 
- Test the completeness of the journal entry population 
- Identify journal entries and any other adjustments that exhibit the characteristics of interest 
- Select journal entries and other adjustments for testing 
- Complete the testing of the selected entries

Document and Conclude

- Document the risk assessment procedures, scoping, and testing
- Conclude on the results of the audit procedures

Most standards were designed before technology had advanced to be able to screen entire populations of data with a multitude of simultaneous tests. Many firm methodologies related to scoping and selection were created to have the best chance of finding anomalies. With the advancement of audit technology, anomalies can now be surfaced by comparing how similar or different each transaction is from each other. This new level of insight into the data allows auditors to tailor and refine their approach in a ledger-specific way so they can focus on what matters.

This guide provides various options for scoping and selection criteria using MindBridge.

4.0 Scoping Approaches Using MindBridge

The concept of [Ensemble AI](#) is to include a variety of tests to surface entries and transactions that are truly anomalous and easily recognizable to an auditor. The use of anomaly detection across the full scale of the ledger allows MindBridge to perform journal entry testing on the full population or a specifically defined scope.

4.1 Full Population Scope

It is appropriate to rely upon the entire population of the ledger as the entire scope. By using MindBridge over the entire population of the ledger, various audit requirements (ISA 240, par. 32(a)(iii), AU-C 240, par. 32(a)(v), AS 2401, par. 62) to test transactions throughout the period are met.

MindBridge allows for the default controls points to be customized and reweighted if auditor judgement requires. This feature allows auditors to adjust the weighting and configuration of the control points.

When testing the full ledger, MindBridge's default risk score weightings or modified weightings can be used. If a firm opts to use only relevant control points to test the full population, auditors should consider using the new Custom Ensembles module outline, see [Appendix A](#) at the end of the paper.⁴

⁴ Note: Modifying the main MindBridge Score weightings may have unintended consequences on how the score is to be used in other areas of the audit, such as risk assessment.

The following MindBridge control points with either default or enhancing weights provide the following direct standards linkage:

- End of reporting period (ISA 240, par. 32(a)(ii), AU-C 240, par. 32(a)(iv), AS 2401, par. 62)
- Complexity (AU-C 240, par. 32(a)(iii), AS 2401, par. 61)
- Non-standard/ outside of normal business (ISA 240, par. 32(c), AS 2401, par. 61)

Figure 2: Example control points from MindBridge that specifically address risks cited in the standards

<div><div>✓</div><div>End of Reporting Period</div><div>i</div></div> <div>This transaction does not contain an entry that occurred in the final days of a reporting period.</div>	<div><div>✓</div><div>Manual Entry</div><div>i</div></div> <div>This transaction does not appear to have been entered manually.</div>
<div><div>✗</div><div>Weekend Post</div><div>i</div></div> <div>This transaction contains at least 1 entry that was posted on a weekend.</div>	<div><div>✓</div><div>Complex Instrument</div><div>i</div></div> <div>This transaction does not contain entries with keywords that indicate a complex instrument.</div>
<div><div>High: 100%</div><div>Rare Flow</div><div>i</div></div> <div>This transaction contains monetary flows that are unusual for this ledger.</div>	<div><div>Medium: 41%</div><div>Complex Structure</div><div>i</div></div> <div>This entry belongs to a transaction that appears to have a moderate level of structural complexity.</div>

For additional details, read about the [different control points available in MindBridge](#).

4.2 Filtered Scope by Attribute(s)

Since journal entry testing is used to address the risk of management override of controls, scoping can be performed to further refine the associated risks and reduce the risk of testing entries that are unlikely to indicate management override risk.

4.2.1 Filter on Certain High Risk Control Point(s)

Auditors can filter on the data table dashboard to find specific control point results and the resultant scores. For example:

- End of Reporting Period
- Manual Entry
- Complex Structure
- Rare Flow
- Complex Instrument
- Weekend Post
- Etc.

See [Appendix B](#) for how to filter on the data table.

In addition, to explore the results of certain data filters, auditors can filter on the risk overview dashboard to visualize the data and determine if more refinement or analysis is needed.

4.2.2 Filter on Certain Criteria of the Data Set

Auditors can use the data table to filter for data characteristics such as:

- Modules, indicators, or transaction types, such as general journal
- Indicators of manual journal entries, such as journal entry ID indicators
- Entries that are debited/credited to specific general ledger accounts
- Entries that flow through certain segments/business divisions (such as administrative departments, eliminations companies, etc.)
- Financial statement areas or transactions that have already been substantively tested

5.0 Test Selection Approaches Using MindBridge

The scoping selection may impact which selection criteria is more relevant depending on the firm's established methodology.

5.1 Top X Transactions

A firm may adopt a methodology to test a set number of journal entries. The data table can be used to sort transactions by risk score, and the top number of transactions within a firm's methodology could be selected for testing by creating an ["audit plan task"](#) in MindBridge.

See [Appendix B](#) for how to filter on the data table.

5.2 All High Risk Transactions

Many firms select all high risk transactions as the criteria to filter on. If this approach is used, a firm should consider allowing alternative approaches with appropriate consultations in the event of unexpected results. Alternative procedures could include recalibrating control points, refining scope, and/or sampling/stratification to make the procedure more relevant to the data file.

5.3 Sampling

5.3.1 Full Population Sample – Stratified or Random

A firm may elect to sample from the entire population of the general ledger with an emphasis on sampling more high risk transactions.

The [Intelligent Sampler](#) is a tool within MindBridge that generates random and risk-stratified samples from a filtered population.

The random sampling feature generates a random sample based on the inputted sample size by the auditor for any filter or unfiltered population in the data table.

The risk-stratified sampling feature stratifies the selected population by their MindBridge risk scores (i.e., entries or transactions). When the Intelligent Sampler generates a risk-stratified sample, it first selects all high risk scores available to be sampled; the remainder of the sample is split to contain 60% medium risk and 40% low risk transactions.

See [Create a sample with the Intelligent Sampler](#) to learn more.

5.3.2 Stratify Based on Specific Criteria

All available filter options within MindBridge can be used to further scope or stratify the population before sampling.

For example, the auditor may consider stratifying the population of exceptions (i.e., high risk transactions) into a homogeneous sub-population. As stated in Financial Reporting Council (FRC)

Addressing Exceptions, in the use of Audit Analytics August 2021 paper⁵, auditors may wish to consider the following:

- *“Monetary value – auditors may wish to stratify by the monetary value of the exceptions, allowing greater focus on larger value items which may be more likely to lead to a material misstatement.*
- *Qualitative characteristics – In addition to quantitative measures by which to stratify the population of exceptions, auditors may wish to consider if any particular qualitative characteristic may be used to stratify a population. For example, on examination of the population of exceptions, the auditor may discover that a large number occurred on a certain date, and in this instance stratifying by date may allow for more meaningful analysis.”*

If transactions of a similar nature are flagged as high risk (a homogeneous sub-population), such as recurring payroll entries, annual depreciation/amortization entries, then auditors can consider sampling one of those transactions to determine whether the sub-population is consistent with the auditor's understanding instead of sampling the full population. Additionally, per SAS 142 Audit Evidence, par. A46⁶, the auditor may design and perform an audit procedure that achieves more than one purpose. Therefore, if the sample is tested as part of a substantive procedure, the auditor can rely on the testing performed in another area of the audit and document their understanding of the transaction.

5.3.3 Sample of a Sample

The FRC also permits a sample to be taken of a sample when the population is not homogenous. Auditors can further stratify the population into homogeneous sub-populations before beginning sampling and substantive testing. In the event that further stratification is not possible, FRC advises auditors to take care when sampling in this manner that the “untested population in a single financial statement line item does not exceed materiality.”⁵

The term “sample of a sample” may be a misnomer in certain jurisdictions. AU-C 530 paragraph A19 deals with the concept of unexamined items in a similar manner to the FRC's concept of a sample of a sample. Paragraph A19 requires that unexamined items be treated as misstatements or deviations in the assessment of the amount of misstatement or deviation in the population. This safeguard is similar to the safeguard outlined by the FRC.

⁵ Source: <https://www.frc.org.uk/getattachment/01327ab3-1d5f-4068-ab9b-ece0efc3c3af/Addressing-Exceptions-In-The-Use-of-Data-Analytics-20210824.pdf>

⁶ ISA 500 A3p

6.0 Iterative Approaches in Scoping and Selection

Firms may opt for an iterative approach to refine the scope and selection criteria of samples. An iterative approach of a predetermined “menu” of permissible methods may be more responsive to engagement-specific risk, as well as data available in the specific ledger.

An iterative approach to audit data analytics is specifically permissible per the Financial Reporting Council (FRC). This approach addresses the risk of sampling on a population that contains a significant number of outliers, not true exceptions. The FRC clearly states this concern:

“In many cases, this volume of outliers is a symptom of poorly defined parameters. In using ADA to understand and assess the population being analyzed, parameters may require re-calibration after initial analysis to ensure the tool is appropriately identifying outliers that merit further investigation as exceptions...”⁷

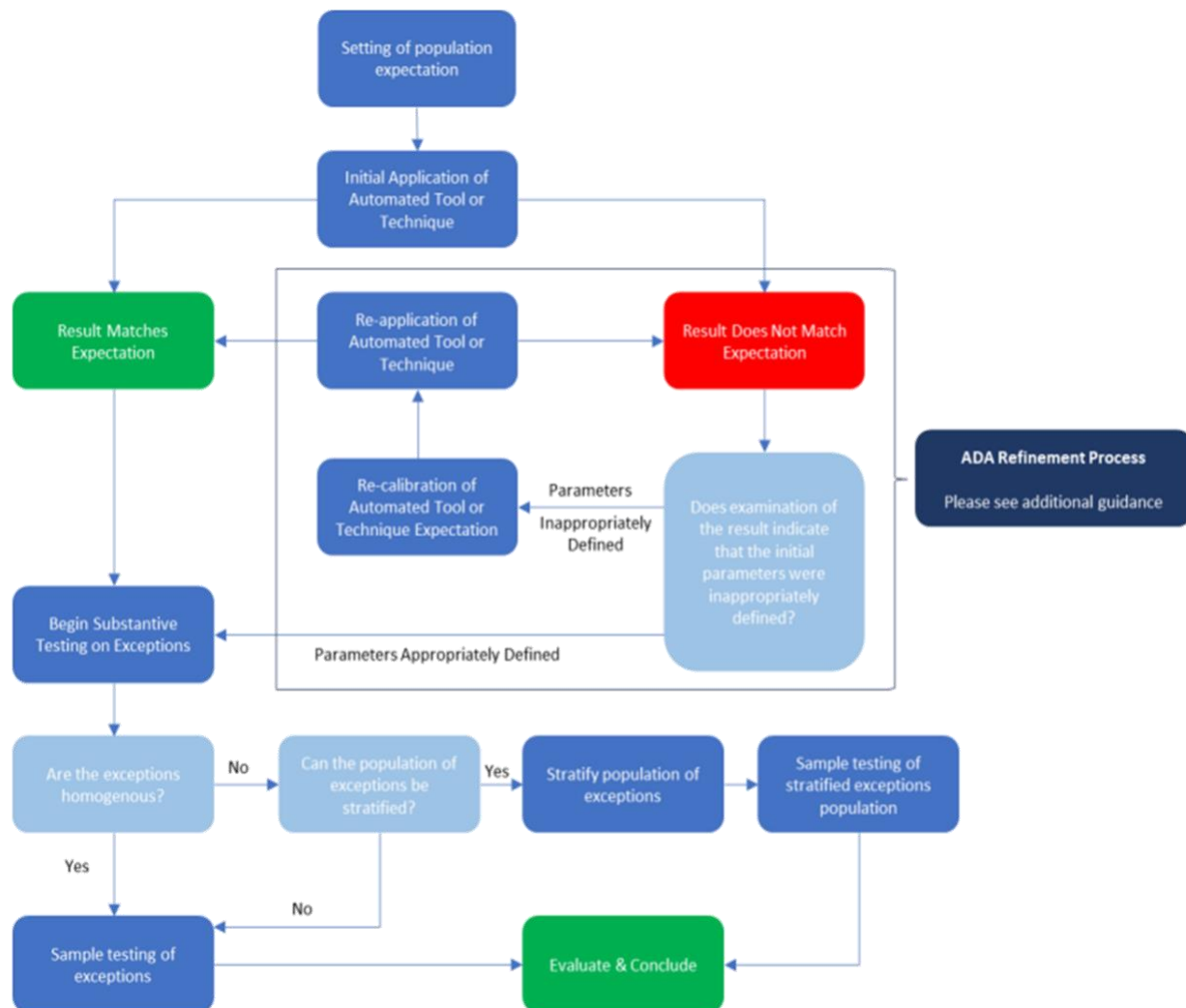
In addition, the above scenario may arise due to a change or lack of understanding about the population, entity, and its environment.

While the FRC outlines various safeguards in refining a data analytic, this model’s existence indicates the need in many circumstances to have iterative or optionality in certain aspects of journal entry testing if the data structure and/or detail does not yield appropriate results for the engagement.

⁷ Source: <https://www.frc.org.uk/getattachment/01327ab3-1d5f-4068-ab9b-ece0efc3c3af/Addressing-Exceptions-In-The-Use-of-Data-Analytics-20210824.pdf>

The following flow chart⁸ is the FRC's decision-making model for the refinement of an audit data analytic:

Figure 3: FRC's ADA Refinement Decision Making Model



⁸ Source: <https://www.frc.org.uk/getattachment/01327ab3-1d5f-4068-ab9b-ece0efc3c3af/Addressing-Exceptions-In-The-Use-of-Data-Analytics-20210824.pdf>

7.0 Additional Testing Considerations

7.1 Interim Testing

As standards cite concepts related to reporting period ends, most auditors perform journal entry testing during year-end procedures. However, due to technological advances in rolling an interim general ledger into a year-end ledger, the auditor has the option to test a portion of their journal entries during interim.

Similarly, interim control testing, the finalization of testing component could be reserved for once the final general ledger is analyzed. Furthermore, scope and selection criteria could differ between interim and year-end testing due to the enhanced focus in the standards of end of reporting period risk in management override.

The benefit of this approach is reduced work at year-end when the auditor may have tight deadlines and staffing constraints. Additionally, interim testing allows the auditor to refine and validate parameters used to identify journal entries prior to year-end testing.

See [Convert an interim analysis to a full analysis](#) to learn how to convert an interim analysis to a full analysis in MindBridge.

7.2 Group Audit

When planning a group audit, the engagement team needs to assess whether each component should be included or excluded from the scope of journal entry testing for management override of controls. Ordinarily the scoping for journal entry testing is consistent with that of the group audit testing scope.

ISA 240, par. A43 and AU-C 240, par. A49 explicitly mentions in audits of entities with several locations or components, consideration is given to the need to select journal entries from multiple locations. When using MindBridge, the auditor can filter for different locations or components on the data table to pick relevant samples.

The following are factors to consider when determining whether there is a risk of management override of controls at a component level:

- Are the transactions recorded at the component level routine or complex?
- Are there incentives or undue pressures on management to produce financial results at the component level?
- Is there a centralized and common accounting process and effective monitoring controls over subsidiaries?
- Are significant estimates recorded at the component level?
- Is there a history of errors at the component level?
- Are there any significant or non-routine transactions recorded at the component level?
- Are there significant account balances and classes of transactions subject to substantive audit procedures?
- Are closing entries recorded by the component?

The auditor may review the risk overview dashboard and use filters to visualize the data for different components to determine whether to exclude a component from journal entry testing for the risk of management override.

If a separate opinion is required for each component, engagement teams must ensure that the testing performed is adequate for the standalone audits. It is possible to run multiple MindBridge analyses for each component within a single engagement. Alternatively, the engagement team can also create separate engagements for each component within the same MindBridge organization.

8.0 Steps to Test Journal Entries in MindBridge

MindBridge uses business rules, statistical methods, and machine learning—algorithms to score each transaction and entry in the ledger. This provides increased visibility into unusual trends or anomalies within the general ledger. However, MindBridge cannot identify only those entries that are fraudulent, the engagement team must use professional judgement and analyze entries in the results to determine which entries to test.

The following are the high-level steps to complete journal entry testing in MindBridge.

Step 1: Ingest Data and Run Analysis

Run an analysis on the population of journal entries in scope.

See [Run an analysis](#) to learn how to run an analysis in MindBridge.

Step 2: Assess Reliability of Analysis

Analyze the output to verify that the risk overview dashboard and financial statements appear reasonable and that there are no data quality issues. The engagement team can also review the [completeness check report](#) to confirm the completeness of the analyzed general ledger.⁹

Step 3: Analyze and Select for Testing

Analyze each journal entry exhibiting a characteristic of a fraudulent entry as identified in the output as defined in accordance with the selected methodology. The entries can be either:

- Exported as a report from the data table or
- A task can be created to add the selection to an audit plan

See [Data table: Export files and other actions](#) to learn how to export reports from the data table.

See [Add an audit plan task](#) to learn how to add a new task to the Audit Plan page.

⁹ There are also [certain checks](#) that can be performed prior to running an analysis to confirm the data meets expectations.

Step 4: Export Audit Plan (if Audit Plan Tasks are Used)

Export the audit plan, which includes a summary of your journal entry selections, and proceed to testing.

See [Audit Plan: Export CSV and XLSX files](#) to learn how to export the audit plan.

9.0 Additional Reliance Considerations

9.1 Data Cleansing

If the data is not of sufficient quality, an auditor can leverage certain features with MindBridge to improve the data's usability without impairing its overall reliability or its source origin.

For example, MindBridge's Smart Splitter can be leveraged to break down large, grouped transactions to improve the accuracy of the risk scores as MindBridge is able to decipher the underlying [monetary flows](#) (i.e. debit/credit pairings) more accurately.

Auditors can also use this feature to address some of the limitations of general ledger accounting packages common in the audits of less complex entities. For example, auditors can create a synthetic transaction ID for ledgers without a transaction ID.

Below are some relevant links from the MindBridge knowledge base on identifying and creating a transaction ID:

- [Understand Transaction ID and data integrity](#)
- [Troubleshooting transaction ID selection](#)

Below are some relevant links from the MindBridge knowledge base on data clean-up and formatting:

- [Data Formatting Guide: Tools and Resources](#)
- [Data formatting tips and tricks](#)
- [Best practices: Before submitting a data formatting request](#)
- [Troubleshooting tools: Smart Splitter and custom running total](#)

Use the MindBridge created [guides for selected ERPs](#) to learn how to export, transform and import general ledger data into MindBridge. The guides include how to generate a transaction ID in MindBridge, if applicable. For example, general ledgers in QuickBooks Online do not always have a transaction ID, but the transaction ID can be generated by following the steps in [this guide](#).

9.2 Data Integrity

Recent and upcoming audit evidence standards¹⁰ remind auditors to validate the accuracy and completeness of information relied upon for the audit. Anytime an auditor is doing journal entry testing, they should validate the completeness of the ledger they are testing.

MindBridge's completeness check report calculates the expected closing balance by adding the ledger activity to the opening trial balance, then compares that to the provided closing trial balance. This helps the auditor identify if the various accounts are balanced, within tolerance, or out of

¹⁰ SAS 142, par. 8b or ISA 500, par. 9A as proposed in June 2022 Board Draft

balance. This is automatically performed on an account-by-account basis to ensure the completeness of the data.

Figure 4: Screenshot of the MindBridge Completeness Report

Trial Balance / General Ledger - Account Completeness Report

Highlighted cells indicate accounts with either no opening or closing balance supplied.

Account Description	Opening Balances Per User Supplied Opening Balances	Net Movement Per Current Year General Ledger	Expected Closing Balance Given Opening Balance and Net Movement From GL	Closing Balances Per User Supplied Closing Balances	Net Difference Between Expected and Supplied Closing Balances	Tolerance Testing
Cash	\$2,578,147.80	\$1,308,953.07	\$3,887,100.87	\$3,887,100.87	\$0.00	Account Balanced
Accounts Receivable	(\$871,087.00)	(\$206,383.00)	(\$1,077,470.00)	(\$1,077,470.00)	\$0.00	Account Balanced
Finished Goods	(\$84,327.46)	(\$645,805.79)	(\$730,133.25)	(\$730,133.25)	\$0.00	Account Balanced
Inventory of Parts and Supplies	\$1,638,183.36	\$643,778.82	\$2,341,963.18	\$2,341,963.18	\$0.00	Account Balanced
Work in Progress	\$509,893.78	\$0.00	\$509,893.78	\$509,893.78	\$0.00	Account Balanced
Returns	\$0.00	\$342,842.12	\$342,842.12	\$0.00	(\$342,842.12)	Out of Balance
Revenue	\$0.00	(\$8,533,330.95)	(\$8,533,330.95)	\$0.00	\$8,533,330.95	Out of Balance

9.3 Rely on MindBridge

Organizations should be aware that a proposed international ethics standard will likely change the ethics rules on how auditors and organizations address technology use.

Under the exposure draft from the International Ethics Standards Board for Accountants, auditors would have to consider specific factors to determine when reliance on technology is reasonable, similar to the way auditors must consider reliance on the work of others. In addition, there are requirements in the various new quality management standards such as ISQM 1 to assess vendors relied upon in the audit.

MindBridge is a global leader in financial risk discovery and anomaly detection, and works diligently to anticipate and meet the highest standards of quality and ethics. As a result, MindBridge technology and tools already meet the proposed standard's reliability requirements. MindBridge has received independent third-party validation of the reliability of its software and algorithms, and is certified [SOC 2®](#) and [ISO 27001](#).

See [Rely on MindBridge](#) for more details.

10.0 Conclusion

Using MindBridge's Ensemble AI, firms are able to use new innovative methods to understand and test general ledgers in accordance with auditing standards. For technical assistance or to discuss further with our Methodology Team, contact your Customer Success Manager, or reach us at info@mindbridge.ai.

Appendix A: Custom Ensembles

MindBridge offers the ability to create custom risk scores¹¹ by account. For example, auditors can choose a selection of accounts that represent additional factors for risk of management override. Auditors can then select the various control point(s) that should be applied to the designated account(s). Therefore, a firm- or engagement-specific risk score could be created that only includes control points that the auditor believes are indicators of risk of management override over the entire population of the general ledger.

This approach is essential when a firm wants to leverage basic overall scoring for overall engagement work, such as risk assessment, and then wants to have specific bundling of tests for specific procedures or other needs.

Figure 5: Screenshots of the MindBridge Custom Risk Score Creator

The screenshot shows the 'Create risk score' dialog box. It is divided into two main panels. The left panel, titled '*Name' and '*Risk group', contains a text input field for the name and a list of risk groups with checkboxes. The right panel, titled '*Control points', contains a search bar and two lists of control points: 'Statistical control points' and 'Rule-based control points'. A 'No data selected' button is at the bottom left, and 'Close' and 'Create' buttons are at the bottom right.

Create risk score

*Name

*Risk group

Enter or select a filter

- ☐ (11000) Assets
- ☐ (12001) Unspecified assets
 - ☐ (13001) Unspecified assets
 - ☐ (14001) Unspecified assets
 - ☐ (14005) Asset clearing
- ☐ (12002) Current assets
- ☐ (12003) Capital assets
- ☐ (12004) Long-term financial assets
- ☐ (21000) Liabilities
- ☐ (31000) Equity

No data selected

Close Create

*Control points

Select control point(s)

Statistical control points

- ☐ 2 Digit Benford
- ☐ Complex Structure
- ☐ POP Change in Risk Profile
- ☐ POP Change in Transaction Values

Rule-based control points

- ☐ Analysis Period Adjustment

To enable this feature, contact your Customer Success Manager.

¹¹ [Library management: Risk Scores](#)

Appendix B: Using Filter Builder

Auditors can use the Filter Builder on the data table dashboard to narrow down details with different combinations of accounts, dates, risk scores, control point results, data characteristics, and more. This will allow auditors to use subsets of the data as a sample population for specific audit tests.

Figure 6: Screenshots of the MindBridge Filter Builder

The top screenshot shows the MindBridge Filter Builder interface. The 'Filter Builder' dropdown menu is open, displaying a list of filter categories: Account, Account scoping, Decreasing Account Tags, Increasing Account Tags, Balance Sheet Impact, Risk scores, Control Points, Credit Value, Debit Value, Effective Date, Entered Date, Income Statement Impact, Keyword, Materiality, Source, and Status. A search bar is visible at the top right of the filter menu. The background shows a data table with columns for Account, Date, Description, Amount, and Risk Score.

The bottom screenshot shows the 'Filters' section of the MindBridge Filter Builder. It displays a complex filter rule: 'is Account Revenue and is MindBridge score Between 50% - 100% a...'. Below this, there are two conditions: 'is Control Points Manual Entry' and 'is Control Points End of Reporting Period', connected by an 'or' operator. The interface includes buttons for 'Add a condition' and 'Search'.

See [Use the filter builder](#) to learn how to use the Filter Builder step-by-step.

Contact Us

For technical assistance or to discuss further with our Methodology Team, contact your Customer Success Manager, or reach us at info@mindbridge.ai.